République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université de Larbi Tébessi –Tébessa-

Faculté des Sciences Exactes et des Sciences de la Nature et de la Vie

Département des mathématiques et de l'informatique

Mémoire de Master
Filière : Mathématiques/Informatique
Option : Réseaux et sécurité informatique

Thème :

Un Système de Détection D'Intrusion pour les Smart Grids

Présenté par : Bouras Ikram

Fethallah Khadra

Encadré par : Dr Ahmim Ahmed

Jury de soutenance :

Président :	M .Laouer	PR	Université de Tébessa
Encadreur :	Ahmim Ahmed	MCB	Université de Tébessa
Examinateur :	Souahi M.saleh	MAA	Université de Tébessa

Promotion : 2016-2017

Remerciements

En préambule à ce mémoire nous remerciant ALLAH qui nous aide et nous donne toute la patience et le grand courage durant ces langues années d'étude.

Nos vifs remerciements à notre professeur encadrant : Dr. Ahmim Ahmed qui s'est dévoué pour nos dispenser de tous conseils et directives utiles pour la réalisation de ce modeste travail. Aussi s'est toujours montré à l'écoute et très disponible tout au long de la réalisation de ce mémoire. Ainsi pour l'inspiration, l'aide, le temps qu'il a bien voulu me consacrer et sans qui ce mémoire n'aurait jamais vu le jour et pour ses précieux conseils et son orientation ficelée tout au long de notre recherche.

Nos vifs remerciements vont également aux membres du jury pour l'intérêt qu'ils ont porté à notre recherche en acceptant d'examiner notre travail Et de l'enrichir par leurs propositions.

Nos remerciements s'étendent également à tous nos enseignants durant les années des études.

On n'oublie pas nos parents pour leur contribution, leur soutien et leur patience.

A nos familles et nos amis /amies qui par leurs prières et leurs encouragements, on a pu surmonter tous les obstacles.

Enfin, nous adressons nos plus sincères remerciements à tous nos proches et, qui nous ont toujours soutenue et encouragée au cours de la réalisation de ce mémoire.

Merci à tous et à toutes. . .

Dédicace

Je Dédie Ce modeste Travail A Celle qui M'a donné La vie, Le symbole de Tendresse.
Mes parents. Aucun hommage ne pourrait être à la hauteur De L'Amour Dont ils ne cessent de me combler.
Que dieu leur procure La Bonne santé Et La Longue vie.
La lumière de mes jours, la source de mes efforts, la flamme de Mon Cœur,
Ma Vie et Mon Bonheur ; Maman Que J'adore.

L'homme de ma vie, Mon Exemple éternel, mon soutien moral et Ma source de joie et de bonheur, celui qui s'est toujours sacrifié pour Me voir réussir,
Que dieu te garde dans son vaste paradis ; A vous Mon Père.

Sans Oublié Jamais Béba « Allah Yarhmou » Et « Yomma SAHRA »
Pareillement à Mes Chère Tantes « IBTISSEM et HASSINA »
A Ma sœur Amina Dhikra et Mon frère Salah Eddine
A toute Mes cousins Et Cousines.
Surtout A toute Ma super Famille.
A Ma Binôme Khadra
A tous Mes Ami(e)s ; Mes Nièces
Amira, wafa, Radja, aicha, sana et bakhta, linda, Sawssen, Marouche et saghrouna.....

A Oubaid ...

A Tous et Toute mes aimables et mes collègues d'étude ;
Et surtout Tous les Étudiant(e)s de la classe mastère réseaux et sécurités informatique Promo 2017.
A Tous Mes Professeurs...

Et tous ceux qui ont contribué de près ou de loin pour que ce Projet possible,
Je vous dis Merci Infiniment...

Aux Personnes qui m'ont toujours Aidé et Encouragé, qui étaient Toujours à mes côtés, et qui M'ont Accompagnaient durant Mon Chemin De Vie

« Ikram »

Sommaire

Chapitre3

Liste des figures

Liste des tableaux

Résumé

L'informatique et de plus en plus présente dans nos vie quotidienne, ce qui rend toute donnée informatisée et automatisée .Ces changements touche même le monde électrique et dans le but de faire face à ces changements ; il est nécessaire de moderniser le système électrique. Cette modernisation a été obtenus grâce l'intégration de la technologie de l'information et de la communication pour un objectif de les rendre plus communicants avec une livraison d'électricité plus efficace, économique et sûre.

Les systèmes électriques dans la plupart des pays les plus développés avaient vus des changements significatifs. Ces changements sont le résultat de la libéralisation du marché électrique et l'augmentation des énergies renouvelables dans le mix énergétique, qui a conduit vers la naissance d'un nouveau type de réseau électrique appelée les smart grids qui permettent de résoudre le problème de la modernisation des systèmes électriques, tels que le problème du système centralisé et unidirectionnel pour devenir aujourd'hui répartie et bidirectionnel.

Le réseau Smart Grid constitue un défi pour la sécurisation des communications et des applications .ce défi est un facteur crucial pour le succès et le large déploiement de ce type de réseaux ; à cause de son architecture complexe qui couvre des dispositifs critiques et des systèmes vulnérables aux attaques. A partir de ces points, et à travers ce mémoire, nous présentons les problèmes de sécurité relatifs à l'architecture des Smart Grids.

Divers outils et mécanismes sont développés pour assurer un niveau de sécurité répondant aux exigences de la vie moderne. Cependant, presque tous les mécanismes de sécurité ont toujours des vulnérabilités et ils ne sont pas suffisants pour assurer la sécurité complète de l'infrastructure et éviter les attaques qui sont continuellement adaptées pour exploiter les faiblesses du système souvent causées par la conception imprudente et les défauts de la mise en œuvre.

Ce qui augmente le besoin des nouvelles technologies de sécurité qui peuvent surveiller les systèmes et identifier les attaques informatiques. Ceux-ci incluent les systèmes de détection d'intrusion(IDS), Parmi eux nous citons les systèmes de détection d'intrusion qui sont conçus pour détecter toutes activités ou comportements anormaux au bon fonctionnement du système ; et qui présente un complémentaire aux mécanismes de sécurité traditionnels.

Ces systèmes sont capables de détecter les attaques dans plusieurs environnements disponibles. Pour le cas de notre étude nous sommes intéressés particulièrement à la sécurité de l'infrastructure des réseaux électriques intelligents (smart grid) qui sont très sensibles au cyber attaques.

Un IDS est classé parmi les meilleurs outils, qui aident à prévoir ou à identifier toute activité non autorisée dans un réseau. Ce type de système est basé sur deux approches principales pour la détection d'intrusion ; l'approche par signature et l'approche comportementale. Chacune des deux exprime des avantages et des inconvénients dépendant des mécanismes et des algorithmes appliqués.

Le développement d'un système de détection d'intrusions étant le principal sujet de ce travail, nous avons consacré une grande partie de notre temps à la recherche des algorithmes et des méthodes de détection en essayant de trouver les plus efficaces qui assure surtout l'analyse des flux en temps réel.

Mot clé : Réseau électrique, Smart Grids, intrusion, détection d'intrusion, sécurité, IDS.

Abstract

Computer science is more and present in our life, which makes all data computerized and automated. This change touches even the electrical world and with the aim of coping with these changes; It is necessary to modernize the electrical system. This modernization was achieved through the integration of information technology and my communication in order to make them more communicating with a more efficient and economical delivery of electricity.

Electrical systems in the most developed countries are undergoing major changes. These changes are the result of the liberalization of the electricity market and the increase of renewable energies in the energy mix, giving rise to a new type of power grid called Smart Grid. The latter solve the problem of modernization of electrical systems such as the centralized and unidirectional system problem to become today distributed and bidirectional.

The Smart Grid is a challenge for securing communications and applications. This challenge is crucial to the success and wide deployment of this type of network; Because of its complex architecture that covers critical devices and systems vulnerable to attacks. From these points, and through this brief, we present the security problems related to the Smart Grid architecture, highlighting the main security problems related to this complex architecture.

Various tools and mechanisms are developed to ensure a level of security that meets the requirements of modern life. However, almost all security mechanisms still have vulnerabilities and they are not sufficient to ensure complete security of the infrastructure and avoid attacks that are continually adapted to exploit system weaknesses often caused by careless design and defects Implementation.

This increases the need for new security technologies that can monitor systems and identify computer attacks. These include Intrusion Detection Systems (IDS). Among them are intrusion detection systems that are designed to detect any abnormal activities or behaviors to the proper functioning of the system; and which is complementary to traditional security mechanisms.

These systems are capable of detecting attacks in several available environments. For the case of our study we are particularly interested in the security of smart grid infrastructure that are very sensitive to cyber-attacks.

An IDS is ranked among the best tools, which help predict or identify any unauthorized activity in a network. This type of system is based on two main approaches for intrusion detection; The signature approach and the behavioral approach. Each of the two expresses advantages and disadvantages depending on the mechanisms and algorithms applied.

Since the development of an intrusion detection system is the main subject of this work, we have spent a great deal of time researching algorithms and detection methods, trying to find the most effective Real-time flow analysis.

Keyword: Power grid, smart grid, intrusion, intrusion detection, security, IDS.

الملخص

إن توغّل الاعلام الآلي أكثر فأكثر أحدث تغيرات ملحوظة في حياتنا العصرية، حيث أصبحت جُل البيانات الشخصية والعامة محوسبة لتسهيل إدارتها وتامين تخزينها. هذه التغيرات شملت بدورها العالم الكهربائي. بهدف تسهيل تسيير النظام الكهربائي. ومن أجل التعامل مع هذه التغييرات من الضروري تحديث هذا النوع من الانظمة.

شَهدت الأنظمة الكهربائية في معظم البلدان المتقدمة تغييرات كبيرة نتيجةً لتحرير سوق الكهرباء وزيادة مصادر الطاقة المتجددة ضمن مزيج الطاقة، مما أدى إلى ظهور نوع جديد من الشبكات الكهربائية والذي سميً بالشبكة الكهربائية الذكية التي اعتبرت كحل لمشاكل تحديث الأنظمة الكهربائية مثل مشكلة النظام المركزي وأُحادي الاتجاه لتصبح الآن موزعة ثنائية الاتجاه.

سهّل تحقيق هذا الهدف دمج تكنولوجيا المعلومات والاتصالات في هذه الشبكات بهدف جعلها أكثر اتصالا وكفاءة، لكن ذلك وضعها في تحدي خطير. اذ استوجب عليها لتأمين هاته الاتصالات والتطبيقات بسبب بنيتها المعقدة التي تغطي أجهزة وأنظمة جدُّ حرجة عرضة للهجوم.

انطلاقا من هذه النقاط، ومن خلال هذه المذكرة التي نحن بصدد مناقشتها، حاولنا تقديم قضايا الأمن المتعلقة ببنية هذا النوع المختلف من الشبكات الكهربائية اين قمنا بتسليط الضوء عليها على وجه الخصوص.

فلمواجهة هذا التحدي وللتصدي لهذه الهجمات ركز الباحثين في هذا المجال على هذه النقطة تحديدا، بحيث اظهروا أن العديد من الهجمات التي يمكن أن تنفذ وتوقف سير هذا النوع الحساس من الشبكات كهجمات سرقة الهوية وتزوير فواتير المستهلكين... تشكل خطرا كبير على امنها، اذ قاموا بتطوير العديد من التقنيات التي سعت الى توفير أقصى قدر من الحماية للأنظمة والشبكات ضد هذه الاخيرة مثل جدار الحماية؛ برامج مكافحة الفيروسات والاجهزة التحليلية... الخ

ومع ذلك، لا تزال جميع آليات الأمن تقريبا تعاني من نقاط ضعف، وهي ليست كافية لضمان الأمن الكامل للبنية التحتية وتجنب الهجمات المتكيفة باستمرار. وهذا ما يزيد الحاجة إلى تكنولوجيات أمنية جديدة مختلفة تماما، شاملة وكاملة بإمكانها رصد وتحديد الهجمات التي تستهدف هذا النوع من الشبكات. والتي تشمل بدورها انظمة كشف التسلل التي تُكمِّل آليات الأمن التقليدية. هذه الانظمة تتميز بخاصية الكشف عن الهجمات والتسلّلات في العديد من البيئات المتاحة. في حالة دراستنا هذه اهتممنا بشكل خاص حول أمن البنية التحتية للشبكة الكهربائية الذكية التي هي حساسة جدا للهجمات السيبرانية.

إن الكشف عن عمليات الاقتحام او التسلل في هذه القضية يمثل مشكلة بالغة الأهمية لمواجهة المخاطر المختلفة التي تنتهك أمن هذا النوع من الشبكات. وهذا ما جعل أنظمة كشف التسلل من بين أفضل الوسائل التي تساعد على التنبؤ أو تحديد نشاط غير مصرح به في الشبكة. ويستند هذا النوع من النظام على نهجين رئيسيين لكشف التسلل. النهج التوقيعي والنهج السلوكي. والتي تعمد في عملية الكشف والتحليل على خوارزميات وطرق كشف تضمن تحقيق هذا الهدف في نفس لحظة التسلل، محاولة بذلك العثور على التحليل الأكثر فعالية.

الكلمات المفتاحية: شبكات الكهرباء , شبكة الكهرباء الذكية, تسلل ,حماية, كشف التسلل, نظام كشف التسلل

Glossaire

AC	:	Autorité de Certification (CA pour Certificate Authority)
ACK	:	Acknowledgment
ACL	:	Access Contrôle Liste (liste de contrôle d'accès)
ADDRES	:	Active Distribution network with full integration of Demand and distributed energy RESourceS
AES	:	Advanced Encryption Standard
AMI	:	Advanced Metering Infrastructure
AMR	:	Automatic Meter Reading
AMM		Advenced Meter Reading
API	:	automates industriels programmable
ARP	:	Address Resolution Protocol
CA	:	Courants Alternatifs
CCTV	:	closed circuit television
CPU	:	control process unit
DA	:	Distribution Automation
DOS		Distributed Denial of Service
DDoS	:	Le Déni de service distribué (Distributed Denial of Service)
DER	:	Ressource énergétiques distribuées (Distributed Energy Ressources)
DER	:	Ressource énergétiques distribuées (Distributed Energy Ressources)
DG	:	Distributed Generation
DIDS	:	l'IDS distribué
DMS	:	Distribution Management System (système de gestion de distribution)
DNP3	:	Distributed Network Protocol
DNS	:	système de noms de domaine (Domain Name System)
DODAG	:	Destination Oriented Directed Acyclic Graph
DR	:	Demand Response
DS	:	Distributed Storage
DSR	:	Dynamic Source Routing
EMS	:	système de gestion d'énergie (Energy Management System)
EPPA	:	Efficient and Privacy Preserving Agrégation
ESI	:	Energy Services Interface
EV	:	véhicules électriques (Electric Vehicle)
FAN	:	Le réseau de Zones (Field Area Networks)
FEP	:	processeurs frontaux (Front End Processors)
FTP	:	Protocol de transfert de fichier (File Transfer Protocol)
GRD	:	gestionnaire du réseau de distribution
GrIDS	:	Graph-Based Intrusion Detection System
HAN	:	Home Area Network
HEMS	:	système de gestion de l'énergie domestique (home energy management system)
HIDS	:	IDS Basés sur l'hôte
HTTP	:	HyperText Transfer Protocol
HVDC	:	Courant Continu Haute Tension (High Voltage Direct Curren)
ICMP	:	Internet Control Message Protocol

ICN	:	Integrated Computing Network
ICS	:	systèmes de contrôle industriels (Industrial Control System)
IDES	:	Intrusion-Detection Expert System
IDS	:	systèmes de détection d'intrusion (Intrusion Detection System)
IED	:	dispositifs électroniques intelligents (Intelligent Electronic Devices)
IEEE	:	Institute of Electrical and Electronics Engineers (Institut des ingénieurs électriciens et électroniciens)
IETF	:	Internet Engineering Task Force
IHD	:	panneau d'affichage à domicile (In-home display)
IHM	:	Interface Homme Machine
IoT	:	Internet of Things
IP	:	Internet protocol
ISO	:	opérateur de système indépendant (Independent System Operator)
LAN	:	réseaux locaux (Local Area Network)
LDAP	:	Lightweight Directory Access Protocol
LDC	:	concentrateurs locaux de données (Local Data Concentrator)
MAC	:	Media Access Contrôle
MCC	:	centres de commande de moteur (Motor Control Centers)
MST	:	Minimum Spanning Tree
MTE	:	Transmission de Minimum énergétique (MTE)
MTU	:	Master Terminal Unit
NADIR	:	Network Anomaly Detection and Intrusion Reporter
NAN	:	Neighborhood Area Network (réseaux de voisinage)
NIDES	:	Next- Generation IDES
NIDS	:	IDS Basés sur le réseau
NIST	:	National International Standard Technology
OMS	:	Outage Management System
OPEN METER	:	Open Public Extended Network Metering
P2P	:	Peer-to-Peer
PDC	:	Phasor Data Concentrator
PHEV	:	véhicule électrique hybride rechargeable (Plug-in Hybrid Electric Vehicle)
PKI	:	L'infrastructure à clés publiques (Public Key Infrastructure°
PLC	:	Contrôleurs logique programmable (programmable logic controller)
PMU	:	Les unités de mesures Phasor (Phasor Measurements Units)
QoS	:	Qualité de Service (Quality of Service)
RCD	:	Remote Connect Disconnect
RIP	:	Routing Information Protocol (protocole d'information de routage)
RTO	:	opérateur de transport régional (Regional Transmission Operator)
RTP	:	Prix en temps réel (Real Time Pricing)
RTU	:	Unités de contrôle à distance (Remote Terminal Unit)
SCADA	:	Système de contrôle et d'acquisition de données (Supervisory Control And Data Acquisition)
SG	:	Smart Grids
SGIRM	:	Smart Grid Interoperability Reference Model
SMILE	:	Smart Ideas to Link Energie
SNMP	:	Simple Network Management Protocol (protocole simple de gestion de réseau)

SQL	:	Structured Query Language (langage de requête structurée)
SSL	:	SSL (Secure Socket Layer)
SSN	:	nœud de sous-station secondaire
SYN	:	Synchronize
TCP	:	Transmission Control Protocol (protocole de contrôle de transmissions)
TIC	:	Technologies de l'information et de la communication
URL	:	Uniform Resource Locator (localisateur uniforme de ressource)
VNC	:	Virtual Network Computing (informatique virtuelle en réseau)
VPN	:	réseau privé virtuel (Virtual Private Network)
WAMPAC	:	Wide Area Monitoring Protection and Control
WAN	:	Réseaux étendus (Wide Area Network)
WLAN	:	Réseaux locaux sans fil (Wireless LAN)
Weka	:	Waikato Environment for Knowledge Analysis

Introduction Générale

Introduction générale

Afin de faire face aux changements dans le monde énergétique, il est nécessaire de moderniser tout d'abord le système d'électricité.

L'intégration de la nouvelle technologie de l'information et de la communication dans les réseaux électrique dans l'objectif de les rendre plus communicants avec une livraison d'électricité plus efficace, économique et sûre. Ce qui assure une gestion souple du système électrique et garantit la gestion des contraintes, telles que l'interruption des énergies renouvelables et le développement des nouvelles utilisations comme les véhicules électriques.

Les réseaux électriques intelligents ou ce qu'on appelle aussi les Smart Grids résout le problème de modernisation des systèmes électriques tels que le problème de système centralisé et unidirectionnel, allant de la production à la consommation pour devenir aujourd'hui répartie et bidirectionnelle.

Le concept de Smart Grid, ou de réseau électrique intelligent est mis en place régulièrement depuis quelques années pour justifier des investissements dans différentes technologies qui permettent de moderniser les réseaux d'électricité.

Les smart grids réfèrent à un ensemble d'applications permettant une modernisation des réseaux électriques par l'intégration des technologies de l'information et de la communication (TIC). Ils peuvent soutenir différents objectifs énergétiques, tant au niveau économique, environnemental et social, qu'en termes de sécurité et de fiabilité du réseau. Les termes Smart Grid, réseaux électriques intelligents et Grille intelligente seront employés comme synonymes dans le domaine de la recherche scientifique.

Plusieurs raisons justifient les investissements qui se produisent dans ce type de réseaux électrique. Parmi eux on peut citer : les problèmes liés à la fiabilité des réseaux et la sécurité énergétique qui ont poussé vers le développement des smart grids, la production décentralisée d'électricité et le développement durable qui a davantage guidé ces changements technologiques. Pour atteindre cet objectif de nombreux acteurs investissent dans ce domaine émerge, malgré ses motivations et ses visions variés.

Le développement des Smart Grids intéresse les compagnies d'électricité, les gouvernements, les acteurs industriels (fabricants de technologies smart grids, firmes spécialisées dans les TIC, etc.), le milieu de la recherche et de l'innovation, ainsi que les groupes sociaux et environnementaux qui s'intéressent surtout aux impacts potentiels de ces technologies sur la santé et l'environnement.

Certains acteurs considèrent que le développement des Smart grids permettra d'apporter des changements progressifs au réseau électrique, comme les différentes améliorations sur le réseau électrique en générale, et l'amélioration de l'efficacité énergétique en particulier.

Tandis que d'autres souhaiteraient que ces réseaux électriques intelligents favorisent des changements radicaux dans le système de production d'électricité grâce à l'intégration des nouvelles technologies et l'électrification des transports, l'application des changements au niveau des normes, ainsi que le réforme des procédures exécutives ... etc.) .

La transition vers un réseau plus automatisé, comporte des changements et des améliorations qui touchent toute la chaîne du réseau, qu'il s'agisse du mode de fonctionnement des fournisseurs d'électricité, du mode de structuration du réseau ou du mode d'interaction entre l'utilisateur final (consommateur d'électricité) et l'infrastructure du réseau.

