Détection d'attaques sur les réseaux temps-réel IEC 61850

M. Kabir-Querrec[1,2], S. Mocanu[1], P. Bellemain[1], J.-M. Thiriet[1], E. Savary[2]
1) Univ. Grenoble Alpes, GIPSA-lab, F-38000 Grenoble, France
CNRS, GIPSA-lab, F-38000 Grenoble, France
2) Euro-System, F-38760 Varces, France

Résumé : Cette thèse porte sur la problématique de la cybersécurité dans les infrastructures IEC 61850, en particulier la détection d'intrusion. Le travail réalisé a d'abord consisté à enrichir ce standard d'une fonction dédiée. Dans un deuxième temps nous avons travaillé à la conception d'une architecture IEC 61850 résiliente aux attaques sur le réseau temps-réel GOOSE. Des sondes de détections ont été développées et testées. Une AMDE est en cours pour nous permettre de synthétiser un mode de fonctionnement alternatif en cas de corruption du réseau GOOSE.

La nécessité de doter l'industrie de moyens de lutte contre la menace cybernétique est aujourd'hui bien acceptée. En particulier dans le domaine de la production et de la distribution électrique. Ce domaine s'est doté dans la dernière décennie d'un standard international, l'IEC 61850 [1], portant sur les systèmes et réseaux de communication impliqués dans l'automatisation des infrastructures électriques. Son objectif premier est l'interopérabilité. Pour cela, il définit un modèle de représentation de l'information ainsi que trois protocoles de communication pour transférer ces données en fonction du niveau opérationnel : niveau procédé, niveau baie de contrôle où opèrent les ICS (Industrial Control Systems, systèmes de contrôle industriels) ou niveau supervision. Le transfert de l'acheminement par voie numérique permet également d'éliminer une grande partie du câblage abondant propre à ces systèmes de contrôle / commande du réseau électrique, réduisant ainsi les coûts en matériel.

Le développement de l'usage de technologies numériques dans les systèmes d'automatisation des réseaux électriques IEC 61850 ne s'est pas accompagné du développement systématique de méthodes et d'outils de cybersécurité, probablement parce que la menace n'était pas initialement identifiée. La nécessité de doter le smart-grid de moyens de protection numérique est désormais largement acceptée et les travaux académiques comme industriels sur le sujet sont abondants, couvrant divers aspects tels que l'analyse de risques, le chiffrement, la signature, la détection d'intrusion [2 – 5]. L'objet de cette thèse est de proposer des méthodes et outils de détection d'intrusion pour les réseaux de contrôle des infrastructures électriques IEC 61850. Les éléments principaux et pertinents du standard IEC 61850 au regard de nos travaux ont été rassemblés dans les premières parties des contributions [6] et [7].

Spécification IEC 61850 d'une fonction de « détection d'intrusion »

Les experts à l'origine du standard IEC 61850 semblent avoir eu conscience de la problématique de la sécurité numérique puisqu'une fonction « System security management » a été définie. Toutefois, il est précisé dans sa description qu'elle se focalise sur les problèmes d'accès non autorisés et la perte d'activité. Son fonctionnement repose sur la sous-fonction (Logical Node) « Generic Security Application » (GSAL) dont le rôle est de surveiller les violations d'authentification et de gestion des privilèges. Le standard IEC 61850 ne définit pas d'éléments pour gérer d'autres aspects de cybersécurité, tels que la détection d'intrusion.

Le premier apport de cette thèse a donc été de définir des fonctions, sous-fonctions (Logical Node), données (Data Attributes, Data Classes), interactions… conforme au modèle de l'information du standard IEC 61850. Ces travaux ont été présentés dans [6] qui détaille notamment la procédure pour enrichir ce modèle de données IEC 61850. La spécification complète des objets dédiés cybersécurité à laquelle nous avons abouti fait l'objet d'un article de journal actuellement examiné.

Sondes de surveillance d'un réseau temps-réel IEC 61850

Après le travail fait sur les concepts en œuvre dans la détection d'intrusion IEC 61850, nous nous sommes intéressés à la question concrète « comment détecter des intrusions sur un réseau temps-réel IEC 61850 ? ». Les réseaux temps-réel IEC 61850 sont dédiés aux échanges d'information entre relais intelligents au niveau de la baie de contrôle (ou d'une baie de contrôle à une autre). Il s'agit d'informations critiques pour la protection électrique du réseau et des équipements et les contraintes sont fortes, tant pour l'intégrité des données qu'en ce qui concerne le temps de transfert. Le protocole en jeu, GOOSE (Generic Object Oriented Substation Event) [8], est mappé sur la couche liaison d'Ethernet et les trames ont une structure précisément définie [7], [9].

