République Algérienne Démocratique et populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Labri Tébessi -Tébessa -
Faculté de Science Exacte et de Science de la Nature et de la Vie
Département : Mathématiques et de l'Informatique

MEMOIRE DE MASTER

Domaine : Mathématiques et de l'Informatique

Filiére : Informatique

Option : Système d'information SI

Thème :

Gestion des risques dans les smart grids

Présenté par :

Saadi Hayette

Boudiaf Radouane

Encadreur :
Dr. Makhlouf Derdour

Co-Encadreur
Dr. AhmimAhmed

Devant le jury :

Mr. A.A.Betouil	MCA	Université de Tébessa	président
Mr. S. Khediri	MMA	Université de Tébessa	Examinateur

Date de soutenance : 24/05/2017

Note :…… **Mention :**…….

Année Universitaire 2016-2017

Résumé

Les réseaux intelligents ont un grand potentiel pour la gestion de la consommation d'énergie. Cependant, passer d'une grille traditionnelle à une smart grid introduit de nouveaux risques importants pour le secteur de l'énergie qui n'étaient pas présents dans les réseaux électriques qui fonctionnaient isolément. Les données générées dans les systèmes de mesure intelligents peuvent nuire à leurs parties prenantes. Il est donc important de protéger toutes les parties prenantes en fournissant des contrôles efficaces aux éléments vulnérables dans le système de mesure intelligente. Cela souligne la nécessité de mener une analyse des risques pour évaluer les méfaits, les menaces et les vulnérabilités introduits dans cette infrastructure critique par la modernisation. Actuellement, il existe de nombreuses méthodes d'analyse des risques disponibles; Il existe de nombreuses différences entre eux, et donc choisir un approprié est un défi. Le risque que les experts techniques perçoivent comme mineurs suscitent souvent de fortes préoccupations du public. Par conséquent, lors de l'analyse des risques, différentes perspectives doivent être prises en considération.

Ce travail met en évidence une analyse complète de la gestion des risques dans le réseau électrique (Smart Grid), ce qui se traduit par un cadre spécialement ciblé sur le réseau intelligent et les systèmes de mesure intelligents.

Abstract

Smart grids have great potential for managing energy consumption. However, switching from a traditional grid to a smart grid introduced new risks important to the energy sector that were not present in power grids that operated in isolation. The data generated in intelligent measurement systems can harm their stakeholders. It is therefore important to protect all stakeholders by providing effective controls to vulnerable elements in the intelligent measurement system. This highlights the need to conduct a risk analysis to assess the harms, threats and vulnerabilities introduced into this critical infrastructure through modernization. Currently, there are many methods for analyzing available risks; there are many differences between them, and so choosing an appropriate one is a challenge. The risk that technical experts perceive as minors is often of great public concern. Therefore, in the risk analysis, different perspectives need to be considered.

This work highlights a comprehensive analysis of the risk management frameworks in the electricity grid, resulting in a framework specifically targeted at the intelligent grid and intelligent measurement systems.

Résumé

ملخص

الشبكات الذكية لديها إمكانيات كبيرة لإدارة استهلاك الطاقة. غير أن التحول من شبكة تقليدية إلى شبكة ذكية يعرض مخاطر جديدة هامة لقطاع الطاقة غير موجودة في شبكات الكهرباء التي تعمل بمعزل عن غيرها. البيانات التي تم إنشاؤها في أنظمة القياس الذكية يمكن أن تضر أصحاب المصلحة. ولذلك فمن المهم حماية جميع أصحاب المصلحة من خلال توفير ضوابط فعالة للعناصر الضعيفة في نظام القياس الذكي. وهذا يبرز الحاجة إلى إجراء تحليل للمخاطر لتقييم الأضرار والتهديدات ومواطن الضعف التي أدخلت على هذه البنية الأساسية الحيوية من خلال التحديث. حاليا، هناك العديد من الطرق لتحليل المخاطر المتاحة. هناك العديد من الاختلافات بينهما، وبالتالي اختيار واحد مناسب هو التحدي. والمخاطر التي يراها الخبراء التقنيون قاصرون غالبا ما تكون مصدر قلق عام كبير. لذلك، في تحليل المخاطر، يجب النظرفي وجهات نظر مختلفة.

ويبرز هذا العمل تحليلا شاملا لأطر إدارة المخاطر في شبكة الكهرباء، مما أدى إلى إطار موجه تحديدا إلى الشبكة الذكية ونظم القياس الذكية.

Table des matières

2. Chapitre 3 systèmes de détection d'intrusion IDS

Liste des figures

Liste des Tableaux

Introduction générale

Le monde a connu une croissance économique et technologique rapide, et de reconstruction massive. Une grande importance a conduit à une demande croissante d'électricité en raison de la croissance de la population et de la demande des industries. De même, cela a conduit à un style de vie avec des appareils plus électriques à la maison. Le réseau traditionnel centralisé et les attentes environnementales quant à la durabilité des installations d'approvisionnement en énergie sont placés près des sources d'énergie pour produire une grande quantité nécessaire pour obtenir le réseau électrique. Ces dernières années, il y a eu des progrès rapides dans la production d'énergie à partir de sources d'énergie renouvelables telles que l'énergie éolienne et solaire, etc.

Les Smart grids sont associé aux réseaux de distribution des technologies modernes de l'information et de la communication (TIC). Ces technologies permettent, notamment, de collecter et consolider l'information au plus proche des producteurs, des consommateurs ou lors de l'acheminement de l'énergie et d'exploiter l'information de manière plus intelligente.

Dans le secteur de l'énergie, l'intelligence des réseaux n'est cependant pas un phénomène nouveau. Les réseaux disposaient initialement de capacités de récupération d'information pour des besoins de pilotage. Cependant, l'ère des Smart grids permet d'accroître la précision des informations relevées : à titre d'exemple, certaines données auparavant relevées globalement par zones, peuvent désormais être collectées à une échelle plus locale, près de points de production ou d'acheminement. Ces données permettent, à terme, une optimisation de la production en limitant les pertes techniques, une augmentation de la durée de vie des réseaux de transport et de distribution d'électricité ou encore une gestion plus fine des dangers liés aux chauffes et aux déformations de lignes. La montée en puissance des énergies de sources renouvelables (pour lesquelles certaines courbes de charges ne sont pas prédictibles) nécessite un relevé d'information de production local (notamment pour les éoliennes, panneaux solaires, etc.). Les compteurs communicants jouent le rôle de maillon de relevé proche des consommateurs. Ces évolutions sont permises, notamment, par l'essor des technologies de la communication, ainsi que par la capacité à traiter de manière intelligente de forts volumes de données.

Cependant, la superposition de l'infrastructure de réseau électrique et des technologies de l'information modernes, l'augmentation du nombre de points d'interaction avec le réseau (utilisateurs de réseau « connectés » et points d'accès distants aux équipements du réseau notamment pour des besoins de télémaintenance) exposent potentiellement les réseaux électriques intelligents aux menaces modernes ciblant les systèmes d'information.

Les systèmes d'information d'autres secteurs d'activités ont déjà pu faire l'objet de cas de vols de données personnelles, perturbation de systèmes, attaques de types dénis de services, fuites d'informations, etc.

De nombreux systèmes industriels n'étaient pas parés à faire face à ces menaces. L'exemple de la cyber-attaque Stuxnet en 2010, ayant mené à la prise de contrôle d'automates industriels pour modifier les paramètres de fonctionnement d'installations industrielles en accélérant leur vitesse de rotation, est encore dans toutes les mémoires des industriels. Les Smart grids deviennent ainsi potentiellement la cible de ces menaces. Si les réseaux électriques ont recours depuis longtemps à des systèmes d'information et de communication électroniques pour transmettre les données nécessaires à la gestion de la production, du transport et de la distribution d'énergie, les systèmes d'information dédiés aux réseaux électriques utilisent des systèmes propriétaires spécifiques à ces réseaux industriels et ils sont, encore pour la majorité, dédiés et fermés : l'intégration des réseaux intelligents de communication et d'échanges de données, qui s'appuient sur des technologies telles qu'Internet Protocol (IP) ou le « Cloud Computing », augmente le niveau de risque.

La superposition de l'infrastructure de réseau électrique et des systèmes de TI modernes augmente considérablement les vulnérabilités et les points d'accès que les criminels et les terroristes peuvent utiliser pour attaquer le système électrique.

La cyber-sécurité a représenté un marché de $21 milliards entre 2010 et 2015 avec un revenu annuel de $3.7 milliards en 2015. Les investissements relatifs à la sécurité devraient correspondre à 15% de l'investissement total dans le Smart Grid.

Pour réaliser notre objectif, ce mémoire est organisé comme suit : trois chapitres après l'introduction générale.

Chapitre I : Nous visons à étudier dans le premier chapitre la définition de l'ancien réseau électrique et intelligent et le système de contrôle et l'accès aux données sur la Smart Grid et le problème qui a émergé lors du renouvellement.

Chapitre II : Le deuxième chapitre considère les attaques des ordinateurs, Les étapes et les types d'attaque et discute l'impact et de sécurité sur le réseau intelligent.

Chapitre III : Dans le dernier chapitre, nous voyons que le système de détection d'intrusion(IDS) a pour objectif d'identifier et de répondre à des malveillants ciblant un ordinateur ou un réseau informatique dans le Smart Grids.

Le problème de détection d'intrusion revient donc à une classification et une architecture de sécurité, ainsi un développement des mécanismes défensifs conçus pour contrecarrer les attaques délibérées, l'exposition involontaire ou la perte des données.

Nous terminerons par une conclusion générale.

Partie 1

État de l'art

Chapitre 1

Le Réseaux de smart grid

1. Introduction

Les besoins nationaux et internationaux en matière d'économie d'énergie font de la modernisation des réseaux électriques une nécessité absolue.

Pendant longtemps, l'électricité était produite principalement à partir des ressources énergétiques non renouvelables (nucléaire, charbon, gaz naturel, pétrole) de manière centralisée. Ces ressources devenaient de plus en plus couteuses et rares (par exemple le coût du pétrole a augmenté de façon exponentielle, les dernières années). Encore, la gestion des pannes n'est pas automatique (par exemple : si une catastrophe naturelle se produit, elle peut laisser des millions de consommateurs dans le noir, durant plusieurs journées). Les problèmes du réseau électrique traditionnel ont accéléré la création d'un nouveau concept nommé réseau électrique intelligent « Smart Grid ».

2. Le réseau électrique

Les réseaux électriques sont des systèmes complexes chargés de transporter l'énergie électrique vers des consommateurs. Ils constituent aussi maintenant le support physique de nombreux échanges économiques autour de la production et de l'électricité

Pour ces raisons, dans nos sociétés, le rôle joué par les réseaux électriques est crucial. Les défaillances des systèmes électriques ont, aujourd'hui plus qu'hier, des impacts économiques et sociaux majeurs.

Pour assurer la sécurité et la qualité de fourniture de l'énergie électrique, les réseaux électriques sont soumis à de nombreuses contraintes de fonctionnement s'appliquant à tous les acteurs du système électrique, de la production à la consommation **[1]**

2.1. Les réseaux électriques classiques

Les réseaux classiques, conçus pour intégrer un flux électrique à seul sens unique, sont en effet incapables d'inclure à grande échelle la production décentralisée d'énergie.

Ils sont essentiellement adaptés au transport de l'électricité des grandes installations nucléaires, hydrauliques, au charbon ou au gaz, qui permettent généralement de faire des économies d'échelle.

Mais si un réseau secondaire local génère plus d'énergie qu'il n'en consomme, le retour de flux peut engendrer des problèmes de sécurité et de fiabilité.

Ces problèmes d'interdépendance ont été mis en exergue en 2006, lorsque 10 millions d'Européens furent plongés dans le noir suite à une vaste panne du réseau électrique panne du réseau électrique **dans** 8 pays (AT, BE, DE, ES, FR, HR, IT, NL).) [2].

Actuellement, les réseaux électriques existants peuvent être décomposés en 4 niveaux **[3]:**

- **Les gros producteurs centralisés**, tels que les centrales à charbon, les centrales nucléaires ou les centrales hydrauliques, fournissant la majeure partie de l'électricité du réseau; Les grands groupes de production d'énergie électrique sont en général basés sur des alternateurs synchrones de grandes tailles, connectés sur le réseau de transport via un transformateur de groupe.

- **Le système de transport de l'énergie**, permettant de transporter de grandes quantités d'énergie à haute tension sur de longues distances ; Afin de minimiser, entre autres, les pertes joules sur les lignes ces réseaux sont à très haute tension. Du point de vue topographique, pour des raisons de sécurité de fonctionnement, les réseaux de transport sont des réseaux maillés.

- **Le système de distribution d'énergie**, caractérisé par des tensions plus faibles, est chargée de délivrer l'énergie aux usagers ; Leur tension est inférieure ou égale à 50 kV. Ils sont constitués de deux types réseaux : le réseau moyenne tension (MT), connecté au réseau de transport, et le réseau basse tension (BT).

- **Les usagers, ou consommateurs**, répartis sur une grande partie du territoire, utilisant l'énergie reçue de façon très variée. Les trois usages classiques de l'énergie électrique sont la production d'énergie thermique (Chauffage), lumineuse (éclairage) et mécanique (moteurs électriques). Ces trois applications se retrouvent aussi bien chez les consommateurs résidentiels qu'industriels. Dans les réseaux, les consommateurs sont appelés charges. Ces charges sont caractérisées par leurs puissances active et réactive consommées ou produites de ces puissances mesurées sur un certain intervalle de temps. Pour connaître l'évolution des charges au cours du temps, des études statistiques sont menées sur les réseaux. En mesurant les courants dans les postes de transformation Entre les réseaux de transport et de distribution, des courbes de consommation temporelle sont calculées. Ces courbes sont appelées courbes de charge. Elles permettent aux gestionnaires de réseau de prédire l'évolution de la consommation sur les réseaux et donc, entre autres, de définir les plans prévisionnels de production.

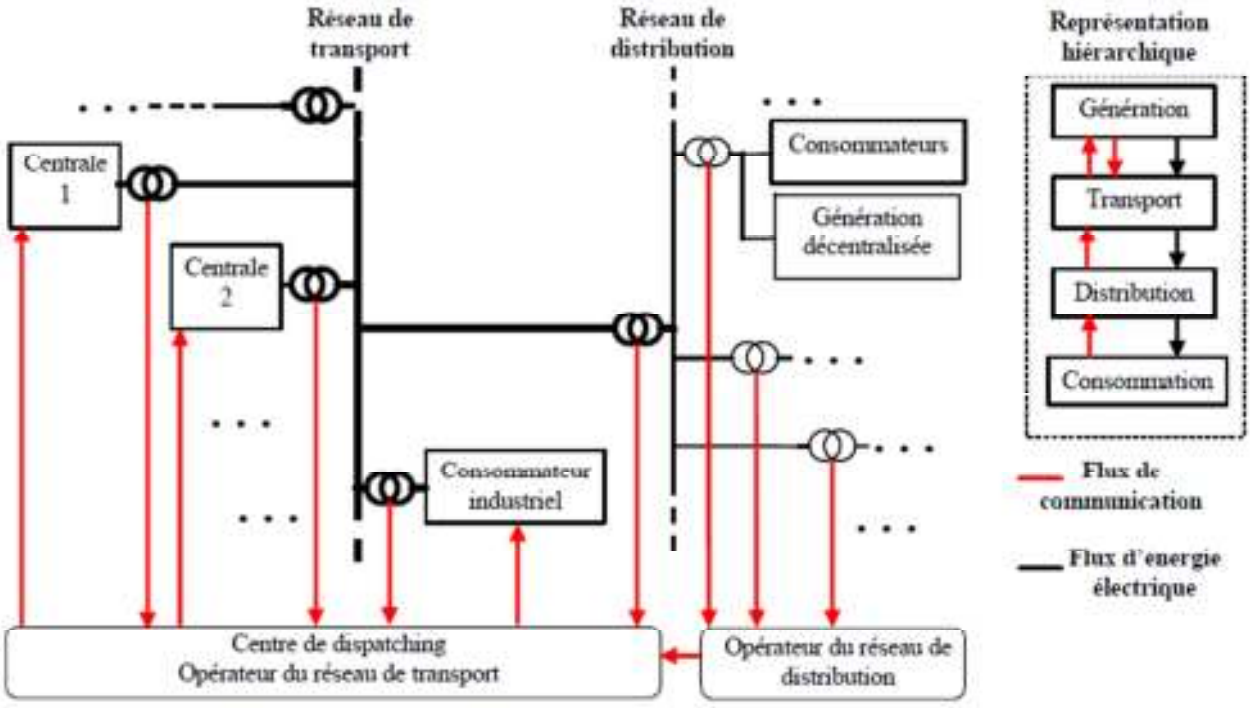

Figure 1.1. Structure traditionnelle du système électrique [3]

Les usagers peuvent demander de l'énergie à tout moment. Il revient alors aux gestionnaires des autres niveaux de fournir l'énergie nécessaire pour répondre aux besoins des consommateurs. L'équilibre offre-demande est un point clé dans l'utilisation des réseaux électriques. Si la stabilité n'est pas respectée, la tension varie, ce qui entraîne une usure prématurée des installations.

Cependant, de nouvelles tendances annoncent de grands changements sur les réseaux ´ électriques. Ils devront devenir plus autonomes qu'ils ne le sont aujourd'hui.

Parmi ces tendances, nous pouvons citer **[4]:**

- **L'augmentation de la demande en énergie** : La demande d'énergie mondiale croît régulièrement du fait de plusieurs facteurs. Ainsi, l'augmentation de la population mondiale implique une plus grande consommation. L'amélioration de la vie dans les pays en voie de développement, notamment les BRICS[1], influe fortement sur la consommation d'énergie.
- **La préoccupation environnementale :** Selon les rapports du GIEC[2], les changements climatiques sont sans équivoque. Depuis les années 1950, beaucoup des changements observés sont sans précédent sur les dernières décennies à millénaires. Le GIEC annonce également comme "très probable" le fait que ces changements soient dus à une influence humaine. Le groupe cite notamment : le réchauffement océanique, la diminution des masses des calottes glaciaires, l'augmentation du niveau de la mer, l'augmentation de la concentration des NO_x dans l'atmosphère.
- **L'intégration des nouvelles sources décentralisées :** Les réseaux électriques actuels ont ´ été conçus pour transporter l'énergie de gros producteurs, que sont les centrales productrices, aux consommateurs. L'intégration des nouvelles sources décentralisées amène des modifications structurelles et comportementales sur le réseau. Les sources d'énergie renouvelable, telles que les panneaux photovoltaïques et les éoliennes, produisent de manière stochastique, irrégulière, et peuvent donc amener une instabilité sur le réseau. Enfin, l'intégration des véhicules électriques ou hybrides devant être rechargés sur le réseau suggère également de tenir compte de nouveaux comportements émergents.
- **Le coût de l'énergie :** L'épuisement prévisible des ressources en énergies fossiles ainsi que le début des démantèlements des centrales nucléaires va impliquer une augmentation du prix de l'énergie. Pour compenser, de nouvelles sources d'énergie ont été développées, mais celles-ci ont un prix de production plus élevé. Cette hausse de prix sera forcément répercutée sur les factures des consommateurs. Il va donc falloir trouver de nouveaux comportements sur le marché pour réduire cette augmentation de tarif afin que l'énergie puisse encore être accessible au plus grand nombre.

Ce sont ces grands changements, autant comportementaux que structurels, qui ont induit le développement d'un nouveau type de réseau : les réseaux intelligents sou **SMART GRIDS**.

[1]Brésil, Russie, Inde, Chine, Afrique du Sud
[2] Groupe d'experts Intergouvernemental sur l'Evolution du Climat

2.2. Réseau intelligent "SMART GRID"

2.2.1. Définitions

Il existe actuellement plusieurs définitions d'un smart grid et également plusieurs objectifs pour une même définition d'un smart grid. **[5]**

Le Software Engineering Institut de l'Université de Carnegie Mellon définit le **SMART GRID**, ou réseau intelligent, comme un terme utilisé pour se référencer à un réseau électrique dont les opérations sont passées d'une technologie analogique à l'utilisation d'une technologie numérique intégrée permettant la communication, la détection, la prévision et le contrôle **[6].**

Un SMART GRID (littéralement « réseau intelligent ») est un réseau électrique reliant ensemble la production, la consommation et le stockage de l'électricité et les coordonnant de manière autonome. **[W1]**

Les Smart Grids sont des réseaux électriques qui intègrent de manière intelligente les comportements et les actions de tous les acteurs connectés — les producteurs, les consommateurs et ceux qui consomment et produisent en même temps — pour garantir une fourniture d'électricité efficiente, durable, économique et sûre [10].

Les Smart Grids américains mettent, quant à eux, l'accent sur la modernisation des réseaux de transport d'énergie souvent très mal entretenus. Les États-Unis doivent en effet faire face à un nombre de coupures de courant qui ne cesse d'augmenter, passant de 76 pannes en 2007 à plus de 300 en 2011 [2014-11]. Ces pannes sont aussi fréquentes .En 2003, un blackout dans l'Ohio prive 50 millions de personnes d'électricité et coûte 6 milliards de dollars [2005-12]. Ces coupures sont dues à la combinaison de trois facteurs [2014-13] :

- Une infrastructure électrique vieillissante, en grande partie mécanisée et souffrant du manque d'investissement ;
- Une forte croissance démographique ;
- Des conditions climatiques de plus en plus extrêmes.

Les réseaux intelligents peuvent être définis selon quatre caractéristiques en matière de : **[W2]**

- **Flexibilité** : ils permettent de gérer plus finement l'équilibre entre production et consommation ;
- **Fiabilité** : ils améliorent l'efficacité et la sécurité des réseaux ;
- Accessibilité : ils favorisent l'intégration des sources d'énergies renouvelables sur l'ensemble du réseau ;
- **Economie** : ils apportent, grâce à une meilleure gestion du système, des économies d'énergie et une diminution des coûts (à la production comme à la consommation).

Au sens large, un réseau intelligent associe l'infrastructure électrique aux technologies numériques qui analysent et transmettent l'information reçue. Ces technologies sont utilisées à tous les niveaux du réseau : production, transport, distribution et consommation.