Le réseau Smart Grid constitue un défi pour la sécurisation des communications et des applications. Un certain nombre de travaux ont focalisés sur ce point et ont montré que plusieurs attaques peuvent être menées telles que les attaques d'usurpation d'identité des équipements, les attaques de rejet des messages de consommation ou de facturation et les attaques d'écoute de trafic…etc.

Pour remédier à ces attaques, les chercheurs dans ce domaine ont développé plusieurs techniques qui peuvent assurer une sécurisation pour les systèmes et les réseaux informatiques contre ces dernières .Telles que les parfeu ; les antivirus ; les scanners …etc.

Cependant, presque tous les mécanismes de sécurité ont toujours des vulnérabilités et ils ne sont pas suffisants pour assurer la sécurité complète de l'infrastructure et éviter les attaques qui sont continuellement adaptées pour exploiter les faiblesses du système, souvent causées par la conception imprudente et les défauts de la mise en œuvre. Ce qui augmente le besoin des nouvelles technologies de sécurité qui peuvent surveiller les systèmes et identifier les attaques informatiques. Parmi eux nous citons les systèmes de détection d'intrusion qui présente un complémentaire aux mécanismes de sécurité traditionnels.

Ces systèmes sont capables de détecter les attaques dans plusieurs environnements disponibles. Pour le cas de notre étude, nous sommes intéressés particulièrement à la sécurité de l'infrastructure des réseaux électriques intelligents (smart grid) qui sont très sensibles au cyber attaques.

La détection d'intrusions dans ce cas est une problématique très importante pour faire face au différent risque qui viole la sécurité de ce type de réseaux.

L'intrusion d'une façon générale est toute utilisation d'un système informatique à des fins autres que celles prévues, généralement dues à l'acquisition de privilèges de façon illégitime. L'intrus est généralement vu comme une personne étrangère au un système informatique qui a réussi à en prendre le contrôle, mais les statistiques montrent que les utilisations abusives (du détournement de ressources à l'espionnage industriel) proviennent le plus fréquemment de personnes internes ayant déjà un accès au système.

Les systèmes de détection d'intrusion (Intrusion Détection Système, ou IDS) permettent de repérer les comportements anormaux visant un réseau ou un hôte, résultant la plupart du temps d'attaques ayant un but malveillant.

1. Problématique

Compte tenu des caractéristiques des réseaux électriques intelligents et les problèmes qu'ils peuvent subir, tels que la sensibilité aux différentes attaques ainsi que le besoin de ce type de réseaux à la sécurisation .La question posée dans ce cas est comment garantir une sécurisation maximale aux Smart Grids.

Notre problématique se présente selon ces deux questions de recherches :

- ✓ Comment détecter les intrusions dans ce type de réseaux électriques et qu'elle est l'efficacité des systèmes de détection d'intrusion dans ce cas ?
- ✓ Comment protéger les réseaux électriques intelligents contre les attaques détectées ?

Pour pouvoir répondre à ces questions, on propose d'établir un modèle de détection d'intrusion pour les Smart Grids.

2. Objectif

L'objectif principal de notre mémoire est de proposer un modèle de détection d'intrusion pour les smart grids et particulièrement pour le système SCADA.

3. Structure de mémoire

Notre mémoire est présentée en deux parties .La première est un État de l'art, elle est composée de trois chapitres selon le plant suivant :

Dans le premier chapitre, nous essayons de faire une étude comparative entre le réseau électrique classique qui est doté seulement des trois parties électriques principales : production, transmission et distribution et les Smart Grids qui sont par contre fusionnés entre le réseau électrique et le réseau de communication.

Le second chapitre contient une étude approfondie sur la sécurité informatique et les différentes attaques qui la menace et comment faire pour remédier face ces dernières .Ensuite l'insuffisance des outils de protection pour garantir une sécurité maximale et le besoin au système de détection d'intrusion pour atteindre cet objectif.

Dans le troisième chapitre, nous essayons de montrer le besoin des smart Grids en termes de sécurité et ses sensibilités aux attaques informatiques. Nous avons mené vers une étude sur les anciens travaux de recherche dans ce cadre ; ces derniers englobent les projets d'amélioration d'automatisation ou de sécurisation ainsi que les différents travaux connexes des systèmes de détection d'intrusions proposés dans le contexte de ces Smart Grids.

La deuxième partie est la partie contribution où on conclut avec un quatrième chapitre qui contient une proposition architecturale d'un système de détection d'intrusion dans le contexte des smart grids. Nous proposons d'établir un IDS discret qui analyse les paquets réceptionnés de la part des capteurs de collection de données qui sont installés dans les points critiques de ce réseau électrique intelligent. Ces derniers collectent les informations qui circulent dans ce réseau et les envoyées à l'IDS qui n'est pas connue même de la part de l'ensemble de réseaux (connu seulement par les administrateurs de réseau) pour qu'il ne soit pas susceptible aux attaques. La tâche principale de ce système de protection est d'analyser le trafic et de signaler des alertes dans le cas de détection d'intrusions.

Partie I : Etat de L'art

Chapitre 1 : Les Smart Grids

Introduction

L'électricité est un élément essentiel dans le monde de la civilisation, qui fournit de l'électricité et de l'information en séquence. Il fournit de l'énergie électrique à l'utilisateur avec des émissions contrôlées ainsi qu'il met à la disposition des consommateurs une gamme améliorée de produits innovants et des services de qualité. Tout ceci constitue ce qu'on appelle le système d'alimentation électrique qu'il se compose des machines électriques, des lignes et des mécanismes pour générer de l'électricité et l'offre aux clients.

Le concept de Smart Grids, ou de réseaux d'électricité intelligents est mis en place régulièrement depuis quelques années pour justifier des investissements dans différentes technologies qui permettent de moderniser les réseaux électrique classique. Les Smart Grids réfèrent à un ensemble d'applications permettant une modernisation des réseaux électriques par l'intégration des technologies de l'information et de la communication (TIC). Ils peuvent soutenir différents objectifs énergétiques, tant au niveau économique, environnemental et social, qu'en termes de sécurité et de fiabilité du réseau**.**

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. Une fois que cet intérêt se profilera et que les pertes de confort seront réduites au minimum, la probabilité d'une mutation de notre réseau électrique actuel en Smart Grid émergera également.

I. Description des réseaux électriques classique et intelligent

1. Qu'est-ce qu'un réseau électrique ?

Selon [abdojell, 2011], un réseau électrique est un ensemble d'infrastructures énergétiques qui permettent d'acheminer l'énergie électrique des centres de production aux consommateurs d'électricité.

IL est formé de lignes électriques exploitées à différents niveaux de tension, connectées entre elles dans des postes électriques. Ces derniers permettent de répartir l'électricité et de la faire passer d'une tension à l'autre grâce aux transformateurs.

Ce réseau électrique doit assurer la gestion dynamique de l'ensemble (production - transport - consommation) mettant en œuvre des réglages ayant pour un but d'assurer la stabilité de l'ensemble.

Le premier but d'un réseau d'énergie électrique est de pouvoir alimenter la demande des clients consommateurs.

Comme on ne peut pas encore stocker économiquement et en grande quantité l'énergie électrique, il faut pouvoir maintenir en permanence l'égalité :

Production = Consommation + pertes

C'est le problème de la **CONDUITE** du réseau.

Dans nos réseaux, les pertes (transport et distribution) sont de l'ordre de 4 à 5 % de la consommation.

De plus la qualité du service est un souci majeur de l'exploitant : maintien de la tension et de la fréquence dans les plages contractuelles (problème de **REGLAGE** du réseau), pris en compte du couplage dynamique entre production et consommation via le réseau (**STABILITE**), assurer l'intégrité des ouvrages (**DIMENSIONNEMENT** approprié et **PROTECTION**).

2. Les différents types de réseaux électriques :

Les systèmes de plus en plus complexes, alimentant des charges elles-mêmes de plus en plus exigeantes, les réseaux électriques couvrent la majorité des territoires des pays électriquement développés, sont omniprésents sur les sites industriels, mais aussi dans les réseaux embarques (voitures, avions, navires) ou les générateurs, moteurs, transformateurs et actionneurs électriques sont de plus en plus utilisés.

2.1. Réseau électrique classique :

2.1.1. Définition :

Un réseau électrique classique ou ce qu'on appelle aussi le réseau électrique traditionnel est un réseau interconnecté pour fournir l'électricité produite aux consommateurs. Il se compose de centrales électriques qui produisent de l'énergie électrique ; des lignes de transmission à haute tension qui transportent l'énergie de sources éloignées vers des centres de demande et des lignes de distribution qui relient des clients individuels (consommateurs). **[**A. B. M. S Ali, 2013]

2.1.2. Architecture d'un réseau électrique classique :

Le réseau électrique classique est de nature unidirectionnelle, l'électricité est souvent produite aux centrales de l'électricité par des générateurs électromécaniques, principalement alimentés par la force de l'eau courante ou des moteurs thermiques alimentés par la combustion chimique ou l'énergie nucléaire. Afin de profiter des économies d'échelle, les centrales sont généralement assez grandes et situées loin des zones fortement peuplées.

Le réseau électrique classique combine le producteur central de l'électricité avec un réseau de transport ainsi que de distribution ; la puissance électrique produite est augmentée à une tension plus élevée pour la transmission sur une grille de transmission.

La grille de transmission déplace l'électricité produite sur de longues distances vers des sous-stations. À l'arrivée à une sous-station, la puissance sera abaissée de la tension de niveau de transmission à une tension de niveau de distribution.

Lorsque la puissance sort de la sous-station, elle entre dans la grille de distribution. Enfin, à l'arrivée à l'emplacement de service, l'alimentation est redescendue de la tension de distribution à la ou aux tension (s) de service requise (s).

Pour comprendre l'architecture et le flux de puissance du réseau électrique ; il faut tout d'abord comprendre la décomposition du réseau électrique ; tel qu'il est illustré à la Figure 1.1.

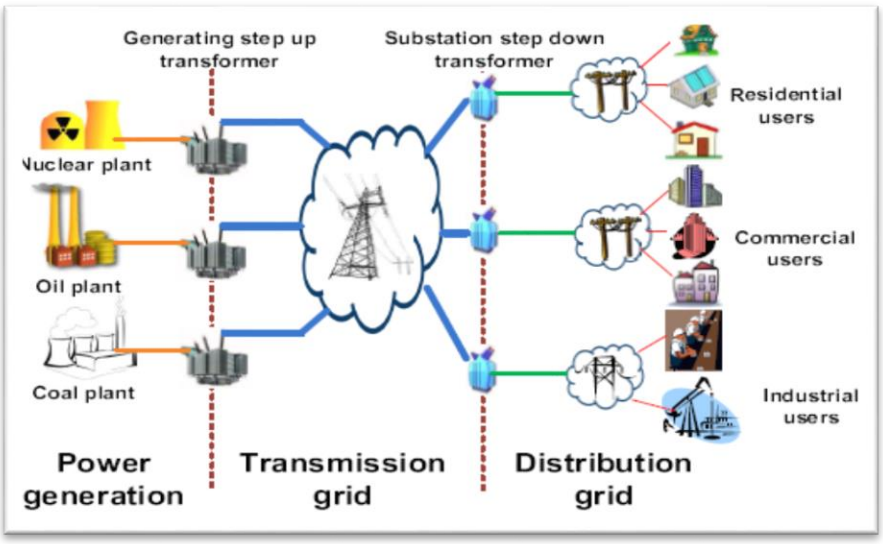

Figure 1.1 : *Architecture typique des réseaux électriques classiques. [Xi Fang et al, 2011]*

a. Production d'électricité :

La production doit en tout instant être capable de satisfaire la demande (consommation+ pertes), elle doit donc prévoir des moyens de production pour couvrir l'extrême pointe de la demande.

La production d'électricité est la première phase de production d'énergie électrique à partir d'autres sources d'énergie primaires. Pour les services d'électricité, c'est le premier processus de livraison d'électricité aux consommateurs. Les autres procédés, le transport et la distribution d'électricité, ainsi que le stockage et la récupération de l'énergie électrique à l'aide des outils de stockage par pompage sont effectués par l'industrie de l'énergie électrique.

L'électricité est le plus souvent générée dans une centrale électrique par des générateurs électromécaniques, principalement alimentés par des moteurs thermiques alimentés par combustion ou par fission nucléaire, mais aussi par d'autres moyens tels que l'énergie cinétique de l'eau courante et du vent. Les autres sources d'énergie incluent le photovoltaïque solaire et la géothermie. [J.L. LILIEN, 2006]

b. Réseaux de transport :

La transmission d'énergie électrique est le processus de déplacement massif de l'énergie électrique d'un site de production, tel qu'une centrale électrique, vers un poste électrique ; à l'aide des lignes interconnectées qui facilitent ce mouvement.

La plupart des lignes de transmission sont de haute tension ; dans le but de résister aux **C**ourants **A**lternatifs triphasés (CA). Tandis que la technologie haute tension à courant continu (HVDC) est utilisée pour une plus grande efficacité sur de très longues distances (généralement des centaines de milles). La technologie HVDC est également utilisée dans les câbles d'alimentation sous-marins (généralement plus de 30 miles (50 km)), et dans l'échange de puissance entre les grilles qui ne sont pas mutuellement synchronisées.

Les liaisons HVDC servent à stabiliser les grands réseaux de distribution d'énergie où de nouvelles charges soudaines ou des pannes d'électricité dans une partie d'un réseau peuvent entraîner des problèmes de synchronisation et des défaillances en cascade.

L'électricité est transmise à des tensions élevées (**115 kV** ou plus) pour réduire la perte d'énergie qui se produit dans la transmission longue distance. Cette puissance est généralement transmise par les lignes aériennes. [Xi Fang et al, 2011]

c. Réseaux de distribution :

La distribution d'énergie électrique est la dernière phase de la livraison d'énergie électrique, où le réseau transporte l'électricité du système de transport vers les consommateurs individuels.

Les sous-stations de distribution se connectent au système de transmission et abaissent la tension de transmission à moyenne de tension comprise entre **2 kV et 35 kV** avec l'utilisation de transformateurs.

Les lignes de distribution primaire transportent cette tension moyenne vers des transformateurs de distribution situés à proximité des locaux des clients.

Les transformateurs de distribution réduisent de nouveau la tension à la tension d'utilisation des appareils électroménagers et alimentent typiquement plusieurs clients par des lignes de distribution secondaires à cette tension.

Les réseaux de distribution ont pour but d'alimenter l'ensemble des consommateurs selon deux sous niveaux de tension la première moyenne (**anciennement MT devenu HTA de 1 à 50 kV**) et la deuxième basse (faible). [Xi Fang et al, 2011]

2.1.3. Fonctionnement d'un réseau électrique classique :

Le réseau électrique se compose de machines de production et de consommation d'électricité, ainsi que de structures (lignes, transformateurs) pour les relier.

- **L'énergie électrique** produite par les centrales électriques est transportée par un réseau électrique (aérien et sous terrain) pour alimenter les clients consommateurs.
- **Les centrales électriques** peuvent être situées à proximité d'une source de carburant, ou sur un site de barrage pour profiter des sources d'énergie renouvelable, ils sont souvent situés loin des zones fortement peuplées. Ils sont généralement assez grands pour profiter des économies d'échelle.
- **L'énergie électrique** qui est générée est portée à une tension plus élevée à laquelle elle se connecte au réseau de transmission d'énergie électrique.
- **Le réseau de transport d'électricité** en vrac déplacera la puissance sur des longues distances, parfois à travers les frontières internationales, jusqu'à ce qu'il atteigne ses clients de gros.

- **À l'arrivée à une sous-station**, la puissance sera réduite d'une tension de niveau de transmission à une tension de niveau de distribution.
- **Lorsqu'il sort de la sous-station**, il entre dans le câblage de distribution. Enfin, à l'arrivée à l'emplacement de service, l'alimentation est redescendue de la tension de distribution à la ou aux tension (s) de service requise (s).

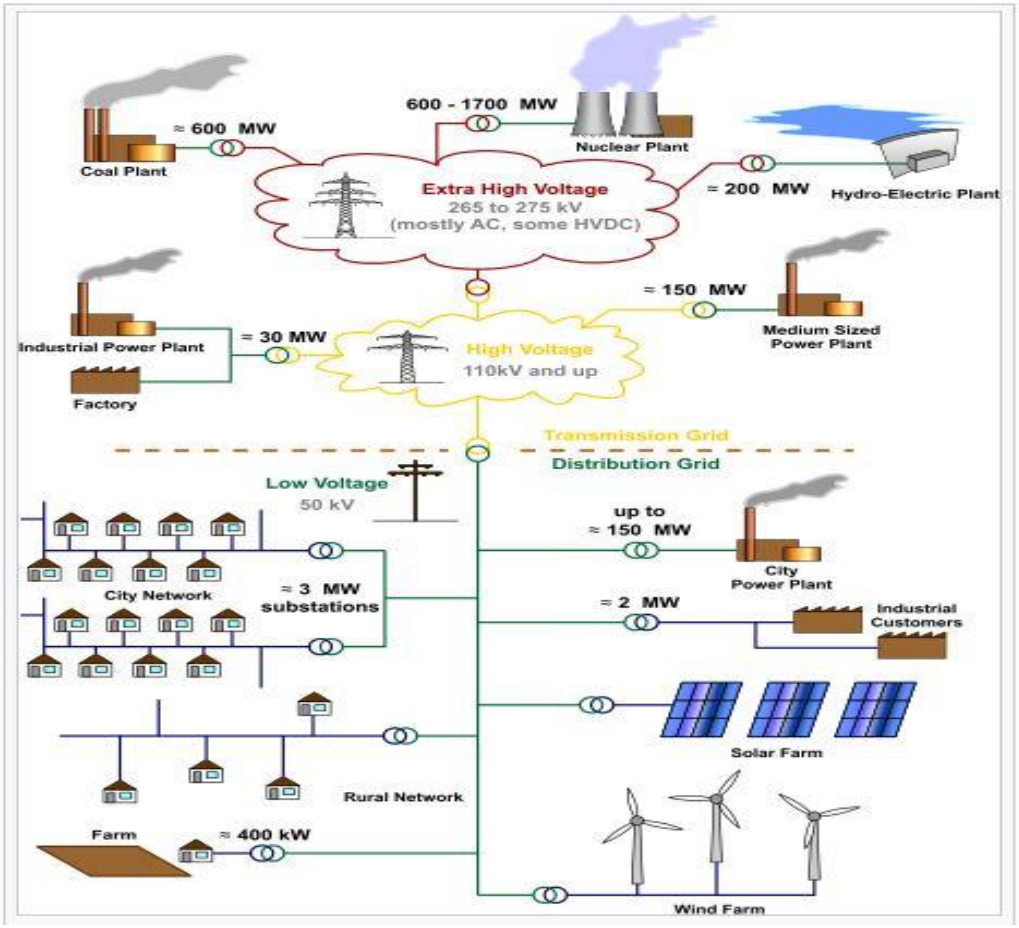

Figure 1.2 : Le fonctionnement des Réseaux électriques classique. [w1]

2.1.4. Les limites d'un réseau électrique classique : [Xi Fang et al, 2011]

- Génération centralisée ;
- Communication unidirectionnelle ;
- Systèmes de protection, de surveillance et de contrôle limités ;
- Restauration et réparations manuelles ;
- Vérification d'équipement manuelle ;
- Contingences limitées du système de contrôle ;

2.2. Réseau électrique intelligent (Smart Grid)

Afin de faire face aux changements dans le paysage énergétique, il est nécessaire de moderniser les systèmes électriques.

Partout dans le monde, les systèmes électriques sont confrontés à des changements radicaux stimulés par la nécessité urgente de dé-carboniser l'électricité, d'échanger les ressources vieillissantes et d'appliquer efficacement les technologies de l'information et de la communication qui sont en évolution rapide.

Le réseau électrique se compose généralement d'un producteur principal d'électricité ainsi que des consommateurs selon une architecture qui relie ces derniers entre eux par des lignes de câblage de haute, moyenne ou faible tension qui assure l'échange de l'énergie électrique .

Cependant, avec le temps, cette structure électrique a fini par souffrir à cause des problèmes de compromis dans la fourniture d'électricité ; de telle sorte que la production de l'électricité ne peut être grande si la consommation est petite et vice-versa. Ainsi, la cohérence de la livraison d'électricité ne peut être assurée et couterait donc plus cher.

L'intégration de la nouvelle technologie de l'information et de la communication dans ce réseau a pour but de le rendre plus communicant avec une livraison d'électricité plus efficace, économique et sûre. Ceci assure une gestion souple du système électrique et garantit la gestion des contraintes telles que l'interruption d'énergie renouvelable et le développement de nouvelles utilisations.

Tous ces objectifs convergent vers la direction des réseaux électriques intelligents «Smart Grids» qui résolvent le problème de modernisation du système électrique, tel que celui du système centralisé et unidirectionnelle allant de la production à la consommation lequel résolu par ce type de réseaux pour devenir aujourd'hui réparti et bidirectionnel.

2.2.1. Définitions

Fondamentalement, la vision de Smart Grid est de fournir une meilleure visibilité aux réseaux électriques à basse tension ainsi que de permettre l'implication des consommateurs dans la fonction du système d'alimentation, principalement à l'aide de compteurs intelligents et Smart meters

Le Smart Grid n'a pas de définition unique et évidente.

a. Définition 1 :

L'expression Smart Grids est généralisée en 2005, elle est mise en place par la Commission Européenne de la plateforme technologique.

