"Vers une cybersécurité de l'Internet des objets des bâtiments par l'utilisation de technologies inspirées des crypto-monnaies : l'exemple de IOTA"

Spécialité : Informatique

Laboratoire : Le2i, www.le2i.cnrs.fr

Directeur de thèse : Nader MBAREK <Nader.Mbarek@u-bourgogne.fr>

Co-encadrant de thèse : Benoît DARTIES <Benoit.Darties@u-bourgogne.fr>

Financement : Contrat doctoral, Dispositif JCE (Jeune Chercheur Entrepreneur) de la région Bourgogne Franche-Comté

Description du sujet :

L'Internet des objets (IoT : Internet of Things) comprend une grande variété de capteurs et d'objets intelligents de diverses natures. En interconnectant ces derniers (de manière physique ou virtuelle) par des technologies interopérables, il est possible de fournir des services avancés ainsi qu'une nouvelle expérience utilisateur. Le développement et le déploiement d'objets connectés au sein d'une infrastructure IoT est emmené à se poursuivre, s'accélérant dans les prochaines années dans de nombreux secteurs, dont le bâtiment, qui fait l'objet d'une attention particulière.

L'IoT pour les bâtiments intelligents offre de nouvelles perspectives et utilisations grâce à la combinaison d'objets connectés non complexes avec des fonctionnalités complémentaires et fonctionnant en réseau. Cet environnement présente également de nouveaux défis de recherche, notamment en matière de sécurisation des périphériques IoT et de leurs interactions avec les applications cloud et d'entreprise. En effet, les périphériques peuvent être accessibles en utilisant le réseau et par conséquent ils peuvent être vulnérables aux attaques. Les contraintes budgétaires importantes à appliquer à la production de dispositifs IoT renforcent ce problème.

La fiabilité d'un système pouvant s'appuyer sur les données collectées par les capteurs embarqués dans un environnement IoT, la cybersécurité dans l'IoT pour les bâtiments intelligents devient un enjeu de plus en plus important. Les solutions à déployer pour résoudre ces problèmes et relever les défis de recherche en termes de sécurité et de vie privée dans une infrastructure IoT doivent être à la fois simples et résilientes. La blockchain est une façon de traiter ce problème en proposant de nouveaux mécanismes permettant l'authentification et la confidentialité des échanges. La montée et le succès de Bitcoin au cours des six dernières années ont prouvé la valeur de la technologie blockchain. Cependant, cette technologie présente également un certain nombre d'inconvénients, notamment en termes d'évolutivité [2].

IOTA [4] est une crypto-monnaie pour l'industrie de l'Internet des objets récemment conçue pour résoudre les inconvénients de la technologie blockchain. La principale innovation derrière IOTA est

l'enchevêtrement (*the Tangle*), une nouvelle architecture de livres de comptes distribuée basée sur un Graphe Acyclique Dirigé (*DAG - Directed Acyclic Graph*). En ce sens, l'IOTA pourrait être une technologie intéressante et innovante pour relever les défis de recherche de la cybersécurité dans l'IoT pour les bâtiments intelligents.

Le but de ce projet de thèse est d'étudier la pertinence et les limites de IOTA et des technologies DAG similaires pour la cybersécurité dans l'IoT pour les bâtiments intelligents. Cette technologie semble être un successeur naturel de la technologie blockchain, en particulier pour ses caractéristiques en termes de gestion de consensus et d'absence de mineurs.

Les objectifs attendus dans le cadre de cette thèse sont les suivants :

1- Une première partie du travail consiste à étudier la technologie IOTA, et plus précisément le mécanisme de l'enchevêtrement, et la définition d'un état de l'art de technologies similaires. Il sera nécessaire de déterminer les forces et les faiblesses de IOTA, dans quels contextes cette technologie peut être pertinente, quelles sont ses limites, et quelles solutions et optimisations IOTA peut fournir par rapport à la blockchain. Une étude comparative entre IOTA et d'autres technologies apparentées telles que Byteball [1], Stellar [3], Ethereum [5] sera effectuée.

2- Une deuxième partie de ce travail est de se baser sur l'état de l'art réalisé mais aussi les défis identifiés afin de trouver une solution pertinente pour sécuriser l'IoT dans les bâtiments intelligents en assurant les services de confidentialité, authentification, intégrité et vie privée. Cette solution doit répondre aux exigences suivantes :

* Promouvoir les accords et la communication directe Machine vers Machine (M2M)

* Fournir un consensus sur la consommation d'énergie et de calcul (similaire à Proof of Stake, sans minage)

* Aucun coût transactionnel et opérationnel (le coût d'exploitation dans le cas de IOTA est nul)

3- Une troisième partie de ce travail concerne la mise en œuvre de la solution proposée à travers une démonstration de faisabilité (preuve de concept) prenant la forme d'un déploiement expérimental sur un banc d'essai de plateforme. Cette étape fournira des informations supplémentaires sur les limitations identifiées, et le banc d'essai sera utilisé pour tester et évaluer les performances des algorithmes et améliorations proposés. Une collaboration en partenariat avec un industriel du domaine, permettra d'étendre la mise en œuvre sur une plateforme de production réelle.

[1] Anton Churyumov. Byteball: A Decentralized System for Storage and Transfer of Value. URL: https://byteball.org/Byteball.pdf.

[2] Ittay Eyal Adem Efe Gencer Ari Juels Ahmed Kosba Andrew Miller Prateek Saxena Elaine Shi Emin Cun Sirer Dawn Song Roger Wattenhofer4 Kyle Croman, Christian Decker. On Scaling Decentralized Blockchains. URL: http://fc16.ifca.ai/bitcoin/papers/CDE+16.pdf.

[3] David Mazières. The Stellar Consensus Protocol: A Federated Model for Internet-level Consensus. URL: https://www.stellar.org/papers/stellar-consensus-protocol.pdf.

[4] Serguei Popov. The tangle. URL: https://iota.org/IOTA{_}Whitepaper.pdf.

[5] Gavin Wood. Ethereum: a secure decentralized generalised transaction ledger. URL: http://gavwood.com/paper.pdf.

Connaissances et compétences requises :

- **Réseaux** : sur les aspects protocolaires des communications dans un réseau de capteurs ou encore les infrastructures IoT
- **Sécurité, cybersécurité** : pour les parties concernant les services de sécurité (confidentialité, authentification, intégrité) à assurer dans un environnement IoT mais aussi les mécanismes inhérents au fonctionnement de la blockchain.
- **Simulation** des réseaux : NS2/ NS3/ OMNET++/ CloudSim/ JSIM
- **Programmation** orientée objet : C++/ Java

Dossier de candidature : Le dossier de candidature doit être envoyé par email à M. Nader MBAREK (nader.mbarek@u-bourgogne.fr) et M. Benoît DARTIES (benoit.darties@u-bourgogne.fr). Il doit comporter les éléments suivants : - un CV détaillé (avec les coordonnées complètes : adresse postale, électronique, téléphone). - une lettre de motivation pour la recherche et l'insertion en entreprise (où figure l'intitulé du sujet et le nom du directeur de thèse *i.e.* Dr. Nader MBAREK (MCF HDR) et Dr Benoît DARTIES (MCF)). - un projet professionnel (de 1 à 2 pages). - les relevés de notes et résultats en L3, M1, M2, ou équivalent. - lettre(s) de recommandation.

Date limite de Candidature : 20 Juin 2018