- **Un contrôle des flux en temps réel** : des capteurs installés sur l'ensemble du réseau indiquent instantanément les flux électriques et les niveaux de consommation. Les opérateurs du réseau peuvent alors réorienter les flux énergétiques en fonction de la demande et envoyer des signaux de prix aux particuliers pour adapter leur consommation (volontairement ou automatiquement).

- **L'interopérabilité des réseaux** : l'ensemble du réseau électrique comprend ***le réseau de transport et le réseau de distribution***. Le premier relie les sites de production d'électricité aux zones de consommation : ce sont les grands axes qui quadrillent le territoire. Le réseau de distribution s'apparente aux axes secondaires. Il achemine l'électricité jusqu'aux consommateurs finaux. Par l'échange instantané d'informations, les smart grids favorise une interopérabilité entre les gestionnaires du réseau de transport et ceux du réseau de distribution.

- **L'intégration des énergies renouvelables au réseau** : les réseaux intelligents reposent sur un système d'information qui permet de prévoir à court et à long terme le niveau de production et de consommation. Les énergies renouvelables qui fonctionnent ***souvent par intermittence*** et de façon peu prévisible (ex : l'éolien) peuvent ainsi être mieux gérées.

- **Une gestion plus responsable des consommations individuelle** : les compteurs communicants (ou **compteurs évolués, *« Linky » pour l'électricité***) sont les premières versions d'application du réseau intelligent. Installés chez les consommateurs, ils fournissent des informations sur les prix, les heures de pointe de consommation, la qualité et le niveau de consommation d'électricité du foyer. Les consommateurs peuvent alors réguler eux-mêmes leur consommation au cours de la journée. De leur côté, les opérateurs du réseau peuvent détecter plus vite les pannes.

- Ce type de réseau permet par conséquent de passer d'un système de production dépendant de la demande à un système de consommation basé sur l'offre, qui devra à l'avenir s'adapter aux variations aléatoires de la production d'énergies éolienne et solaire.

- Associé à d'autres technologies telles que le pompage-turbinage ou encore les installations à gaz à cycle combiné, particulièrement flexibles, ce réseau doit contribuer à améliorer la sécurité d'approvisionnement, à réduire les coûts relatifs au réseau de distribution et à l'énergie de réglage, à intégrer les énergies renouvelables au réseau et à améliorer l'efficacité de l'ensemble du système.

- Un smart grid associe le réseau électrique déjà existant à des applications issues des technologies de l'information et de la communication.

- Cependant, si plusieurs technologies actuelles peuvent d'ores et déjà être utilisées, elles doivent être tout d'abord testées sous la forme de composants individuels, car la réalisation technique dépend de la stabilité et de l'efficacité de leur interaction.

- En effet, à part dans certains projets de recherche, aucun smart grid garantissant un pilotage complètement automatisé des appareils consommateurs et des installations de production n'existe encore dans le monde : il ne s'agit pour l'heure que d'un concept.

  Les tests effectués actuellement sur les smart mètres, déjà déployés à large échelle dans certains pays, constituent une première étape dans la mise en œuvre de ces réseaux intelligents.

- Cette technologie doit inciter les consommateurs finaux à économiser l'électricité et encourager la maîtrise de l'injection décentralisée.

- Le succès des smart grids dépendra en grande partie de l'intérêt économique ainsi que de l'atteinte au confort individuel des différentes parties prenantes.

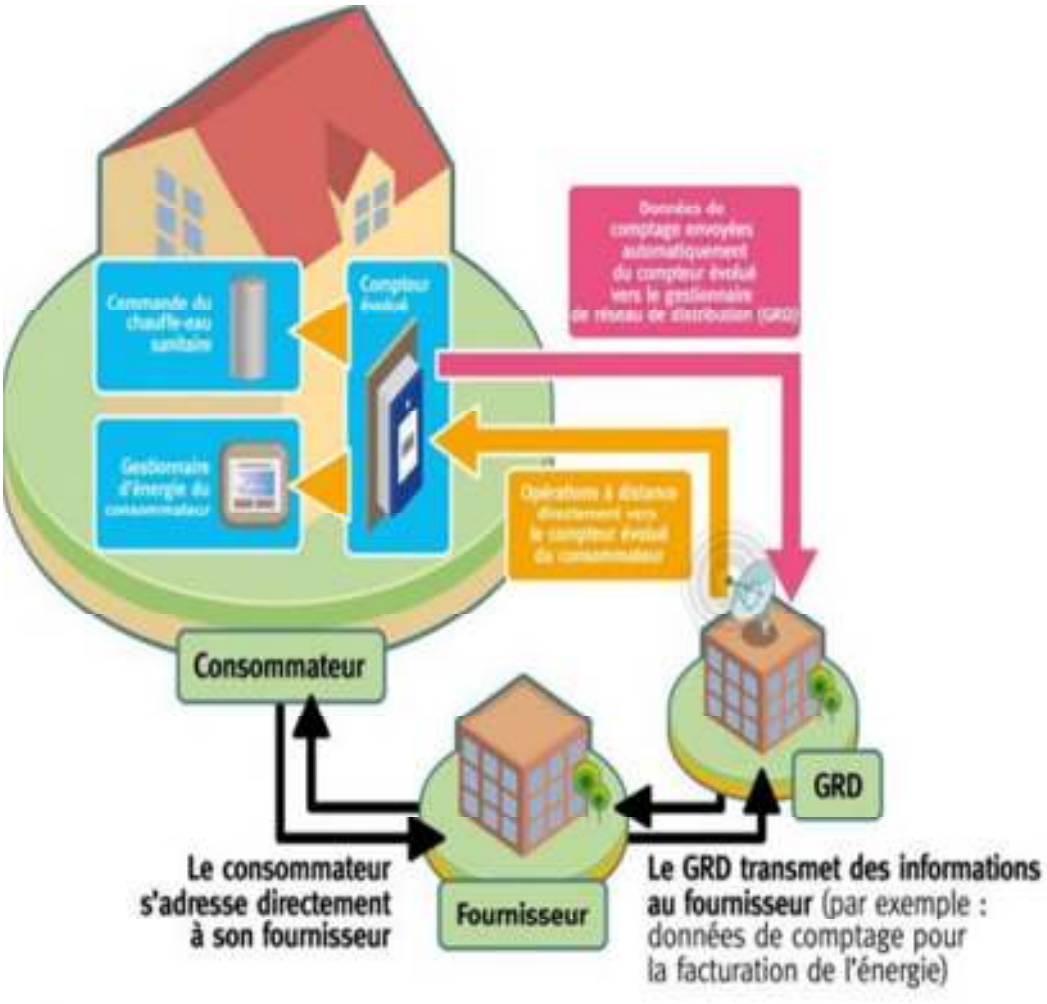

Figure 1.2: Principe des compteurs électriques évolués [W2]

2.2.2. Acteurs majeurs

Le développement des réseaux intelligents nécessite le concours de nombreux acteurs :

- **Les consommateurs**, en régulant eux-mêmes leur consommation d'électricité, participent à l'efficacité du système ;
- **Les producteurs d'électricité** alimentent les réseaux de transport d'électricité et doivent être capables de répondre en temps réel à la demande. Le développement des smart grids permet également aux producteurs décentralisés de petites capacités (ex : les éoliennes ou les panneaux photovoltaïques appartenant à des particuliers) d'être raccordés ;
- **Les gestionnaires des réseaux de transport** et de distribution ainsi que les constructeurs de matériel électrique gèrent et installent les équipements de mesure assurant la sécurité et le fonctionnement des réseaux. Ils sont les acteurs techniques majeurs du développement des smart grids ;
- **Les gestionnaires de processeurs et de systèmes informatiques** comme info vista, Intel, Google ou Cisco system, développent les technologies d'information indispensables au fonctionnement des réseaux intelligents ;
- **Les pouvoirs publics** soutiennent et encadrent le développement des réseaux intelligents notamment par la définition de normes de communication et la protection des systèmes contre les intrusions ou détournements. **[7]**

2.2.3. Structure des Smart Grids

Pour faire face aux mutations du contexte énergétique, les gestionnaires de réseaux électriques ne peuvent plus compter uniquement sur la conduite prévisionnelle du réseau électrique (peu réactive face à l'intermittence des énergies renouvelables par exemple), ni envisager le redimensionnement du réseau (onéreux et non optimal).

La solution réside dans l'automatisation de la conduite des réseaux électriques, grâce à l'acquisition et l'exploitation en temps réel d'informations sur l'état des réseaux. Cela passe par le déploiement d'un réseau informatique au niveau des infrastructures électriques, et la mise en place dans le Système d'Information (SI) d'outils pour l'exploiter.

Ainsi équipés, les réseaux électriques s'apparentent à une toile d'araignée où les mailles interagissent constamment via des liens de communication. Ces mailles correspondent aux acteurs du système électrique : consommateurs, producteurs ou les deux à la fois. Outre l'électricité, ces acteurs produisent et consomment de l'information en temps réel grâce aux modules logiciels dont ils sont équipés et à divers moyens de télécommunication, tels que les réseaux mobiles ou le Courant Porteur de Ligne (CPL). Ce partage permanent et instantané d'informations entre les équipements préserve la stabilité du système électrique tout en augmentant son efficacité énergétique.

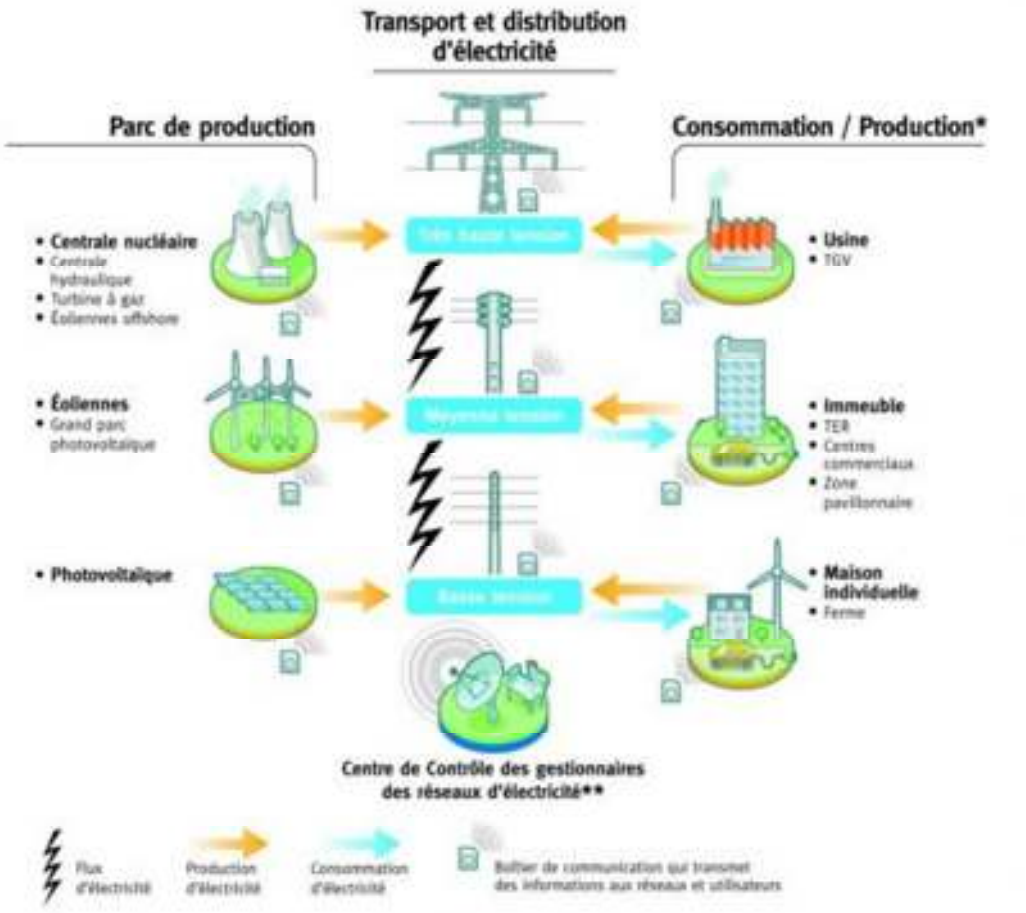

Figure1.3: Structure du réseau électrique intelligent [8]

Nés de la convergence des réseaux électriques, les Smart Grids se composent ainsi de trois couches que nous retrouvons dans la figure 1.3 :

- **Le premier niveau** correspond à l'infrastructure et aux équipements électriques acheminant l'électricité tels que les lignes et les transformateurs ;
- **Le second niveau** correspond à l'infrastructure de communication composée de différentes technologies de télécommunication comme la fibre optique, le CPL, ou encore la Troisième Génération (3G) ;
- **Le troisième niveau** correspond aux applications informatiques qui incarnent « l'intelligence» du réseau. En utilisant des informations délivrées en temps réel, ces applications calculent des consignes à envoyer aux équipements concernés et automatisent ainsi la conduite du système électrique. Cette intelligence est centralisée au niveau des centres de conduite du réseau ou distribuée sur les équipements électriques.

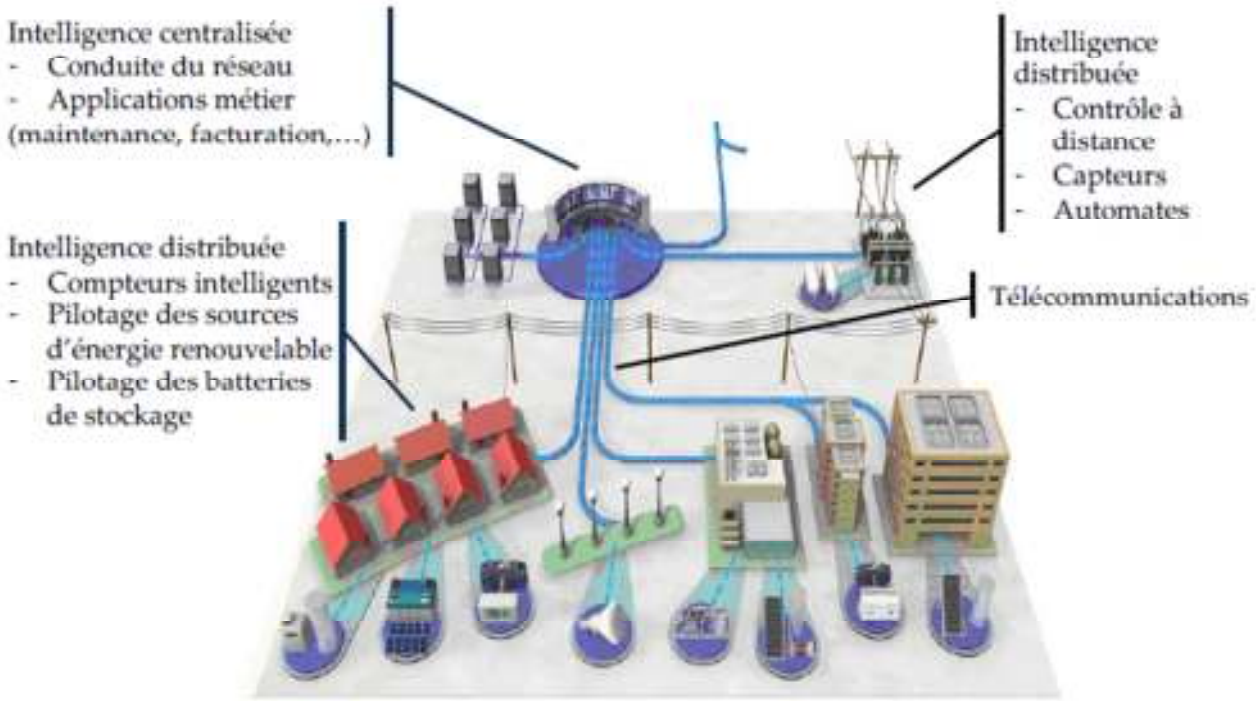

Figure 1.4 : Architecture des Smart Grids [8]

2.2.4. Organisation d'un Smart Grid

La Figure 1.4 est un exemple de référence pour réseaux intelligents. Les éléments ci -après y sont représentés[3]:

- **Réseau domestique (HAN)** – Réseau d'appareils de gestion de l'énergie, d'équipements électroniques numériques grands publics, d'appareils électroménagers commandés ou activés par un signal et d'applications dans un environnement domestique qui constitue l'extrémité domicile du compteur électrique.
- **Réseau de jonction extérieure (FAN)** – Réseau conçu pour assurer la connectivité aux appareils d'acquisition des données sur le terrain. Le réseau FAN peut assurer une connectivité à la sous -station située en amont des appareils d'acquisition de données sur le terrain ou une connectivité qui permet d'éviter les sous -stations et de relier les appareils d'acquisition de données sur le terrain pour former un système de gestion et de commande centralisées (appelé communément système SCADA).
- **Réseau de proximité (NAN)** – Système réseau visant à assurer une connectivité directe avec les dispositifs terminaux des réseaux intelligents dans une zone géographique relativement petite. Dans la pratique, un réseau NAN peut couvrir quelques pâtés de maison dans un environnement urbain ou des zones de plusieurs kilomètres carrés dans un environnement rural.

[3]Les définitions et la figure sont tirées de la norme NISTIR 7761.

- **Réseau étendu (WAN).**
- **Point d'agrégation des données (DAP)** – Ce dispositif est un acteur logique qui correspond, dans la plupart des réseaux AMI, à la limite entre les réseaux étendus et les réseaux de proximité (par exemple collecteur, relais de cellule, station de base, point d'accès, etc.).
- **Infrastructure de comptage évoluée (AMI)** – un système réseau conçu spécialement pour prendre en charge une connectivité bidirectionnelle aux compteurs d'électricité, de gaz et d'eau, et plus particulièrement aux compteurs AMI et, éventuellement, à l'interface des services d'énergie de l'entreprise de services collectifs.
- **Surveillance et acquisition de données (SCADA)** – Systèmes utilisés pour contrôler au quotidien les opérations du réseau de distribution d'électricité et mener des activités de surveillance selon les besoins.
- **Processeur frontal (FEP)** – Appareil servant de conduit principal pour envoyer les commandes provenant du système DMS/SCADA et recevoir les informations envoyées par les appareils déployés sur le terrain dans le réseau de distribution.

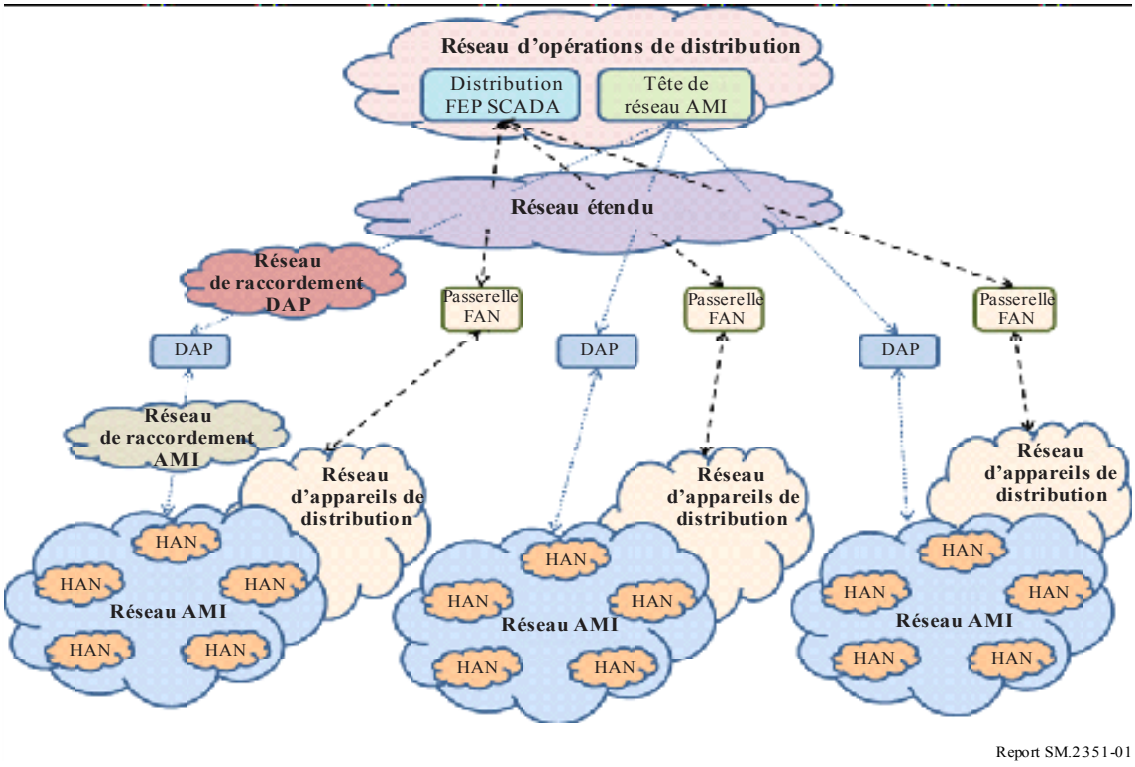

Figure 1.5 : Exemple d'organisation d'un réseau intelligent [9]

2.2.5. Stratégie orientée Smart Grids

En traitant les données envoyées en temps réel par les capteurs installés sur les équipements électriques et chez les consommateurs, les SI calculent des consignes destinées à des organes télécommandés permettant ainsi de piloter les réseaux électriques à distance. Cette automatisation de la gestion des réseaux est une solution pour les adapter rapidement face aux contraintes qu'introduit l'intégration des énergies renouvelables et des nouveaux usages . Les SI sont donc au cœur des enjeux des Smart Grids.

L'implémentation des Smart Grids va ainsi de pair avec la mise à niveau des SI des gestionnaires du réseau électrique. En effet, ces SI doivent pleinement intégrer les évolutions qu'induisent les Smart Grids au niveau des processus métier du gestionnaire de réseau, des acteurs impactés, des informations échangées ainsi que des applications informatiques et des infrastructures techniques sous-jacentes. Parmi ces évolutions nous citons :

- Les nouveaux flux d'information provenant du réseau électrique ; L'entrée en jeu de nouveaux acteurs tels que les producteurs décentralisés (éolien, Photovoltaïque) ;
- Les nouveaux équipements communicants comme le compteur Linky ;
- Les nouvelles réglementations et directives européennes (dans le cas des gestionnaires de réseaux européens) ;
- Les nouveaux usages comme les véhicules électriques ou encore les maisons connectées.