La plate-forme technologique européenne[1] définit le Smart Grid comme suit :

Un Smart Grid est un réseau électrique capable d'intégrer intelligemment les actions de tous les utilisateurs qui y sont connectés (les producteurs, les consommateurs et ceux qui font les deux) ; et assurer l'approvisionnement en électricité. [A. B. M. S Ali, 2013]

b. Définition 2 :

Selon le ministère de l'Énergie des États-Unis :

Un réseau électrique intelligent utilise la technologie numérique pour améliorer la fiabilité, la sécurité et l'efficacité (économique et énergétique) du système électrique, depuis la grande production jusqu'aux consommateurs et un nombre croissant des ressources de génération distribuée et de stockage. [A. B. M. S Ali, 2013]

c. Définition 3 :

Le Smart Grid est la nouvelle forme de réseau électrique avec un contrôle de flux d'haute-fidélité, auto-guérison, la fiabilité énergétique et la sécurité énergétique à l'aide des communications numériques et de la technologie de contrôle. [Ye.Yan et all ,2012]

Le concept de Smart Grid regroupe un certain nombre de technologies, de solutions clients et répond à plusieurs facteurs stratégiques et réglementaires. Il est défini comme étant un réseau électrique intelligent qui utilise la détection, le traitement intégré et les communications numériques pour permettre au réseau électrique d'être observable (mesurable et visualisé), contrôlable (manipulable et optimisé), automatisé (Auto-réparé), entièrement intégré et entièrement interopérable avec les systèmes existants et avec la capacité d'intégrer un ensemble diversifié de sources d'énergie. [A. B. M. S Ali, 2013]

[1]**La plate-forme technologique européenne PTE :** sont des entités indépendantes et autofinancées. Ils mènent leurs activités de manière transparente ; sous forme des forums d'acteurs dirigés par l'industrie, reconnus par la Commission européenne comme des acteurs clés de l'innovation, du transfert des connaissances et de la compétitivité européenne.

d. Définition 4 :

Le Smart Grid (SG) est la génération suivante de réseaux électriques, où la transmission, la distribution, la production d'énergie, l'utilisation et la gestion sont entièrement retravaillées pour améliorer l'efficacité, l'agilité, l'environnement, l'économie, la sécurité et la fiabilité.

Il offre une communication bidirectionnelle entre les stations de base et les sites de production d'énergie, et optimise les performances globales du système en profitant des réseaux de capteurs sans fil (WSNs) en utilisant des capteurs intelligents et en mettant en œuvre des solutions d'énergie renouvelable.

Étant donné que ces SG se composent de nombreuses applications différentes avec des exigences différentes en matière de communication et de qualité de service (QoS), elle implique des technologies de communication hétérogènes basées sur une infrastructure de communication multicouche. [HUSSEIN T.MOUFTAH et al, 2016]

Il est possible d'affirmer que les réseaux électriques intelligents ou « Smart Grids » sont des réseaux électriques qui grâce à des technologies informatiques, ajustent les flux d'électricité entre fournisseurs et consommateurs.

Ils seront capables de surveiller et de contrôler le débit d'électricité en temps réel. Ils fournissent également plus de contrôle, où ils sont capables de traiter plus d'informations, ce qui offre de nombreux avantages pour les consommateurs. Ces réseaux offrent une alternative plus efficace et plus fiable, plus propre et plus sûre et sécuritaire au système de réseau actuel.

Les réseaux intelligents sont des réseaux électriques qui favorisent un fonctionnement énergétiquement efficace et rentable pour les besoins futurs. Grâce à une gestion coordonnée, ils utilisent une communication bidirectionnelle en temps réel entre : [w2]

- Les composants des réseaux ;
- Les producteurs ;
- Le stockage ;
- Les consommateurs.

2.2.2. Caractéristiques

L'une des principales caractéristiques des Smart Grids est la communication à double sens ou autrement dit « Bidirectionnelle » entre les fournisseurs d'électricité et leurs clients consommateurs. Ce réseau de communication sera construit pour permettre ce concept de transmission.

Comme il devient possible d'extraire les quatre caractéristiques suivantes :

- **La flexibilité** : ils permettent de gérer plus finement l'équilibre entre la production et la consommation ;
- **La fiabilité** : ils améliorent l'efficacité et la sécurité des réseaux électriques;
- **L'accessibilité** : ils favorisent l'intégration des sources d'énergies renouvelables sur l'ensemble du réseau ;
- **L'économie** : 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).

En bref, un Smart Grid utilise des produits et des services innovateurs avec des technologies intelligentes de surveillance, de contrôle, de communication et des technologies d'auto-guérison.

La littérature suggère les attributs suivants des Smart Grids : [A. B. M. S Ali, 2013]

- Un Smart Grids permet aux consommateurs de jouer un rôle dans l'optimisation du fonctionnement du système et il fournit aux consommateurs une plus grande information et le choix des offres.
  - ✓ Ils permettent de répondre à la demande et de gérer la demande en intégrant les compteurs intelligents, les appareils intelligents, la micro-génération et le stockage de l'électricité (véhicules électriques) toute en fournissant aux clients des informations sur la consommation d'énergie et des prix.
  - ✓ Il est prévu que les clients recevront des informations et des incitations pour modifier leur mode de consommation afin de surmonter certaines des contraintes du système d'alimentation.
- Les smart Grids facilitent la connexion et le fonctionnement des générateurs selon ces différentes tailles et ces différentes technologies comme ils permettent des options intermittentes de génération et de stockage.

- ✓ Ils accueillent toutes les sources d'énergie renouvelables, la production distribuée, la micro-génération résidentielle et les options de stockage, réduisant ainsi considérablement l'impact environnemental de l'ensemble du système d'approvisionnement en électricité. Il fournira une interconnexion simplifiée semblable à «plug-and-play».

- Ils optimisent et gèrent efficacement les actifs par une exploitation intelligente du système de livraison (redirection, fonctionnement autonome) et une gestion efficace des actifs. Cela comprend l'utilisation d'actifs en fonction de ce qui est nécessaire et quand il est nécessaire.

- Ils opèrent de manière résiliente dans les catastrophes, les attaques physiques ou les cyber-attaques et offrent des niveaux accrus de fiabilité et de sécurité d'approvisionnement en énergie.
- Ils assurent et améliorent la fiabilité et la sécurité de l'approvisionnement en anticipant et en répondant de manière auto-guérissant et en renforçant la sécurité d'approvisionnement grâce à des capacités de transfert améliorées.

- Ils fournissent la qualité de l'alimentation électrique pour s'adapter à des équipements sensibles qui favorisent l'économie numérique.

- Ils ouvrent l'accès aux marchés grâce à des voies de transmission accrues, à des initiatives globales de réponse à l'offre et à la demande et aux services auxiliaires.

2.2.3. Pourquoi utiliser les Smart Grids ?

L'introduction de Smart Grid sur l'infrastructure du réseau électrique permettra : [A. B. M. S Ali, 2013]

- D’assurer la fiabilité de la grille à des niveaux inimaginables ;
- De tenir compte des progrès et des gains d'efficience encore à envisager ;
- D’exercer une pression à la baisse sur les prix de l'électricité ;
- De maintenir l'accessibilité financière des consommateurs d'énergie ;
- De fournir aux consommateurs une information et un choix ;
- De tenir compte des ressources énergétiques renouvelables et traditionnelles ;
- De permettre une meilleure pénétration des sources de production d'électricité intermittente ;

- De révolutionner non seulement le secteur des services publics, mais aussi le secteur d'intégration de véhicules électriques en tant que dispositifs de génération et de stockage ;
- De favoriser la qualité environnementale en permettant aux clients d'acheter une production plus propre et à faible émission de carbone ;
- Le déploiement de sources d'énergie renouvelables, et permettre l'accès à la production de stations centrales respectueuses de l'environnement.
- La satisfaction des consommateurs aux prix, ce qui réduira le besoin de capacités supplémentaires de production de carburant fossiles, réduisant ainsi les émissions de CO2 et les autres polluants.

2.2.4. Avantages & inconvénients

a. Les Avantages des Smart Grids

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. [w3]

Les Smart Grids ont aussi un avantage pour les consommateurs, car ils permettront d'avoir : [w4]

- Des maisons plus intelligentes,
- Des factures plus précises,
- Des pannes mieux détectées et plus rapidement réparées,
- Des offres tarifaires plus diversifiées.

b. Les inconvénients des Smart Grids

- Du côté de la mise en œuvre, le coût des investissements est élevé. Ainsi, ils doivent être implantés sur l'ensemble du réseau et impliqués tous les acteurs pour être efficaces ;
- 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 ;

- Le Problème de confidentialités des informations sur les horaires ou les activités des consommateurs et des producteurs. Donc il est nécessaire d'appliquer des normes sur la protection et la sécurité des données. [w3]

2.2.5. Architecture des Smart Grids

a. Architecture à niveaux :

Les Smart Grids ont une architecture à plusieurs niveaux pour fournir de l'électricité aux consommateurs. Cette architecture commence par la production d'électricité à partir des sources énergétiques et passe par les réseaux de transport jusqu'à la distribution, et finalement aux consommateurs comme il est illustré dans la figure 1.3.

Cette architecture est segmentée selon trois niveaux : [w5]

- **Le premier niveau** : montre l'infrastructure du réseau électrique en général, il se compose de matériels et d'équipements qui servent à l'acheminement d'électricité (lignes, transformatrices, etc.).
- **Le second niveau** : combine les architectures de communication (multi-supports et multi technologies) avec les données issues de différents capteurs réseau.
- **Le troisième niveau** : formé à l'aide des applications informatiques et des services, comme le monitoring, les systèmes d'intervention à distance, l'automatisation des réponses à la demande d'électricité en utilisant des informations en temps réel.

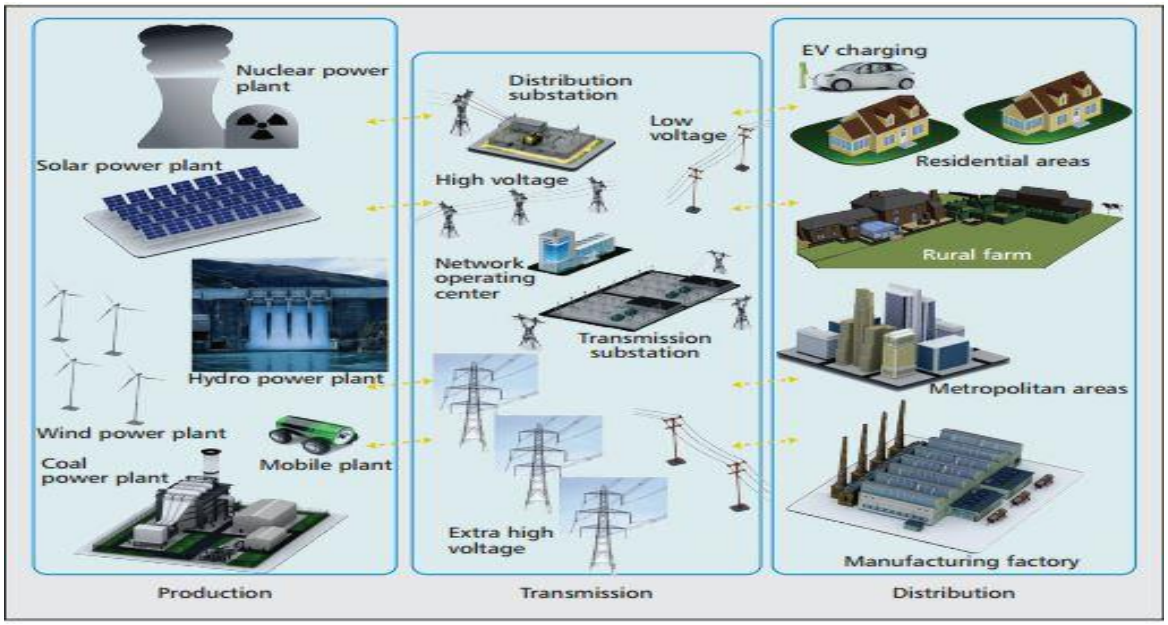

Figure 1.3 : *Architecture générale des Smart Grids. [B.-H. Elias, 2013]*

Les Smart Grids s'efforcent d'utiliser et de coordonner la génération diverse et des mécanismes de production. De plus, les usines de production peuvent être mobiles ou fixes selon des architectures spécifiques. Du côté de la transmission, un grand nombre de sous-stations et de centres d'exploitation de réseau gèrent cette tâche.

Un grand nombre de lignes de tension mixtes transmettent l'électricité produite de diverses sources à l'architecture de distribution.

Enfin, un ensemble de topologies de distribution complexes délivre l'électricité aux régions, aux voisins et aux lieux d'utilisation et de consommation.

b. Les standards

Plusieurs organismes de standardisation ont défini des standards pour le déploiement des Smart Grids. L'organisme américain «National Institute of Standards and Technology» NIST a défini une architecture pour les Smart Grids. De plus l'organisme américain IEEE « Institute of Electrical and Electronics Engineers » a défini les trois couches de ce type de réseaux. Il a ajouté le concept de la gestion centralisé de l'énergie renouvelable. Dans cette section, nous allons détailler l'architecture proposée par NIST, ainsi que l'architecture proposée par l'IEEE.

b.1. L'architecture proposée par NIST :

L'organisme américain «National Institute of Standards and Technology/ NIST a proposé une architecture de base pour les Smart Grids. Cette architecture comporte sept domaines présentés dans la figure 1.4 « distribution, transmission, client consommateur (customer), marchés (markets), opérations (opérations), production en vrac (bulk Generation), fournisseurs de services (service provider) [w6].

- **Le domaine des clients consommateurs (Customer) :** Le domaine de la clientèle contient les utilisateurs finaux de l'électricité. Il peut également générer, stocker et gérer l'utilisation d'électricité. Il est divisé en trois sous-domaines : Résidentiel (Home), Commercial (Building/commercial) et Industriel (Industrial) [w6]. Il contient plusieurs composants par exemple :
  - ✓ **Les compteurs intelligents ou les Smart Meters :** Un smart meter (compteur intelligent) est un appareil de mesure d'électricité. Il intègre des technologies avancées pour mesurer de manière efficace, fiable et en temps réel l'électricité consommée et produite par un client dans un réseau décentralisé.

Les compteurs intelligents peuvent être utilisés pour contrôler la lumière, la chaleur, la climatisation et d'autres appareils. En outre, les compteurs intelligents peuvent être programmés pour maintenir un horaire pour le fonctionnement de l'électroménager et le contrôle de fonctionnement des autres dispositifs. [S.Shekara, 2011]

- ✓ **Appareils domestiques (Home devices) :** désignent l'ensemble des dispositifs (Thermostats, chauffe-eau, réfrigérateur, machine à laver…) qui sont utilisés au sein d'une maison.
- ✓ **Ressource énergétiques distribuées DER (Distributed Energy Ressources) :** DER est définie comme une ressource reliée au réseau de distribution d'électricité. Ils sont de petites sources de production et de stockage d'électricité qui sont connectés au réseau de distribution. Les utilisateurs peuvent être équipés d'une source d'électricité renouvelable (panneaux solaires ou une éolienne) pour produire de l'électricité. [S .salinas et al ,2013]

- **Le domaine du marché (Markets) :** ce domaine contient les exploitants et les acteurs des marchés de l'électricité. Il se compose de détaillants qui fournissent de l'électricité aux utilisateurs, fournisseurs, et commerçants. [W .wang et al ,2011]

- **Le Domaine de la Transmission :** Il contient les transporteurs de grandes quantités d'électricité sur des longues distances [w6].

  L'électricité produite est transmise au domaine de la distribution par l'intermédiaire de multiples sous-stations et lignes de transmission. La transmission est généralement exploitée et gérée par un opérateur de transport régional RTO[2] (Regional Transmission Operator) ou un opérateur de système indépendant ISO (Independent System Operator). [W .wang et al ,2011]
- **Le domaine de la distribution :** Ce domaine contient les distributeurs d'électricité . L'envoi de l'électricité aux utilisateurs finaux et mis en œuvre en faisant usage de l'électricité et l'infrastructure de communication qui relient les domaines de transmission et les clients, il interagit avec les capteurs à travers une interface de communication.

  Le domaine de la distribution prend la responsabilité de délivrer l'électricité aux consommateurs en fonction des demandes des utilisateurs et la disponibilité d'électricité. [W .wang et al ,2011]

[2]Le RTO est responsable de maintenir la stabilité des lignes de transport régionale en équilibrant entre l'offre et la demande. Pour réaliser des fonctions de guérison de soi, beaucoup d'informations sont capturées à partir du réseau et transmettre aux centres de contrôle.

- **Le domaine d'opérations :** ce domaine contient les gestionnaires de la circulation d'électricité. Les acteurs dans le domaine des opérations sont responsables du bon fonctionnement du système d'alimentation. Ce domaine gère les opérations efficaces et optimales des domaines de transmission et de distribution à l'aide d'un système de gestion d'énergie EMS (Energy Management System) dans le domaine de la transmission et un système de gestion de distribution DMS(Distribution Management System) dans le domaine de la distribution. [W .wang et al ,2011]
- **Le domaine des fournisseurs de services (Service Provider) :** ces fournisseurs sont responsables sur la fourniture d'électricité aux clients consommateurs et aux services publics.

  Ils gèrent des services comme la facturation et la gestion des profils des clients pour les entreprises de services publics.

  Ce domaine communique avec le domaine d'opérations pour obtenir les informations de consommation ainsi que les informations de connaissance de la situation et de contrôle du système. Il doit également communiquer avec les réseaux HAN dans le domaine de la clientèle grâce à l'interface ESI (Energy Services Interface) pour fournir des services intelligents comme la gestion des utilisations d'énergie. [W .wang et al ,2011]
- **Le domaine de la production en vrac (Bulk Generation) :** Ce domaine contient les grands producteurs d'électricité. L'électricité est produite en utilisant les ressources énergétiques non renouvelables comme le pétrole, le charbon, fission nucléaire, etc ; et renouvelables comme l'eau qui coule, la lumière du soleil, le vent, etc.

  Ce domaine peut également stocker l'électricité pour gérer la variabilité des ressources renouvelables telles que, le surplus d'électricité qui est stocké pour la redistribution en période de pénurie des ressources.

  Ce domaine est connecté au domaine de la transmission. Il comprend des équipements électriques, y compris les contrôleurs logiques programmables, les moniteurs d'équipement, et les enregistreurs de défauts. [W .wang et al ,2011]

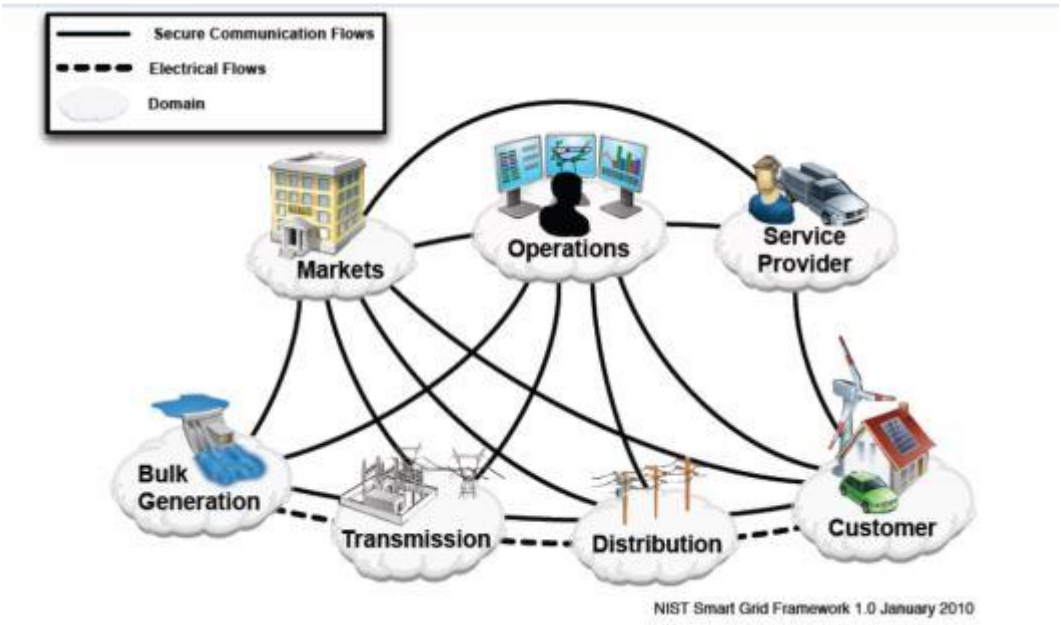

Figure 1.4 :*l'architecture Smart Grid proposée par NIST. [W .wang et al ,2011]*

b.2. L'architecture proposée par IEEE :

Dans l'architecture de NIST, chaque consommateur peut produire de l'électricité en utilisant les ressources renouvelables. Le surplus d'électricité produite est géré par le consommateur lui-même et la gestion de ce dernier est décentralisée.