Nous avons développé deux sondes à partir de modules Linux de monitoring du réseau. La première est une sonde de mesure de la bande passante développée à partir d'un moniteur de bande qui permet de détecter une tempête Ethernet (flooding). La seconde sonde permet, à partir d'un analyseur de trafic, de vérifier la légitimité des messages GOOSE circulant sur le réseau. Elle permet notamment de détecter des attaques de type *spoofing*.

Ces sondes sont présentées dans [7]. Le protocole GOOSE fonctionne en broadcast sur un modèle d'éditeur / abonné. Afin de garantir la fiabilité de la transmission, un même message est réémis périodiquement, avec une période T1 très courte d'abord, lorsqu'un changement d'état déclenche la publication d'un nouveau message GOOSE, puis avec une période de plus en plus grande T2 puis T3… jusqu'à T0, période de retransmission en situation stable. Le suivi des messages (s'agit-il d'une nouvelle information ou bien de la même information que celle contenue dans le message précédemment reçu ?) est assuré par l'incrémentation de compteurs d'état (nouvelle information) et de séquence (même information, nouveau message). La sonde de messages GOOSE frauduleux repose sur la vérification de l'horodatage des messages et la cohérence de ces compteurs. Ce mécanisme particulier fait que même une attaque parfaite sera détectée après au maximum un temps égal à la période de réédition d'une même information (cf. figure 1). Cette période est d'1ms ou 2 ms selon les implémentations.

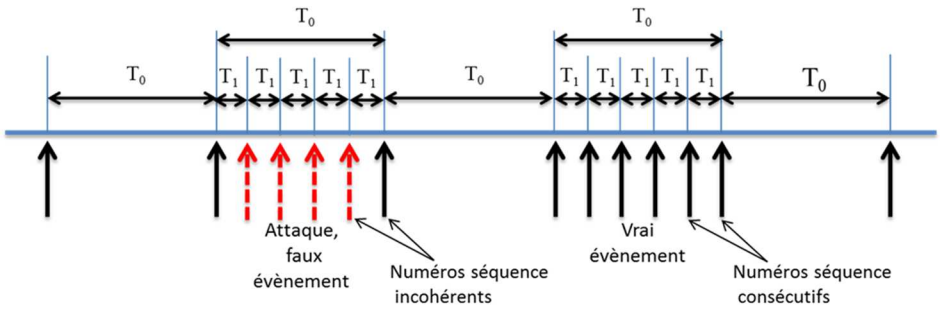

Figure 1. Chronologie d'une attaque GOOSE

Afin de tester cette sonde, nous avons développé un générateur de messages GOOSE frauduleux à partir d'un module permettant de fabriquer des trames, Scapy [10], [11]. Le fonctionnement de ce générateur d'attaques est le suivant : il renifle l'ensemble du trafic GOOSE du réseau, le décode, change la valeur d'une variable du jeu de données transmis dans le message, modifie les compteurs de façon appropriée, encode le message et l'envoie.

Les expériences ont été faites sur la plateforme GICS (GreEn-ER Industrial Control systems Sandbox) [12], dédiée à l'interopérabilité et la cybersécurité des systèmes de contrôle industriels.

Architecture d'un poste électrique intégrant ces sondes

Ces sondes ont été conçues dans l'idée d'être intégrées à une architecture d'un système d'automatisation de poste (SAS – Substation Automation System) résiliente aux attaques sur les messages GOOSE. Rappelons que le trafic GOOSE est primordial pour les opérations de contrôle / commande du réseau électrique, en particulier pour la protection électrique. Les fonctions de protection électrique reposent sur la sélectivité (choix des appareils à déconnecter selon la localisation du défaut électrique et les mesures prises ou non par les équipements les plus proches, physiquement, de ce défaut). Cette sélectivité est assurée par la communication GOOSE dans les infrastructures IEC 61850. L'architecture proposée doit apporter une alternative au transfert de

l'information normalement assuré par le réseau GOOSE lorsque celui-ci est soupçonné de corruption (cf. figure 2).

Lorsqu'une attaque est détectée par les sondes, une alerte est remontée à la supervision (SCADA – Supervisory Control and Data Acquisition) via une communication Modbus. Le SCADA envoie l'ordre aux IEDs (Intelligent Electronic Devices ou relais intelligents) d'entrer en mode sûr, c'est-à-dire de ne plus tenir compte de la communication GOOSE jusqu'à ce que l'alerte soit levée.

Pour assurer un mode de fonctionnement alternatif sûr, indépendant du réseau GOOSE, il est nécessaire de développer les programmes exécutés par les IEDs. Pour cela, notre démarche est de réaliser une analyse de risques et une analyse des modes défaillances et leurs effets (AMDE) sur une architecture de SAS classique et simple. La définition de cette architecture et le développement de scenarios de défaillances liées à la corruption de la communication GOOSE est en cours au moment de la rédaction de ce document. Nous travaillons en collaboration avec un expert qui nous apporte ses compétences en électrotechnique.