Le tableau1.1. Suivant décrit sous les différentes sources d'information sur les différentes étapes du schéma de distribution dans un réseau SMART GRID

Production	• Surveillance de l'état des équipements de production. • Capteurs de l'interconnexion avec les réseaux de transport. • Niveau de charge des systèmes de production.
Transport	• Capteurs pour contrôler les systèmes de lignes à haute tension. • Surveillance de l'état de l'équipement dans les postes de transformations. • Surveillance et gestion des unités de mesure de phraseur (pmu). • Information des travailleurs du secteur de la maintenance des lignes a haute tension. • Surveillance de la condition environnementale dans les différentes étapes.
Distribution	• Surveillance de l'état des lignes. • Gestion et surveillance de l'équipement dans les postes de transformation (moyenne-haute tension). • Surveillance et gestion des systèmes d'alimentation au réseau. • Information des travailleurs du secteur de la maintenance des lignes a haute tension. • Surveillance des sous –stations. • Information de l'énergie consommée.
Consommateur	• Information de l'énergie consommée. • Information sur les modes consommation. • Informations sur les consommations par les appareils électrodomestiques. • Surveillance et gestion sur la production et l'alimentation au réseau de la part du consommateur.

Tableau 1.1 : Sources d'information dans les réseaux Smart Grid [10]

Les gestionnaires de réseaux électriques doivent faire évoluer leurs stratégies de développement en envisageant de nouveaux modèles métier et de nouveaux partenaires, tout en tenant compte de l'émergence des nouvelles technologies et des exigences du législateur.

Une étude américaine, menée et South Carolina Edison, fait état de cinq thèmes stratégiques clés pour l'implémentation des Smart Grids :

- Permettre au consommateur de contrôler sa consommation d'énergie et de réduire son empreinte carbone en utilisant des équipements intelligents et des véhicules électriques et en produisant de l'énergie renouvelable à domicile ;

- Améliorer la sécurité et la productivité des employés en mettant par exemple à leur disposition des outils performants pour le contrôle à distance, des équipements de protection, et des applications mobiles ;
- Intégrer des sources d'énergie renouvelables distribuées sur le réseau en assurant la protection des équipements électriques, le stockage de l'énergie et la stabilité du réseau ;
- Améliorer l'efficience et la résilience du réseau à travers les systèmes de mesure en temps réel, l'analyse et le contrôle à distance ;
- Fournir les informations et la connectivité nécessaires en développant une infrastructure tic pour répondre aux besoins d'informatisation du réseau électrique.

2.2.6. Comparaison entre Réseaux classiques et les Réseaux intelligents [11]

Un des principaux problèmes soulevés par les smart Grids est leur intégration dans les réseaux électriques physiques utilisés quotidiennement par des millions d'usagers. Le tableau 1.2.compare les caractéristiques des réseaux électriques d'aujourd'hui et ceux potentiels des smart grids

	RESEAUX CLASSIQUES	**SMART GRID**
Caractéristiques participation des consommateurs	Les consommateurs ne sont pas informés et ne participent pas.	Les consommateurs sont informés et potentiellement actifs.
Intégration des sources et systèmes de stockage	Dominés par les producteurs d'énergie centralisée	Déploiement d'un grand nombre de producteurs distribués
Nouveaux produits, services et marchés	Limité, peu d'intégration du marché pour les consommateurs	Grande intégration du marché augmentation de l'utilisation du marché de l'énergie de pour les consommateurs.
Qualité de l'énergie	Centrée sur les pannes, réponse lente problèmes de qualité de l'énergie	Priorité sur la qualité de l'énergie avec une grande variété de qualité et de prix, rapide résolution des problèmes.
Optimisation des actifs	Peu d'intégration des donnés opérationnelles de gestion d'actifs.	Nombreuses acquisitions de données élargies et des paramètres du réseau.
Auto cicatrisation	Prévention pour réduire l'impact des dégâts en se concentrant sur la protection des infrastructures suit à une panne	Détection automatique et correction des problèmes, centrés sur la prévention pour minimiser l'impact sur le consommateur.
Résistance aux attaques	Très vulnérables aux attaques.	Résistance aux attaques avec restaurations rapides en cas de problèmes

TABLE 1.2 : Comparaison des réseaux classiques et des smart grids [11]

2.2.7. Les Avantages des Smart Grids [11]

- Les smart grids améliorent la sécurité des réseaux électriques. En équilibrant l'offre et la demande.
- Ils augmentent l'efficacité énergétique globale : ils réduisent les pics de consommation, ce qui atténue les risques de panne généralisée.
- Ils limitent l'impact environnemental de la production d'électricité en réduisant les pertes et en intégrant mieux les énergies renouvelables.
- Les smart Grids ont aussi un avantage pour les consommateurs car ils permettront d'avoir:

  - ✓ Maison plus intelligente,
  - ✓ Factures plus précises,
  - ✓ Pannes mieux détectées et plus rapidement réparées,
  - ✓ Offres tarifaires plus diversifiées.

2.2.8. Les limites des Smart grids [11]

- On de la mise en œuvre tel que le coût des investissements élevé.
- Les smart grids doivent être implantés sur l'ensemble du réseau et impliquer tous les acteurs pour être efficaces ;
- Sans oublier l'obstacle de la diversité des acteurs, car ils doivent mettre au point des systèmes communicants variés avec des logiques convergentes ;
- Ainsi que les données recueillies sont complexes à gérer et à stocker ;

3. Les applications du Smart Grid

Le Smart Grid est équipé d'un nombre énorme d'applications, les plus intéressantes sont :

3.1. La tarification dynamique

Cette application envoie aux consommateurs les prix horaires d'énergie. Dynamic Pricing aide les utilisateurs à diminuer leur montant de facturation par la réduction des charges pendant les heures critiques (les heures de pique de consommation**) [12**].

3.2. Réponse de la demande

L'application Demand Response (DR) se rapporte à la gestion d'une demande accrue de réduction de la demande ou d'augmentation de la puissance fournie à la grille. Elle permet de garder la stabilité du réseau électrique pendant les heures de pointe (les périodes où la demande en électricité est la plus élevée) **[13].**

3.3. Lecture de compteur d'Automatico (AMR)

AMR est connu aussi sous le nom de Smart Mètre Measurements. Il assure la collecte automatique et périodique des taux de consommation. Ces mesures d'intervalle sont nécessaires une fois par heure ou une fois toutes les 15 minutes ou même à raison d'une fois toutes les 5 min, cette application empêche les consommateurs illégaux de contourner ou trafiquer le compteur. Les acteurs de cette application sont le Smart Mètre et le centre contrôle (control center) **[13].**

3.4. Stockage distribué

Le terme stockage distribué (DS) est utilisé pour désigner un dispositif de stockage de l'électricité connecté au Smart Grid , qui est capable de stocker l'énergie électrique provenant de la grille (charge) et de livrer l'énergie accumulée à la grille (décharge) lorsque c'est nécessaire. La consommation d'énergie provenant du stockage de l'énergie électrique peut être utilisée pour compenser les variations de la demande **[14].**

3.5. Automatisation de la distribution

DA est l'intégration de la technologie de l'énergie, la technologie de l'information et la technologie de la communication. DA a un rôle critique au sein du Smart Grid.

Dans son contexte plus large, l'automatisation de la distribution se réfère à l'automatisation de toutes fonctions liées au système de distribution à travers les données recueillies auprès des dispositifs de sous station, dispositifs déployés sur les départs (feeders) et mètres (meters) déployés à l'emplacement des consommateurs (consumer**) [15]**

3.6. Chargement des véhicules électriques :

Les batteries des véhicules électriques (EVs) peuvent être rechargées à partir d'une infrastructure de recharge. Evs reçoivent l'énergie électrique à partir de la grille ou des lignes électriques à usages spéciaux **[16]**

4. Système de contrôle et d'acquisition de données pour Smart Grid

Les réseaux électriques sont des systèmes complexes qui, en l'absence d'un système de gestion de l'énergie, ne peuvent pas être exploités de manière efficace et sûre. Avec l'évolution de nos réseaux vers des réseaux intelligents, l'intégration de quantités d'énergie croissantes provenant de sources renouvelables jour.

Les systèmes de contrôle et d'acquisition de données(SCADA) surveillent, commandent, optimisent et coordonnent les systèmes de production et de transport. SCADA/DMS (Distribution Management System) remplit les mêmes fonctions pour les réseaux de distribution d'énergie.

Les deux types de systèmes permettent aux entreprises d'alimentation en électricité de collecter, d'enregistrer et d'analyser les données de centaines de milliers de points de mesure dans les réseaux nationaux ou régionaux, de modéliser leurs réseaux, de simuler le fonctionnement de l'alimentation en énergie, de localiser les dérangements, de prévenir les pannes et d'être présentes sur les marchés du négoce de l'énergie.

Les systèmes font partie intégrante des réseaux électriques modernes. Ils permettent le développement de réseaux intelligents, qui sont les systèmes énergétiques fortement automatisés du futur. Les réseaux intelligents doivent intégrer de grandes quantités d'énergie provenant de sources renouvelables, issues d'installations de production de plus ou moins grande dimension. Pour maintenir la stabilité du réseau en dépit des pannes susceptibles d'affecter ces sources d'énergie et garantir le flux d'énergie dans les deux sens (dans un système qui n'était prévu que pour un seul sens).

4.1. Qu'est-ce qu'un système SCADA

Un SCADA comporte du matériel, des contrôleurs, des réseaux et communications, une base de données, un logiciel de gestion d'entrées-sorties et une interface homme-machine. Les informations de terrain du dispositif SCADA sont centralisées sur une unité centrale.

L'environnement SCADA collecte des données de diverses appareils d'une quelconque installation, puis transmit ces données à un ordinateur central, que ce soit proche ou éloigné, qui alors contrôle et supervise l'installation, ce dernier est subordonné par d'autres postes d'opérateurs.

Il s'agit d' un système de gestion à distance pour traiter en temps réel un grand nombre de mesures et de contrôler à distance les installations techniques. Ce système peut être utilisé pour gérer les réseaux électriques, comme il peut aussi être utilisé sur d'autres applications ou domaines comme les canalisations de gaz et de pétrole, le transport de produits chimiques, etc **[W3].**

4.2. Composants :

Un dispositif SCADA, utilisé comme un outil de sécurité de consignation d'appareil électrique, est généralement composé : **[W4]**

- D'une interface homme-machine qui présente les données à un opérateur humain et qui lui permet de superviser et commander les processus.
- D'un système de supervision et contrôle informatique, faisant l'acquisition des données des processus et envoyant des commandes (consignes) aux processus.
- D'une unité terminale distante reliant les capteurs convertissant les signaux en flux de données numériques et envoyant les données numériques au système de supervision.
- Des automates programmables industriels utilisés sur le terrain pour leur versatilité et flexibilité due à leur capacité d'être configurables.
- D'une infrastructure de communication reliant le système de supervision et contrôle aux éléments terminaux.
- De divers instruments d'analyse.

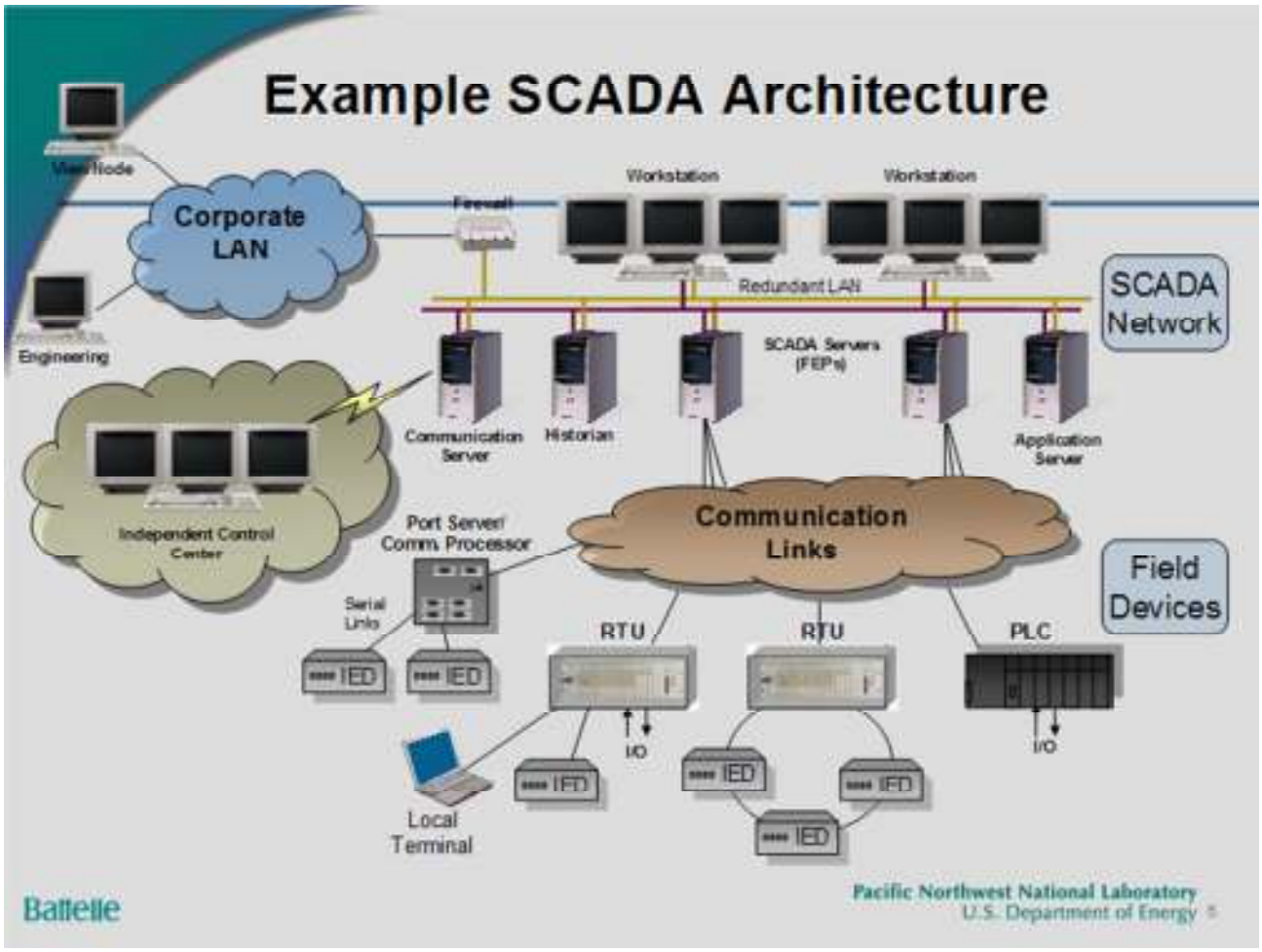

Figure 1.6 : Composants d'un système SCADA [17]

4.3. Avantages de SCADA dans le Smart Grid

- Le suivi de près du système ; voire l'état du fonctionnement de procède dans des écrans même s'il se situe dans une zone lointaine.
- Le contrôle et l'assurance que toutes les performances désirées sont atteintes ; de visualiser les performances désirées du système a chaque instant, et s'il y aurait une Perte de performance, une alarme se déclenchera d'une manière automatique pour Prévenir l'opérateur.
- Produire une alarme lorsqu'une faute se produit et visualise même la position ou situe la faute et l'élément défectueux, ce qui facilite la tâche du diagnostic et de l'intervention de l'opérateur.
- Donne plusieurs informations sur le système ainsi aide l'opérateur à prendre la bonne Décision, et ne pas se tromper dans son intervention. **[17]**

5. Défis et Problèmes des SMART GRID

5.1. Problème de cyber sécurité dans la smart grid

Les vrais incidents de sécurité de cyber et les événements relatifs qui seront présentés, et le nombre d'acteurs augmentera de manière significative (par exemple des prestataires de service, des acheteurs, des prosumers, etc.). Ceci présentera de nouveaux risques, et donc des stratégies originales devraient être définies pour faire face à eux.

Les attaques contre la grille de puissance peuvent directement effectuer le mode de vie de la société. Les organismes publics et le personnel des utilités actionnant les réseaux de distribution et de transmission, comme des organismes d'acheteurs de l'électricité et de génération devraient se rendre compte de cette situation. Sans eux il serait impraticable de mettre en place les mécanismes nécessaires pour améliorer le maintien de sécurité de leurs réseaux courants et pour inclure la sécurité de cyber comme premier objectif des grilles futées.

Nous rappellent que les systèmes à régulation de processus généralement et en particulier des infrastructures d'ICS de grille de puissance (par exemple systèmes de SCADA), commencent à être les cibles attrayantes. La protection des systèmes de contrôle industriels couvre largement beaucoup d'aspects appropriés qui s'appliquent directement aux grilles futées. Le lecteur est encouragé à employer les rapports associés comme source d'information complémentaire.

5.2. Problèmes de smart grid /smart mètre

Les clients ont vu leurs factures monter pour le même usage d'énergie, factures doublant parfois, triplement et plus incluant pour les maisons vides. Ceci a apprêté à Bakersfield et à Fresno au commencement, et contrairement aux réclamations, les augmentations de facture ont commencé dans l'horaire d'hiver, pas en été, selon le chroniqueur californien Lois Henry de Bakersfield. Le groupe de structure a été loué pour évaluer ces issues, mais leur location en a créé polémique.

La « structure aide des compagnies en mettant en application leurs initiatives smart grid »

5.3. AMÉLIORATION DE LA DÉTECTION D'INTRUSION

Les problèmes de la surcharge de l'information et des positifs faux actuellement sont abordés par un certain nombre de chercheurs et fournisseurs d'identification. Les approches prometteuses incluent la corrélation alerte (interdire et Wespi, 2001 ; Valdés et Skinner, 2001), exploitation de données (Lee, et autres, 2000), et groupement d'alerte (par exemple, Julisch, 2003).

Cependant, les problèmes sont non seulement liés à l'identification. Se rappeler que le travail d'identification implique les systèmes multiples et les ressources en information. Les solutions vraies doivent engager le travail identification de manière holistique, impliquant tous ses éléments. Les solutions techniques aideront, mais ne garderont pas le pas à mesure que la taille des réseaux augmentent et des exigences de sécurité deviennent plus rigoureuse. Donné notre

arrangement de ceci comme problème sociotechnique, ceci première recherche nous dirige vers les deux domaines du développement d'organisation de changement et d'outil pour une solution intégré.

Classés en problèmes de sécurité pour AMI:? Confidentialité et notamment la vie privée, qui peut fortement affecter la vue des clients de déployer un réseau intelligent. Les clients pourraient ne pas aimer les personnes non autorisées, ou les entreprises à connaître leurs habitudes d'utilisation. Les modèles d'utilisation peuvent également révéler les habitudes de vie et même la présence / absence de résidents qui pourraient être utilisés par des voleurs. Si les préoccupations des gens ne sont pas satisfaits, ils peuvent refuser de coopérer dans le déploiement de réseaux intelligents, à savoir, ils peuvent refuser de laissez les fournisseurs de services publics installation des compteurs intelligents à leur place.

La smart grid est un système composé qui combine des systèmes, des réseaux et des processus différents. Il comprend également un certain nombre de technologies telles que les technologies de l'information et la communication avec le réseau électrique. La smart grid comporte deux infrastructures, une infrastructure électrique et une infrastructure de communication. L'infrastructure de communication contrôle l'infrastructure électrique. Donc, le succès de la smart grid dépend de la sécurité de l'infrastructure de communication.

6. les Challenges de sécurité dans smart grid

- Un changement important nécessite généralement des défis importants, smart grid ne fait pas exception. les systèmes de vue réseau moderne, énumère les éléments suivants :
  - exigences de sécurité de données et d'information
  - Un grand nombre de dispositifs intelligents (la sécurité dans la chaîne d'approvisionnement)
  - Sécurité physique et périmètre de la grille (coopération internationale)
  - Les protocoles de communication sécurisés
  - Un grand nombre d'intervenants et de synergies avec d'autres services publics
  - L'absence de définition du concept de réseau intelligent et de ses exigences en matière de sécurité
  - Le manque de sensibilisation des parties prenantes des réseaux intelligents
  - Promouvoir l'échange d'informations sur les risques, les vulnérabilités et les menaces

Conclusion

Le Smart Grid est un réseau complexe de point de vue architecture et fonctionnement .Dans ce chapitre nous avons défini le concept du Smart Grid. Puis, nous avons cité les avantages obtenus par l'introduction des technologies des communications dans la grille traditionnelle .Et enfin, nous avons cité quelques applications.

Chapitre 2

Sécurité Informatique dans le smart

1 .Introduction

En effet de plus en plus d'entreprises subissent des attaques qui peuvent entraîner des pertes conséquentes. Nécessité d'institutions dans le domaine de la sécurité informatique dans le réseau intelligent est devenu plus important et un élément clé d'une bonne politique de sécurité est l'utilisation de l'IDS pour. Contenir les systèmes informatiques et les réseaux, les diverses formes de faiblesse. Répondre à ces problèmes de sécurité dans le réseau intelligent, a développé divers mécanismes en place pour éviter toute sorte d'attaque comme les pare-feu, l'authentification, les agents, etc ... Malheureusement, ces mécanismes ont des limites où certains types d'attaques peuvent nuire à la voie de contournement à la confidentialité, l'intégrité et la disponibilité. Pour résoudre ce problème, l'introduction du système de détection d'intrusion comme une deuxième ligne de défense pour renforcer la sécurité des systèmes informatiques dans un nouveau concept de réseau intelligent.

2. Les attaques en informatique

2.1. Quelques concepts de base :

2.1.1. Définition d'une attaque : est une action malveillante qui tente d'exploiter une faiblesse dans le système et de violer un ou plusieurs besoins de sécurité

2.1.2. Définition d'une intrusion :

C'est une violation d'une politique de bien sécurités d'un système donnée, c'est –a- dire une violation d'une des propriétés de confidentialité, d'intégrité ou de disponibilité du système en question.