En raison de la complexité de la tâche de la gestion, l'IEEE a proposé une architecture basée sur celle de NIST, mais elle définit un nouveau domaine nommé Distributed Energy Resources (DER) qui permet de gérer le surplus d'électricité produite, de sorte que cette gestion est centralisée [w7]

En outre l'IEEE a fourni des lignes directrices permettant de comprendre et de définir l'interopérabilité des Smart Grids. Elle définit trois perspectives architecturales intégrées : la couche énergie, la couche communication et la couche information tel qu'il est illustré dans La figure 2.3 qui présente l'extension européenne du modèle NIST. [w7]

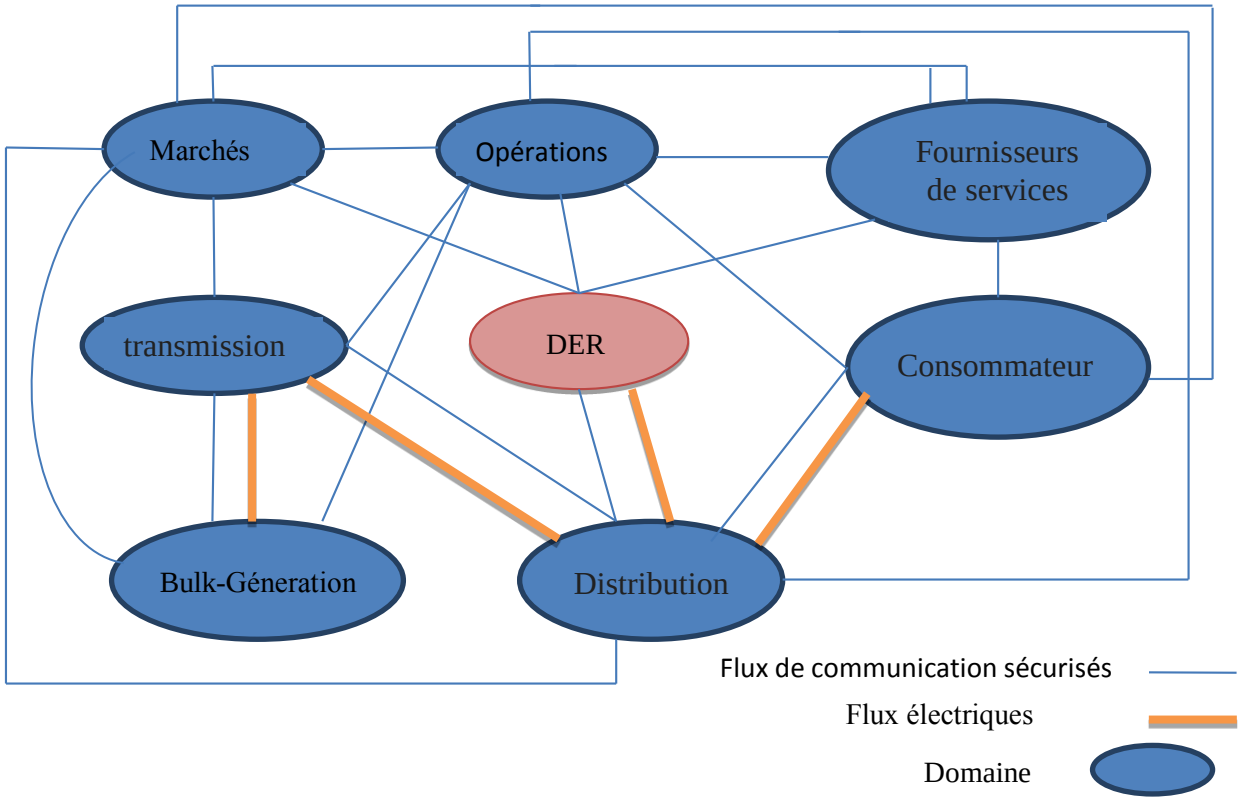

Figure 1.5 : *Extension européenne du modèle NIST. [w7]*

- **La couche d'énergie :** malgré la complexité des smart grids, cette couche offre une interopérabilité au système électrique ; elle a pour objectif d'assurer l'alimentation électrique à tous les clients consommateurs avec une haute fiabilité et disponibilité, de qualité de puissance élevée, et à un coût qui rend l'électrique une forme économique d'énergie.
- **La couche de communication** : Cette couche couvre les réseaux de communication avec les technologies utilisées dans le Smart Grid ; tel que les informations utilisées pour la surveillance et le contrôle.
- **La couche d'information :** L'IEEE SGIRM (Smart Grid Interoperability Reference Model) représente le Smart Grid du point de vue des applications informatiques et des flux de données associées à ces applications qui sont utilisées pour faire fonctionner et gérer le système d'alimentation avec un objectif principal de permettre l'interopérabilité indépendamment des systèmes développés.

L'objectif de l'IEEE n'est pas de définir une nouvelle architecture d'échange d'informations, mais plutôt de travailler avec les meilleures pratiques et technologies actuelles. Encore pour identifier et combler les lacunes d'échange d'informations nécessaire entre les sept domaines. Des efforts explicites ont été faits pour adopter la terminologie utilisée par NIST et le Groupe de Smart Grid Interoperability afin d'assurer un cadre architectural cohérent pour le Smart Grid. [IEEE Standards Association et al, 2011].

C. Les applications utilisées dans les Smart Grid

Le Smart Grid est équipé d'un nombre énorme d'applications qui contribuent à un ou plusieurs objectifs ; comme le déploiement à grande échelle des sources d'énergie propre et la gestion efficace de l'énergie.

Dans cette section, nous allons détailler certaines de ces applications, en les classant en trois catégories les applications de contrôle, les applications de gestion d'électricités et les applications dans les réseaux domestiques.

C.1. Les applications de contrôle :

Parmi Les applications de contrôle qui ont un rôle important dans les réseaux Smart Grid on trouve :

- **Dynamic Pricing :** Cette application envoie aux consommateurs les prix horaires d'électricité. Elle aide les utilisateurs à diminuer leur montant de facturation par la réduction des charges pendant les heures de pic de consommation. [Shengrong Bu et al ,2011]. Par exemple, elle offre aux consommateurs la possibilité de planifier les activités de ménage dans les heurs non critique, où le prix de l'énergie est moins cher (exemple : du lundi à vendredi de 8h à 12h du matin puisque la consommation est généralement faible dans cette période).
- **Demand Response (DR) :** cette application (DR) se rapporte à la gestion d'une demande accrue de réduction de la demande ou d'augmentation de l'électricité fournie à la grille. Elle assure la stabilité du réseau électrique pendant les heures où la demande d'électricité est plus élevée).

  Elle permet d'avoir une meilleure gestion des ressources énergétiques et de minimiser les risques de panne. [W .wang et al, 2011]
- **Outage Management :** Cette application permet de contourner les pannes au sein du réseau électrique [Wayes Tushar et al ,2012]. Elle peut évaluer toutes les actions de commutation possible d'isoler une défaillance permanente et de restaurer le service électrique le plus rapidement possible.

- **Automatic Meter Reading(AMR) :** AMR est connu aussi sous le nom de Smart Meter Measurements [Kenneth_C._Budka et al, 2014]. Elle assure la collecte automatique et périodique des taux de consommation.

  Cette application empêche les consommateurs illégaux de contourner ou trafiquer le compteur [Q GAO et al, 2008]. Les acteurs de cette application sont le Smart Meter et le centre contrôle (control center) [Ishtiaq Rouf et al, 2012].

- **Remote Switching:** Dans la littérature [Yasir Arafat et al, 2014], Remote Switching a plusieurs nominations comme "remote ON/OFF switch" et "remote connect / disconnect".

  Cette application peut être utilisée surtout pour la coupure d'électricité à distance :

  - ✓ Couper l'alimentation aux clients qui n'ont pas payé ;
  - ✓ Couper l'électricité dans les heures ou quelqu'un n'est pas présent dans le département. Cette fonction est paramétrable par le client, elle lui donne la possibilité de payer que son utilisation utile et se débarrasser des frais de consommation des voleurs d'électricité ;
  - ✓ Couper l'alimentation à un ensemble d'utilisateurs, si tous les consommateurs ne peuvent pas être servis (dans les heures, pique). Les utilisateurs sont choisis selon des critères (exemple : les utilisateurs âgé et malade sont exclus de la déconnexion). Lorsque la crise est terminée, les clients seront progressivement reconnectés au réseau ;
  - ✓ Couper l'alimentation lorsqu'il y a des pannes catastrophiques ;
  - ✓ …etc.

C.2. les applications de gestion d'électricités :

- **Distributed Generation (DG) :** ce type d'applications fait référence aux ressources de génération d'électricité chez les consommateurs. Ils sont fondés sur les sources d'énergies renouvelables (solaires, les éoliennes. . .). Les sources DG sont déployées pour prendre en charge les besoins énergétiques de leur propriétaire. Ils sont connectés directement au système de transmission. [Kenneth_C._Budka et al, 2014]
- **Distributed Storage DS :** Le terme stockage distribué 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'électricité 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. [Kenneth_C._Budka et al, 2014]

- **Distribution Automation (DA) :** l'automatisation de la distribution se réfère à l'automatisation de toutes les fonctions liées au système de distribution à travers les données recueillies par les dispositifs de sous station. [Kenneth_C._Budka et al, 2014]

C.3. Les applications dans les réseaux domestiques :

- **Chargement des véhicules électriques :** Les batteries des véhicules électriques (EV) peuvent être rechargées à partir d'une infrastructure de recharge.

  Les EV reçoivent l'énergie électrique à partir de la grille ou des lignes électriques à usages spéciaux. [Kenneth_C._Budka et al, 2014]

2.2.6. Les acteurs principaux qui ont une influence sur les Smart Grids

Parmi les acteurs qui ont un rôle renforcé dans les Smart Grids, on peut citer : [w8]

- **Les consommateurs :** Les utilisateurs finaux qui sont au cœur des réseaux électriques. L'évolution de ses comportements, que ce soit en matière de la demande (consommation) ou d'offre d'électricité (production), aura un impact sur le fonctionnement global du système électrique.

  Ainsi, la flexibilité de la demande, de la production décentralisée ou du stockage des consommateurs, contribue significativement à l'équilibre offre/demande du système électrique.
- **Les producteurs d'électricité** : qui alimentent les réseaux de transport d'électricité et qui sont capables de répondre en temps réel à la demande ;
- **Les gestionnaires des réseaux de transport et de distribution** :
- **Les constructeurs de matériel électrique** : qui gèrent et installent les équipements de mesure et assurent la protection et le fonctionnement des réseaux électriques ;
- **Les gestionnaires des outils informatiques** : tel que les processeurs et les systèmes informatiques comme info vista, Intel, Google ou Cisco System ; ces gestionnaires sont responsables sur le développement des technologies d'information indispensables au fonctionnement des réseaux électriques intelligents ;
- **Les pouvoirs publics :** ces acteurs 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.

2.2.7. FONCTIONNEMENT DES SMART GRIDS

Les Smart Grids associent l'infrastructure électrique aux technologies numériques qui analysent et transmettent l'information reçue ; dont elle est utilisées à tous les niveaux du réseau : production, transport, distribution et consommation. [w8]

a. Concernant le flux électrique :

- **L'interopérabilité des réseaux :** La grille 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 favorisent une interopérabilité entre les gestionnaires du réseau de transport et ceux du réseau de distribution.

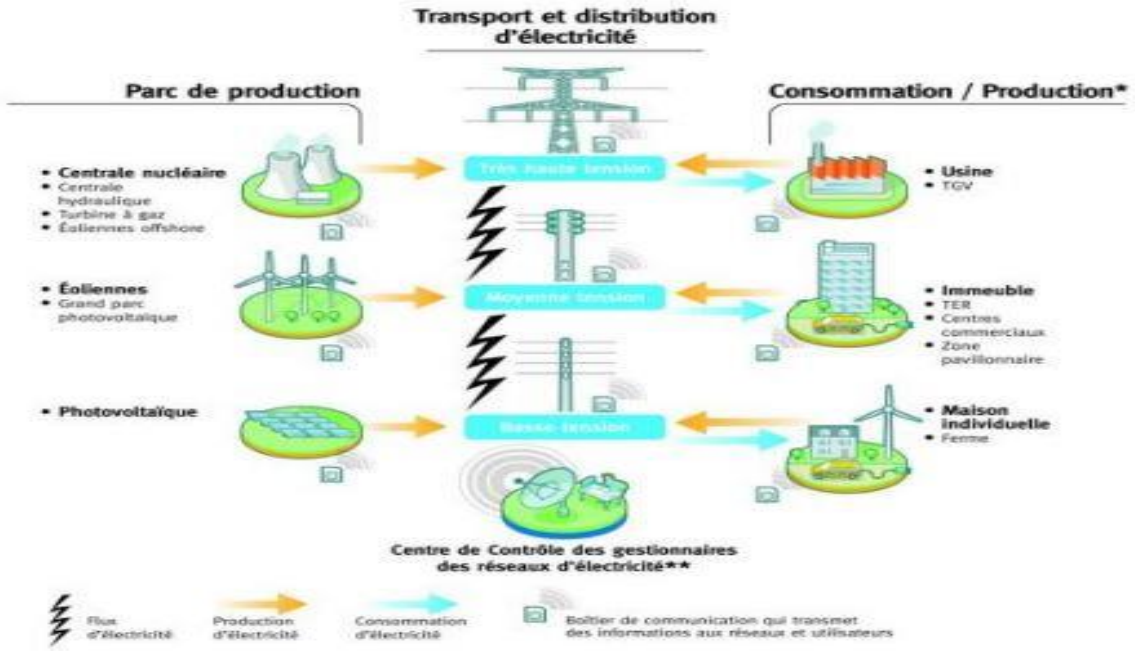

Figure 1.6 : *schéma illustrant la transmission d'électricité dans les Smart Grids***.**

- **L'intégration des énergies renouvelables au réseau :** Les Smart Grids 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 peuvent ainsi être mieux gérées.

b. Concernant le flux de données :

- **Un contrôle des flux en temps réel :** Avec des capteurs installés sur l'ensemble du réseau indiquant 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 l'envoyer des signaux de prix aux particuliers pour adapter leur consommation d'une façon automatique.
- **Une gestion plus responsable des consommations individuelles :** Les compteurs communicants (ou compteurs évolués, ou les smart meters) sont les premières versions d'application du réseau électrique intelligent.

  Ces smart compteurs sont installés chez les consommateurs, ils fournissent des informations sur les prix, la qualité et le niveau de consommation d'électricité du foyer, comme l'illustré la figure 1.7.

  Les consommateurs peuvent alors réguler eux-mêmes leur consommation au cours de la journée. De leur côté, et les opérateurs du réseau peuvent détecter plus vite les pannes.

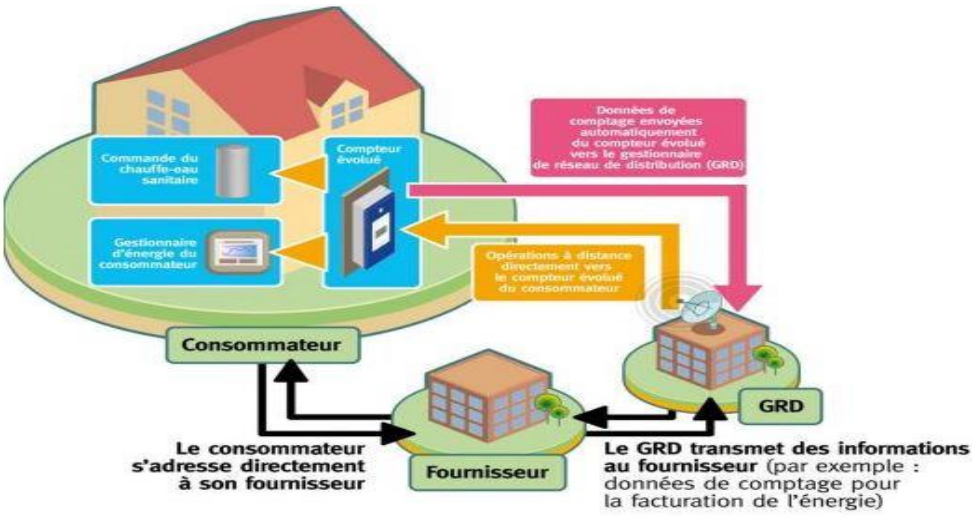

Figure 1.7 : *schéma illustre la transmission d'informations entre les smart meters et Le gestionnaire du réseau de distribution GRD dans les Smart Grids.*

2.3. Smart Grid vs réseau électrique classique

De nombreuses questions contribuent à l'incapacité de la grille traditionnelle à la demande pour une alimentation électrique cohérente. Ce tableau contient une comparaison entre les caractéristiques générales de la grille traditionnelles avec la grille intelligente. [A. B. M. S Ali, 2013]

Tableau 1.1 : *Tableau comparatif entre le Réseau électrique classique et le Smart Grid.*

Réseau électrique classique	Smart Grid
• Électromécanique ; • Communication unidirectionnelle et bidirectionnelle locale ; • Génération centralisée ; • Systèmes de protection, de surveillance et de contrôle limités 'Aveugle' ; • Restauration manuelle ; • Vérifier l'équipement manuellement ; • Contingences limitées du système de contrôle ; • Fiabilité estimée.	• Numérique / microprocesseur ; • Communication bidirectionnelle globale intégrée ; • Adapte la production distribuée ; • WAMPAC, Protection adaptative ; • Surveillance Automatique ; • Auto-guérison ; • Surveillance d'équipement à distance ; • Système de contrôle envahissant ; • Fiabilité prédictive.

II. Les Système de supervision au sein des Smart Grid

Les systèmes de supervision / SCADA sont des systèmes de contrôle/commande qui permettant de superviser et de prendre en main un système industriel complet à distance.

À partir des années 1960 et avec l'augmentation du besoin de la surveillance et du contrôle des équipements industriels, le système SCADA est devenu très populaire.

Les systèmes de supervision tel que le système SCADA représentent un système informatique de conduite qui nous permet de prendre en compte un système physique en temps réel via des **ordinateurs de contrôle** ou des **panels de supervision industriels**.

Le système de conduite, connu dans la littérature technique anglo-saxonne sous le nom de SCADA (Supervisory Control and Data Acquisition), il est conçu pour assurer une très haute disponibilité des fonctions de supervision et de décision.

Le système SCADA représente le cœur de la surveillance et du contrôle.

1. Le système de contrôle et d'acquisition de données (SCADA)

1.1. Définition et fonctions

Définition 1 : "SCADA" est le terme le plus connu pour représenter les systèmes d'information des industries et leurs composants informatiques. Le système SCADA fait partie d'une famille plus générale des systèmes de contrôle industriel ICS "Industrial Control System".

Il désigne le contrôle et l'acquisition de données. Il s'agit d'une classe de logiciels destinés au contrôle informatisé des processus industriel, il est utilisé pour recueillir et analyser les données en temps réel (collecte de données) dans le but de suivre, surveiller et contrôler les équipements industriels dans des différents types d'industries. [w15]

Définition 2 : SCADA est un système de contrôle central qui se compose d'interfaces réseau de contrôleurs, des outils d'entrées / sorties, des équipements de communication et de logiciels.

Ils sont utilisés pour surveiller et contrôler les équipements dans le processus industriel qui inclut la production, le développement et la fabrication.

Définition 3 : Un système de supervision/SCADA (anglais : **S**upervisory **C**ontrol And **D**ata **A**cquisition, sigle : SCADA) est un système de **contrôle/commande** permettant de superviser et de prendre en main un **système industriel complet à distance**. Avec le système de supervision SCADA, on peut donc simuler un système physique en temps réel via des **PCs de contrôle** ou des **panels de supervision industriels**.

Il s'agit d'un système de télégestion à grande échelle permettant de traiter en temps réel un grand nombre de télémesures et de contrôler à distance des installations techniques. C'est une technologie industrielle dans le domaine de l'instrumentation, dont les implémentations peuvent être considérées comme **des frameworks**[3] d'instrumentation incluant une couche de type **middleware**[4].

[3]**Frameworks :** C'est une structure logicielle qui désigne un ensemble d'outils et de composants logiciels structurels, elle est conçue et utilisée pour former l'architecture des logiciels applicatifs, des applications web, des middlewares et des composants logiciels. (Https://fr.wikipedia.org/wiki/Framework)

[4]**Middleware :** Système d'exploitation du serveur, il représente l'interface entre le dispositif (matériel) et le programme d'application (Dictionnaire informatique éditer par cyril serrano 2012)

Le système SCADA permet une exploitation en local, sur site d'une installation. Toutes les valeurs mesurées localement et en temps réel peuvent être visualisées. Dans cet objectif, des analyses de haute qualité, graphiques des flux et gestion intelligente des alarmes sont fournis.

Le système SCADA collecte des données de divers appareils d'une quelconque installation, puis transmit ces données à un ordinateur central, que ce soit proche ou éloigné, qui contrôle et supervise l'installation. Ce dernier est subordonné par d'autres postes d'opérateurs. Ce dernier est subordonné par d'autres postes d'opérateurs, l'allure générale d'un système SCADA est illustrée dans la figure ci-dessous.

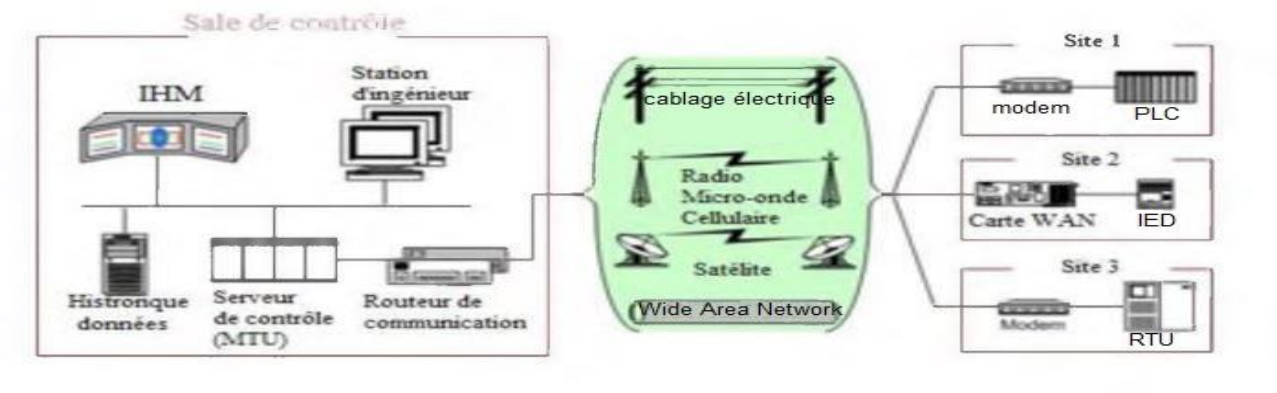

Figure 1.8 : *Schéma général d'un système SCADA. [w18]*

Les données sont enregistrées sur un serveur industriel sur site. Cela permet une gestion technique d'exploitation et une gestion des données indépendamment d'une connexion internet stable. Le système est modulaire : un certain nombre de stations peut être connecté afin d'assurer une sécurité maximale des données et leur sauvegarde, un serveur de secours additionnel peut être installé.

