Université
franco-allemande
Deutsch-Französische
Hochschule

RÉSUMÉ :

Les réseaux actuels sont souvent caractérises par une intégration dynamique de nœuds étrangers. La possibilité qu'une entité dissidente égoïste exploite un noeud augmente alors, ce qui peut constituer une violation du protocole de collaboration en vue d'accroitre un avantage personnel. Si de telles violations diffèrent des objectifs du système, elles peuvent même être considérées comme une attaque. Si des techniques de tolérance aux fautes existent pour affaiblir l'impact sur le système, celui-ci ne peut pas totalement se prémunir de ce type d'attaque. Cela justifie la nécessité d'une approche pour maintenir un degré de collaboration noeuds égoïstes dans les systèmes distribues.
Dans cette thèse, nous considérons le problème d'atteindre un niveau ciblé de collaboration dans une architecture repartie intégrant des noeuds égoïstes, qui ont intérêt à violer le protocole de collaboration pour tirer parti du système. L'architecture et le protocole seront modifies le moins possible. Un mécanisme d'inspection de chaque noeud sera mis en place pour décider de la légitimité de ses interactions avec ses voisins. Le concepteur du système d'inspection est confronté avec une situation complexe. Il doit corréler plusieurs aspects tels que les circonstances particulières de l'environnement ou des préférences individuelles du noeud. En outre, il doit tenir compte du fait que les noeuds peuvent connaitre l'état de ses voisins et construire ses décisions en conséquence. La surveillance proposée dans cette thèse correspond à une classe de modelés de la théorie des jeux connus sous le nom « Inspection Game » (IG). Ils modélisent la situation générale où un « inspecteur » vérifie par des inspections du comportement correct d'une autre partie, appelée « inspectee ». Toutefois, les inspections sont couteuses et les ressources de l'inspecteur sont limitées. Par conséquent, une surveillance complète n'est pas envisageable et un inspecteur tentera de minimiser les inspections.
Dans cette thèse, le modèle initial IG est enrichi par la possibilité d'apparition de faux négatifs, c'est à dire la probabilité qu'une violation ne soit pas détectée lors d'une inspection. Appliqué sur des systèmes distribués, cette approche permet de modéliser les choix collaboratifs de chacun des acteurs (violer le protocole ou pas, inspecter ou pas). Comme résultat, le modèle IG retourne les paramètres du système pour atteindre le niveau de collaboration souhaité. L'approche est conçue comme un « framework ». Elle peut donc s'adapter à toutes les architectures et toutes les techniques de fiabilité. Cette approche IG sera présentée à l'aide d'un exemple concret d'architecture Publish/Subscribe.
L'approche du jeu d'inspection de cette thèse pour objectif de sécuriser l'ensemble du protocole de collaboration. Ceci constitue un nouveau concept de mécanisme de fiabilité. Afin de permettre une large application, la généralité de cette approche est renforcée par la contribution RCourse. En simplifiant les évaluations de la robustesse des systèmes, elle permet la vérification de l'approche IG et le calibrage des paramètres du système.