Une intrusion est définie comme étant une faute opérationnelle, externe, intentionnellement nuisible, résultant de l'exploitation d'une vulnérabilité dans le système **[19].**

2.1.3. Vulnérabilités :

Les vulnérabilités d'un outil informatique représentent tous les bugs de conception ainsi que toutes les lacunes causées par la configuration. Donc les vulnérabilités d'un système informatique représentent la combinaison des vulnérabilités des outils qui le compose. Souvent la présence de certains outils ensemble crée et favorise d'autres vulnérabilités .Toutes ces vulnérabilités représentent des faiblesses pour le système et ainsi des opportunités d'attaques pour les intrus.

La superposition de l'infrastructure de réseau électrique et des systèmes de TI modernes augmente considérablement les vulnérabilités et les points d'accès que les criminels et les terroristes peuvent utiliser pour attaquer le système électrique.

2.1.4. Politique de sécurité

Une politique de sécurité est un plan d'actions et de mécanismes mis en œuvre afin d'assurer la disponibilité, l'intégrité ainsi que la confidentialité des services et des données d'un système d'information cette politique doit assurer que chaque utilisateur fait son travail et utiliser les services du système facilement et que cet utilisateur fait confiance ce système, pour cela il faut : **[20].**

- ✓ Utiliser des outils matériels et logiciels sur les différents niveaux afin de contrôler la circulation des informations.
- ✓ Préciser les droits d'accès aux différentes personnes chargées a utiliser le système.

2.1.5. Signature d'attaque

Une signature d'attaque est un motif représentant toute l'information concernant une attaque connue. C'est par ce moyen que l'administrateur réseau configure les systèmes de détection d'intrusions.

2.1.6. Alerte

Une alerte représente l'information transmise par l'IDS à l'intention de l'administrateur. Elle doit être claire, nette et précise.

2.1.7. Faux positif

On parle de faux positif lorsque l'IDS considère un fonctionnement normal comme une attaque.

2.1.8. Faux négatif

On parle de faux négatif lorsque L'IDS ne détecte pas une vraie attaque.

2.1.9. Lib Pcap

C'est une bibliothèque de fonctions qui sert d'interface à la capture de paquets réseau.

2.2. Les différentes étapes d'une attaque

La plupart des attaques, de la plus simple à la plus complexe fonctionnent suivant le même schéma : **[21]**

- **Identification de la cible :** cette étape est indispensable à toutes attaques organisées, elle permet de récolter un maximum de renseignements sur la cible et utilisant des informations

publiques et sans engager d'actions hostiles .on peut citer par exemple : l'utilisation des bases whois, l'interrogation des serveurs DNS ?....

- **Le Scanning :** l'objectif est de compléter les informations réunies sur une cible visées.
  IL est ainsi possible d'obtenir les adresses IP utilisées accessibles de même qu'un grand nombre d'informations de topologie détaillée (OS, versions des services, subnet, règles de firewall….). IL faut noter que certaines techniques de scans entrainent la défaillance de certains systèmes.
- **Les exploitations :** cette étape permette à partir des informations recueillies d'exploiter les failles identifiées sur les éléments de la cible, que ce soit au niveau protocolaire, des services et applications ou des systèmes d'exploitation présents sur le réseau.
- **La progression :** c'est quand l'attaquant réalise ce pourquoi il a franchit les précédentes étapes .Le but ultime étant d'élever ses droits vers root (ou système) sur un système afin de pouvoir y faire tout ce qu'il souhaite (inspection de la machine, récupération d'informations, installation de bachdoors, nettoyage des traces,….)

2.3. Les différents types d'attaques

IL existe un grand nombre d'attaques permettant à une personne mal intentionnée de s'approprier des ressources, de les bloquer ou de les modifier requièrent plus de compétences que d'autres, en voici quelques-unes :

2.3.1. Le sniffing

Grâce a un logiciel appelé sniffer, il est possible d'intercepter toutes les trames que notre carte reçoit et qui ne nous sont pas destinées. Si quelqu'un se connecte par Telnet par exemple à ce moment la, son mot de passe transitant en clair sur le net, il sera aisé de le lire.de même, il est facile de savoir à tout moment quelles pâques web regardent les personnes connectées au réseau, les sessions ftp en cours, les mails en envoi ou réception. Une restriction de cette technique est de se situer sur le même réseau que la machine ciblée.

2.3.2. L'IP spoofing

Cette attaque est difficile à mettre en œuvre et nécessite une bonne connaissance du protocole tcp. Elle consiste, le plus souvent, à se faire passer pour une autre machine en falsifiant son adresse IP de manière à accèder à un serveur ayant une relation de confiance avec la machine «

spoofée » cette attaque n'est intéressant que dans la mesure où la machine de confiance dont l'attaquant a pris l'identité peut accéder au serveur cible en tant que root.

2.3.3. Le Dos (denial of service)

Le Dos est une attaque visant à générer des arrêts de service et donc à empêcher le bon fonctionnement d'un système **[22].**Cette attaque ne permet pas en elle-même d'avoir accès à des données .En général, le déni de service va exploiter les faiblesses de l'architecture d'un réseau ou d'un protocole. IL existe de plusieurs types comme le footing, le tcp -syn. flooding le smurf ou le débordement de tampon (buffer- over flow).

Sur un dispositif du Smart Grid peut saturer la puissance de calcul du CPU, la mémoire ou la bande passante et se traduira par le retard de l'échange de données en temps réel. En conséquence, les opérateurs de centres de contrôle n'ont pas une vision complète de l'état de la grille de puissance, conduisant à des décisions incorrectes.

"

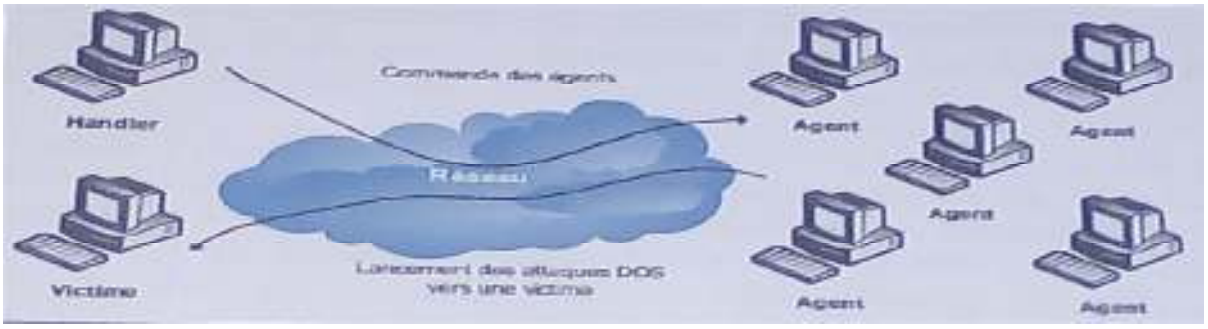

Figure 2.1 : L'attaque Dos [22]

2.3.4. Le cheval de Troie

Un cheval de Troie est un programme installé discrètement par un pirate sur votre ordinateur simulant une certaine action, mais faisant tout autre chose en réalité. Le nom vient du fameux "Cheval de Troie", offert en cadeau pour la paie entre les Pays, mais qui avait en fait pour but de causer la ruine et la destruction de la ville ayant reçu ce cheval .Un cheval de Troie sur un ordinateur est un programme exécutable qui est présenté comme ayant une action précise, généralement bénéfique pour l'ordinateur. Mais lorsque ce programme est lancé, il va causer des actions plus ou moins graves sur votre ordinateur, comme supprimer des mots de passe, voler des mots de passe, envoyer des informations confidentielles au créateur du programme, formater votre disque dur.

2.3.5. Les programmes cachés ou virus

IL existe une grande variété de virus. On ne classe cependant pas les virus d'après leurs dégâts mais selon leur mode de propagation et de multiplication. On recense donc les vers (capables de se propager dans les réseaux), les troyens (créant des failles dans un système), les bombes logiques (se lançant suite a un événement du système (appel d'une primitive, date spéciale)), virus d'infection des fichiers (parasites).

2.3.6. L'ingénierie sociale (social engineering)

Ce n'est pas vraiment une attaque informatique en soit, mais plutôt une méthode consistant à se faire passer pour que l'on n'est pas afin de recueillir des informations.

2.3.7. Le craquage de mots de passe

Cette technique consiste à essayer plusieurs mots de passe afin de trouver le bon. Elle peut s'effectuer à l'aide d'un dictionnaire des mots de passe les plus courants (et de leur variantes).Ou par la méthode de brute force (toutes les combinaisons sont essayées jusqu'à ce qu'on trouve la bonne). Cette technique longue et fastidieuse, souvent peu utilisée à moins de bénéficier de l'appui d'un très grand nombre de machines.

2.4. Exemple d'un scénario d'attaque sur le réseau

Les attaquants peuvent appliquer un plan d'attaque bien précis pour réussir leurs exploits **[23].** Leurs objectifs sont distincts et multiples. On distingue l'attaquant pirate, dans un but d'approfondissement de connaissances, essaie de découvrir les failles de sécurité dans un système informatique. Cette personne partage librement ses découvertes et évite la destruction intentionnelle des données. Le deuxième type d'attaquant, appelé Crack, cherche à violer l'intégrité du système. Généralement, il est facilement identifiable à cause de ses actions nuisibles. Néanmoins il faut distinguer un expert qui cherche les exploits et conçoit lui- même les programmes, d'un gamin scripteur (script kiddy) qui utilise la technologie existante pour ses fins malveillants. Les différents types d'attaquants cherchent à découvrir les propriétés du réseau cible avant de lancer les attaques . On parle généralement de la reconnaissance qui peut être passive ou active. Ayant récolté les informations nécessaires, ils lancent leurs vraies attaques pour exploiter le système. En suite ils créent des portes dérobées pour garantir des futurs accès faciles au système compromis. Enfin ils effacent leurs traces des journaux de sécurité. Nous détaillons dans la suite ces différentes étapes en les illustrant par des vrais scénarios d'attaques.

2.4.1. Attaque passive

IL s'agit d'une phase d'attaques ou l'intrus n'effectue pas une action pour collecter les informations. [**24]**

Il se restreint à observer passivement les événements afin d'en tirer les conclusions. Une des attaques les plus répandues est l'écoute du trafic (sniffing). Le principe consiste à installer une sonde sur le réseau pour capter le trafic et le sauvegarder dans des fichiers journaux. L'analyse de ces fichiers permet de connaitre les machines installées sur les réseaux et de déterminer les ports ouverts et les systèmes d'exploitation utilisés. L'attaque est considérée lente si l'attaquant cherche une information précise sur une machine particulière du réseau. En revanche, elle est discrète si il est difficile de la détecter.

En analysant les fichiers journaux, les attaquants cherchent les valeurs pas défaut des champs des protocoles. Ces valeurs dépendent du système d'exploitation.

Les intrus profitent alors de ces différences pour distinguer les systèmes d'exploitation et s'informer des services réseaux offerts par l'entreprise. Parmi les champs surveillés, on distingue :

- La taille initiale d'une fenêtre tcp (Windows).
- La durée de vie d'un paquet.
- La taille maximale d'un segment TCP.
- Le bit de non fragmentation.
- Le facteur multiplicateur de la fenêtre de réception.
- L'acquittement sélectif (SAck, SAckOK).
- L'option « aucune opération »(NOP).
- L'option de setampille de temps (TS).

Une attaque passive se réalise grâce a des outils tels que : les sniffer, les scanners,

Un sniffer est un dispositif, logiciel ou matériel, qui permet de capturer des informations (exemple : trames) qui transitent sur un réseau ou destinées à une machine.

Alors qu'un scanner est un programme qui permet de savoir quels ports sont ouverts sur une machine donnée. Les scanners servent pour les hackers à savoir comment ils vont procéder pour attaquer une machine. Exemples de scanners et sniffers : Nmap, wifi scanner, aircrack (wifi),…etc.

2.4.2. Attaque active

Contrairement a une attaque passive, ici l'attaquant n'est plus en mode écoute. Elle consiste à modifier des données ou des messages, à s'introduire dans des équipements réseau ou a pertuber le bon fonctionnement de ce réseau, a interroger le réseau (ou la machine) cible, contourner le dispositif de sécurité existant par diverses méthodes : Déni de Service(Dos), les Virus,….etc.

Parmi les outils les plus utilisées pour acquérir ces informations nous évoquons les utilitaires : PING, sLookup, ssh et Trace route.

2.4. 3. Exploitation du système :

Les deux types de reconnaissance passive et active permettent à un attaquant de localiser les applications vulnérables pour exploiter ensuite leurs faiblesses. L'intrus cherche à gagner un accès au réseau cible, élever son privilège ou lancer des attaques par déni de services. **[25]**

Pour accéder au système, il peut se baser sur les mauvaises installations des services .En effet, certaines configurations par défaut activent toutes les options disponibles pour prouver les richesses de l'application. Seulement ces options présentent le plus souvent des failles de sécurité facilement exploitables pour mener une attaque. Par exemple, le premier demande activait tous ses services dont une bonne partie étaient vulnérables.

L'exploitation des interactions entre deux programmes constitue également un moyen pour accéder aux systèmes informatiques. Diverses failles apparaissent si une application fort privilège ne protège pas ses méthodes, utilise des communications inter processus défaillantes ou crée des fichiers temporaires accessibles par d'autres programmes.

La Figure2.2 montre un scénario ou un utilisateur fort privilège accède au « fichier /trnp/racel ! »la période qui sépare la vérification du privilège et l'ouverture du fichier est critique puisque un utilisateur malveillant peut remplaces le fichier « /tmp /race »par un lien symbolique vers un autre fichier plus important comme « /ect / passrd ». Ainsi, en manipulant le lien symbolique, la victime peut corrompre involontairement les fichiers système ou ajouter des lignes qui correspondent a des nouveaux comptes utilisateurs.

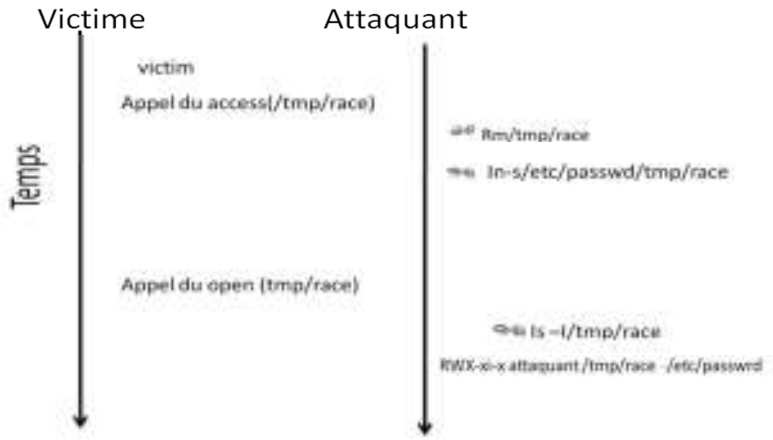

Figure 2.2 : Accès concurrents au contenu du fichier [25]

Par ailleurs un attaquant peut introduire des données imprévues pour tromper les applications mal conçues. Réussit ainsi des dépassements de tampon, altère des requêtes SQL et détourne de mécanises d'authentification. La Figure2.3 présente le mécanisme de

Débordement de tampon. Il s'agit de copier dans la pile une grande quantité de données dans un espace mémoire assez petit, prévu pour contenir les variables locales des fonction .Les données en excès contiennent du code malveillant et pénètrent dans des espaces mémoires voisins.

De plus, le pointeur retour de la fonction se voie écrasé pas une autre adresse qui pointe directement vers le code malveillant. Par conséquent, l'attaquant exploite le privilège de l'application pour créer de nouveaux comptes utilisateurs, élever privilège ou copier des données sensibles du système.

Contourner les mécanismes d'authentification, est encore possible via les entrées imprévues.

Considérons par exemple la requête SQL (1.1). Cette requête permet de vérifier le mot de passe de l'utilisateur var Nom en consultant la table utilisateur. Seulement un intrus peut s'identifier avec un nom d'un utilisateur légitime puis entré un mot passe de la forme.

La requête SQL (1.1) se transforme (1.2) et sera toujours vérifiée si l'utilisateur svar Nom existe dans la table utilisateur.

Select*from utilisateur where nom svar Nom and mot2passe svar passé (1.1)

Select*from utilisateur where nom= svar Nom and true (1.2)

En outre, un intrus utilise les attaques déni de services pour exploiter les systèmes informatiques. Il empêche l'exécution normale des services par la saturation de la bande passante ou l'épuisement des ressources système. La Figure 2.3 montre le détournement de session .Ce dernier a pu, via une inondation SYN, isoler la machine A qui maintient des relations d'approbation avec la machine B.

Ensuite il accède à la machine B en détournant la session de A. Les différents exploits présentés permettent d'accéder au système cible ou d'élever le privilège d'un utilisateur. Il existe cependant une solution plus rapide qui assure simultanément les deux attaques. Il s'agit des œufs qui comportent un code spécial contenant à son tour un autre code actif d'attaque. Le premier objectif est d'exploiter un programme doté d'un faible privilège puis d'attaquer et exploiter par l'intermédiaire du code actif, un morceau des droits d'accès plus élevés.

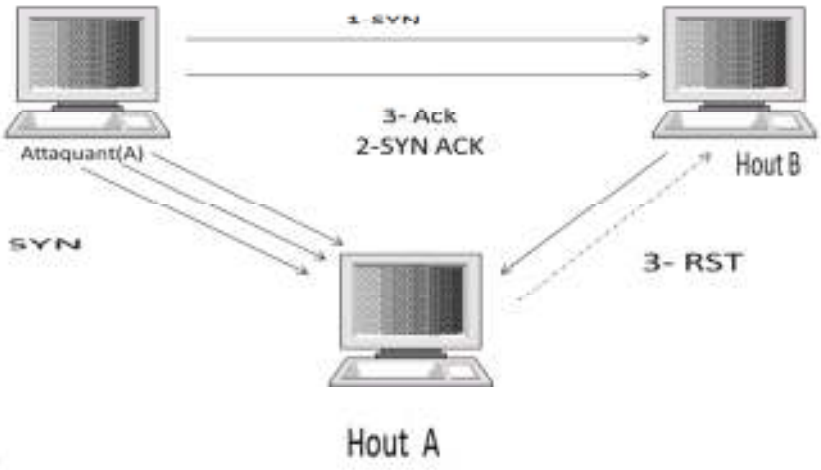

Figure 2.3 : Attaque de détournement de session [26]

2.4.4. Préservation de l'accès

Les attaquants installent des portes dérobées pour retourner facilement aux systèmes compromis. Par exemples, ils créent de nouveaux comptes et les utilisent lors des prochains accès.

Seulement cette procédure est facilement détectable si un administrateur vérifie constamment l'intégrité des fichiers des mots de passes. Un attaquant prudent utilise des chevaux de Troie qu'il télécharge aussitôt qu'il gagne son premier accès .Pour ce faire, il dispose de plusieurs sources d'informations, les pages web, le partage point et les dépôts.

2.4.5. Effacement des traces

Un attaquant qui compromet une machine et crée une porte dérobée, cherche aussitôt a effacer ses traces. IL nettoie ces entrées des fichiers journaux de sécurité. Une telle approche déclenche néanmoins des alarmes en vérifiant l'intégrité des fichiers.

L'attaquant essaie de restituer les mêmes propriétés des fichiers (date de création, de modification, dernière utilisation, etc.) pour garder la même signature .Ceci force les administrateurs à enregistrer les événements suspects sur des machines distantes pour mieux protéger les fichiers de sécurité .Ils multiplient également les utilitaires d'archivage pour résister aux intrus qui tentent de désactiver ces fonctionnalités ou de les modifier par d'autres programmes dés le premier accès a la machine.

2.5. La sécurité informatique

La sécurité informatique est la protection de l'information et des systèmes d'information contre l'accès, l'utilisation, la divulgation, la modification ou la destruction ; afin de granité et la disponibilité **[27].**

2.5.1. La mise en œuvre d'un politique de sécurité

La mise en œuvre d'un politique de sécurité globale est assez difficile, essentiellement par la diversité des aspects à considérer .Un politique de sécurité peut se définir par un certain nombre de caractéristiques : les niveaux ou elle intervient, les objectifs de cette politique et enfin les outils pour assurer cette sécurité. Chaque aspect différent doit être pris en compte, de façon a atteindre les objectifs de sécurité désirés, en utilisant de façon coordonnée les différents outils à disposition.

Nous allons tout d'abord parler des différents aspects un politique de sécurité, avant de définir les objectifs visés, puis de voir les outils disponibles pour appliquer cette politique.

Objectifs

Les objectifs d'une politique de sécurité sont de garantir la sécurité des informations et du réseau de l'entreprise **[27].**Ces impératifs peuvent étre définis plusieurs niveaux :

- **Disponibilité :**les données doivent rester accessibles aux utilisateures (une attaque de type DoS, par exemple, vise a empecher les utilisateurs normaux d'un service d'y accéder).

- **Confidentialité :**les données ne doivent étre visibles que pour des personnes habilitées.

- **Intégrité :**il faut pouvoir garantir que les données protégées n'ont pas été modifiées par une personne non autorisée.

- **Non répudiation**

On doit pouvoir certifier ,quand un fichier a subi des modifications ,la personne qui l'a modifié.

2.5.2. protection des systèmes informatiques

Les attaquants disposent de plusieurs moyens pour réussir chaque phase d'attaque.la disponibilité des outils d'attaques et la richesse des sources d'informations accentuent le risque de l'intrusion. Par conséquent les administrateurs sécurisent de plus en plus leurs systèmes informatiques, Ils s'appuient sur diverses solutions comme les pare feux, la cryptographie, les scanners de vulnérabilités et le système de détection d'intrusions.

a. Pare feux

Un pare feu (firewall) est un système physique ou logique qui inspecte les flux entrant et sortant du réseau.