- Les fonctions principales du SCADA peuvent se résumer en :

- Acquisition et contrôle des données à distance ;
- Validation / invalidation des informations ;
- Traitement et surveillance ;
- Traitements des signalisations et des compteurs ;
- Gestion des éditions ;
- Gestion des alarmes ;
- Archivages et restitutions ;

- Télécommande ;
- Rapports et statistiques.

➢ **Pourquoi superviser ?**

- Contrôler la disponibilité de services / fonctions ;
- Contrôler l'utilisation des ressources ;
- Détecter et localiser les problèmes ;
- Faire le diagnostic des pannes ;
- Prévoir les évolutions ;

1.2. Domaines d'utilisation

Généralement les systèmes SCADA se trouvent dans différents contextes tels que la surveillance de processus industriels que ce soit :

- **Les centrales électriques :** La commande de la production d'énergie électrique ainsi que la distribution électrique ;
- **Les industries pétrolières :** Le domaine du pétrole et du gaz comme les canalisations de gaz et de pétrole ;
- **Les réseaux de chaleur ;**
- **Les télécommunications ;**
- **La gestion de l'eau :** Les systèmes d'approvisionnement d'eau (Eau et eaux usées)) ;
- **Le transport ;**
- **Les recherches et les études scientifiques et industrielles ;**
- **le Recyclage ;**
- **etc…**

1.3. Caractéristiques

Les fonctions principales d'un système SCADA se déroulent entre la surveillance, le contrôle et l'alarme des systèmes d'exploitation des installations à partir d'un emplacement centralisé. Ce système est généralement caractérisé par:

- La visualisation détaillée des données mesurées en temps réel
- Les alarmes permettent une identification rapide des pannes
- Graphique des flux de puissance, du niveau des chaînes au niveau de connexion moyenne ou haute tension
- Permets le déclenchement d'actionneurs
- Utilisation multi-écran et interface multilingue (IHM)
- Enregistrement des données redondantes à long terme sur site
- Possibilité d'incorporer un système de sécurité local (CCTV/ contrôle des barrières de sécurité, périmètre). [w19]

1.4. Architecture et composants

Le système SCADA généralement comporte deux couches, la première est la couche client qui est utilisée pour l'interface opérateur humain, et la seconde est la couche serveur de données qui gère les processus de contrôle du système.

Ce système fonctionne de manière multitâche sur la base d'un système de base de données en temps réel situé dans différents serveurs. (A, B. M. Shawkat Ali, 2013)

Les systèmes SCADA comprennent des composants matériels et logiciels. Les composants matériels collectent les données et les rassemblent sur un ordinateur équipé d'un logiciel SCADA. L'ordinateur traite alors ces données et les présente en temps opportun. En outre, le système SCADA enregistre et journalise tous les événements dans un fichier stocké sur un disque dur ou les envoie à une imprimante. [w20]

D'une manière générale, un système SCADA se compose :

1.4.1. Une Interface Homme-machine (IHM) :

C'est un dispositif d'entrée-sortie qui présente les données de processus à contrôler par un opérateur humain.

Les interfaces homme-machines (IHM) permettent de :

- Définir les moyens et outils mis en œuvre afin qu'un humain puisse contrôler et communiquer avec une machine. Les IHM sont généralement reliées à la base de données du système SCADA et à des programmes capables de calculer des tendances, sélectionner des données de diagnostic et des informations de gestion telles que les procédures d'entretien prévisionnelles, informations logistiques, des schémas détaillés d'un capteur ou d'une machine particulière, et d'un guide de dépannage basé sur un système expert.
- De fournir à la fois des vues graphiques de l'état des terminaux à distance et leurs historiques d'alarmes.
- De visualiser l'ensemble des données du procédé et d'intervenir à distance sur les machines. Il génère des rapports d'exploitation et de contrôle de données environnementales. Il archive la synthèse des données dans ses bases d'historiques.
- Représenter un système complet sous forme de synoptiques interactifs. L'opérateur peut donc visualiser en temps réel l'ensemble des alarmes, défauts et autres anomalies permettant une prise de décision rapide. [w18]

1.4.2. Unités de contrôle à distance (RTU) :

Les RTU « Remote Terminal Unit » sont des dispositifs électroniques reliant à des capteurs permettant la conversion des signaux analogiques en flux de données numériques et envoyant les données numériques au système de supervision. Elles sont conçues pour le contrôle et la supervision des grandes installations industrielles. Ces unités sont des unités de raccordement à distance, elles se connectent à des capteurs et des actionneurs dans le processus industriel.

Les RTU sont des «E / S intelligentes, elles ont des capacités de contrôle intégrées. Elles fournissent des solutions intégrées puissantes lors de la mise à niveau des équipements électriques installés à distance. Elles sont dotés de canaux d'entrée pour la détection ou la mesure et de canaux de sortie pour la commande, l'indication ou l'alarmes ainsi d'un port de communication. [w17]

1.4.3. Contrôleurs logiques programmables (PLC):

Les **PLC** « programmable logic controller »sont des automates industriels programmables ou **API**, dotés d'intelligence interne permettant le contrôle-commande d'effecteurs (moteurs, lampes, vannes etc..).

Ces API sont des ordinateurs numériques industriels constitués d'un CPU (contrôle process unit), d'une alimentation et de cartes d'entrée/sorties. Le CPU correspond au centre de traitement, il exécute le programme et scrute de manière cyclique l'ensemble des entrées/sorties afin de vérifier s'il y'a changement d'état afin de mettre à "0" ou à "1" à une sortie qui va commander via un pré actionneur un moteur ou une vanne. [w18]

Ils ont été développés pour des plateformes industrielles et ils ont démontré leurs fiabilités et la tolérance élevées pour la chaleur, la vibration, et l'interférence électromagnétique

Ces contrôleurs sont connectés au système de supervision de la même manière que les RTU. Ils sont connectés à des capteurs et des actionneurs dans le processus, fournissant une interface matérielle pour les capteurs d'entrée et les actionneurs de sortie.

1.4.4. Le système de supervision :

C'est la partie principale d'un système SCADA, elle représente le noyau de ce système. Le système de supervision est un logiciel spécifique qui se trouve dans un ordinateur conçu pour contrôler tous les autres périphériques connectés, exécuter des algorithmes, envoyer des commandes aux autres périphériques, etc.

Ce système de surveillance est utilisé comme un serveur de communication entre les équipements du système SCADA tels que les RTU, les PLC et les différents capteurs, ainsi que l'interface homme machine utilisé dans les postes de travail de la salle de contrôle.

Dans les systèmes SCADA les plus petits, la station maîtresse ou la station de supervision qui représente le dépôt des données collectées à partir des unités des terminaux distants qui y sont connectées, comprend un seul ordinateur de supervision, dans ce cas l'IHM fait partie de cet ordinateur.

Par contre, dans les systèmes SCADA les plus grands, la station maîtresse ou ce qu'on appelle la MTU [5] peut inclure plusieurs IHM hébergées sur des ordinateurs clients, plusieurs serveurs pour l'acquisition de données, des applications logicielles distribuées et des sites de reprise après les incidents ; pour augmenter l'intégrité du système.

Les systèmes SCADA de la dernière génération sont reliés aux capteurs et aux actionneurs via un réseau complexe de dispositifs très évolués et intelligents, comme le montre la Figure 1.9 : [w24]

- **Des processeurs frontaux (FEP « Front End Processors ») :** c'est un type particulier des processeurs qui s'appelle aussi les frontaux de télécommunication, ces processeurs assurent toutes les tâches de télécommunication auprès d'un ordinateur central. Ils fournissent une passerelle à partir des protocoles et des supports propriétaires utilisés par le réseau de capteurs au système informatique général qui exécute le système SCADA.
- **Des dispositifs électroniques intelligents (IED « Intelligent Electronic Devices ») :** Les IED sont de très petits systèmes informatiques dédiés qui se connectent directement aux capteurs et aux actionneurs et les contrôlent.

Un **IED** est un capteur / actionneur intelligent qui contient les informations nécessaires pour acquérir des données, communiquer avec d'autres appareils et effectuer des traitements et des contrôles locaux. Il peut combiner :

- ✓ un capteur d'entrée analogique ;
- ✓ une sortie analogique ;
- ✓ des capacités de commande de bas niveau ;
- ✓ un système de communication ;
- ✓ une mémoire de programme dans un seul appareil.

- **Des centres de commande de moteur (MCC « Motor Control Centers ») :** Les MCC sont des systèmes informatiques dédiés qui contrôlent les performances d'un moteur électrique.

[5] MTU : signifie l'abréviation du « Master Terminal Unit », elle représente la station maîtresse qui se connecte à plusieurs RTU, consolidant le contrôle et le trafic de données des RTU vers le système SCADA.

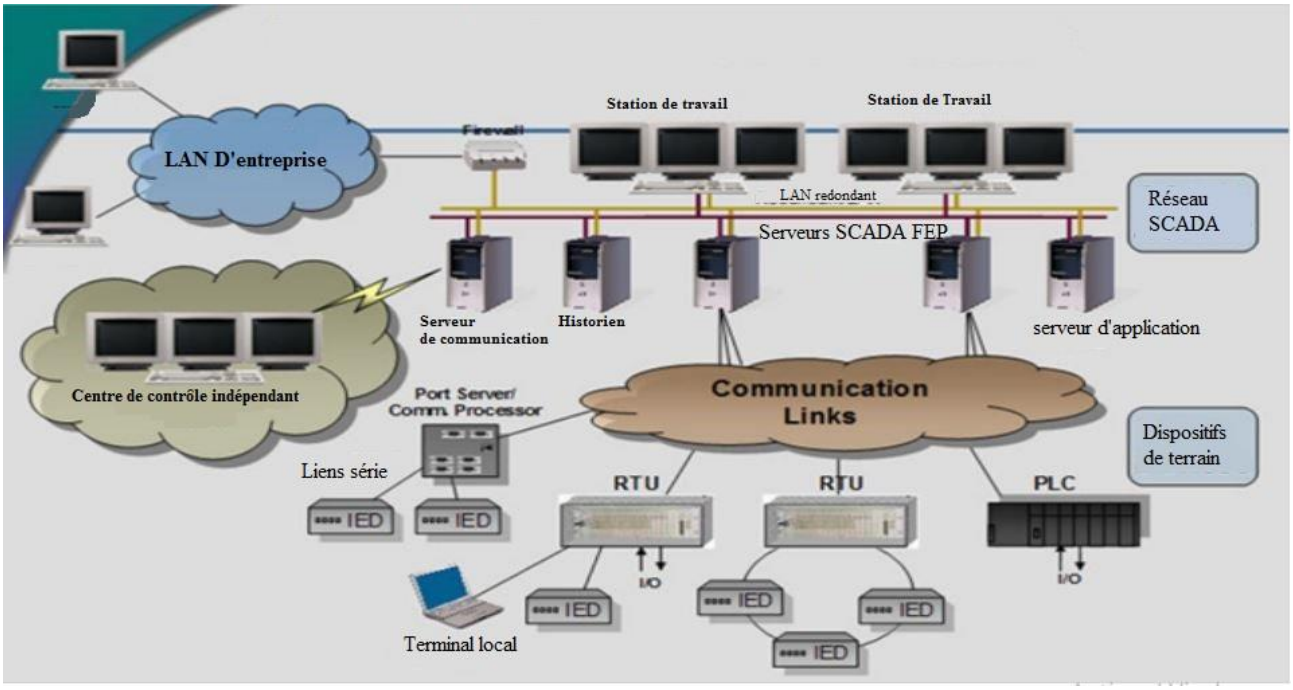

Figure 1.9 : *Représentation générale d'une architecture SCADA. [w24]*

1.4.5. Infrastructure de communication :

L'infrastructure de communication connecte le système informatique de supervision aux RTU et aux PLC à l'aide de l'utilisation des protocoles propriétaires industriels qui sont normalisés et reconnus par les fournisseurs SCADA.

Cette infrastructure relie un nombre énorme de dispositifs électriques et elle gère les communications compliquées entre ces derniers, elle est construite dans une architecture hiérarchique avec des sous-réseaux individuels interconnectés et chacun prenant la responsabilité de régions géographiques séparées.

Un exemple illustratif de cette architecture est représenté dans la Figure1.10, où A est une sous-station d'électricité, B est un segment de lignes de transmission d'électricité, C est une station de charge PEV, D est une subdivision résidentielle installée avec des panneaux solaires, E est un complexe résidentiel avec AMI, et F est une maison intelligente d'électricité avec des appareils électriques connectés au Smart Grids. (W. Wang et al, 2011)

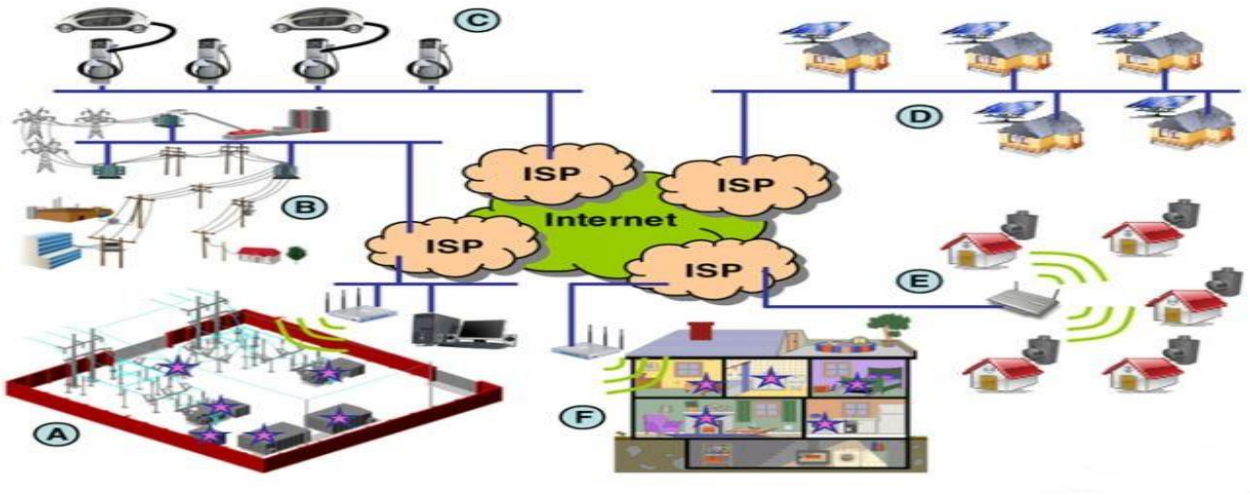

Figure 1.10 : *Un exemple d'architecture de communication dans les Smart Grids. (W.Wang et al ,2011)*

D'un point de vue topologique, les entités de communication dans le réseau électrique intelligent peuvent être classées en quatre types d'architectures réseau composé physiquement selon la distance et le débit de données, comme l'illustre la figure 1.11 : les réseaux de zone résidentielle ou bien les réseaux locaux (HAN/LAN), les réseaux de voisinage (NAN), les réseaux de zone (field area networks) et les réseaux étendus pour les grandes surfaces (WAN).

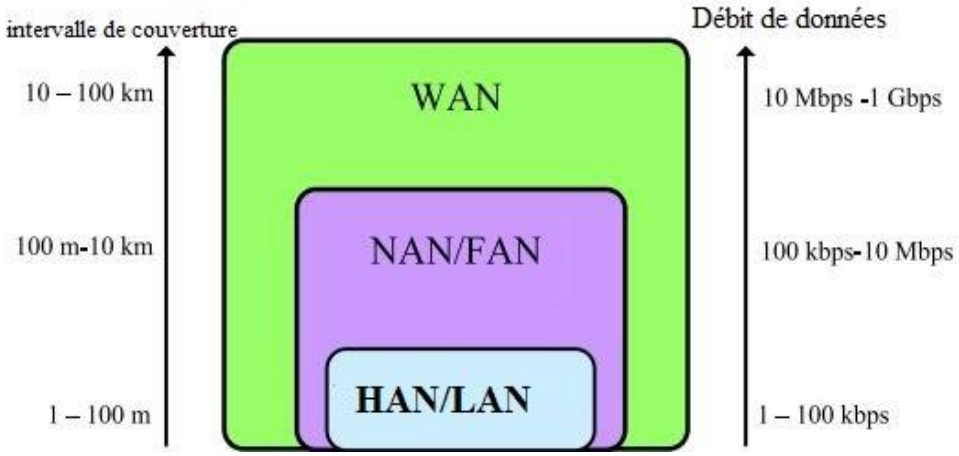

Figure 1.11 : *La décomposition de l'infrastructure de communication dans les smart grids.*

a. Les réseaux résidentiels (HAN) / les réseaux Locaux (LAN) :

Ce sont des réseaux de communication au sien d'une maison intelligente**,** ils représentent l'élément de base du système de réseautage des Smart Grid.

Le HAN est un réseau qui est déployé et exploité avec une couverture limitée, comme une maison ou un bureau. Il gère les communications entre les appareils domestiques et le compteur intelligent. Il est nécessaire dans les locaux des clients consommateurs pour l'implémentation de la surveillance et du contrôle des appareils intelligents et pour mise en œuvre des nouvelles fonctionnalités telles que la DR et l'AMI.

Le HAN est généralement géré par un système de gestion de l'énergie domestique HEMS (home energy management system) qui permet au processus de gestion de l'énergie d'être plus interactif et dynamique.

Il aidera à optimiser la consommation d'électricité pour assurer une facture minimale pour le consommateur. Par exemple, certaines tâches nécessitent des quantités d'électricité plus élevées, mais n'ont pas besoin d'être exécutées immédiatement, de sorte qu'elles peuvent être programmées automatiquement à un moment où le tarif énergétique est plus bas, c'est-à-dire pendant la nuit.

Un autre exemple est le nouveau véhicule électrique hybride rechargeable (PHEV), où la voiture peut être rechargée pendant la nuit lorsque le prix spot de l'électricité tombe à une certaine valeur qui peut être préréglée par l'utilisateur. (A. B. M. Shawkat Ali, 2013)

Dans les locaux des clients, une interface des services énergétique appelée ESI (Energy services interface) agit comme une interface de communication bidirectionnelle sécurisée entre l'utilitaire et le client consommateur. Elle peut être reliée au compteur intelligent soit par câblage fixe soit par l'intermédiaire des réseaux locaux.

L'ESI reçoit également les Prix en temps réel (RTP: Real Time Pricing) de l'utilitaire sur l'infrastructure AMI pour les fournir aux clients. Cette ESI peut prendre en charge différents types d'interfaces, comme :

- **L'interface interactive sécurisée :** pour les communications bidirectionnelles sécurisées ;
- **L'interface de diffusion publique d'utilité :** pour la réception unidirectionnelle des signaux d'événement et de prix aux dispositifs du client.

On outre, les clients peuvent utiliser un panneau d'affichage à domicile IHD (In-home display) relié à cette l'ESI et répondre aux signaux de tarification de l'utilitaire.

La Figure 1.12 montre un schéma synoptique d'un réseau HAN, tel que les appareils électroménagers seront connectés au compteur intelligent qui transférera d'abord les données de mesure vers le hub domestique, puis vers l'entité de gestion centrale.

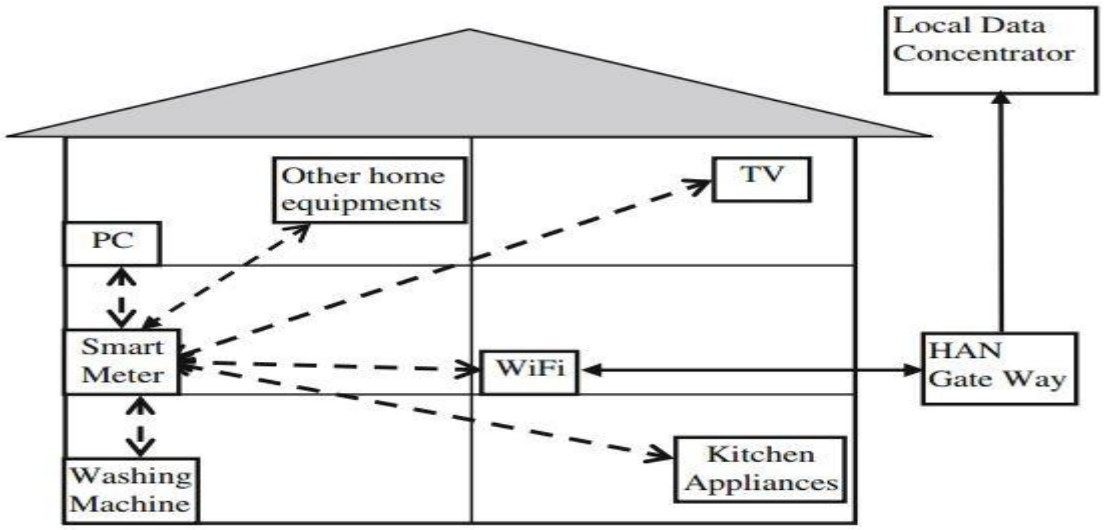

Figure 1.12 : *Un schéma illustratif d'un HAN (Ye Yan, and all, 2013).*

Le HAN peut utiliser différentes technologies de communication telles que : [Murat Kuzlu et al ,2014]

- **IEEE 802.15.4 (ZigBee)[6] :** est une norme qui spécifie la couche physique et le contrôle d'accès aux médias pour les réseaux personnels sans fil. C'est la technologie la plus adapté pour les réseaux HAN. [Murat Kuzlu et al ,2013]
- **IEEE 802.11 (LAN sans fil « Wireless LAN (WLAN) » ou Wi-Fi) :** est une norme sans fil développé par la Wi-Fi Alliance. Les plus populaires parmi ces versions sont IEEE 802.11b et IEEE 802.11g. La dernière version est la norme IEEE 802.11n.. [Ahmad Usman, Sajjad Haider Shami ; 2013]

[6]**ZigBee:** est une technologie populaire de faible puissance de communication sans fil développé par la ZigBee Alliance. Il offre de faibles débits jusqu'à 300 kbps et il est très populaire dans les applications domestiques(les applications HAN). **[Ahmad Usman, Sajjad Haider Shami ; 2013]**

b. Les réseaux de voisinage NAN " Neighborhood Area Network " :

D'une manière générale le réseau NAN connecte plusieurs HAN à des points d'accès locaux qui sont des concentrateurs locaux de données (LDC).

