AVIS DE SOUTENANCE DE THESE
DE DOCTORAT

Le **13-12-2019**
A **14h** Amphi Minatec

CEA Leti
17 Rue des Martyrs
38054 Grenoble

Soutiendra en vue de l'obtention du titre de Docteur de l'Ecole Nationale Supérieure des Mines de Saint-Etienne dans la spécialité : MICROELECTRONIQUE

Meriem **SMACHE**

Une thèse ayant pour sujet :

La sécurité des réseaux déterministe de l'Internet industriel des objets (IIoT)

MEMBRES DU JURY :

Président
(Le président est désigné le jour de la soutenance)

Rapporteurs :

Beroulle	Vincent	Pr, HDR	École Na. sup. d'ingénieurs
Chaput	Emmanuel	Pr, HDR	École Na. Sup d'électrotechnique

Examinateurs :

Rivano	Hervé	Pr	Institut Na. Sciences Appliquées
Watteyne	Thomas	D. de recherche	Inria paris
El-Mrabet	Nadia	HDR, MC, ENSMSE	Mines de Saint-Étienne
Fourati	Alia	Ingénieur R&D EDF	Électricité de France
TRIA	Assia	Ingénieur R&D CEA	CEA Leti
Olivereau	Alexis	Ingénieur R&D, CEA	CEA List

Thèse préparée dans le centre CMP-GC à l'Ecole Nationale Supérieure des Mines de Saint-Etienne.
Travail co-encadré par : ASSIA Tria

Destinataires : DRI, Accueil, SCIDEM, Centre,
D.CORTIAL « Le Progrès », 24 rue de la robotique – 42000 Saint-Etienne

Résumé

La synchronisation entre les dispositifs distribués dans les applications de l'Internet des Objets Industriels (IIoT) est un domaine d'application important, pour preuve les organismes de normalisation internationaux travaillent à l'élaboration de protocoles permettant de déployer la nouvelle génération de réseaux de capteurs industriels sans fil (IWSN).

Ceci a conduit à l'émergence de plusieurs normes sans fil basées sur le protocole IEEE802.15.4e avec son mode TSCH (Time-Slotted Channel-Hopping) telles qu'ISA100.11a, WirelessHart, et 6TiSCH. TSCH est la toute dernière génération de protocoles MAC fournissant une réponse aux exigences industrielles telles que la synchronisation et le déterminisme. Le mode TSCH est conçu pour ordonnancer la communication des trames de données de longueur variable aux nœuds du réseau ainsi qu'à leurs liens respectifs.

Cet ordonnancement est composé d'un ensemble d'intervalles de temps positionnés dans un canal donné, assurant les communications. Chaque intervalle est programmé de façon déterministe dans le temps et en fréquence. Il est construit sur un mécanisme de sauts de canal afin d'éliminer les interférences, et par conséquent, d'atteindre une grande fiabilité, tout en employant la synchronisation temporelle pour obtenir un fonctionnement à faible puissance. TSCH est devenu une technologie de facto pour les applications industrielles.

Cependant, le timing dans IWSN est une cible évidente pour les cyber-attaques donnant naissance à une nouvelle génération d'attaques de synchronisation. Plus précisément, il existe un certain nombre d'attaques critiques par synchronisation liées aux mécanismes d'ordonnancement de TSCH telles que l'attaque Timeslot-Template et l'attaque ASN.

Le but de cette thèse est de fournir une analyse de vulnérabilité de la synchronisation avec le mode TSCH et de concevoir de nouvelles techniques d'auto-détection et d'auto-défense tout en tenant compte des capacités d'apprentissage et d'intelligence de l'attaquant, du nœud légitime et la nature distribuée, dynamique et temps réel.

Dans cette thèse, nous avons commencé par compromettre un nœud matériel équipé d'un protocole de communication matériel IEEE802.15.4g réputé inattaquable par une analyse par canal auxiliaire. Ensuite, nous avons exploité le code d'un nœud compromis pour construire de multiples scénarios d'attaques de synchronisation sur le mode TSCH du protocole MAC IEEE802.15.4.e.

Les premières analyses de l'efficacité de l'attaque ont été effectuées via l'analyse du comportement global du réseau, telles que la capture du trafic réseau et le calcul de l'offset global du réseau. Une deuxième étape consiste à exploiter l'effet des attaques sur le nœud uniquement. Nous avons ainsi défini de nouvelles métriques de détection basées sur l'expression interne et locale de la machine d'état TSCH de chaque nœud dans le réseau, sans avoir besoin de communications supplémentaires, ni de captures ou d'analyse des traces des paquets. Ensuite, nous avons défini statistiquement des hypothèses d'intervalle de confiance et nous les avons utilisées pour déterminer statiquement les conditions de synchronisation. Cependant, nous avons constaté que la détermination d'un seuil dynamique, continu et spécifique n'est pas un problème trivial. Nous avons donc utilisé de nouvelles métriques de détection TSCH pour générer un jeu de données, qui a été, par suite, utilisé comme entrée pour les algorithmes d'apprentissage automatique. L'expérimentation a été effectuée à l'aide d'un ensemble d'algorithmes supervisés, non supervisés et semi-supervisés afin de trouver la technique d'auto-détection comportementale la plus efficace. Par ailleurs, nous avons pris en compte l'intelligence et l'apprentissage dynamique des nœuds du réseau 6TiSCH et la créativité de l'attaquant pour en définir une réponse aux attaques par synchronisation. Des systèmes de réponses aux intrusions (IRS) automatiques et autonomes ont été proposés : d'une part, l'IRS automatisée est une interaction basée sur des règles préconfigurées. Il permet au nœud de suivre un ensemble d'entrées traçables et les rétroactions associées avant d'effectuer une interaction (réponse). Quelle que soit l'action que le nœud entreprendra après avoir détecté l'attaque, celle-ci est considérée comme prévisible. D'autre part, l'IRS autonome permet à chaque nœud de fonctionner en tant qu'agent intelligent capable d'apprendre, d'interpréter et d'interagir par lui-même tout en se basant sur les observations d'état local pour maintenir correctement son état de synchronisation. C'est une application de l'algorithme d'apprentissage par renforcement où l'agent-nœud traite toutes sortes d'entrées bruyantes et se comporte avec son environnement sous la stratégie action-état.

Meriem SMACHE, CMP