Il existe principalement trois types de pare feux **[28] .**

- **Pare feu avec filtrage des paquets :** ce pare feu filtre les paquets en utilisant des règles statiques qui testent les champs des protocoles jusqu'au niveau transport. Ces fonctionnalités sont généralement incorporées dans un routeur appelé routeur à écran.
- **Pare feu avec filtrage des paquets avec mémoire d'états :** ce mode conserve les informations des services utilisés et des connexions ouvertes dans une table d'états. Il détecte alors les situations anormales suite à des violations des standards protocolaires.
- **Pare feu proxy :** Ce pare feu joue le rôle d'une passerelle applicative, en analysant les données jusqu' au niveau applicatif, il est capable de valider les requêtes et les réponses lors de l'exécution des services réseaux .Malgré leurs grands intérêts, les pare feux présentent quelques lacunes. En effet, un attaquant peut exploiter les ports laissés ouverts pour pénétrer au réseau local, ce type d'accès est possible même a travers des pare feux proxy. Il suffit d'utiliser un protocole autorisé tel que http pour transporter d'autres types de données permet a l'attaquant de contourner le parafe. Les scripts constituent aussi des sources d'intrusion que les pare feux échouent a détecter.

  Par exemple la vulnérabilité du RDS (remote data Service) sur les serveurs web.

c. Cryptographie

La cryptographie garantit la confidentialité, l'intégrité, la non répudiation et l'authenticité des données. Elle est fréquemment utilisée dans diverses applications réseaux telles que la messagerie, les connexions a distance, les réseaux privés et les serveurs web. Effectivement, diverses implémentations des protocoles de sécurité se sont révélées vulnérables. De plus la sécurité peut être rompue via plusieurs types d'attaques.par exemple l'homme du milieu (mitm) qui constitue une menace lors des créations des clés. Par ailleurs les courts et les simples mots de passes utilisés comme des clés de sécurité par les algorithmes symétriques sont facilement cassables via des clés privées suite a un mauvais stockage de ces informations ou la crypte analyse appliquée sur des algorithmes a faible encodage tels que le XOR,…etc.

En outre la cryptographie empêche l'analyse aisée du contenu des paquets et rend donc difficile la détection des attaques si elles sont déjà insérées dans des protocoles réseaux .Elle constitue même un moyen pour camoufler les attaques et par suit contourner les pare feux et les systèmes de détection d'intrusions. **[28].**

d. Pots de miels

Un pot de miel est une machine qui présente ou simule des failles de sécurité très répandues **[29].** Disposant des moyens renforcés de surveillance, la machine peut servir d'appât pour apprendre la stratégie des attaquants et construire des signatures exactes d'attaques.

Un pot de miel dispose de plusieurs outils de surveillance et d'archivage, nécessaires pour collecter les informations des activités suspectes, ces outils doivent être maintenus en permanence puisqu'ils sont déployés dans un environnement fréquenté principalement par des attaquants, de plus, l'isolation du pot de miel du reste du réseau est indispensable pour qu'il ne se transforme pas en une base pour compromettre d'autres machines.

2.6. Les attaques sur un réseau

- **L'attaque d'écoute**

  Lors de cette d'attaque d'écoute , le nœud malveillant écoute le trafic du réseau dans l'espoir d'extraire ou de collecter les données transmises dans le réseau. Une telle écoute peut être utilisée pour rassembler des informations et pour commettre de nouvelles attaques. Par exemple, un attaquant peut rassembler et examiner le trafic du réseau pour déduire des informations et des modèles de communication, les informations cryptées sont aussi interceptées.

- **L'attaque par injection de fausses données**

L'attaque par injection de fausses données en anglais « false-data injection attack » consiste à porter atteinte à la cohérence des informations acheminées dans le réseau en les modifiant ou en injectant des informations erronées. **[30]**

- **Usurpation d'identité**

L'attaque del' usurpation d'identité « **spoofing »** est l'utilisation de l'identité d'un nœud légitime pour bénéficier de ces privilèges.

- **Attaque de rejeu (Replay attack)**

L'attaque de rejeu en anglais « Replay attack» consiste à rejouer un message valable après l'avoir capturé. Exemple : l'attaquant rejoue un message de panne pour perturber le fonctionnement du Smart Grid. L'attaquant s'interpose entre deux parties d'une communication sans qu'aucune des parties n'en ait conscience et se fait passer pour l'autre parti pour chacune des deux entités légitimes.

- **L'attaque de déni de service**

les attaques par déni de Service (Dos) en anglais « Dénia of Service », regroupe les attaques destinées à rendre indisponible les services d'un smart grid. Cette attaque pourrait entraîner le système à l'instabilité **[31].** Exemple : L'attaque de brouillage « Jamming » consiste à diffuser constamment des interférences radio. Il constitue une menace de sécurité principale à fin d'empêcher le déploiement de réseaux sans fil dans le Smart Grid **[32].**

- **Attaques de synchronisation (Timing Attacks)**

L'attaquant va présenter un retard dans la transmission du signal **[31].**

Exemple : retarder les messages de pannes pour influencer l'image du réseau auprès des fournisseurs.

2. La sécurité dans les Smarts grids

Les Smarts Grids sont des réseaux capables d'échanger des informations sur toute la chaîne de valeur, de permettre un pilotage au plus près. Ils deviennent ainsi flexibles, plus efficaces,

tout en offrant davantage de maîtrise de l'énergie à une échelle locale. Cependant, l'écosystème ne peut tirer profit de ce réseau que lorsque les maillons finaux, consommateurs et producteurs, sont complètement impliqués, en acceptant d'y être liés physiquement via un compteur communicant et en adoptant les différents services proposés.

On retrouve les risques « classiques » associés à des solutions technologiques innovantes. En effet, ces systèmes sont récents et l'on manque de recul quant à leur interopérabilité, leur fiabilité et le risque d'obsolescence. À titre d'exemple, le système italien de smart meetings déployé il y a 10 ans est aujourd'hui remis en cause (utilisation de standards propriétaires, durée de vie faible…). Mais le principal risque est celui de la sécurité des systèmes.

En effet, les nouvelles fonctionnalités apportées résident dans la possibilité de communiquer au distributeur des données à caractère personnel, tels que l'identité du consommateur ou sa consommation électrique, des informations sensibles. De plus, l'utilisation de gestionnaire d'énergie pouvant avoir comme rôle de contrôler les appareils électroménagers et le chauffage, multiplie la sensibilité des données transmises par le compteur avec des risques de perte de contrôle ou d'utilisation illégale.

L'aspect communicant du compteur ouvre le chemin à tout type d'attaque. L'attaquant, en tant que consommateur / client, peut chercher à reprogrammer son compteur avec un tarif moins cher ou bien leurrer le distributeur vis-à-vis de sa consommation. Par ailleurs, une personne malveillante cherchant à récupérer des informations personnelles pour rait espionner la vie de ses voisins, changer leurs tarifs ou leur couper l'accès en énergie ! Les attaques peuvent aussi remonter le réseau amont avec un risque extrême de provoquer des coupures d'électricité sur l'ensemble du territoire ou la volonté d'attaquer les systèmes d'information afin de collecter des données sur les clients et consommateurs.

La standardisation des équipements est un facteur essentiel pour le développement et la mise en œuvre des smart grids notamment à cause de la complexité des écosystèmes matériels et de la diversité des acteurs proposant des solutions. La pédagogie et l'éducation du consommateur, acteur indispensable au succès du smart grid , représentent un second point de vigilance. Enfin, le fournisseur devra rassurer ses clients quant à la transparence du service fourni sans dégradation de la qualité d'approvisionnement (coupure / délestage / baisse de puissance), ni intrusion gênante dans la vie privée (politique de sécurité et de confidentialité). Ceci passe forcément par l'inclusion des bonnes pratiques dans le cycle projet (analyse de risques, liaison avec les autorités, mise en œuvre

de systèmes de contrôles robustes avec des capacités de mise à jour, audits réguliers et transparents des systèmes…) et une forte communication avec les acteurs du secteur et les utilisateurs**.[33]**

La sécurisation des communications d'un réseau exige l'utilisation de services et de mécanismes de sécurité pour contrer les attaques qu'on peut mener sur ce type de réseau. Dans cette partie, nous allons décrire les différents attaques, services et mécanismes de sécurité.

3.1. Les services de sécurité dans smart grid [34]

- **Authentification :** assure que seules les entités autorisées ont accès au système.
- **Disponibilité :** permet la disponibilité des informations et ressources quand un composant légitime en a besoin.
- **Intégrité :** assure que les données n'ont pas été modifiées durant le transfert.
- **Confidentialité :** garantit que seules les parties autorisées peuvent accéder aux données transmises à travers le réseau. Il protège l'information contre sa divulgation non autorisée.
- **Non répudiation** : c'est l'assurance que l'émetteur d'un message ne puisse pas nier l'avoir envoyé et que le récepteur ne puisse pas nier l'avoir reçu.
- **Contrôle d'accès :** ce service permet de donner aux utilisateurs exactement les droits dont ils ont besoin.
- **privée(Privacy)** : garantir qu'un nœud malveillant ne peut pas avoir des informations sur la vie privé des consommateurs.

Exemple du système AMI (Advanced Metering Infrastructure)

L'intégrité des systèmes AMI

Visant à empêcher tout changement dans les données de mesure reçues se forme des ordres de commande envoyés à des compteurs. L'un des scénarios qui peuvent arriver est quand un pirate envoie une commande de déconnexion en enfreignant dans un système de gestion des compteurs et des millions de compteurs intelligents.

- **La disponibilité**

Est considéré comme l'exigence la plus importante dans certains systèmes AMI depuis ou les applications sont en temps réel et ils traitent peut-être avec la disponibilité de l'énergie.

- **La non-répudiation**

Est également nécessaire puisque les différentes entités impliquées dans les transactions financières, posséder des données et même de générer des commandes de contrôle. Les journaux

d'audit des interactions sont principalement utilisés pour la non-répudiation, bien que ces journaux peuvent être affectés par l'intégrité et attaques de disponibilité. Dans AMI, la disponibilité et l'intégrité des données sont prioritaires sur la confidentialité **[35].**

3.2. Les mécanismes de sécurité

Les mécanismes de sécurité permettant de mettre en œuvre les déférents services de sécurité sont :

3.2.1. Le mécanisme de chiffrement

Le chiffrement inclut le concept de clé, qui est utilisée par un algorithme pour chiffrer ou déchiffrer un message. On distingue trois types de chiffrement :

- **Le chiffrement symétrique :** Le chiffrement symétrique (ou le chiffrement à clé secrète) utilise la même clé pour chiffrer et déchiffrer un message. La valeur de cette clé (unique) doit être un secret partagé uniquement entre l'émetteur et le destinataire. Exemple d'algorithme de chiffrement symétrique : AES (Advanced Encryptions Standard).
- **Exemple d'algorithme de chiffrement symétrique :** RSA (Rivest Shamir Adleman).
- **Le chiffrement asymétrique :** Le chiffrement asymétrique utilise une paire de clés (Publique, Privée) pour chaque nœud de la communication. La clé publique est publiée, elle est utilisée pour crypter les données envoyées vers le nœud. Étant donné que la clé privée est gardée secrète, elle est utilisée pour le déchiffrement.
- **Le chiffrement hybride :** Le chiffrement hybride combine l'usage des chiffrements symétriques et asymétriques. D'abord, le message est chiffré par une clé symétrique. Ensuite, cette clé est cryptée par une clé asymétrique.

3.2.2. La signature électronique

Les signatures électroniques sont utilisées pour identifier les auteurs des données électroniques. Il s'agit d'appliquer une fonction de hachage (MD5, SHA-1) sur le document à signer pour obtenir une empreinte de taille fixe. Une fonction de hachage est un algorithme permettant de calculer une empreinte de taille fixe à partir d'une donnée de taille quelconque.

La signature numérique consiste à chiffrer cette empreinte avec la clé privée et garantie l'authentification de l'émetteur et l'intégrité. **[36].**

3.2.3. Le certificat électronique

Un certificat est en quelque sorte une carte d'identité numérique. Il permet d'associer une clé publique à un nœud. Il garantit que la clé publique, utilisée pour vérifier la signature, est celle de l'entité émettrice **[36].** Les certificats numériques sont délivrés à partir d'une autorité de certification (Certificate Authority, ou CA). Parmi les informations qu'il peut contenir nous pouvons citer :

- Une clé publique
- Le nom du propriétaire de cette clé (le propriétaire peut être une personne, une machine, un logiciel.. etc.
- La durée de validité du certificat. Exemple : le certificat x509**[37].**

3.2.4. **Public Key Infrastructure (PKI)**

L'infrastructure à clés publiques, PKI « Public Key Infrastructure » est constituée de l'ensemble de matériels, logiciels, personnes, règles et procédures nécessaires à une autorité de certification (AC) pour créer, gérer et distribuer des certificats. **[36].** Elle fournit un ensemble de services pour ses utilisateurs, comme : la publication du certificat, le renouvellement d'un certificat, la révocation des certificats compromis, la publication de la liste de révocation de chaque AC.

2.5. Types d'attaques dans les Smart Grid

Parmi les types d'attaques dans les smart grid, nous citons :

- **Les attaques sur l'architecture du Smart Grid**

Le déploiement des technologies de l'information et de la communication sur les réseaux électriques fait peser plus d'inquiétudes sur la sécurité du système électrique et la protection des données de consommation qu'avec les réseaux électriques traditionnels. Dans cette section, nous passons en revue quelques attaques qui peuvent être menées sur les réseaux des Smart Grids. Pour présenter les attaques, il existe dans la littérature différentes façons de les classifier (selon le type d'attaque, structure du réseau, etc.).

Nous avons choisi la classification de qui nous facilite l'identification des attaques du Smart Grid, puisqu'elle s'intéresse aux differents composants du réseau Smart Grid, à savoir : Dispositifs Systèmes et Réseaux

- **Les attaques sur les Dispositifs du réseau Smart Grid**

Les déférents Dispositifs (smart mètre) d'un réseau du Smart Grid peuvent être affectés par plusieurs types d'attaques. Dans cette partie, nous allons présenter ces attaques.

Smart métre[38]

Un nœud malveillant peut perturber le fonctionnement des smart mètre en effectuant plusieurs types d'attaques :

- **L'attaque de brouillage** : peut être lancée pour empêcher le Smart Mètre (compteur intelligent) de communiquer avec les autres nœuds du réseau Smart Grid.
- **L'attaque d'écoute :** peut être effectuée pour détecter des informations sensibles sur la consommation d'énergie du client. De même, cette attaque peut aboutir à une attaque sur la vie privée des consommateurs. En effet, l'attaquant peut récupérer plusieurs informations privées. Par exemple, il peut savoir si la maison est habitée ou pas (pas de consommation d'énergie voulant dire que la maison est vide). Cette information est critique puisqu'elle peut être exploitée par des voleurs.
- **L'attaque false data injection attaque** :(connue sous le nom stealthy attacks **[39]** l'attaquant peut injecter des informations fausses de prix de l'électricité (prix bas d'électricité), ce qui peut augmenter sensiblement les factures des consommateurs. L'application intitulé Rempote Connect Disconnet (RCD) peut être utilisée par les attaquants pour réaliser une attaque de déconnexion à distance du smart Meter privant ainsi le client d'électricité. Encore, les attaquants peuvent utiliser cette application pour connecter un Smart Meter et bénéficier d'une énergie illégale.
- **Attaque de rejeu (Replay attack):** l'attaquant peut utiliser les compteurs intelligents hors usage en injectant des données incorrectes au système ce qui peut conduire à des prix incorrects de l'énergie ou à des prédictions inexactes (prédictions de l'utilisation future de l'énergie).
- **Rui Tan :** ont étudié l'impact de l'attaque de modification sur l'application Real Time Pricing (RTP). Ils ont montré que le RTP risque d'être déstabilisée si l'adversaire peut compromettre les prix annoncés aux compteurs intelligents.
- **Remote Terminal Unit (RTU)** : Les Remote Terminal Unit (RTU) sont traditionnellement utilisées pour configurer et dépanner les périphériques du réseau intelligent à distance. Cette fonctionnalité d'accès distant peut donner lieu à des attaques qui permettent à des nœuds malveillants de prendre le contrôle des dispositifs **[40].**

- **Une attaque de déni de service (Dos) :** sur un dispositif du Smart Grid peut saturer la puissance de calcul du CPU, la mémoire ou la bande passante et se traduira par le retard de l'échange de données en temps réel. En conséquence, les opérateurs de centres de contrôle n'ont pas une vision complète de l'état de la grille de puissance, conduisant à des décisions incorrectes **[41].**

    - **AMI (Advanced Metering Infrastructure)** : l'infrastructure de communication pour les compteurs intelligents. Elle est utilisée pour assurer la communication bidirectionnelle entre les clients et les fournisseurs **[42].** Les canaux de communication utilisés par l'AMI pour communiquer les données entre les compteurs intelligents et les services publics sont également vulnérables aux cybers attaques. Le transit de données par ces canaux peut être intercepté **[43].** Modification de la circulation, fausse injection de données, relecture et les attaques d'analyse de trafic tentent de compromettre le réseau **[45]** alors que le nœud compromis et l'usurpation d'identité des appareils de mesure, la violation d'authentification et d'accès aux clés de chiffrement sont des exemples des attaques qui ciblent les systèmes **[46].** Défauts ou dérives de routage, la configuration, le nom résolution et brouillage du signal sont considérés comme des attaques Dos.

- **L'attaque man in the middle :** peut être éventuellement lancée. Les données de consommation d'énergie peuvent être modifiées avant la transmission des messages. Aussi, en écoutant le canal de communication sans fil, un attaquant pourrait obtenir les informations échangées entre les compteurs intelligents et le centre de contrôle **[47].**

- **Demand Response (DR) :** est un élément essentiel de la gestion automatique de charge et s'appuie sur la capacité de l'infrastructure de communication AMI à envoyer les demandes de réduction de charge pour les compteurs intelligents et autres appareils, pour gérer dynamiquement la charge globale du système.

  Les perturbations des opérations DR peut avoir des effets immédiats sur la résilience opérationnelle du smart grid par la déstabilisation du réseau électrique. Zhuo Lu et al. ont étudié la minimisation du retard des messages pour les applications de réseau intelligent en cas d'attaque de brouillage **[47].**

- **Outage Management System (OMS) :** La gestion automatisée de panne (outage management) nécessite des compteurs intelligents pour envoyer les informations de pannes. L'utilitaire utilise les informations (l'heure, le lieu de la panne . . .) pour rétablir le courant en temps réduit. Une perturbation de cette application affecte directement en retardant la détection et la correction des pannes. La gestion de la panne est résiliente si l'utilitaire peut

toujours identifier et récupérer des pannes dans un délai limité, où le temps est dépendant des exigences septiques des utilitaires **[48].**

Un attaquant peut usurper l'identité d'un Smart Meter et envoyer un message de panne, encore il peut modifier le message envoyé (Message de médication and false data injection attaque) pour influer la résilience de la grille. À plus grande échelle, plusieurs attaquants peuvent usurper l'identité de plusieurs Smart Meter dans la même zone géographique et envoyer des messages presque identiques pour renseigner sur une catastrophe. Le centre de contrôle peut prendre la décision de couper le courant sur cette zone géographique.

- **Les attaques sur les réseaux du Smart Grid**

Les Smart Grids sont connectés et contrôlés par des réseaux de communication **[49].** Nous avons choisi de classifier les attaques qui peuvent être menées sur les réseaux, en deux catégories. Les attaques sur les protocoles de routages utilisés et Attaques sur les protocoles de communication utilisés.

- **Les attaques sur les protocoles de routage**

Parmi les protocoles de routage qui peuvent être utilisés dans les réseaux NAN on cite **[50]:** Le protocole de routage des réseaux de faible puissance et avec perte défini dans la RFC6553 par l'IETF (Internet Engineering Task Force). Il a été conçu afin de prendre en charge les exigences spécifiques de ces réseaux. Le RPL est un protocole de routage proactif à vecteur de distance qui construit un DODAG (Destination Oriented Directed Acyclic Graph). Le DODAG construit permet à chaque nœud de transmettre les données qu'il a récolté jusqu'au DODAGroot (racine).

Chaque nœud dans le DODAG sélectionne un parent selon une métrique de routage donnée et une fonction objective. Les données récoltées sont acheminées d'enfant à parent jusqu'à la racine.

- **Le protocole de routage RPL pour IoT (Internet of Things)**

Peut être affecté par les attaques de transfert sélectif (Sélective Forwarding Attacks) : les nœuds malicieux essaient d'arrêter les paquets dans le réseau en refusant de transférer ou de supprimer les messages qui les traverse. Avec ces attaques, il est possible de lancer des attaques Dos où les nœuds malicieux transmettent sélectivement des paquets. Cette attaque est

principalement destinée à perturber les chemins de routage. Par exemple, un attaquant pourrait transférer tous les messages de contrôle RPL et laisser tomber le reste du trafic .

Cette attaque a des conséquences plus sévères lorsqu'il est couplé avec d'autres attaques, par exemple, l'attaque sinkhole (un attaquant tente de se faire passer pour un faux puits en se montrant trés attractif aux nœuds avoisinants puis crée une topologie erronée du réseau.)**[51].** Le protocole de Transmission de Minimum énergétique (MTE) reprend le protocole DSR (Dynamic Source Routing) de base (sans les caches) et assignent à chacun des liens un poids qui est fonction de l'énergie nécessaire pour transmettre un paquet sur cette voie. Le routage se fait suivant les routes de plus faible poids, en aggrégant l'ensemble des liaisons constitutif d'un chemin **[52].**

- **Les attaques du réseau de capteurs sans fil**

  Sont applicables au protocole de routage MTE (Dos,....) **[53].**

- **Les attaques sur les protocoles de communication**

Les travaux **[54]** ont montré que les protocoles de communication utilisés au sein d'un Smart Grid sont également une source importante de vulnérabilités. Certains protocoles (zigbee, wimax . . .) peuvent être affectés par les attaques : DOS, écoute, modification, brouillage. Dans cette partie, nous allons étudier la sécurité des protocoles ZigBee, C37.118, DNP3

- ✓ **ZigBee**

ZigBee à un inconvénient majeur, tous les mots de passe sont stockés en clair dans l'espace de stockage. Si l'attaquant obtient un accès physique à l'appareil, il peut copier la mémoire de l'appareil dans l'ordinateur, puis il peut trouver la clé . Le Zigbee peut aussi être affecté par les attaques de type DoS. **[56].**

- ✓ **Protocole C37.118 (Synchrophasor Protocol)**

Est une norme de l'IEEE pour l'utilisation des synchrophasors dans les systèmes d'alimentation **[57].** Le protocole C37.118 ne crypte pas les messages échangés entre le PDC et PMU.