Ces concentrateurs ont la responsabilité d'accumuler des données provenant de diverses lectures de compteurs à différents moments de la journée. Ils jouent également un rôle essentiel dans la gestion de la réponse à la demande DR, car ils permettent à l'entité centrale d'exploiter les données en interprétant les modèles d'utilisation, de sorte que des stratégies de facturation appropriées puissent être développées pour distribuer la demande sur une période de temps défini. (A, B. M. Shawkat Ali, 2013)

Le NAN couvre les communications entre les compteurs intelligents dans une zone géographique spécifique [Thomas Basso , Richard DeBlasio;2011]. D'une part, il permet aux périphériques dans une petite zone, comme un quartier de communiquer entre eux. Par exemple, tous les compteurs intelligents dans un quartier peuvent communiquer entre eux à l'aide d'un routeur pour former un maillage interconnecté de périphériques intelligents. D'autre part, il permet de collecter de façon fiable le trafic des maisons intelligentes et le transmettre au centre de contrôle, à travers la collecte des informations sur la consommation d'électricité des HAN et de les stocker dans les LDC.

Le NAN prend en charge plusieurs applications et peut utiliser les réseaux sans fil ou câblés (ligne électrique, fibre, paire torsadée, etc.).

Il est le responsable sur le transfert des relevés de consommation à partir des compteurs intelligents au centre de contrôle.

c. Le réseau de Zones FAN « Field Area Networks » :

Le FAN est un composant essentiel de l'infrastructure des Smart Grid. Il forme le moyen de communication pour les systèmes de distribution d'électricité [w .wang et al ,2011].

Il est constitué de plusieurs NAN ainsi que quelques autres dispositifs .Ce réseau couvre le signal de l'état des équipements critiques du système de distribution en cas de panne ; tout en agissant comme un pont pour les données du compteur à la sous-station (substation). Il est nécessaire pour automatiser le système de distribution du Smart Grid. [R KOPMEINERS et al ,2014]

Pour le réseau FAN la technologie la plus adaptée est la technologie WIMAX [7] .

d. Les réseaux Etendus WAN « Wide Area Network » :

Les réseaux étendus sont des réseaux à grande surface, ces derniers forment l'épine dorsale du réseau de communication, pour connecter des petits réseaux hautement distribués. Ils permettent de connecter les réseaux du Smart Grid au centre de contrôle.

Le WAN est un réseau qui permet aux périphériques dans une grande zone géographique de communiquer entre eux.

Par exemple, plusieurs lecteurs de données de mesure, plusieurs lecteurs de compteurs mobiles et les dispositifs d'automatisation de sous-stations peuvent envoyer des informations aux bureaux d'utilité sur un WAN.

Lorsque les centres de contrôle sont situés loin des stations ou des consommateurs finaux, les mesures en temps réel pris sur les dispositifs électriques sont transportées vers ces centres de contrôle par l'intermédiaire des réseaux étendus (Ye Yan, and all, 2013).

Le WAN se compose de plusieurs HAN et NAN comme l'illustre dans la figure1.13, il fournit des liens de communication entre les NAN et les systèmes d'utilité pour le transfert des informations. De plus il comprend d'autres entités comme les Contrôleurs de la charge directe LDC et le contrôleur central. Il maintient les communications entre toutes les autres entités telles que les unités de production et de distribution. (A, B. M. Shawkat Ali, 2013)

[7]**WiMAX(World wide Interoperability for Microwave Access)** est une technologie de communication développée sous la norme de haut débit sans fil l'IEEE 802.16.La technologie WiMAX utilise deux bandes de fréquences (11-66 GHz et 2-11GHz). Elle est spécifiquement conçue pour les communications point à multipointdes applications fixes et mobiles avec des taux de donnés jusqu'à 70 Mbps sur unedistance de 50 kilomètres. Cette technologie est considérée comme une solution de backbone pour le Smart Grid [w.wang et al ,2011]

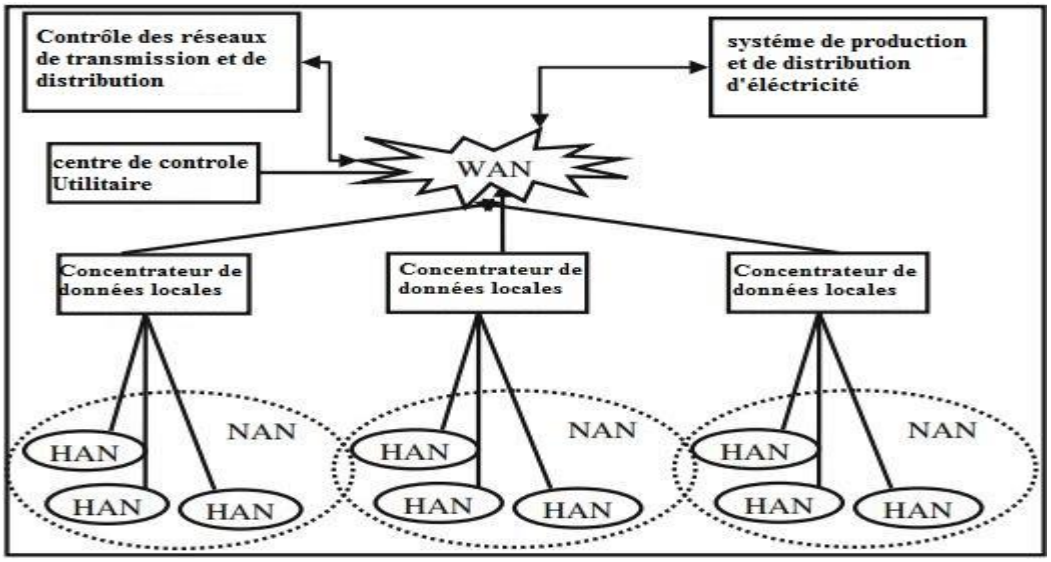

Figure 1.13 : *Diagramme schématique des réseaux de communication dans le réseau électrique intelligent.(A, B. M. Shawkat Ali, 2013)*

Les technologies de communication utilisées dans ce type de réseaux sont : Le WIMAX, La Fibres Optique qui est considérée comme la technologie la plus appropriée pour ce réseau. [Murat Kuzlu et al ,2014]

1.5. Avantages de système SCADA :

Parmi les avantages du SCADA on trouve :

- Il aide les entreprises de services publics à atteindre une fiabilité accrue de l'approvisionnement et de réduire les coûts d'exploitation et d'entretien ; [w23]
- Il fournit des informations mécaniques et graphiques embarquées ;
- Le système SCADA est facilement extensible. Nous pouvons ajouter un ensemble d'unités de contrôle et de capteurs selon l'exigence.
- La capacité du système SCADA à exploiter des situations critiques.
- Il permet le suivi de près du système ;
- facilite la tâche du diagnostic et de l'intervention de l'opérateur. Grace à la production des alarmes lorsqu'une faute se produit et même la détermination de la position où situent la faute et l'élément défectueux ;
- Donne plusieurs informations sur le système ainsi qu'il aide l'opérateur à prendre la bonne décision, et ne pas se tromper dans son intervention.
- Diminue la tâche du personnel en les regroupant dans une salle de commande.

1.6. Sécurité des systèmes SCADA :

Les systèmes de contrôle industriel (**ICS « I**ndustriel **C**ontrol **S**ystem») deviennent de plus en plus vulnérables, car ils deviennent de plus en plus interconnectés avec d'autres systèmes.

D'une part, le passage des technologies propriétaires à des solutions plus standardisées et ouvertes ainsi que l'augmentation du nombre de connexions entre les systèmes SCADA et les différents réseaux tel que l'Internet, les rend plus vulnérables aux attaques. [w21]

D'autre part, la sécurité des systèmes SCADA en temps réel représente un défi important dans le monde actuel. Les menaces de cyber sécurité de hauts niveaux sont un phénomène qui met ces systèmes dans un danger. Tout simplement parce que la cyber-sécurité n'était pas prise en compte au moment de la conception initiale et de l'installation de ces systèmes. [w22]

La sécurité n'était pas la principale préoccupation des concepteurs des outils et des protocoles industriels les plus couramment utilisés. Aujourd'hui, certaines fonctions d'authentification de base sont absentes de ces outils et protocoles. De plus, les réseaux industriels n'ont jamais été formés pour prendre en considération les intrusions potentielles.

Les attaques qui visent les systèmes SCADA se sont graduellement sophistiquées, tel que Stuxnet qui était la première attaque à avoir mis en évidence la faiblesse d'un ICS.

En 2010, le ver informatique Stuxnet[8] viser et compromettre les équipements gérés par certains systèmes SCADA, surtout par le logiciel WinCC[9] de Siemens[10]. Ce virus a la capacité de reprogrammer les automates programmables industriels et de dissimuler ses modifications. Ce virus aurait modifié les commandes de turbines de centrales nucléaires et de centrifugeuses, en provoquant des dégâts considérables. Cette attaque évolutive fait un grand bourdonnement aux menaces sur les environnements informatiques industriels.

1.6.1. Les dix principales défaillances des systèmes SCADA : [w23]

- **Absence de développement sécurisé** dû à des développements internes qui répondent aux besoins internes. Il en résulte des comptes d'accès stockés en clair ou encodés trivialement (par exemple, le nom de la société comme mot de passe principal).

8Stuxnet : Est un ver informatique indésirable ; conçus par la NASA pour s'attaquer aux centrifugeuses iraniennes d'enrichissement d'uranium. Il a été identifié pour la première fois en 2010, il cible les systèmes informatiques industriels ; et il est le premier responsable sur les dégâts considérables au programme nucléaire iranien.(https://en.wikipedia.org/wiki/Stuxnet)

9 WinCC est un système de contrôle et d'acquisition de données (SCADA) avec une interface homme-machine développés par Siemens.

10 Siemens : est un groupe international d'origine allemande spécialisée dans les hautes technologies et présent dans les secteurs de l'industrie.

- **L'absence de test de sécurité** découle en toute logique de l'absence d'intégration de la sécurité informatique dans les projets.
- **Une mauvaise gestion des comptes** où l'on retrouve l'usage d'identifiant par défaut (user/user…), des mots de passe trop faibles ou inexistants (vides, nom du client…) ou encore des utilisateurs disposant de privilèges administrateur sur l'OS.
- **L'interconnexion des systèmes de gestion avec les systèmes industriels pas assez sûre**. Une perméabilité qui permet à un attaquant qui s'introduirait dans le système de gestion informatique de poursuivre sa route sur le réseau industriel.
- **L'absence d'antivirus** sur les postes de travail et serveurs qui laissent tout loisir aux agents malveillants de se propager. Lexsi a ainsi constaté la présence du vers Conficker[11] sur des postes de supervision industrielle dans 50% des cas.
- **Absence de veille en cybersécurité** qui rend difficiles la détection de signaux d'alerte et la remontée d'information.
- **Des sessions Windows non verrouillées** qui rendent l'accès permanent aux interfaces de contrôle (IHM) ou consoles de pilotage. Là encore, en cas d'attaque, la prise de commande distante est un jeu d'enfant pour l'assaillant.
- **Absence d'outils de surveillance** des systèmes (sondes de détection/prévention d'intrusion) et pas de centralisation des journaux système et de leur analyse.
- **Des protocoles courants** (FTP, Telnet, SNMP…) utilisés sans chiffrement qui ouvre l'accès à la récupération de login/mot de passe, à des connexions illégitimes aux serveurs, à des attaques hors ligne, des dénis de service par modification des configurations réseau…
- **Des OS et firmware obsolètes** et non mis à jour. Si Windows XP est encore très présent dans le monde industriel, Lexsi constate également encore la présence de Windows 2000. Une obsolescence qui permet des prises en main rapides sur le SCADA avec pour conséquence des compromissions instantanée des équipements et le risque de rebondir sur d'autres périmètres.

[11] **Conficker :** (connu aussi sous les noms de **Downup**) est un ver informatique qui est apparu fin novembre 2008. Ce ver exploite une faille du Windows Server. Il est principalement installé sur les machines fonctionnant sous Windows XP.

1.6. 2. Comment protéger les systèmes SCADA ?

Pour réduire les risques liés à une attaque, les administrateurs réseau doivent contrôler l'accès à ce dernier, bloquer les menaces et réduire les interruptions de service provoquées par de telles situations.

Les entreprises pourraient ainsi mettre en place un système capable de contrôler le trafic sur le réseau et de prévenir les menaces. L'idée serait alors de centraliser la gestion de la protection de l'infrastructure principale contre les cybers menaces et de garantir la disponibilité du réseau pour poursuivre la continuité des opérations. Il existe cinq manières de protéger les réseaux SCADA. [w21]

- **Mise en œuvre des mesures de cyber protection avancée :** Le déploiement de pare-feu de nouvelle génération permet de protéger les ressources et de créer des micros segments dans toute l'entreprise. Grâce à une meilleure visibilité, les menaces d'attaques peuvent être réduites.
- **Accès sécurisé à la zone SCADA :** La mise en place de procédés liant les règles de sécurité aux identités des utilisateurs est recommandée pour bloquer l'accès aux utilisateurs non autorisés. Le déploiement de systèmes comme les VPN SSL (réseau privé virtuel sécurisé par SSL [Secure Socket Layer]) est parfaitement indiqué dans ce cas.
- **Suppression du risque lié à la gestion de plusieurs ports :** La protection de plusieurs ports devra être assurée par un seul et même pare-feu.
- **Déploiement d'un framework de protection complet contre les vulnérabilités :** L'ensemble du trafic traversant la zone SCADA est inspecté par un framework complet afin de détecter les exploits, malwares, botnets et autres menaces ciblées.
- **Protection des systèmes d'exploitation non pris en charge** : L'utilisation d'un pare-feu de nouvelle génération assure une protection efficace sur l'ensemble du réseau en détectant les attaques qui ciblent certains systèmes d'exploitation.

Conclusion

À travers ce chapitre, nous avons essayé de présenter les principales caractéristiques des réseaux électriques actuels. Ces explications ont mis en évidence la structure statique des réseaux électriques. La volonté généralisée des autorités d'atténuer leur impact environnemental se traduit pour l'industrie électrique par l'impératif de réduction des émissions de CO2. Les deux leviers principaux dont elles disposent dans ce domaine résident dans les politiques de soutien aux énergies vertes et la maîtrise de la demande.

Actuellement, les réseaux électriques sont composés de gros producteurs d'électricité devant répondre aux variations des demandes des consommateurs. Avec l'augmentation du nombre de consommateurs et l'augmentation de leurs consommations, il ne sera plus possible pour ces gros producteurs de satisfaire la consommation.

Il est donc nécessaire de faire une modification sur ce réseau électrique en intégrant de nouveaux producteurs d'électricité afin de créer un équilibre énergétique. Ces producteurs doivent de produire une énergie propre, donc les consommateurs doivent devenir de nouveaux acteurs du réseau en modifiant leurs consommations en fonction de la production d'électricité.

L'introduction de nouveaux réseaux électriques, les Smart Grids, qui sont actuellement clairement définis offre une réponse à ces évolutions futures. La diversité des producteurs dans les nouveaux réseaux, les nouveaux comportements des consommateurs ainsi que leurs diversités géographiques posent un problème de contrôle de l'ensemble de ces utilisateurs du réseau. Une intelligence localisée pour satisfaire la demande de chaque usager apparaît comme une solution intéressante pour conserver une stabilité sur le réseau.

Les réseaux intelligents sont généralement perçus comme la solution aux nombreux défis auxquels sont confrontés nos systèmes électriques et à la voie vers une économie d'électricité à faible intensité de carbone.

Pour mettre à niveau un réseau électrique existant et le rendre un réseau intelligent (Smart Grid), il faut tout d'abord construire une dépendance importante à l'égard d'infrastructures de communication intelligentes et sécurisées. Elle nécessite des cadres de sécurité pour les communications réparties, l'informatique omniprésente et les technologies utilisées dans ce smart Grid.

Ce chapitre montre un aperçu général sur ce type exceptionnel de réseaux électrique intelligents en termes descriptifs de leur concept, son fonctionnement ainsi que son système de communication.

Chapitre 2 : Les Systèmes de détection d'intrusions

Introduction

L'ordinateur est de plus en plus présent dans nos vies quotidiennes, l'Internet relie des centaines de millions d'ordinateurs à travers le monde fonctionnant sur plusieurs plateformes matérielles et logicielles. Il sert d'innombrables besoins personnels et professionnels pour les personnes et les entreprises industrielles.

Les entreprises ont besoin d'ouvrir leurs systèmes d'information à leurs partenaires ou leurs fournisseurs, donc ils doivent lier leurs réseaux locaux à un réseau externe. En reliant le réseau local à un réseau externe, il est nécessaire de connaître les ressources de l'entreprise à protéger et ainsi maîtriser le contrôle et les droits d'accès des utilisateurs au système d'information.

Cependant, cette interconnexion des ordinateurs permet également aux utilisateurs malveillants d'utiliser ces ressources à des fins abusives. Ce qui rend La mise en place d'une politique de sécurité autour de ces systèmes d'application essentiel.

Les mécanismes de sécurité ont presque toujours des vulnérabilités et ils ne sont pas suffisants pour assurer la sécurité complète de l'infrastructure et éviter les attaques qui sont continuellement adaptées pour exploiter les faiblesses du système souvent causées par la conception imprudente et des défauts de mise en œuvre. Cela a créé le besoin de la technologie de sécurité qui peut surveiller des systèmes et identifier des attaques informatiques. Cette composante est appelée le système détection d'intrusion, il représente un complémentaire aux mécanismes de sécurité conventionnels.

En outre la mise en place de pare-feu et de systèmes d'authentification de plus en plus sécurisés, il est nécessaire, pour compléter cette politique de sécurité, d'avoir des outils de surveillance pour bien analyser le système d'information et détecter d'éventuelles intrusions.

Ce que nous appelons intrusion signifie la pénétration des systèmes d'information, mais aussi tentatives des utilisateurs locaux d'accéder à de plus hauts privilèges que ceux qui leur sont attribués, ou tentatives des administrateurs d'abuser de leurs privilèges.

Les systèmes de détection d'intrusion (IDS) est défini comme une combinaison de composants logiciels et/ou matériels qui surveillent les systèmes informatiques et déclenchent une alarme lorsqu'une intrusion se produite.

Dans ce chapitre nous présentons d'abord quelques définitions concernant la sécurité informatique avec les différents types d'attaques, la description d'un système de détection d'intrusions (IDS) ainsi que son architecture interne et ses différents types, ensuite les techniques utilisé pour attaquer un IDS. Enfin nous présentons la classification des systèmes de détection d'intrusions selon plusieurs critères tels que les méthodes de détection et la source de donnée.

1. La sécurité informatique

1.1. Définition :

La sécurité informatique est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires et mis en place pour conserver, rétablir, et garantir la sécurité des systèmes informatiques. Elle est intrinsèquement liée à la sécurité de l'information et des systèmes d'information.

« La raison principale de l'existence de l'industrie de la sécurité informatique est que les produits et services informatiques ne sont pas naturellement sûrs. Si les ordinateurs étaient protégés des virus, il n'y aurait pas besoin de produits antivirus. Si le mauvais trafic réseau ne pouvait être utilisé pour attaquer les ordinateurs, personne ne s'inquiéterait d'acheter un pare-feu. Alors que, si les produits informatiques que nous achetons étaient sûrs par défaut, nous n'aurions pas besoin de dépenser des milliards chaque année pour les rendre plus sûrs. » [Bruce Schneier ,2007]

1.2. Les services de sécurité

Les principaux services de sécurité sont

- **Confidentialité**, qui doit assurer la protection des données contre les attaques non autorisées.
- **Authentification**, qui doit permettre de s'assurer que celui qui se connecte est bien celui qui correspond au nom indiqué.
- **Intégrité,** qui garantit que les données reçues sont exactement celles qui ont été émises par l'émetteur autorisé.
- **Non-répudiation**, qui assure qu'un message a bien été envoyé par une source spécifiée et reçu par un récepteur spécifié.
- **Disponibilité**, qui doit permettre de satisfaire les conditions logicielles et matérielles pour une application ou une communication du réseau pour les utilisateurs légitimes.

[Guy Pujolle ,2008]

1.3. Les mécanismes de sécurité

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

1.3.1 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 Encryption Standard).
- **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. Exemple d'algorithme de chiffrement symétrique : RSA (Rivest Shamir Adleman).
- **Le chiffrement hybride** : Le chiffrement hybride combine l'utilisation des chiffrements symétriques et asymétriques.

  L'application de chiffrement à clé publique pour partager une clé qui sera utilisée pour l'application de chiffrement symétrique.