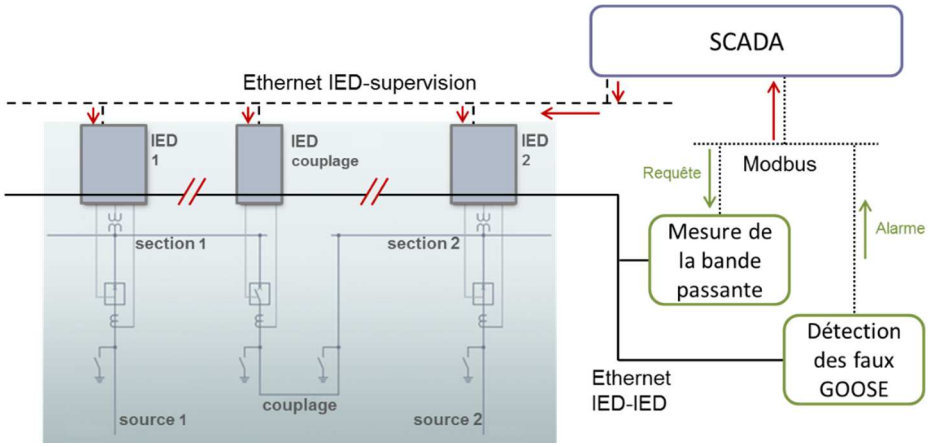

Figure 2. Architecture globale d'un SAS résiliente aux attaques sur GOOSE

Perspectives

Nous nous sommes d'abord penchés sur la définition des concepts en œuvre dans la cybersécurité, en particulier la détection d'intrusion, conforme au standard IEC 61850. Sur cette base « théorique », nous avons développé des outils nous permettant de faire de la détection d'intrusion sur un réseau GOOSE. Afin d'intégrer ces développements à une architecture globale d'un SAS, nous travaillons actuellement à une AMDE d'un système réaliste simple qui nous permettra de synthétiser un mode de fonctionnement résilient aux attaques GOOSE. Ces développements sont en cours d'intégration à un IDS open-source.

Références

[1] IEC 61850 Communication networks and systems for power utility automation - Part 1: Introduction and overview, 1. Ed., 2003

[2] A. R. Metke, and R. L. Ekl, "Security Technology for Smart Grid Networks", *IEEE Trans. Smart Grid*, vol. 1, no. 1, pp. 99-107, June 2010

[3] Symantec Corp., C. Leita, and M. Dacier. (2012, April). "Security of power grids: a European perspective", NIST Cybersecurity for Cyber-Physical Systems Workshop. http://csrc.nist.gov/news_events/cps-workshop/slides/presentation-6_leita-dacier.pdf

[4] A. Cioraca, I. Voloh, and M. Adamiak, "What protection engineers need to know about networking", *Protective Relay Engineers, 2015 68th Annual Conference for*, 2015, pp.597-607

[5] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber–Physical System Security for the Electric Power Grid", *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210-224, Jan. 2012

[6] M. Kabir-Querrec, S. Mocanu, J.-M. Thiriet, et E. Savary, “Power Utility Automation Cybersecurity: IEC 61850 Specification of an Intrusion Detection Function”, *European Safety and Reliability Conference*, 2015

[7] M. Kabir-Querrec, S. Mocanu, P. Bellemain, J.-M. Thiriet, et E. Savary, “Architecture des systèmes d’automatisation des postes résiliente aux attaques des trames GOOSE”, *Computer & Electronic Security Applications Rendez-Vous*, 2015

[8] IEC 61850 Communication networks and systems for power utility automation - Part 8-1: Specific communication service mapping (SCSM) - Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3

[9] C. Kriger, S. Behardien, et J. Retonda-Modiya, “A Detailed Analysis of the GOOSE Message Structure in an IEC 61850 Standard-Based Substation Automation System”, *INT J COMPUT COMMUN*, vol. 8, no. 5, pp. 708-721, Oct. 2013

[10] Scapy. http://www.secdev.org/projects/scapy/

[11] J. Hoyos, M. Dehus et T. X. Brown, “Exploiting the GOOSE protocol: A practical attack on cyber-infrastructure”, *IEEE Globecom Workshops*, 2012

[12] G-ICS. https://persyval-lab.org/en/platform/g-ics-sandbox-green-er-industrial-control-systems-sandbox

---

Maëlle Kabir-Querrec a commencé ses études supérieures avec une classe préparatoire en Physique-Chimie avant d’intégrer l’ENSE3 Grenoble-INP. Elle y a suivi la filière Automatique, Systèmes et Information. A l’obtention de son diplôme, en 2013, il lui a été donné l’opportunité de poursuivre en thèse avec une PME de la région grenobloise, Euro-System, bureau d’études en Automatisme et Informatique industrielle et le laboratoire GIPSA-lab sur les problématiques de cybersécurité des smart-grids. Elle s’intéresse en particulier à la détection d’intrusion dans les systèmes d’automatisation IEC 61850.