Un attaquant peut effectuer une attaque d'écoute. Encore, il est vulnérable aux attaques de type man in the middle, car il ne vérifie pas la source des messages qu'il reçoit du PMU **[58].**

DNP3

DNP3 (Distributed Network Protocol) est un protocole de communication largement utilisé par les services publics d'électricité. Il utilise iperf (un générateur de trafic réseau) pour occuper le canal de communication, ce qui réduit la disponibilité du réseau. ont montré que les paquets DNP3 longs sont plus vulnérables aux attaques DoS que les paquets DNP3 courts **[60]**.

Le protocole DNP3 est un protocole documenté, il peut être sujet du reverse engineering **[61].**

3. Systèmes de détection d'intrusions

Les IDS s'appuient généralement sur deux sources d'information : les paquets transitant sur le réseau et les informations collectées sur les machines (les fichiers d'audit, ….).

On parle alors de deux types de systèmes de détection d'intrusions : les IDS basés réseau et les IDS basés hôte .Ces deux catégories d'IDS emploient généralement deux principes de détection : l'approche comportementale et l'approche par scénario. La détection par scénario définit des signatures d'attaques qui décrivent les intrusions. Ces signatures ne sont autres que les empreintes laissées par les intrus au cours de leurs exploits.

La deuxième approche de détection (comportementale) se réfère au comportement normal et habituel des différents acteurs du système a protéger (application, utilisateur, etc.). Ensuite une déviation importante par rapport au normal représente une activité suspecte et révèle éventuellement une attaque. Nous détaillons les différentes approches de détection ainsi que leurs limites dans le chapitre 3.

Conclusion

Les techniques de protection contre les attaques permettent de réaliser les bases de la sécurité : confidentialité, intégrité, authentification, disponibilité. Mais malgré toutes ces techniques utilisées pour empêcher les attaques, les attaquants suivent une stratégie d'attaque pour réussir leurs exploits. Ils disposent de plusieurs sources d'information et de divers outils pour compromettre le système informatique. Par conséquent, les administrateurs déploient des solutions de sécurité plus efficaces capables de protéger le réseau de l'entreprise. Dans ce contexte, les systèmes de détection d'intrusions constituent une bonne alternative pour mieux sécuriser le réseau informatique dans le smart grid.

Nous détaillons dans le chapitre 3 les systèmes de détection d'intrusions.

Chapitre 3

Système de détection d'intrusion IDS

1. Introduction

Les systèmes et réseaux informatiques contiennent diverses formes de vulnérabilité. Pour faire face à ces problèmes de sécurité, un nouveau concept appelé système de détection d'intrusion a été introduit comme une seconde ligne de défense afin de renforcer la sécurité des systèmes informatiques.

Dans ce chapitre nous allons élaborer ce concept de détection, afin de l'introduire dans les smarts grids, présentant les différents challenges de sécurité dans ce domaine, et les travaux connexe pour obtenir à la fin une classification selon les attaques.

2. systèmes de détection d'intrusions

2.1. Définition

Un système de détection d'intrusion(ou IDS) est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte), afin de remédier aux problèmes dans les plus brefs délais **[61].**

Il permet ainsi d'avoir une connaissance sur les tentatives réussies comme échouées des intrusions. Vu leur utilité pratique, les IDS ont été étudiés massivement durant les 20 dernières années dans le but d'améliorer leur efficacité .Les fruits de ces études sont des différentes classes d'IDS qui se basent sur différentes techniques de détection dont chacune est mieux appropriée pour un contexte bien particulier. Entre autres, nous trouvons les systèmes de détection d'intrusions qui basent leurs décisions sur des informations trouvées dans des machines hôtes et appelés HIDS et les systèmes de détections d'intrusions qui fondent leurs décisions uniquement sur des informations qui circulent dans un réseau et sont appelés NIDS.

4 . Architecture des IDS :

Un IDS est essentiellement constitué d'un sniffer couplé avec un moteur qui analyse le trafic et entreprend des actions suivantes les règles définies dans l'IDS. Ces règles décrivent le comportement de l'IDS selon le trafic analysé trafic : Alertes, journalisation des événements dans des fichiers logs.

Le schéma suivant illustre le fonctionnement d'un IDS :

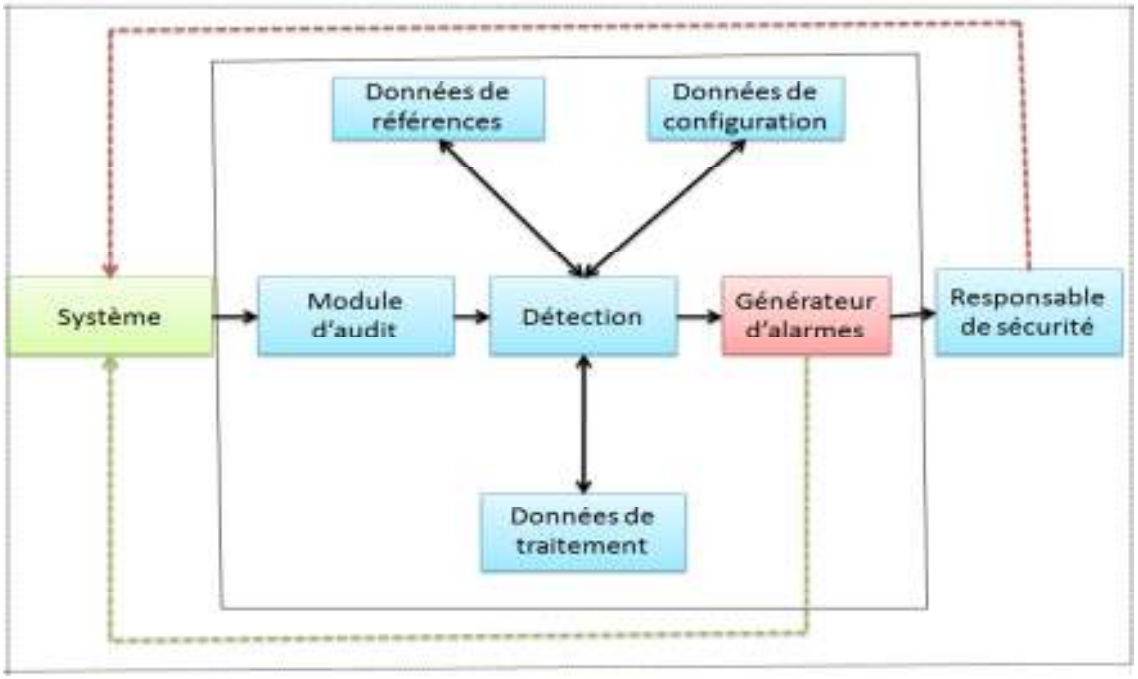

Figure 3.1: architecture type en module d'un IDS. [62]

Un IDS peut analyser les couches suivantes :

- Couche réseau (IP, ICMP)
- Couche transport (TCP, UDP)
- Couche application (http, Telnet)

Selon le type de trafic, l'IDS accomplit certaines actions définies dans les règles. Certains termes sont souvent employés quand on parle d'IDS :

Faux positif : une alerte provenant d'un IDS mais qui ne correspond pas à une attaque réelle (fausse alerte).

Faux négatif : une intrusion réelle qui n'a pas été détectée par IDS.

Le schéma suivant illustre les caractéristiques d'un IDS :

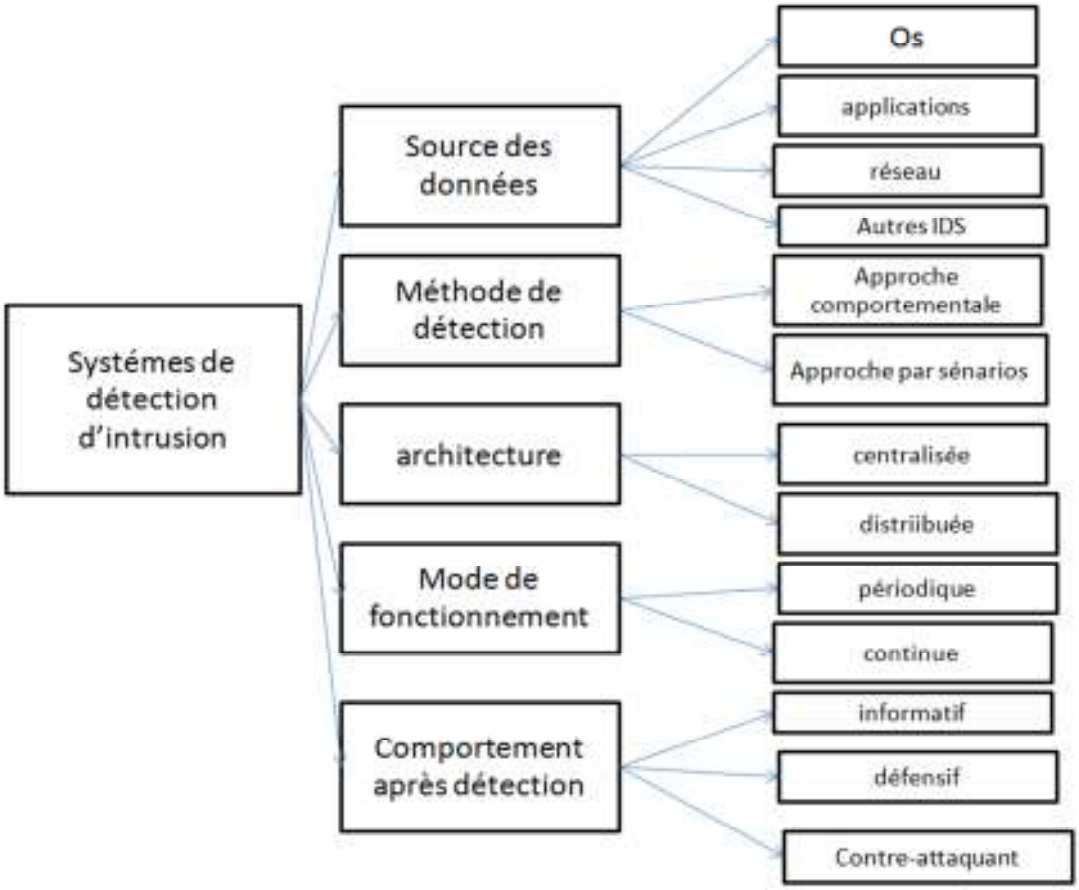

Figure3.2 : Caractéristiques et Fonctionnement des IDS.

5. Classification des IDS

5.1 Classification selon l'emplacement d'IDS

Les pirates utilisent dans leurs attaques des failles réseaux ou bien des failles de programmation, donc et par conséquent il existe plusieurs types d'IDS **[63]**

A. systèmes de détection d'intrusions de type hôte (HIDS)

Ces systèmes sont en fait les premiers systèmes mis en œuvre pour la détection d'intrusion. Ils sont installés sur une machine hôte pour la protéger. Thierry Evangelista a dit dans son livre « les IDS », « un HID est un agent logiciel que l'on installe généralement sur la machine à protéger et qui analyse en temps réel les flux relatifs à cette machine ainsi que les journaux » **[64]**

Un HIDS est chargé d'analyser :

- Les activités d'une machine (liste des processus exécutés, ressources utilisées…etc.)
- Les activités des utilisateurs des machines (durée de connexion, programmes utilisés…etc)
- les activités anormales d'un ver, virus ou bien cheval de trois.
- Le noyau du système en utilisant l'analyse protocolaire.
- La table d'adressage des interruptions.

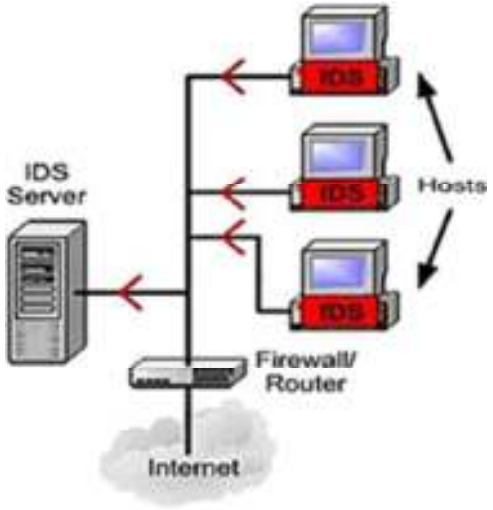

Figure 3. 3 : exemples de NIDS.

Ces systèmes sont avantageux lorsque le trafic réseau est chiffré et offre plus de précision dans la surveillance de l'activité sur l'hôte.

Par contre, ils sont moins performants contre les attaques de déni de service et les scans, le déni de service se produit quand le serveur est submergé par des requetés et qu'il n'arrive pas à répondre. Les scans sont de simples requêtes qui permettent à l'attaquant de savoir quels sont les ports ouverts sur une machine et ainsi déduire les services disponibles.

Inconvénients

Les scans sont détectés avec moins de facilité ; ils sont plus vulnérables aux attaques de types Dos ; l'analyse des traces d'audit du système est très contraignante en raison de la taille de ces derniers ; ils consomment beaucoup de ressources CPU, etc.

b. systèmes de détection des intrusions réseaux(NIDS)

Ces systèmes sont mis en œuvre pour la protection des réseaux. Ils se basent sur le principe de l'analyse du trafic réseau, Ils sont composés de sondes (capteurs) qui surveillent les données acheminées dans le réseau et d'un moteur pour analyser les données **[64]** l'architecture du réseau et la politique de sécurité permettent de définir l'emplacement des sondes.

Les NIDS sont efficaces contre les scans, mais ils sont confrontés au problème des réseaux cryptés.

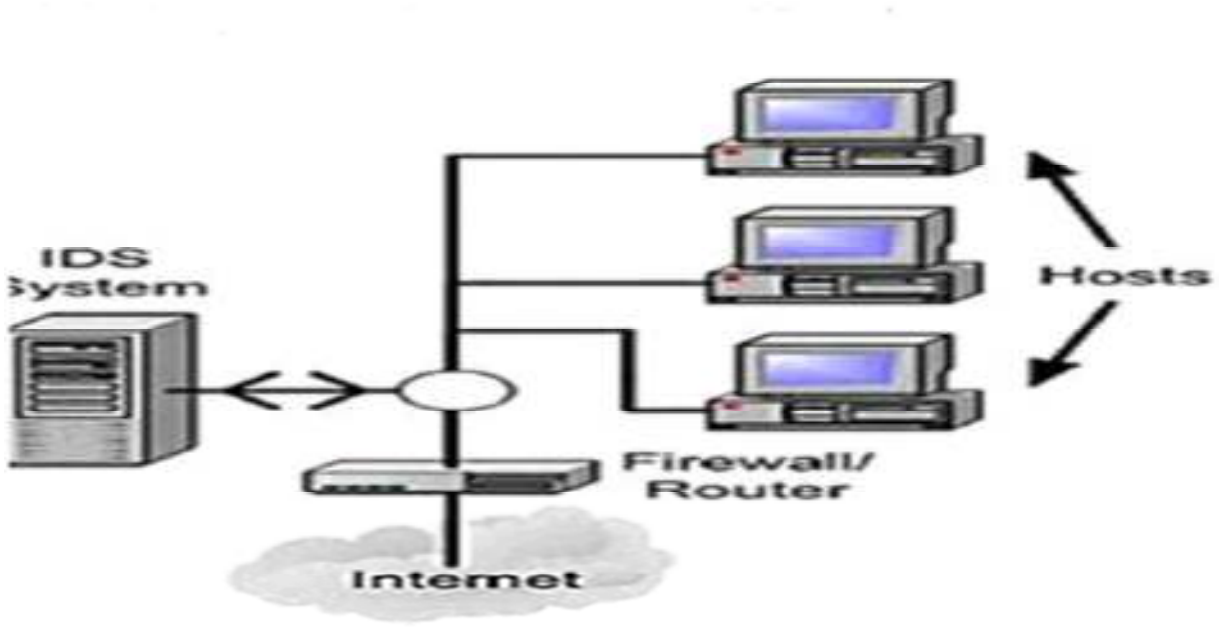

Figure 3.4 : exemples de HIDS.

Un NIDS se découpe en trois grandes parties b : la capture, les signatures et les alertes

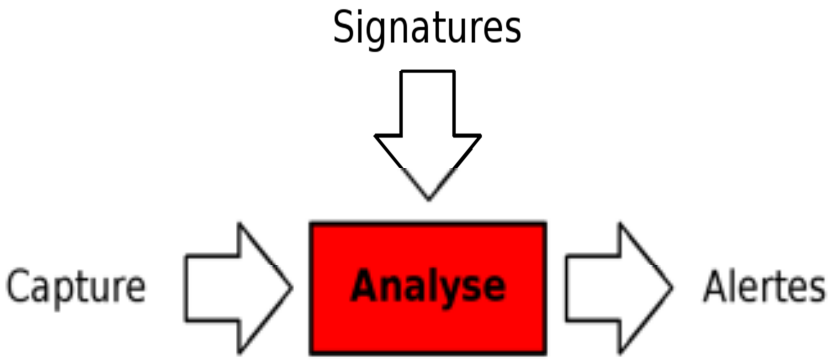

Figure 3.5 : Les étapes initiales d'une détection par un NIDS

Les IDS hybrides sont basés sur une architecture distribuée, où chaque composant unifie son format d'envoi d'alert (typiquement IDMEF) permettant à des composants divers de communiquer d'extraire des alertes plus pertinentes.

Les avantages des IDS hybrides sont multiples

- Moins de faux positifs
- Meilleure corrélation
- Possibilité de réaction sur les analyseurs

La corrélation

La corrélation est une connexion entre deux ou plusieurs éléments, dont un de ces éléments crée ou influence un autre. Elle se traduit plus généralement par la transformation d'une ou plusieurs alertes en attaque. Cela permet de faciliter la compréhension sur les attaques au lieu de s'éparpiller parmi les alertes.

Idéalement elle nécessite un IDS hybride car plus il y a d'informations hétérogènes sur un événement, plus la corrélation se fait d'une façon pertinente. Les formats ayant été normalisent (IDMEF), il ne reste plus qu'à faire des associations afin de détecter des alertes qui n' auraient jamais eu lieu sur un analyseur seul.

Si l'on prend l'exemple d'une authentification échouée, cela génère une alerte de faible intensité. Mais s'il y a une série d'authentifications échouées avec des utilisateurs différents, on peut conclure à une attaque de force brute .La corrélation permet de générer de nouvelles alertes de celles existantes. C'est une étape préalable à une contre- mesure efficace.

Il y a diverses façons de faire de la corrélation.

La corrélation permet de générer de nouvelles alertes a partir de celles existantes c'est une étape préalable a une contre –mesure efficace.Il y a diverses facons de faire de la corrélation. Cependant on peut définir deux catégories :

La corrélation passive,correspondant a une génération d'alerte basée .La corrélation active, qui va chercher les informations correspondant a des alertes émises.par exemple, lorsqu'une personne se connecte en dehors des heures de travail, cel a un impact élevé qui n'aurait pas été en temps normal d'activité. Le format IDMEF(Intrusion Detection Message Exchange Format) décrit une alerte de facon objet et exhaustive.Une alerte est le message qui est émis depuis un analyseur,qui est une sonde en langage IDMEF, vers un collecteur le but d'IDMEFest de proposer

un standard permettent d'avoir une communication homogéne quel que soit l'environnement ou les capacités d'un analyseur donné .

Ces alertes sont définies au format XML, offrant possibilité de validation de chaque message .En général, les implémentations restent binaires, afin d'éviter les problémes connus d'ajout d'information inutiles en dehors d'XML lorsque l'on envoie un message sur le réseau.

IDMEF offre aussi un vocabulaire précis , qu'il est courant d'utiliser dans le domaine de la détection d'intrusion.par exemple, une classification correspond au nom d'une alerte ;un impact celui d'un niveau d'attaque

6. Classification selon la méthode de détection

LesIDS fonctionnent suivant deux approches :

6.1.Approche par scénario ou par signature (knowledge based detection)

Elle ressemble beaucoup aux techniques utilisées par les antivirus.Elle est basée sur la notion de signatures d'attaques.La signature d'une attaque représente les caractérisatiques de cette attaque.La technique consiste donc, a analyser les flux de données en les comparants aux signatures pour identifier d'éventuelles intrusions.

Il existe plusieures mécénismes pour mettre en œuvre cette approche.

Voici trois d'entre eux :

(a)Analyse par comparaison (pattern matching)

Le principe de cette approche est de faire correspondre a chaque signature d'attaque un motif (patten)qui est sous forme d'une chaine de caractéres.Durant l'analyse du flux de données qui est aussi une chaine de caractéres, le systéme de détection d'intrusion tente de reconnaitre les motifs d'attaques déjà connus **[64].**

(b) systéme expert

Technique qui repose sur une base de connaissances et un moteur d'inférence.La base de connaissances est composée elle-méme d'une base de régles décrivant les attaques et d'une base de faits contenant les événements relatifs aux attaques .Durant la phase de déction, le moteur d'inférence est capable de détecter les attaques en en utilisant la base des connaissances.

Cette technique consiste a détecter les attaques des systémes d'exploitations et non pas les attaques réseaux, elle consiste à sauvegarder les résultats des instructions si elle existe dans la base des signatures afin de modéliser une attaque.

Cette approche ne peut détecter que les attaques connues précédemment et qui déroulent selon la méme signature adaptée à la base, par exemple si un attaquant change l'ordre des instructions de son attaque, l'IDS trouve une difficulté pour le détecter. Pour cela, il est nécessaire de mettre à jour la base des signatures d'une facon réguliére.

(c)Analyse de transition d'états

Dans cette approche on représente les attaques sous forme d'un ensemble d'états par les quels passe le systéme. Les transactions représentent les actions suivant les événements qui surviennent.

Le plus grand inconvénient de l'approche par scenario réside dans le fait qu'elle ne détecte que les attaques connues.Elle est impuissante devant de nouvelles attaques **[65]**

6. 2.Approche comportementale (anomaly detection)

On l'appelle aussi détection d'anomalie, elle cosiste a récupérer des paramétres relatifs à l'utilisateur puis les comparer avec un comportement habituel et normal de méme utilisateur **[65]**.