  Le message envoyé est chiffré en utilisant la clé publique puis transmis au destinataire. Comme l'échange de clés symétriques est sécurisé, la clé symétrique utilisée est différente pour chaque message envoyé (utilisée une seule fois). C'est pour cela elle s'appelle la clé de session, car si un attaquant arrive à déchiffrer cette clé, elle pourra seulement être utilisée pour lire le message qui a été chiffré avec cette dernière. Il devra alors recommencer et déchiffrer une autre clé de session pour lire un autre message.

  Le destinataire utilise sa clé privée pour déchiffrer la clé de session et la clé de session est ensuite utilisée pour déchiffrer le message [NC Batista et al, 2012]

1.3.2. La signature électronique

Les signatures électroniques sont utilisées pour identifier les auteurs des données électroniques. Il s'agit d'appliquer une fonction de hachage (exemple : 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. [F. Bao, et al, 2012]

1.3.3. Public Key Infrastructure (PKI)

L'infrastructure à clés publiques, PKI « Public Key Infrastructure » est constitué de l'ensemble de matériels, logiciels, personnes, règles et procédures nécessaires à une autorité de certification (AC) pour créer, gérer et distribuer des certificats. 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.[F. Bao et al, 2012]

1.3.4. 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. 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. . .)
- La durée de validité du certificat. [F. Bao et al, 2012]

2. Les attaques

Les informations ou les systèmes d'informations d'une entreprise peuvent subir des dommages de plusieurs façons : certains par accident, d'autres intentionnels ou malveillants. Dans ce contexte on parle « des attaques ».

2.1. C'est quoi une attaque ?

Une attaque est l'exploitation d'une faille d'un système informatique connecté à un réseau pour un accès ou une tentative d'accès illégale.

Une attaque cybernétique[1] est un acte malveillant envers un dispositif informatique via un réseau cybernétique. Un cyber attaque peut émaner des personnes isolées, d'un groupe de pirates ou plus récemment de vastes organisations ayant des objectifs géopolitiques.

2.1.1. La source d'une attaque

Les attaques informatiques peuvent être lancées à partir d'un emplacement unique (attaques source unique) ou de plusieurs emplacements différents (attaques réparties / coordonnées). La plupart des attaques proviennent généralement d'un seul emplacement, mais dans le cas de grandes attaques DoS distribuées ou d'autres attaques organisées, plusieurs lieux sources peuvent participer à l'attaque.

2.1.2. Anatomie d'une attaque

L'attaque informatique possède une structure désignée généralement par les «5P », qui sont des acronymes des cinq verbes anglophones : Probe, Penetrate, Persist, Propagate, Paralyze.

- **Probe** : consiste à collecter des informations par le biais d'outils comme whois, Arin, DNS lookup sur un système cible qui peut s'effectuer de plusieurs manières, par exemple un scan de ports avec le programme Nmap pour déterminer la version des logiciels utilisés, ou encore les logiciels firewalls.
- **Penetrate :** Cette attaque réalisée par utilisation des informations récoltées pour s'introduire dans un réseau.

  Des techniques comme la force brute ou les attaques par dictionnaires peuvent être utilisées pour outrepasser les protections par mot de passe ou par une autre alternative, pour s'infiltrer dans un système.
- **Persist :** création d'un compte avec des droits de super utilisateur pour pouvoir se réinfiltrer ultérieurement. Une autre technique consiste à installer une application de contrôle à distance capable de résister à un reboot (ex : un cheval de Troie).
- **Propagate :** cette étape consiste à observer ce qui est accessible et disponible sur le réseau local (analyse des communications internes).

[1]La **cybernétique** (en anglais *cybernetics*) est la science des mécanismes autogouvernés et du contrôle, elle met essentiellement en relation les principes qui régissent les êtres vivants et des machines dites évoluées. La cybernétique est une science transdisciplinaire (https://fr.wikipedia.org/wiki/Cybern%C3%A9tique)

- **Paralyze :** cette étape peut consister en plusieurs actions (attaque). Le pirate peut utiliser le serveur pour mener une attaque sur une autre machine, détruire des données ou encore endommager le système d'exploitation dans le but de planter et paralyser le serveur. [David Burgermeister et Jonathan Krier 06]

2.2. Les types d'attaques

On peut classer les attaques ont:

- des attaques passives (acquisition sans autorisation d'informations, perte de confidentialité)
- des attaques actives (changement non autorisé des données, perte de l'intégrité, perte de disponibilité). [Hervé Debar et all ,2000]

2.2.1. Les attaques passives:

Elles sont celles où l'attaquant souhaite obtenir l'information. Ils ne souhaitent pas modifier le contenu du message original. Il est très difficile à détecter, car il ne modifie pas les données ; parmis les techniques d'attaque passives : les rejets de message, l'analyse du trafic, le reniflement (sniffing)et les enregistreurs de clés. [Khaleel Ahmad1et al ,2011]

- **L'Interception :** L'interception est un type d'attaque qui se fait sans l'autorisation ou la connaissance des utilisateurs. Il viole également les règles de confidentialité dans le principe de sécurité.

  En mots simples, on peut dire que l'interception cause la perte de confidentialité des messages. C'est un type d'attaque passive. Il est classé en deux sous-types, à savoir l'analyse du trafic et la publication du contenu du message. C'est de quatre types: -

  - ✓ **La Libération de messages (Release of message):** lorsque vous envoyez un message à votre ami, vous souhaitez que cette personne est la seule puisse lire ce message. En utilisant certains mécanismes de sécurité, nous pouvons empêcher la publication du contenu du message. Par exemple, nous pouvons coder le message à l'aide d'un tel algorithme de chiffrement.
  - ✓ **L'Analyse du trafic (Traffic analysis):** l'attaquant analyse le trafic, détermine l'emplacement, identifie les hôtes de communication, observe la fréquence et la durée des messages. Tous les trafics entrants et sortants du réseau sont analysés, mais non modifiés.
  - ✓ **Reniflement (sniffing):** est une méthode pour renifler les données transférées qui ont été envoyés par l'expéditeur. Il tente simplement de savoir quel type de message ou de données est transféré par l'expéditeur sans l'autorisation de ce dernier.

- ✓ **Keyloggers:** C'est un programme qui fonctionne en arrière-plan, enregistrant toutes les frappes. Une fois que les frappes de touches sont enregistrées, elles sont cachées dans la machine pour une récupération ultérieure, ou expédiées vers l'attaquant.

  L'attaquant les examine ensuite attentivement dans l'espoir de trouver des mots de passe ou éventuellement d'autres informations utiles qui pourraient être utilisé pour compromettre le système ou être utilisées dans une attaque d'ingénierie sociale. Par exemple, un keylogger révélera le contenu de tous les e-mails composés par l'utilisateur.

2.2.2. Les attaques actives :

Les attaques actives sont des attaques qui apportent une certaine modification dans les messages originaux ou la création des faux messages. Ces attaques sont très complexes et ne peuvent pas être empêchées facilement. Elles peuvent être catégorisées en 3 types: Interruption, Fabrication et Modification. Dans ces catégories, le Déni de service (DoS), DDoS, DRDoS, SQL Injection, Replay attack, Masquerading, Man in Middle Attacks sont les attaques les plus courantes. [Khaleel Ahmad1et al, 2011]. Comme il existe d'autres attaques actives qui sont connus tel que l'attaque de débordement de tampon (Buffer overflow) , l'IP et le ARP spoofing et l'attaque de fishing .

a . L'Interruption: Les attaques d'interruption sont une attaque active. Dans ce type d'attaque, une entité autorisée prétend être une autre entité. Par exemple, il y a trois utilisateurs A, B & C. L'utilisateur A peut être posé comme utilisateur C et envoyer un message à l'utilisateur B. L'utilisateur B croit que ce message provient de l'utilisateur C. L'interruption met la disponibilité des ressources en danger. Elle est classé en quatre types:

- **Le Déni de service « DOS » :** Cette attaque est bien nommée, car elle entraînera l'indisponibilité d'un service (application spécifique) ou d'une machine cible. Nous distinguerons deux types de déni de service : [Eric Detoisien ,2003]

  D'une part, ceux exploitant un bug d'application : Si les vulnérabilités d'une application peuvent conduire à la capacité de prendre le contrôle sur une machine (exemple de débordement de mémoire tampon), elles peuvent également conduire à un déni de service. L'application deviendra indisponible soit par manque de ressources allouées, soit par un plantage.

  Et d'autre part ceux liés à la mauvaise mise en œuvre d'un protocole ou aux faiblesses d'un protocole.

- **Le Déni de service distribué « DDoS** "Distributed Denial of Service"**» :**Le déni de service distribué est un type d'attaque très évolué visant à faire planter ou à rendre muette une machine en la submergeant de trafic inutile.

Plusieurs machines à la fois sont à l'origine de cette attaque (c'est une attaque distribuée) qui vise à détruire des serveurs, des sous réseau, etc. D'autre part, elle reste très difficile à contrer ou à éviter. C'est pour cela que cette attaque représente une menace que beaucoup craignent.

✓ **SYN Flooding**

Syn Flood est une technique d'attaque informatique de type DDOS, effectuée contre les serveurs et les réseaux pour les rendre complètement indisponibles. Elle s'applique dans le cadre d'un protocole Tcp.

La connexion TCP s'établit en trois étapes (TCP Three Way Handshake) ; le SYN Flooding exploite ce mécanisme. Ces trois étapes sont :

- L'envoi d'un SYN (paquet de synchronisation) ;
- La réception d'un SYN-ACK ;
- Et l'envoi d'un ACK.

Le principe est de laisser sur la machine ciblée un nombre important de connexions TCP en attentes (demandes d'ouverture de la session TCP) avec l'envoi massif des demandes de connexion(drapeau SYN = 1). D'une part, la machine ciblée renvoie les SYN-ACK pour répondre à la SYN reçus. D'autre part, l'attaquant ne répondra pas avec un ACK ; donc pour chaque SYN reçu la cible aura une connexion TCP en attente.

Puisque ces connexions semi-ouvertes consomment des ressources mémoires au bout d'un certain temps, la machine est saturée et ne peut plus accepter aucune autre connexion TCP. [Burgermeister, D.et Krier ;2006]

- **Distribué DoS avec des réflecteurs (DRDoS):** il consiste en un réflecteur qui aide l'attaquant à exécuter une attaque plus efficace et sécurisée. Il en résulte une augmentation des dégâts et diminue le risque de retrait. [Khaleel Ahmad1et al, 2011]
- **SQL Injection :**L'injection SQL est une vulnérabilité de sécurité qui se produit dans les couches de base de données d'une application. Il est le fait de passer le code SQL dans les applications Web interactives qui utilisent des services de base de données. [Khaleel Ahmad1et al, 2011]

Injection signifie tromper une application en incluant des commandes inattendues dans les données envoyées à un interprète. Toute application Web acceptant l'entrée de l'utilisateur comme base d'une requête de base de données peut être vulnérable à SQL Injection. Il utilise des failles dans l'application Web qui interagissent avec la base de données. [Eric Detoisien ,2003]

b. La Fabrication : Dans cette attaque, les utilisateurs utilisent un service d'accès auquel ils ne sont pas admissibles. Il est possible en l'absence de mécanismes d'authentification appropriés .En vertu de ces deux techniques d'attaque utilisées : [Khaleel Ahmad1et al, 2011]

- **L'Attaque par rejeu (Replay attack):** Une attaque par rejeu est une forme d'attaque active dans lequel une transmission de données valide est répétée avec malveillance ou retardée. Un attaquant capture les données autorisées et les retransmet à son usage personnel.

  Par exemple l'utilisateur A souhaité transférer une certaine somme sur le compte bancaire d'un utilisateur C. Les utilisateurs A et C ont un compte dans la Banque B. L'utilisateur A envoie un message électronique à la Banque B, en demandant un transfert de fonds. L'utilisateur C pourrait capturer ce message et envoyer une deuxième copie à la Banque B, mais la Banque B ne pourrait pas avoir l'idée qu'il s'agissait d'un message non autorisé. Ainsi, l'utilisateur C bénéficierait deux fois du transfert de fonds.

  L'attaque par rejeu peut être empêchée en utilisant des signatures numériques puissantes qui incluent des horodatages et l'inclusion d'informations uniques de la transaction précédente, telles que la valeur d'un numéro de séquence constamment incrémenté. [Khaleel Ahmad1et al, 2011]
- **L'attaque de masquage (Masquerading):** est un type d'attaque dans laquelle un système suppose l'identité d'un autre. C'est une technique utilisée par l'attaquant pour se faire comme une personne autorisée afin d'obtenir l'accès aux informations confidentielles de manière illégale.

c. La modification : La modification entraîne des pertes de principe d'intégrité. Par exemple, une personne a effectué une transaction en ligne de Rs.100. Mais l'attaquant l'empêche et le modifie à Rs.1000. ; c'est le cas d'intégrité. Dans le cadre de cette technique d'attaque est l'homme de l'attaque du milieu.

- **L'attaque de l'homme dans le milieu (Man in the middle) :** Il est abrégé en MITM. Il s'agit d'une attaque Internet active qui tente d'intercepter, de lire et de modifier les informations se situant entre l'utilisateur d'un réseau public et tout site Web demandé. L'attaquant utilise l'information obtenue illégalement pour le vol d'identité et d'autres types de fraude. [Khaleel Ahmad1et al, 2011]

  L'objectif principal de cette attaque est de détourner le trafic entre deux machines. Il s'agit d'intercepter, de modifier ou de détruire les données circulant pendant la communication.

Cette attaque est plus un concept qu'une attaque réelle. Il y a diverses attaques mettant en œuvre le principe de l'homme dans le milieu, comme l'homme DNS dans le milieu qui utilise la falsification du DNS pour détourner le trafic entre un serveur Web et un client Web. [Viardin, 2006]

d. l'attaque de débordement de tampon (Buffer overflow) : Buffer overflow ou dépassement de la pile est une vulnérabilité causée par une mauvaise programmation. Il apparaît quand une variable passée comme un argument à une fonction est copiée dans un tampon sans vérifier sa taille. Si la variable a une taille plus grande que l'espace mémoire réservé pour ce tampon, il suffit pour que le débordement de mémoire tampon se produise. Il sera exploité en passant à la variable un fragment de programme. Si un pirate réussit dans cette attaque, il aura la possibilité d'exécuter à distance des commandes sur la machine cible avec les droits de l'application attaquée. [Eric Detoisien, 2003]

e. IP Spoofing : Le but de cette attaque est d'usurper l'adresse IP d'une machine. Cela permet au pirate de cacher l'origine de son attaque (utilisée dans les attaques de déni de service) ou de bénéficier d'une relation de confiance entre deux machines. Ici, nous allons expliquer cette deuxième utilisation de l'IP Spoofing. [Eric Detoisien ,2003]

Le principe de base de cette attaque consiste, pour le pirate, à forger ses propres paquets IP a l'aide des programmes spécialisés tels que hping2 [2] dans lesquels il va changer, entre autres choses, l'adresse IP source. Cependant, il existe deux méthodes pour obtenir les réponses:

- **Source Routing :** Le protocole IP a une option appelée Source Routing qui vous permet de définir l'itinéraire que les paquets IP doivent prendre. Cette route est une série d'adresses IP des routeurs que les paquets devront suivre. Assez le pirate de fournir un itinéraire pour les paquets, jusqu'à un routeur qu'il contrôle. De nos jours, la plupart des implémentations de pile TCP / IP rejettent les paquets en utilisant cette option.
- **Reroutage:** Les tables de routeurs utilisant le protocole RIP peuvent être modifiées en leur envoyant des paquets RIP avec de nouvelles informations de routage. Ceci est fait pour rediriger les paquets vers un routeur que le pirate gère. [Eric Detoisien ,2003]

[2] Hping2 : est un outil réseau capable d'envoyer des paquets TCP / IP personnalisés et d'afficher les réponses cibles comme le programme ping avec les réponses ICMP. La fragmentation de la poignée hping2, le corps et la taille des paquets arbitraires et peuvent être utilisés pour transférer des fichiers encapsulés sous des protocoles pris en charge (http://www.hping.org/manpage.html)

f. ARP Spoofing : Cette attaque, également appelée ARP Redirect ou bien la redirection ARP, redirige le trafic réseau d'une ou plusieurs machines vers la machine du pirate. Il est fait sur le réseau physique des victimes. [Eric Detoisien ,2003]

g. Attaque de phishing:

Il obtient des informations sensibles telles que le nom d'utilisateur, le mot de passe et les détails de la carte de crédit. Les attaquants tentent d'obtenir ces détails et ils modifient ces messages. [Eric Detoisien, 2003]

3. Dispositif de sécurité

3.1. Définition

La sécurité vise à garantir la confidentialité, l'intégrité et la disponibilité des services. Il faut mettre en place des mécanismes pour s'assurer que seules les personnes autorisées ont accès à l'information et que le service est rendu correctement.

3.2. Les Types de dispositifs de sécurité

3.2.1. Les Pare-feu

Un pare-feu (Firewall) est un système physique ou logique qui inspecte les paquets entrants et sortants du réseau afin d'autoriser ou d'interdire leur passage en se basant sur un ensemble de règles appelées ACL.

Le pare-feu (firewall) est une solution matérielle ou logicielle mise en place au sein de l'infrastructure du réseau afin de filtrer l'accès à des ressources réseau définies. Il ne laisse entrer que les utilisateurs autorisés, disposant d'une clef ou d'un badge, et crée une couche protectrice entre le réseau et le monde extérieur. Il est doté de filtres intégrés qui peuvent empêcher des documents non autorisés ou potentiellement dangereux d'accéder au système. Il enregistre également les tentatives d'intrusions dans un journal transmis aux administrateurs du réseau. Il permet également de contrôler l'accès aux applications et d'empêcher le détournement d'usage. [Brigitte Ulmann ,2004]

Il existe trois types de pare-feu :

- **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.

- **Pare-feu à filtrage des paquets avec mémoire d'états :** ce modèle 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 de protocole.
- **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 réseau.

Malgré leurs grands intérêts, les pare-feu présentent quelques lacunes. En effet, un attaquant peut exploiter les ports laissés ouverts pour pénétrer le réseau local. Ce type d'accès est possible même à travers des pare-feu proxy. Il suffit d'utiliser un protocole autorisé tel que HTTP pour transporter d'autres types de données refusées. Ainsi l'opération supplémentaire d'encapsulation/décapsulation des données permet à l'attaquant de contourner le pare-feu. Les scripts constituent aussi des sources d'intrusion que les pare-feu échouent à détecter.

3.1.2. Le Cryptage

Pour transmettre des données de manière confidentielle et afin de protéger un message, on lui applique une transformation qui le rend incompréhensible; c'est ce qu'on appelle le chiffrement ou bien le cryptage.

Le principal objectif du chiffrement consiste à garantir la confidentialité des données numériques stockées sur des systèmes informatiques ou transmises via Internet ou d'autres réseaux. Les algorithmes de chiffrement modernes jouent un rôle crucial dans la sécurité des systèmes informatiques et des communications, car ils assurent non seulement la confidentialité, mais également les éléments de sécurités essentielles telles que l'authentification, l'intégrité et le non répudiation.

3.1.3. Les Antivirus

Un antivirus est un logiciel qui protège une machine contre les virus. L'antivirus se fonde sur des fichiers de signatures et compare alors les signatures génétiques du virus aux codes à vérifier. Certains programmes appliquent également la méthode heuristique tendant à découvrir un code malveillant par son comportement. [Brigitte Ulmann ,2004]

3.1.4. Les IDS :

Malgré l'existence de différents mécanismes de sécurité tel que les pare-feu, les antivirus, les scanners de vulnérabilités .Cependant, chaque système de protection peut être spécialisé à des menaces particulières pour les systèmes d'informations, car chacun d'entre eux à ses points faibles. Ce qui augmente la nécessité d'une meilleur protection et lorsque on parle d'une meilleur sécurisation dans ce cas-là il apparait le système de détection d'attaque ou de détection d'intrusion appelé le système de détection d'intrusion (l'IDS) qui est examiné dans notre étude.

4. les Systèmes de détection d'intrusion

Afin de détecter les intrusions qui peuvent subir un réseau, il est nécessaire d'avoir un logiciel spécialisé dont le rôle serait de surveiller les données qui circulent sur ce réseau, et qui seraient capables de réagir si ces données semblent suspectes. Les systèmes de détection d'intrusions conviennent parfaitement pour réaliser cette tâche.

4.1. Définitions

4.1.1. La définition d'Intrusion

L'intrusion est toute utilisation d'un système informatique à des cibles non autorisées, pour obtenir l'acquisition de privilèges de façon illégitime. L'intrus est généralement vu comme un utilisateur étranger au système informatique qui a réussi à en prendre le contrôle. [Philippe Biondi ,2001]. Les intrusions peuvent être catégorisées selon l'environnement où elles se produisent :

- **Les intrusions sur la machine hôte :** sont des intrusions sur une machine spécifique. Ces attaques sont généralement détectées en examinant les informations système (par exemple, les commandes du système, les journaux du système). L'identité de l'utilisateur qui effectue une attaque.
- **Les intrusions de réseau** : sont des intrusions qui se produisent via des réseaux informatiques habituellement de l'extérieur de l'organisation. La détection de ces intrusions est effectuée en analysant les données de trafic réseau (par exemple, les flux de réseau, les données de tcp dump).Cependant, une telle analyse ne peut souvent pas révéler l'identité précise des attaquants, car il n'existe aucune association directe entre les connexions réseau et un utilisateur réel.
- **Les intrusions dans un environnement P2P** : sont des intrusions qui se produisent dans un système où les ordinateurs connectés agissent comme des pairs sur l'Intemet. Contrairement aux architectures de réseau "client / serveur" standard, dans l'environnement P2P, les ordinateurs ont des capacités et des responsabilités équivalentes et n'ont pas d'adresse IP fixe.