En effet, dans un premier temps, on fait correspondre un profil à chaque entité en se basant sur son comportement normal dans un dexiéme temps , pendant la phase de détection, on observe l'entité modélisée et tous les événements qui ne sont pas représentés dans le profil, déclenchent des alertes d'attaques.

Pour faire correspondre un profil a chaque entité on a besoins de politique de sécurité et d'une phase d'apprentissage.Initialement les profils ne corresponent qu'a la politique de sécurité.Durant la phase d'apprentissaqe, les profils sont améliorés en définissant le comportement normal de chaque entité.Cette phase d'apprentissage peut étre limitée dans le temps ou bien continue tout au long de l'exploitation.La mise en œuvre effective de la détection d'anomalies dépend beaucoup de l'approche utilisée pour construire les profils.

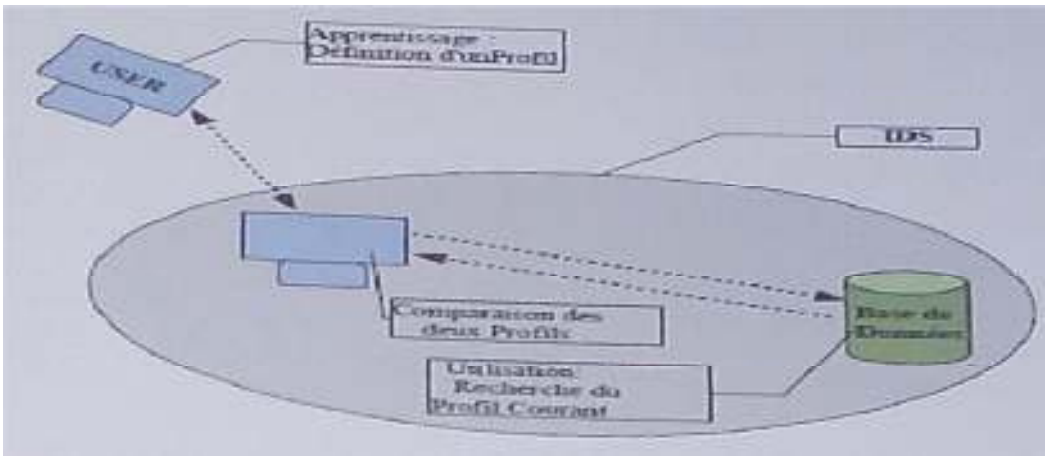

Figure 3.6 : Illustration de l'approche comportementale.[66]

Nous présentons ici les trois approches les plus populaires

(a)Approche probabiliste

Dans cette approche la constuction des profils se base sur la probabilité qu'un événement ait lieu par rapport à une séquence d'autres événements.

(b)Approche statistique (modèle de DENNING)

Ici la construction des profils se base sur mesures quantitives de l'utilisation des ressources systémes.

(C)Approche par réseau de neurones

Cette approche se base sur le comportement de chaque utilisateur. Le profil d'un utilisateur est construit en prenant en compte les activités de l'utilisateur comme les outils préférés, les habitudes de travail, la vitesse de frappe au clavier, etc. Le profil est ensuite représenté par un réseau de neurones qui enregistre les opérations de l'utilisateur durant une fenêtre temporelle et il tente de prédire la prochaine opération.**[64].**

En utilisant l'approche comportementale, la détection d'intrusions puise sa force dans l'habilité à détecter des attaques inconnues. Quelle que soit l'approche utilisée, les IDS peuvent déclencher une alerte en l'absence d'attaque (faux positif) ou encore pas d'alerte en présence d'attaque (faux négatif).

(d) comparaison entre l'approche par scénario et l'approche comportementale :

- Voici un tableau comparatif entre l&approche comportementale et par scénario :

Scénarios	Comportements
Spécification complexe	Taille des automates générés
Pas de faux positifs	Phase critique d'entrainement.
Aucune prise en compte des nouvelles attaques	Prise en compte des nouvelles attaques.
mise à jour rapide	Mise à jour délicate (phase d'entrainement).
Protection facile a contourner	Faux positifs nombreux
Prise en compte incomplète des environnements parallèles	

Tableau3.1 : comparaison entre l'approche par scénario et l'approche comportementale.

8. Classification selon le comportement de détection

On distingue deux types d'IDS actifs et passifs : **[67]**

- **Les IDS actifs**

Ce types d'IDS a des réactions selon l'attaque détectée, en cas d'une attaque faible, l'IDS fournit des messages d'alertes à l'administrateur du système ou une personne chargée de la sécurité du système. Dans le cas d'une intrusion dangereuse I'IDS doit réagir des actions contre cette intrusion telles que :

- La modification de la table de routage du routeur lié au système.
- Refus ou l'arrête d'une connexion.
- L'arrêt d'un processus.

- Demande au pare feu de modifier ses règles …etc.

- **Les IDS passifs**

Ce type ne peut pas réagir contre les attaques, il consiste à analyser le système, les signatures s'ils existent ainsi que l'échange des messages d'aletes.

9 . Classification selon la fréquence d'utilisation

Pour cela on distingue deux types : online et offline :

- **IDS online (continue)**

Ce sont des IDS qui font l'analyse d'une façon continue ou permanence afin de détecter une attaque au moment de sa Production, c'est une détection en temps réel.

Ce type d'IDS consomme un taux élevé de ressources systèmes ce qu'il le rend non préférable en cas de ressources précieuses telle que les serveurs de messagerie.

- **IDS offline (périodique)**

Ce type d'IDS fait l'analyse dans une durée périodique (généralement en fin de journée) afin de détecter des traces d'attaques au but de modéliser des signatures d'attaques pour la base du système, l'avantage de ce type est qu'il ne consomme pas beaucoup de ressources système.

L'inconvénient majeur de ce type est qu'il détecte les attaques en retard ce qu'il peut provoquer des dégâts dangereux.

10 . Sources de données

Pour surveiller l'infrastructure informatique le système de détection d'intrusions comptent sur une ou plusieurs sources de données qui fournissent l'information à analyser. Une ou plusieurs sources de données qui fournit un rapport sur les activités qui se sont produites dans le système à surveiller.

C'est un flux de données acquis par le système de décision d'intrusion et analysé pour déterminer si des événements anormaux par rapport à l'algorithme d'analyse se produisent dans ces données. Cependant ce flux de données peut provenir de plusieurs points d'un système informatique et la détection d'intrusion considère trois sources importantes **[64].**

(A)Le trafic réseau :

Le trafic réseau constitue la source de données pour les sondes NIDS. Ces sondes placées sur le réseau en monde promiscuité captent et analysent les données, passant à travers le réseau pour détecter d'éventuelles attaques .Les avantages quant à l'utilisation de cette source de données sont multiples .La promiscuité de la sonde constitue un atout majeur, elle empêche sa détection et annule son impact sur le système surveille. Une sonde NIDS surveille une portion d'un réseau, elle offre donc la possibilité de détecter des attaques combinées les données utilisées sont dans un format standard et donc plus accessibles. Il est aussi à noter que les sondes NIDS sont simples à installer et à utiliser.

Toutefois, cette technique basée sur les échanges réseaux se retrouve impuissante devant des attaques qui n'impliquent pas un trafic réseau. Il faut aussi noter que le débit des réseaux, de nos jours, éméché le traitement exhaustif des données.

(B)Les données systèmes

Elles représentent les fichiers d'audits produits pas les systèmes d'exploitation où sont installées les sondes HIDS. La force de cette technique réside dans la fiabilité et la richesse des données. En effet, les fichiers d'audits reflètent ce qui' s'est réellement passé sur une machine.la faiblesse pas contre de cette technique réside dans :

- Les volumes important des données à traiter.
- Les faits d'être limitée à la surveillance d'une seule machine.

(C)L'audit applicatif :

Au lieu de traiter toutes les interactions qui se produisent sur une machine, l'audit applicatif favorise le ciblage de certaines applications (serveur web, Ftp etc.).Cette technique présente l'avantage de traiter des données spécifiques avec un volume réduit. Toutefois, les applications en question doivent être configurées pour produire des fichiers d'audit.

11. Challenges de sécurité dans le smart grid [68]

Il est clair que les smart grid amélioreront sensiblement le contrôle de la consommation d'électricité et de la distribution au profit des consommateurs, des fournisseurs de l'électricité et des opérateurs de grille. Néanmoins, les opérations et les services améliorés viendront au coût d'exposer le réseau entier de l'électricité à de nouveaux défis, en particulier dans le domaine de la sécurité des réseaux de transmission et des systèmes d'information.

- **Exigences de sécurité de données et d'information**

Les circulations de l'information inonderont tous les domaines. Dans les aspects opérationnels de l'intégrité des données et de la disponibilité de grille (automation c.-à-d. de production, de transmission et de distribution) est d'importance primordiale. De même, quand on traite des données connexes par consommateur, telles que des données de consommation ou même des données personnelles aux systèmes de facturation, la confidentialité devra être garantie pendant le passage et le stockage.

D'ailleurs, dans certains cas l'application smart grid déterminera quelle dimension de sécurité est plus importante pour un même morceau de données. Par exemple, dans des applications qui exige une réponse, des lectures de consommation Smart Meter ont pu être employées d'une façon agrégée pour des flux de puissance. Dans ce cas, la disponibilité et l'intégrité est absolument nécessaire pour garantir que le système de contrôle de surveillance prend les décisions appropriées.

Les conditions de protection des données pour chaque domaine et application du smart grid devront être bien définies de sorte que les fabricants, les opérateurs et d'autres acteurs participant au développement et à l'exécution du smart grid puissent établir les contrôles de sécurité nécessaires aussi bien que développent les technologies appropriées données pour protéger des smart grid . Le chiffrage de flux de données, le perçage d'un tunnel, l'authentification et aucun reniement, certificat numérique et également d'autres matières telles que la sécurité dans la chaîne d'approvisionnements, la validation de progiciels ou la gestion de pièce rapportée ne devraient être adressés.

- **Un grand nombre de dispositifs « intelligents »**

La smart grid aura comme conséquence le déploiement d'un nombre important de dispositifs électroniques et de traitement de l'information configurant une maille énorme. Les mètres et les dispositifs intelligents et l'infrastructure de communication de l'AMI est en général probablement l'exemple le plus significatif. Cependant, l'automation de sous-station dans le domaine de distribution ainsi que smartening des centres de transformateur apportera également un nombre important d'IED et de technologies relatives des TCI. Non seulement le déploiement mais également concevoir et maintenir une solution extensible et fiable seront un grand défi pour les opérateurs de grille qui ne sont pas employés. En cas d'attaques, ces solutions/infrastructure doivent être bloquées considérant toutes les interconnexions en place, des processus (par exemple les mises à jour de progiciels, actions de gestion, etc.), ou même les dispositifs eux-mêmes. Ceci ajoutera beaucoup de complexité à l'issue. Probablement, le système ou le logiciel comme service, le calcul de nuage, et les stratégies détaillées de sécurité devraient être considérés, particulièrement dans la situation des opérateurs de petite ou moyenne taille.

- **sécurité physique**

les périmètre de grille : L'attention particulière devra être prêtée aux aspects de sécurité physique dans des smart grid . L'interconnexion au niveau des TCI des ménages, des bâtiments et de l'industrie avec des réseaux de l'information de DSO et de DER prolongera de manière significative le périmètre de sécurité de grille.

Le protocole de communication protégée

Beaucoup des protocoles de transmission actuellement en service pour la commande et l'automation de la production d'électricité, de transmission et de distribution n'ont été jamais conçues avec la sécurité à l'esprit. Plusieurs de ces protocoles ont été au commencement conçus en tant que protocoles périodiques sans l'authentification de message intégrée. Pour cette raison les dispositifs accepteront des raccordements de n'importe quel dispositif essayant de communiquer avec eux étourdis, ils sont autorisés ou pas. En outre, aucun de ces protocoles n'emploie le chiffrage ou des mécanismes d'intégrité de message et en conséquence des communications sont exposées à l'écoute clandestine et la manipulation de session.

Quoique ces vulnérabilités aient été autour pendant des années, les nouveaux facteurs ont augmenté le vrai risque. Beaucoup de fournisseurs d'ICS ont commencé à ouvrir leurs protocoles de propriété industrielle et à éditer leurs caractéristiques de protocole pour permettre à de tiers fabricants de construire les accessoires compatibles. Les organismes transit également des systèmes de propriété industrielle aux protocoles de gestion de réseau communs tels que TCP/IP (c.-à-d. Modbus/TCP, CEI 104, etc.) ou aux protocoles ouverts de nouvelle norme tels que l'OPC pour réduire des coûts et pour améliorer l'exécution. De même, des protocoles de transmission standard de legs tels que le CEI 101 peuvent maintenant être trouvés dans sa version encapsulée par TCP/IP, mais toujours sans le mécanisme de sécurité en place. Les opérateurs devront pouvoir traiter ces derniers points faibles dans les années à venir, définissant des stratégies originales telles que se servir des mesures compensatoires telles que le perçage d'un tunnel de protocole.

D'une part un ensemble totalement nouvel de protocoles de transmission émerge afin de faire face à de nouvelles applications dans des grilles futées. C'est le cas des protocoles connexes tels que la PERFECTION, le DLMS/COSEM, etc. Heureusement, ces protocoles sont conçus avec des principes de sécurité à l'esprit, y compris la cryptographie pour l'authentification et le chiffrage de bout en bout. Néanmoins, pour mettre en application avec succès la sécurité la plus élevée, le matériel cryptographique (c.-à-d. clefs, certificats, etc.) doit être parvenu décisif et efficace. Car on lui a déjà énoncé avant que le nombre de dispositifs intelligents dans des grilles futées soit vraiment haut et donc, le matériel cryptographique de gestion sera une tâche complexe et dure. [65]

- **le Grand nombre des dépositaires et des synergies avec d'autres utilités**

L'infrastructure futée de grille est complexe, et par sa définition même, elle doit d'un grand nombre de dépositaires divers collaborer ensemble afin de fournir la structure physique et logique pour une solution de fonctionnement. Traditionnellement, le système d'alimentation a été composé d'un nombre restreint d'acteurs (c.-à-d. générateurs en bloc, TSOs, et DSOs).

Cependant, en raison de la déréglementation du service de l'électricité, suivie de la redéfinition du concept de système d'alimentation au moyen de la grille futée, nous sommes venus à une situation où un grand nombre de dépositaires sont maintenant consacrés à la distribution d'énergie et aux services connexes de valeur ajoutée. Il y a différents types de dépositaires, mais ce qui est plus important, qu'il y a beaucoup plus d'acteurs impliqués : les consommateurs finaux, petits producteurs de puissance, détaillants d'énergie, les prestataires de service avancés d'énergie,.. etc. La difficulté se situe en coordonnant rapidement les activités d'un groupe si divers de dépositaires, chacun avec ses propres processus d'organisation, priorités d'affaires, conditions de communication de l'information, met en référence des normes de normalisation et des pratiques, etc. pour fournir un service fiable, bloqué, et de haute qualité de la fourniture de courant.

On rencontre souvent le concept de mesure avancé affectera non seulement l'énergie de secteur, mais on envisage que dans les années prochaines d'autres utilités telles que le gaz/chauffage et l'eau se serviront de ces mesure intelligents à distance pour lire et traiter des données de consommation. Les synergies sont possibles et nécessaires puisque d'un point de vue d'affaires il ne semblerait pas beaucoup raisonnable de déployer autant d'AMIs que les services on besoin pour atteignent leur besoins. Par exemple, un AMI simple pourrait être employé pour lire n'importe quel type futé (par exemple gaz, chauffage, eau, électricité), des données seraient alors fournies aux systèmes d'en arrière-bureau de l'opérateur de l'AMI (par exemple DSO, du détaillant d'énergie, du distributeur de gaz, etc.). Par conséquent, il semble nécessaire de développer une infrastructure flexible, interopérable et bien communiquée qui peut soutenir tout le partage d'informations requis entre différentes utilités. Cependant, ceci aura comme conséquence un système bien plus complexe des systèmes, où non seulement tous les nouveaux dépositaires de grille de puissance mais également d'autres acteurs d'utilités devront être considérés quand fixant la smart grid. [65]

- **Manque de définition du concept smart grid et de ses exigences de sécurité**

Un grand nombre de technologies et de concepts très originaux émergent avec les grilles futées. Elles apparaissent d'un seul trait quoique l'image finale quelles grilles futées sont ne soit pas bien définie encore. En conséquence, des exigences de sécurité doivent toujours être définies, prenant en compte les différents domaines impliqués et leur importance pour la sécurité nationale ou l'intimité de données personnelle de citoyens'. Il est donc nécessaire de créer une architecture de référence établissant les aspects de base des grilles futées. En outre, la définition des méthodologies d'évaluation des risques aussi bien que de l'interopérabilité des pratiques de sécurité et du système d'adressage de normes et considérer la sécurité comme aspect fondamental est également nécessaire. [65]

- **Manque de conscience parmi les dépositaires de smart grid**

Plusieurs des défis précédents ne peuvent pas être résolus sans vrai engagement des fabricants et des opérateurs de grille et d'autres dépositaires. En fait, un des défis principaux dans le domaine des infrastructures critiques est de faire le C-niveau fournir averti de personnel des problèmes de sécurité de cyber qu'elles feront face dans les courts et longs termes. C'est particulièrement vrai dans le cas des grilles futées, où les TCI joueront un rôle principal. Par conséquent, les initiatives de sensibilisation sont nécessaires. Demandant la conformité aux normes

spécifiques de sécurité, les analyses de risques de conduite, faisant des essais de pénétration, et favorisant des événements professionnels ou activement impliquant CSIRTs /CERTs sont quelques exemples des initiatives possibles qui pourraient aider à ce but.[65]

- **Sécurité dans la chaîne d'approvisionnements**

Une des matières de discussion courante qu'on parle de la sécurité de CI( ) est comme les chaînes d'approvisionnements courantes peuvent être vulnérables. En fait, le risque que la chaîne d'approvisionnements pour les composants électroniques dite les technologies des TCI, y compris des puces, a inclus le logiciel, les applications de SCADA et de commande, les logiciels d'exploitation, etc. pourrait être infiltré à un certain moment par les agents hostiles est très vrai. Ces agents hostiles ont pu changer les circuits des composants électroniques ou des composants contrefaits de remplacement avec les circuits changés. D'ailleurs, les backdoors et les bombes logiques et tout autre logiciel malveillant ont pu être inclus en tant qu'élément des progiciels de beaucoup d'IED, de contrôleurs, ou de mètres intelligents. En conséquence les états ennemis, ou les terroristes, ou n'importe quelle autre menace pourraient se servir d'un backdoor pour arriver à télécommander des systèmes d'information affectés ou tirer profit des bombes logiques préinstallé qui pourraient causer le mal terrible.

La sécurité de la chaîne d'approvisionnements est d'importance primordiale pour la protection futée de grilles. Cela vaut particulièrement pour ces applications et composants qui pourraient être appropriés pour la sécurité nationale. La conception, la fabrication, l'ensemble, et la distribution des composants électroniques et des applications devront être commandés et ont convenablement réglé. Il est important d'avoir à l'esprit la dimension économique du problème et d'établir les objectifs de sécurité qui sont économiquement viables. La clef à résoudre le problème des progiciels malveillants est de rendre la chaîne d'approvisionnements globale entière plus bloquée. [65]

- **processus de gestion de sécurité dans les utilités**

Les fournisseurs de système joueront un rôle très approprié en fixant les grilles futées. Si les produits sont intégrés sans fonctionnalité de sécurité ou ne pas considérer des exigences de sécurité pendant le cycle de développement, la protection de la grille de puissance serait une tâche très difficile. Cependant, la sécurité des grilles de puissance dépend non seulement d'avoir les produits bloqués. C'est un processus continu qui comptera fortement dans des entreprises d'électricité telles que DSO s et TSO s, mais Les opérateurs de grille doivent aussi évaluer le degré de sécurité de leurs systèmes actuels, particulièrement d'ICS et de nouveaux déploiements d'infrastructure. En outre, ils doivent évaluer et prévoir de nouveaux investissements pour améliorer le maintien de sécurité, pour définir des politiques de sécurité et pour établir des procédures, employés de train, et enfin et surtout, établir un cadre de gestion de sécurité de l'information qui s'assure que tous ces objectifs obtiennent faits et sans interruption améliorés.

Travaux connexes

[Yang et autres 2005] étudier une identification pour des applications de service futées (de puissance)

Cela emploie le Simple Network Management Protocol (SNMP) pour conduire la prévision, résiduelle modules de calcul et de détection pour un banc d'essai expérimental. Les auteurs exécutent leur étude à une exécution de MATLAB. Ils emploient une approche semi-dirigée.

Les auteurs emploient le travail antérieur [régression auto associative de grain (AAKR) et essai de rapport de probabilité séquentiel (SPRT)] pour leur fonction d'analyse, ils ont obtenu un taux de positif faux de 1% et un taux de négatif faux de 10% mais ne fournissent pas des données numériques pour démontrer cette performance à métrisation d'allumettes d'exécution.

Avantages

L'ensemble de données de Yang et autres inclut, l'impact le plus complet étaient : l'utilisation de processeur, le temps à vide de processeur ensemble de données des auteurs le' s'est composé d'un 1000 ensemble de données (normal) de formation d'observation et un ensemble de données d'essai de 300 observations (intrusions y compris).

Inconvénients

Le modèle de menace de Yang et al. est peu sophistiqué : Il comporte seulement l'inondation de cinglement, le jolt2 et les attaques buboniques de DOS. Cette recherche ne considère pas le matériel de legs : seulement postes de travail et serveurs des produits.

[Manikopolous 2010]: (IDS statistique)

Approche

L'utilisation de classificateur de réseau neuronal pour distinguer entre les données la normale et anormales. Toutes les données supérieures ou inférieures à un seuil prédéfini sera identifiée comme étant anormale

Avantage

Avoir un taux élevé de détection lorsque l'intensité du trafic est élevée

Inconvénients

Le taux de détection a diminué de façon significative lorsque intensité de l'attaque devient faible.

[Shin et al. 2010]

Basé sur le réseau de vérification, (Beaucoup d'IDSs) .

Cette activité auditant Basé sur le réseau d'étude d'utilisation pour déterminer si un nœud est compromis. Cet audit peut être général (analyse par exemple, du trafic ou de fréquence) ou Protocol spécifique (par exemple, inspection profonde de paquet).

Avantage

Concernant la gestion des ressources, les différents nœuds sont exempts de condition de maintenir ou analyser leurs notations.

Inconvénient

Concernant la collecte de données, la visibilité des nœuds rassemblant des données d'audit limite l'efficacité d'une technique basé network c'est-à-dire, il les provocant pour arranger les sondes basé network d'audit pour obtenir les images complètes d'intra-cell et d'inter-cellule de l'activité de réseau.

[Gao et autres 2010] **Comportement/centre serveur**

L'Étude de Gao et al. [Gao et autres 2010] propose un modèle d'identification pour des applications de service futées (de l'eau) qui emploie un réseau neurologique artificiel de propagation arrière à trois étages (ANN) basée sur Modbus.

[Jokar, Leung 2011] (Spécification IDS)

Approche : sept cahiers des charges (4 PHY et MAC 3) pour construire un comportement normale modèle.

Avantages

Il peut détecter les attaques inconnues

Inconvénients

Un taux d'alertes élevé (faux positifs), car il utilise les valeurs nominales seulement.

[Mitchell ET Chen 2012b; 2012a]

Cet auditer géré par le système central d'utilisation analysent des notations maintenues par un nœud ou autre auditent des données, telles que des détails de système de fichiers, pour déterminer s'il est compromis.

Avantage

- Principal employer auditer géré par le système central est commande distribuée ; c'est attrayant pour des configurations à fort débit comme des smart grid.
- L'employer auditer géré par le système central facilite la spécification/détectant de la mauvaise conduite de centre niveau parce qu'on peut appliquer la connaissance spécifique bien définie pour détecter des intrus.

Inconvénient

- Chaque nœuds doit effectuer le travail additionnel pour se rassembler
- Principal de cette technique est qu'un attaquant sophistiqué peut couvrir leurs voies en modifiant les données d'audit sur le nœud capturé.
- Un troisième inconvénient de cette technique est que ce peut être dos ou spécifique à l'application (selon le contenu particulier des notations).

[Namboodiri 2013] (Secure HAN)

Déroulement

HAN en 4 groupes, et chaque groupe a son propre pouvoir, enregistreur historique pour protéger les données Advanced Mètre Infrastructure(AMI)

Avantages

La sensibilité du temps ajouter aux préoccupations de sécurité

Inconvénients

Il ne peut détecter les attaques connues.

L'utilisateur est toujours digne de confiance.

Classification de travaux connexe

Attaque autres	DOS	Ecoute	**man in the middle**	rejeu (Replay)	Inconnues	multi-packet modbus
[Yang et al. 2005]	✓	-	-	-	-	-
[Manikopolous 2010]	-	-	-	-	-	✓
[Gao et al. 2010]	✓	-	✓	-	✓	-
[Shin et al. 2010]	✓	-	-	-	-	
[Jokar, Leung 2011]	-	-	-	-	✓	-
[Mitchell and Chen 2012b]	-	-	-	-	-	✓
[Namboodiri 2013]	-	✓	-	-	-	-

Tableaux 3.2. Classification de travaux connexe

Conclusion générale

Les travaux menés, dans le cadre mastère, ont pour objectif de proposer une solution de sécurité smart grid. Le smart grid est un réseau de distribution d'énergie qui utilise les technologies de communication afin d'optimiser la production, la consommation ainsi que la distribution d'électricité.

« Les smart grids, ou réseaux électrique « intelligents », visent à intégrer de manière efficiente les actions de l'ensemble des utilisateurs (producteurs et consommateurs) afin de garantir un approvisionnement électrique durable, sûr et au moindre coût ».

Les Smart grids associent les technologies de l'information et de la communication (TIC) aux réseaux. Les systèmes communiquant, en parallèle des réseaux de distribution, ainsi que l'intelligence embarquée doivent permettre un meilleur ajustement entre production et consommation d'électricité et l'intégration des énergies renouvelables.

Dans la littérature, plusieurs chercheurs se sont intéressés à la sécurité du réseau smart grid et ont identifié un certain nombre d'attaques qui peuvent être menés à savoir des attaques d'usurpation d'identité d'un smart mètre un des composants essentiel du réseaux smart grid .De même , l'attaquant peut rejouer des messages de consommation d'énergie qui ont pour but de perturber le système de facturation des utilisateurs certaines attaques peuvent même priver le client d' électricité.

Les premières expériences acquises à l'occasion de démonstrateurs Smart Grids révèlent que les nouvelles architectures se développent sous la forme de combinaisons de nouveaux cas d'utilisation et d'acteurs, venant s'ajouter aux infrastructures existantes. Ce qui nécessite l'interconnexion des sous-systèmes existants avec les nouveaux éléments. Cela induit intrinsèquement une augmentation de la surface d'attaque et nécessite donc de prendre de nouvelles mesures de réduction des risques en prenant en compte l'impact potentiel d'une attaque sur la stabilité du réseau électrique de bout en bout.

Cela nécessite une nouvelle approche pour gérer les cyber-risques de manière consistante par rapport aux risques traditionnels liés à la gestion des réseaux électriques. Cela nécessite également de permettre aux opérateurs de réseaux électriques de pouvoir évaluer la situation en cas de cyber-attaque.

Ce n'est qu'en ayant une parfaite connaissance de ce qu'est le Smart Grid, de ses forces, de ses faiblesses et des menaces auxquelles il doit faire face qu'il sera possible de construire des architectures Smart Grid intrinsèquement sécurisées dès la conception.

Grand stratège militaire, Sun Tzu expliquait déjà au VIe siècle av. J-C : "Si tu connais ton ennemi et si tu te connais, tu n'auras pas à craindre le résultat de cent batailles. Si tu te connais toi même sans connaître ton ennemi tes chances de victoires et de défaites seront égales. Si tu ne connais ni ton ennemi ni toi-même tu perdras toutes les batailles.

À long terme, le développement des smart grids devrait s'étendre à l'ensemble des réseaux interconnectés. Toutefois, l'implantation des réseaux intelligents dépend de l'efficacité des dispositifs techniques et de l'implication des parties prenantes.

Parmi elles, les consommateurs auront un rôle clé. En effet, l'équilibre du système électrique sera davantage géré par l'utilisateur final. Une sensibilisation du public sur les

enjeux du système sera alors nécessaire pour en comprendre l'utilité. Cela exigera aussi un accès aisé aux informations via des interfaces multiples et simples (smartphones, ordinateurs, etc.).

Bibliographiques

[1] O. Richardot, Réglage coordonné de tension dans les réseaux de distribution à l'aide de la production décentralisée, Ph .D. dissertation, INP Grenoble, 2006.

[2] Amy Shifflette Smart Grids, repenser les réseaux électriques research eu n° 60 - Juin 2009 www.smartgrids.eu Adresse 25 partenaires - 11 pays (ES, FR, IT, CH, BE, UK, NL, DE, FI, SE, RO) www.addressfp7.org.

[3] J.-C. Sabonnadière and N. Hadjsaïd, Lignes et réseaux électriques 3 : fonctionnement dans le cadre de la libéralisation des marchés, B. Multon, Ed. Lavoisier, 2008, vol. 3.

[4]Source: ABB, Deutsche Telekom, 2010. Smart Grid les architectures, les applications, les avantages et les standardisations.

[5] COLL-MAYOR D., PAGET M., LIGHTNER E., [2007], "Future intelligent power grids : Analysis of the vision in the European Union and the United States", *Energy Policy*, Vol.35, n°4, p. 2453-2465.

[6] Team, 2011] Team, S. (2011). Smart grid maturity model. Technical Report CMU/SEI-2011-TR-025

[7]*Guillaume Guérard* Optimisation de la diffusion de l'énergie dans les Smart Grids le 27/11/2014 https://tel.archives-ouvertes.fr/tel-01241153/document

[8] Jean-Marie FAVRE, Jacky ESTUBLIER, and Mireille BLAY-FORNARINO.L'ingénierie dirigée par les modèles. Au-delà du MDA (Traité IC2, série Informatique et Systèmes d'Information), 2006. xi, 6, 37, 38, 39

[9] National Institute of Standards and Technology (NIST). Nist special publication

1108r2: Nist framework and roadmap for smart grid interoperability standards,

Release 2.0[r], 2012.

[10] Weisser, D. (2004) on the economics of electricity consumption in small island developing states: a role for renewable energy technologies? *Energy policy,* 2004, 127-140.

[11][Schneider ET a l., 2008] Schneider, K. P., Chen, Y., Chassin, D. P., Pratt, R. G., Enge l, D. W., and Thompson, S. (2008). Modern grid initiative: Distribution taxonomy final report. Pacific Northwest National Laboratory.

[12]Shengrong Bu, F Richard Yu, and Peter X Liu. Dynamic pricing for demand-side Management in the smart grid. In *Online Conference on Green Communications (Green Com), 2011 IEEE*, pages 47–51. IEEE, 2011.

[13]Armando Ferreira and Carlos Dortolina. Implementation of fast and effective dynamic

Pricing schemes in smart grids. In *Integration of Renewable into the Distribution Grid, CIRED 2012 Workshop*, pages 1–4. IET, 2012.

[14] K Ashna and Sudhish N George. Gsm based automatic energy meter reading System with instant billing. In *Automation, Computing, Communication, Control And Compressed Sensing (iMac4s), 2013 International Multi-Conference on*, pages 65–72. IEEE, 2013.

[15] Q GAO, JY Yu, PHJ Chong, PL So and E Gunawan. Solutions for the silent node Problem in an automatic meter reading system using power-line communications.*Power Delivery, IEEE Transactions on*, 23(1):150–156, 2008.

[16] Antonio J Conejo, Juan M Morales, and Luis Baringo. Real-time demand response Mode l. *Smart Grid, IEEE Transactions on*, 1(3) : 236–242, 2010.

[17] Me moire de Find 'Etudes Envue de l'obtention du diplôme : MASTER *Thème:* Etude d'un système de supervision et de contrôle SCADA de la région de transport est Skikda. Présente par : B O U N A B Z a i d Soutenu le : 05 Juin 2014, Propose par : CHELIHI Abd Elghan i .

[18] M , AMAND, MED NSIRI**,** Etude d'un système de détection d'intrusion comportemental pour l'analyse du trafic aéroportuaire, 2011.

[19] Powell, R. Stroud(Eds),Malicious- and Accidental –Fault Tolerance for Internet Applications: Conceptual Model and Architecture, Final Version, Rapport LAAS n 03011, propjet IST-1999-11583 MAFTIA ,Deliverable D21, Javier 2003, 123pp, disponible a http://www.research . ec .org /maftia /deliverables/

[20] Schneider, NETWORK SECURITY ESSENTIALS, *APPLICATIONS AND STANDARDS* FOURTH EDITION, 2004.

[21] cole et al, cours sécurité informatique https://www.google.com/search?q=(Cole+et+al%2C+2005)+cours+pdf&ie=utf-8&oe=utf-8#q=(Cole+et+al,+2005)+cours+pdf+securit

[23] JR, Graham, R. Graham, Les système de détection intrusions informatiques .paris : Dunod, 2004, r. Graham. FAQ: Network intrusion detection Systems .version 0.8.3, March 21, 2000

[24] romuald.thion, SÉCURITÉ DES SYSTÈMES D'INFORMATION http://liris.cnrs.fr/~rthion/dokuwiki/enseignement:tiw4

[25](J. Justen, Nessus, 2003)

[26] l spitzner , Honeypots Catching the insider threat IN Proceedings of the 19th Annual Computer Security Applications Conference, page 170.IEEE Computer Socity ,2003 .

[27] NCbatista, RMelicio,JCO Matias, and JPS Catalao. Photovoltaic and wind energy systéms monitoring and building/home energy management using zigbee deviees within a smart grid .Energy, 49 :306-315,2013.

[28] siddharth sridhar, hahn, and maimaran govindarasou. Cyber attack-resilient control for smart grid technologie (ISGT), 20120IEEE PES,page 1-3.IEEE,2012

[29] Siddhartha Sridhar, Adam Hahn, and Manimaran Govindarasu. Cyber attack resilient control for smart grid In Innovative smart grid Technologies (ISGT), 20120IEEE PES, pages 1-3.IEEE, 2012.

[31] F.bao, p.samarti ,and J.zbou .Applied Gryptography and Network security:10th international conference, ACNS2012, singapore berlin heidelberg,2012.

[32]**Cleveland, Frances.** *White Paper: Cyber Security Issues for the Smart Grid.* s.l.: http://www.xanthus-consulting.com/Publications/White_Paper_Cyber_Security_Issues_for_the_Smart_Grid.pdf, 2009.

[33] F.Bao , P.samarati ,and J. Zbou.Applied Cryptography and Network security, 10th International Conference, ACNS2012, Singapore, June 26-29,2012, Proceedings . Lecture Notes in Computer science. Springer Berlin Heidelberg, 2012.

[34] David solo, Russell housley, and Warwick ford. Internet x.509 public infrastructure certificate and Revocate revocation list (crl) rofile.2002.

[35] Thien –Toan Tran, oh –soon shin, and Jong –ho Lee. Detection of attacks in smart grid systems .In computing .Management and Telecommunications (com-Man Tel) ,2013 International conference en , pages 298-302.IEEE,2013.and

Zhifeng Xiao, Yang Xiao, and DH D u. exploring malicious meter inspection in neighborhood area smart grids. Smart grid, IEEE Transaction on , 4(1):214-226,2013.

[36] Salvatore D'Antonio, Luigi coppolino, Ivano Alessandro Elia, and Valerio fomicola. Security issues of a phasor data concentrator for smart grid infrastructure .In Proccedings of the 13 thEuropean Workshop on dependable computing, pages 3-8, ACM, 2011

[37]. Fadi Aloula, AR AI-Alia, Rami AI-Dalkya, Mamoun AI-Mardinia, and wassim EL-Hajj. Smart grid security, Threats, vulnerabilities and solutions. International Journal of smart grid and clean energy, 1(1):1-6, 2012.

[38] .Dong Wei, Yan Lu, Mohsen Jafari, Paul M skare, and Kenneth rohde. Protecting smart grid automation systems against cyber attacks. Smart grid, IEEE Transactions on , 2(4):782-795,2011

[39]NIST Framework, Roadmap For smart grid interoperability standards, release 1.0(jan.2010)(nist special publication 1108).

[40] Sheeraz Niaz Lighari, Dil Muhammad Akbar hussain, Asad Ali Shaikh, and Bogi Jensen. Attacks and their defenses for advanced metering infrastructure. In Ultra Mo dern Telecommunication s and control systems and workshops (ICUMT), 2014 6th International congress on, pages 148-151.IEEE, 2014.

[41] Imen Aouini and lamia ben Azzouz, smart meter, applications, security issues and challenges.

[42] Anas Almajali, Arun Viswanathan, and Clifford Neuman Analyzing resiliency of the smart grid communication architectures under cyber attack In Cset, 2012

[43] zhuo lu ,wenye wang ,and chingyue wang.traffic: minimizing message delay for smart grid applications under jamming.dependoble and secure commputing, IEEEtransactions on, 12(1):31-44,2015

[44] Millésime, Les Types D'attaques Informatique www.ofppt.info août 14

[45] Jun Yan, Yida Yang Wenkai Wang Haibo He, and Yan sun .An integrated visualization approach for smart grid attacks .In Intelligent Control and Information processing (ICICIP), 20120Third International Conference on, pages 277-283. IEEE, 2012.

[46] Ahmad Usman and Sajjad Haider shami. Evolution of communication technologies for smart grid applications, Renewable and sustainable Energy Reviews, 19:191-199, 2013. And Nico Saputro, kamal akkaya, and suleyman uludag. A survey of routing protocols for smart grid communications. Computer Networks, 56(11): 2742-2771, 2012.

[47] Linus Wallgren , shahid Raza, and Thiemo Voigt. Routing attacks and counter measures in the rpl based internet of things, International Journal of Distributed sensor Networks, 2013.

[48] Y, Xiao communication and networking in smart grids, Taylor and Francis, 2012. And Alaoui Nabih. Cooperative Communications in Mobile Ad Hoc NET works, PhD thesis, Limoges, 2013.

[49] 57Imen Aouini and lamia ben Azzouz, smart meter, applications, security issues and challenges

[**50]** Elias Bouharb, claud fachkha , Makan Pourzand Debbabi , and Chadi Assi.communication security for smart grid distribution networks .communications Magazine , IEEE, 51(1):42-49,2013.and ▌Anas Almajali, Arun Viswanathan , and Clifford Neuman Analyzing resiliency of the smart grid communication architectures under cyber attack In Cset ,2012and Fadi Aloula, AR AI-Alia , Rami AI-Dalkya , Mamoun AI-Mardinia , and wassim EL-Hajj. Smart grid security, Threats, vulnerabilities and solutions. International Journal of smart grid and clean energy, 1(1):1-6, 2012.

And zhuo Lu, LU, Wenye Wang, and cliff Wang .Review and evaluation of security threats on the communication networks in the smart grid. In MILITARY COMMUNICATIONS CONFERENCE? 2010-MILCOM2010, pages 1830-1835, IEEE, 2010.

And Jan durech and Maria Franek ova. Security attacks to zigbee technology and their practical realization. In Applied Machine Intelligence and Informatics (SAMI), 20140IEEE 12th International symposium on, pages 345-349.IEEE? 2014.

[51] Wenge Wang and Lu .Cyber security in the smart grid survey and challenges. Computer Networks, 57(5): 1344-1371, 2013.

[52] Jan durech and Maria Franek ova. Security attacks to zigbee technology and their practical realization. In Applied Machine Intelligence and Informatics (SAMI), 20140IEEE 12th International symposium on, pages 345-349. IEEE, 2014.

[53] Alaoui Nabih . Cooperative Communications in Mobile Ad Hoc NET works, PhD thesis, Limoges, 2013.

[**54]** Salvatore D'Antonio, Luigi coppolino, Ivano Alessandro Elia, and Valerio fomicola. Security issues of a phasor data concentrator for smart grid infrastructure .In Proceedings of the 13 the European Workshop on dependable computing, pages 3-8, ACM, 2011.

[55] Zhuo Lu, LU, Wenye Wang, and cliff Wang .Review and evaluation of security threats on the communication networks in the smart grid. In MILITARY COMMUNICATIONS CONFERENCE, 2010-MILCOM2010, pages 1830-1835, IEEE, 2010.

[56] Dong Wei, Yan Lu, Mohsen Jafari, Paul M skare, and Kenneth rohde. Protecting smart grid automation systems against cyber attacks. Smart grid, IEEE Transactions on, 2(4):782-795, 2011.

[57] Endorf, c, Schultz, E, Millender, J, Intrusion Detection and Prevention, ISBN: 00722295443, 2004.

[58] Denning, D.E.(1987),An intrusion detection mode l. IEEE Transaction on software engineering,Vol.SE-13,NO2,pp.222-232 (**Denning, 1987).**

[59] Me L .V.Alanou. Intrusion détection, A bibliography. Technical report SSIR-2001-01, suppléé, rennes, France, september2001

[60] Endorf , c, Schultz, E, Mellander , J, Intrusion detection by machine learning ,A review ,Expert systems with Applications, vol 36,NO 10,pp 11994,12000 Endorf et al, 2004) .

[61] Xiaonan Wu, S B anzhaf, W. (2010), THE use of computational intelligence in intrusion detection systems A review Applied soft computing, vol.10, NO1.

[63] les systèmes de détection intrusions informatique. Paris : Undo 2004R. GRAHAM. FAQ: Network intrusion detection Systems. Version0.8.3, March 21, 2000

[64](T.Evangelista,2004) les systemes de détection intrusion informatiques .paris dunod ,2004 R ,GRAHAM ,faq ,network intrusion detection systems.version 0.8.3,March 21,2000.

[65] P.de Boer et M.Pels, Host –based intrusion detection systems.Technical report , february 4,2005.

[66] les systèmes de détection intrusions informatique. Paris : Undo 2004R. GRAHAM. FAQ: Network intrusion detection Systems. Version0.8.3, March 21, 2000

[67]Porass,Schnager, 1998)

Webographe

[w1] http://www.connaissancedesenergies.org/fiche-pedagogique/reseau-intelligent-smart-grid

[w2] William Beaucard et Réseau intelligent (Smart Grid) standardisations http://www.connaissancedesenergies.org/fiche-pedagogique/reseau-intelligent-smart-grid rapport d'activité 2009.

[w3] APERÇU GENERAL SUR LES SYSTEMES ELECTRIQUES MODERNESHttp://www.institut-numerique.org/iii-1-apercu-general-sur-les-systemes-electriques-modernes-51fba1b2d0d2702/08/2013

[w4] Les systèmes de supervision scadahttp://www.automation-sense.com/blog/automatisme/les-systemes-de-supervision-scada.htmlLe 17/02/2016

[22] Lorens et al, cours informatique https://coursinformatiquepdf.com/cours-informatique/cours-pdf-sur-la-securite-informatique.html,2006

[24] romuald.thion, SÉCURITÉ DES SYSTÈMES D'INFORMATION http://liris.cnrs.fr/~rthion/dokuwiki/enseignement:tiw4

[30] QUELLES MESURES DE SÉCURITÉ POUR ACCOMPAGNER LES SMART GRIDS]https://www.riskinsight-wavestone.com/2012/02/quelles-mesures-de-securite-pour-accompagner-les-smart-grids/

[62] A. Abou El Kalamα, M. Gad El Rabβ et Y. DeswarteβClassification des Attaques pour l'évaluation*https://www.google.com/search?q=Classification+sellant+l%E2%80%99emplacement+d%E2%80%99IDS+pdf&ie=utf-8&oe=utf-8* des IDS

[68]P.K.Agrawal, security challenges to power grid and smart grid infrastructures, https://www.slideshare.net/pkagarwal/security-challenges-to-power-grid-and-smart-grid-infrastructures?qid=109b835b-e4a8-45d1-ab02-d48126eabfc8&v=&b=