- **Les intrusions dans les réseaux sans fil :** sont des intrusions entre des ordinateurs connectés via un réseau sans fil. La détection des attaques dans les réseaux sans fil est basée sur l'analyse des informations sur les connexions dans les réseaux sans fil, qui sont généralement collectées aux points d'accès sans fil.

  Les menaces de sécurité dans les réseaux sans fil peuvent être classées comme suit :

  - écoute : si l'intrus n'écoute que les données ;
  - intrusions : si l'intrus tente d'accéder ou de modifier les données ;
  - le détournement de communication, lorsqu'un nœud parasite capte le canal, pose comme un point d'accès sans fil et attire les nœuds mobiles pour se connecter à lui et collecte ensuite des données confidentielles (par exemple, mots de passe, clés secrètes, noms de connexion);
  - attaque de déni de service (brouillage), lorsqu'un attaquant perturbe le canal de communication, les obstacles physiques et désactive toutes les communications sur le canal.

4.1.2. La Définition de La détection d'intrusion

La détection d'intrusion est un domaine qui est apparu en 1980. Elle représente un processus de surveillance des événements se produisant dans un système informatique ou un réseau et de les analyser.[Hussain Ahmad Madni Uppal et al, 2014]**.**

a. La détection d'intrusion au niveau système

- **L'observation du flot de contrôle :** L'approche la plus classique au niveau système est celle qui consiste à vérifier que l'enchaînement des appels système émis par une application est conforme à celui préalablement appris durant une phase d'apprentissage réalisée dans un environnement exempt d'attaque. Toute la difficulté de l'approche consiste à mesurer la taille de la séquence d'appels qui doit être retenue pour réaliser la détection.

  Cette approche propose donc de construire par apprentissage un comportement fonctionnel de l'application (l'ordre de l'enchaînement des appels système) dont on imagine qu'il sera violé lors d'une attaque contre l'application.
- **Observation du flot de données :** L'approche précédente se focalise uniquement sur le flot de contrôle d'une application vu depuis le système. L'inconvénient de cette dernière est qu'elle est vulnérable à des attaques contre des données qui ne modifient pas le flot de contrôle.

b. **La détection d'intrusion au niveau applicatif** :

Grâce à des mécanismes de prévention tels que les pare-feu, les systèmes d'information ne sont accessibles à distance qu'au travers de logiciels serveur (pour lesquels certains ports spécifiques sont ouverts), qui deviennent ainsi la cible des attaques.

4.1.3. Définition d'un système de détection d'intrusion (Intrusion Détection System ou IDS)

Le système de détection d'intrusion est un outil logiciel ou matériel qui permet d'écouter le trafic réseau de façon furtive dans le but de détecter des activités anormales qui pourraient être assimilées à des intrusions. Ils visent à détecter les attaques contre les systèmes et les réseaux informatiques, car il est difficile de fournir des systèmes d'information protégés à 100% et de les maintenir dans un état sécurisé pour toute leur durée de vie et pour chaque utilisation. [Hussain Ahmad Madni Uppal et al, 2014]

La tâche principale des IDS est de surveiller constamment le réseau et contrôler l'utilisation de tels systèmes et de détecter l'apparition d'états incertains. Ils détectent les tentatives et la mauvaise utilisation active par les utilisateurs légitimes des systèmes d'information ou des parties externes pour abuser de leurs privilèges ou exploiter les vulnérabilités de sécurité.

Il analyse les flux de paquets de données transitant par le réseau, à la recherche d'activités non autorisées (telles que les attaques de pirates) et permet aux utilisateurs de traiter les failles de sécurité avant que les systèmes ne soient compromis.

4.2. Types d'IDS

Il existe de nombreux types d'IDS qui sont classées en trois catégories comme se suit :

4.2.1. IDS Basés sur l'hôte (HIDS)

Dans l'IDS basé sur l'hôte, les caractéristiques d'un hôte unique sont surveillées et les événements de cet hôte sont observés pour toute activité malveillante. Ils peuvent surveiller le trafic réseau, les journaux, les processus, les opérations effectuées par les applications, l'accès et la modification des fichiers et tout changement de configuration dans le système. Le déploiement de HIDS est généralement effectué sur des hôtes critiques. L'hôte critique comprend des serveurs ou des systèmes accessibles au public et disposant d'informations sensibles. Ils sont placés sur un serveur ou poste de travail, où les données sont collectées à partir de différentes ressources et la machine analyse les données localement.[Hussain Ahmad Madni Uppal et al,2014]

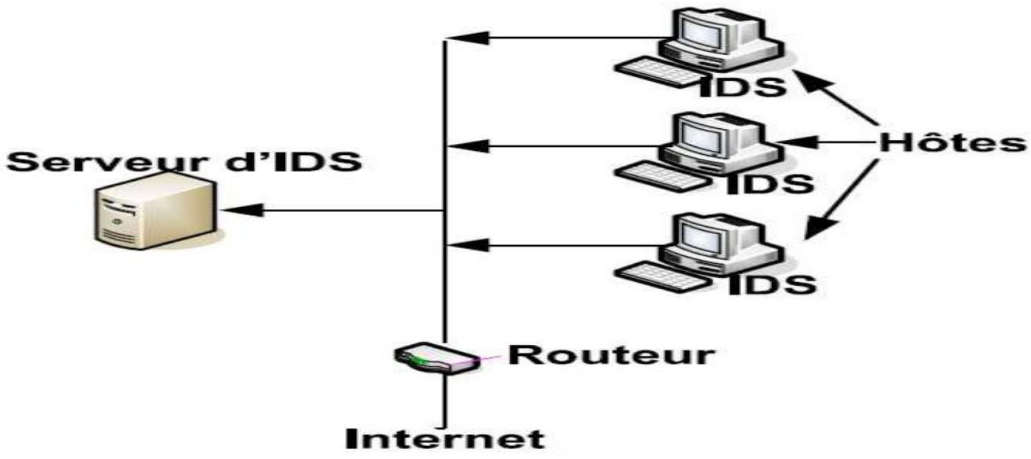

Figure 2.1 : *Exemple de HIDS [Hussain Ahmad Madni Uppal et al, 2014]*

4.2.2. IDS Basés sur le réseau (NIDS)

Les IDS Basés sur le réseau sont des Appliance matérielles autonomes qui incluent des capacités de détection d'intrusion réseau. Ils sont principalement déployés sur un point stratégique dans l'infrastructure réseau, comme à une frontière entre les réseaux, les serveurs de réseau privé virtuel, les serveurs d'accès distant et les réseaux sans fil. NIDS surveille le trafic réseau passant par des segments de réseau ou des périphériques particuliers. Il peut capturer et analyser des données pour détecter des attaques connues ou des activités illégales ou analyser les activités du réseau et du protocole d'application afin d'identifier les activités anormales et suspectes par le balayage de trafic. Les NIDS peuvent également être appelés "snifers-paquets", car ils captent et collectent les données sous forme des paquets Internet passant par des moyens de communication. [Hussain Ahmad Madni Uppal et al, 2014]

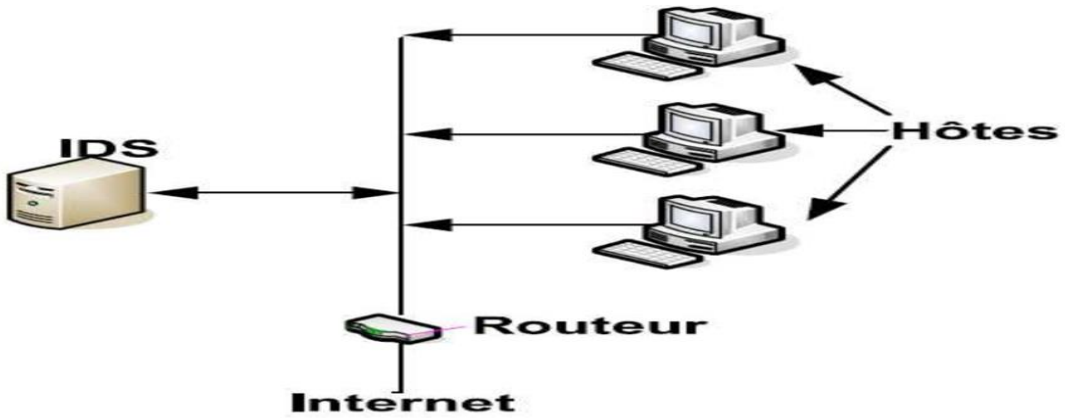

Figure 2.2 *: Exemple de NIDS [Hussain Ahmad Madni Uppal et al, 2014]*

4.3. Les composants d'un système de détection d'intrusion

Nous décrivons les composants qui constituent classiquement un système de détection d'intrusions comme il est illustré dans la figure 4:

- **Le dispositif de collecte de données (capteur)** est responsable de la collecte des données du système surveillé.
- **Détecteur (moteur d'analyse de détection d'intrusion (ID Engine))** traite les données collectées à partir des capteurs pour identifier les activités intrusives.
- **La base de connaissances (base de données)** contient des informations collectées par les capteurs, mais en format prétraité (par exemple base de connaissances d'attaques et leurs signatures, données filtrées, profils de données, etc.). Cette information est généralement fournie par des experts en réseau et en sécurité.
- **Le dispositif de configuration** fournit des informations sur l'état actuel du système de détection d'intrusion (IDS).
- **Le composant de réponse** déclenche des actions lorsqu'une intrusion est détectée.

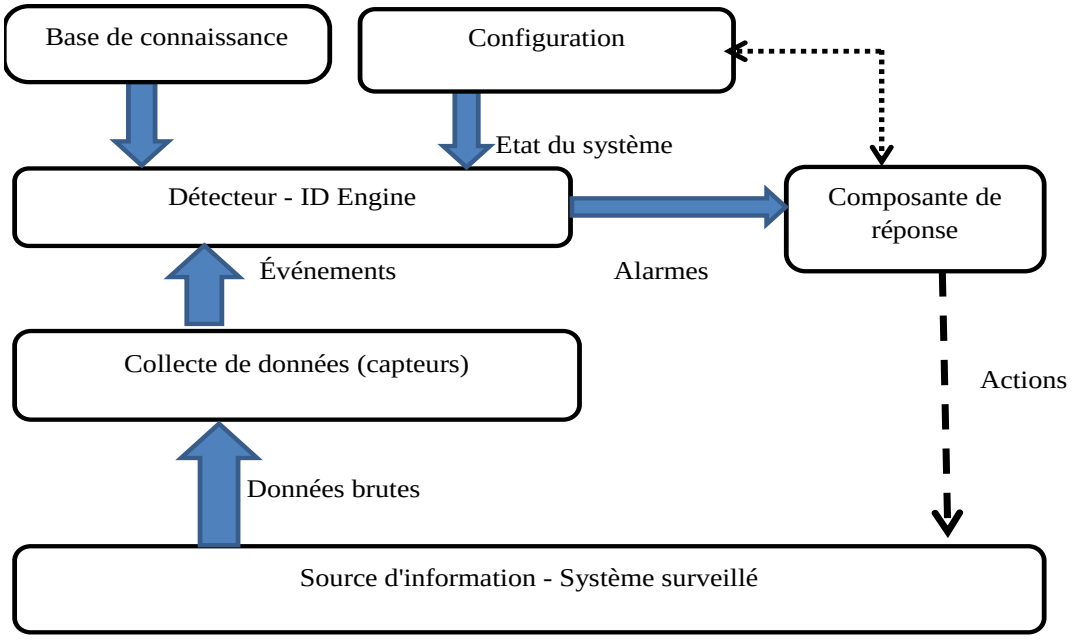

***Figure 2.3** : L'architecture d'un IDS.[Aleksandar Lazarevic et al , 2005]*

4.4. Les acteurs principaux dans les IDS :

A. Sujets : Utilisateurs qui ont le droit d'accès au système

B. Objets : ressources gérées par les fichiers système, les commandes, les périphériques, etc. (hard/soft).

C. Enregistrements d'audit : généré par le système cible en réponse à des actions effectuées ou tentées par des sujets sur des objets « connexion utilisateur, exécution de commande, accès au fichier, etc. (ensemble des actions faites par les sujet sur les objets) ».

D. Profils : Structures qui caractérisent le comportement des sujets par rapport aux objections en termes de métriques statistiques et de modèles d'activité observée. Les profils sont automatiquement générés et initialisés à partir de modèles.

E. Enregistrements d'anomalie : générés lorsque le comportement anormal est détecté.

F. Règles d'activité : les actions prises lorsqu'une condition est satisfaite, les profils de mise à jour, la détection de comportements anormaux, les anomalies des intrusions présumées et la production de rapports.

4.5. Les fonctions principales d'un IDS

Les systèmes de détection d'intrusion remplissent diverses fonctions : [Hussain Ahmad Madni Uppal et al, 2014]

- **Observer et Surveiller :** utilisé pour observer et surveiller les activités des utilisateurs,
- **Reconnaître les modèles :** la capacité de reconnaître les modèles d'attaques.
- **Rapports sur les intrusions :** Préparer un rapport détaillé sur les événements capturés. Les administrateurs système utilisent ces rapports pour analyser des modèles d'activité anormaux, des configurations système et la configuration de sécurité pour déterminer les vulnérabilités.
- **Contrôler la violation du politique utilisateur** : utilisé pour suivre les violations des règles utilisateur, évaluer l'intégrité du système et des fichiers.
- **Enregistrer les événements :** lorsqu'il rencontre une activité suspecte, l'IDS enregistre les informations relatives à l'activité observée.

- **Alerter les administrateurs système :** l'IDS envoie des alertes à l'administrateur système via des pages Web, des courriels, des messages, etc., lorsqu'un événement suspect se produit dans une base de données.

4.6. Caractéristiques des systèmes de détection d'intrusion

Un certain nombre de caractéristiques souhaitées pour les systèmes de détection d'intrusion (IDS) ont été identifiés comme suit :

- **Précision** : un IDS ne doit pas identifier une action légitime dans un environnement système comme une intrusion, un tel événement est appelé faux positif.
- **Exhaustivité** : un IDS ne devrait pas échouer à détecter une intrusion. Une intrusion inaperçue est appelée un faux négatif.
- **Performance** : est le taux auquel des données sont traitées par un IDS. La performance d'un IDS doit être suffisamment bonne pour réaliser une ID en temps réel. Ici, le temps réel signifie qu'une intrusion doit être détectée avant qu'un dommage significatif ait été causé.
- **Tolérance aux pannes** : un IDS doit lui-même être résistant aux attaques. Comme expliqué dans le fait que l'IDS a été déployé sur un réseau, certains intrus sont susceptibles d'attaquer l'IDS d'abord, de le désactiver ou de le forcer à fournir de fausses informations.
- **Opportunité** : un IDS doit effectuer et diffuser son analyse le plus rapidement possible de manière à permettre une réaction avant que trop de dommages ne soient infligés. [Aleksandar Lazarevic et al,2005]

4.7. Les techniques anti-IDS

Comme tout système informatique, ou presque, il existe des failles dans les IDS, ou plutôt des techniques qui permettent d'outrepasser ces systèmes sans se faire repérer. Si un pirate détecte la présence d'un IDS, il peut le désactiver, ou mieux encore, générer de fausses attaques pendant qu'il commettra son forfait tranquillement.

Il existe trois catégories d'attaques contre les IDS :

- **Attaque par déni de service :** rendre l'IDS inopérant en le saturant.
- **Attaque par insertion :** le pirate, pour éviter d'être repéré, injecte des paquets de leurre qui seront ignorés par le système d'exploitation de la cible, mais pris en compte par l'IDS : l'IDS ne

détecte rien d'anormal, alors que sur le système cible, l'attaque a bien lieu puisque les paquets superflus sont ignorés.

- **Attaque par évasion :** il s'agit de la technique inverse à l'attaque par insertion. Ici, des données superflues sont ignorées par l'IDS, mais prises en compte par le système d'exploitation.

4.7.1. Détecter un IDS

Comme nous l'avons déjà signalé, il est très dangereux que la présence d'un IDS soit remarquée par un pirate. Car dans ce cas, il tente d'obtenir un maximum d'informations sur l'IDS installé (ex : la version utilisée) pour pouvoir l'outrepasser et attaquer sans se faire remarquer.[David , Jonathan ;2006]

Voici quelques techniques qui permettent de détecter un IDS :

- **Usurpation d'adresse MAC:** les NIDS mettent l'interface de capture en mode promiscuité (promiscuous mode), il est donc possible de détecter l'IDS en envoyant par exemple un ICMP « echo request» à la machine soupçonnée d'être un NIDS avec une adresse MAC inexistante. Si la machine répond alors elle est en mode promiscuous et peut donc être un NIDS.
- **Mesure du temps de latence:** puisque l'interface est en mode promiscuous, les temps de réponse sont plus longs.
- Le pirate sature ensuite le réseau en broadcast[9] dans le but de ralentir l'IDS, qui recevra tous les paquets. Enfin, le pirate réémet la même série de pings en mesurant les nouveaux temps de réponse. S'ils sont bien plus élevés que les premiers temps obtenus, il est fort possible que la machine soit en mode promiscous.
- **Exploiter les mécanismes de réponses actives:** Les systèmes de prévention d'intrusions (IPS) réagissent à certaines attaques (fermer la session, bloquer un port, ...), mais en faisant cela, ils laissent souvent des empreintes (header des paquets) permettant d'identifier le type de ces systèmes.
- **Observation des requêtes DNS :** Les IDS génèrent souvent des requêtes DNS lors des alertes. En observant le DNS primaire lors de fausses attaques, on peut détecter qu'il y a un IDS.

4.7.2. Déni de services contre un IDS

Le but est de désactiver l'IDS en saturant ses ressources (ex : SYN Flood ou paquets fragmentés incomplets). L'IDS sera dès lors incapable d'exécuter sa fonctionnalité de détection, et le pirate pourra réaliser son attaque.

4.7.3. Techniques d'insertion

Comme nous l'avons vu, ces techniques consistent à injecter des données supplémentaires de telle sorte que :[David, Jonathan ; 2006]

- l'IDS les estime inoffensives

la cible ne les décode pas.

Voici quelques méthodes permettant d'utiliser des techniques d'insertion :

- ✓ en utilisant la fragmentation IP qui est gérée de manière différente selon l'OS, lors de cas anormaux (ex : recouvrement de paquets) : soit les fragments anciens sont favorisés, soit les nouveaux le sont. Par exemple, il est donc possible que les IDS favorisent les anciens paquets alors que le système d'exploitation utilisé favorise les nouveaux. Pour utiliser le recouvrement de fragments (fragmentation overlap), il faut modifier artificiellement les champs « longueur » et « décalage » (offset) des fragments IP.
- ✓ en utilisant l'écrasement de fragments (fragmentation overwrite) : même principe que précédemment, mais des fragments entiers sont remplacés, et non seulement des parties de paquets.
- ✓ en utilisant le timeout de fragmentation : les systèmes conservent en général les fragments pendant 60 secondes pour le réassemblage; mais les IDS les gardent souvent moins longtemps. On peut donc espacer les fragments dans le temps pour ne pas se faire repérer par l'IDS tout en réalisant une attaque complète sur le système d'exploitation.
- ✓ découpage de sessions TCP (session splicing) : la requête TCP est divisée en paquets, tout en modifiant le numéro de séquence pour créer des recouvrements : même principe qu'avec la fragmentation IP + possibilité de timeout (Apache Linux : 5min dans tampon, IIS : 10min). L'un des outils pour réaliser ce genre d'attaques se nomme fragroute.
- ✓ insérer un faux paquet avec une somme de contrôle[3] (empreinte) erroné : certains IDS ne verront pas l'attaque, car il existe peu d'IDS qui vérifient cette somme, donc le système rejettera le paquet erroné.

[3]Somme de contrôle (checksum): est un nombre qu'on ajoute à un message à transmettre pour permettre au récepteur de vérifier que le message reçu est bien celui qui a été envoyé

4.7.4. Les techniques d'évasion

Les techniques d'évasion ont pour le but d'insérer des données qui seront ignorées par l'IDS, mais qui ne gêneront nullement l'attaque.[David , Jonathan ;2006]

- **Evasions HTTP** : le principe est de modifier la syntaxe des URL, mais sans changer la sémantique. La première personne à avoir présenté ce genre d'attaques avait pour pseudonyme Rain Forrest Puppy qui est l'auteur du très célèbre outil Whisker, un scanner de vulnérabilités Web.[[David , Jonathan ;2006]
- **le shellcode** :c'est-à-dire le code qui sera exécuté sur la machine et qui permettra de donner l'accès à un shell de commandes. une adresse de retour de procédure (qui pointe souvent vers les NOP) qui permettra lors du dépassement de buffer d'exécuter le shellcode.[David ,Jonathan ;2006]
  - ✓ **Shellcodes polymorphiques** : parmi les attaques décrites précédemment, nous avons vu les tentatives de buffer overflow. Des instructions pour remplir le buffer.

4.8. Quelques Systèmes de Détection D'intrusions existants

Actuellement, Il existe plusieurs systèmes de détection d'intrusions qui ont été développés, certains sont commercialisés et d'autres sont encore dans les laboratoires de recherche. Nous présenterons quelques systèmes de détection d'intrusions existants.

4.8.1. IDES

IDES (Intrusion-Detection Expert System) a été développé par SRI International. Il représente le modèle de référence pour un grand nombre de systèmes de détection d'intrusions. Il a été conçu pour surveiller un seul hôte et il traite uniquement les données d'audit. Ce système de détection d'intrusions est indépendant du système surveillé, il fonctionne sur une machine dédiée, reliée au système par un réseau. Afin de détecter les violations de sécurité en temps réel, IDES s'appuie aussi bien sur une approche statistique que sur un système expert.

4.8.2. NIDES

NIDES (Next- Generation IDES) est une version améliorée du système de détection d'intrusions IDES. Il assure la détection d'intrusions sur plusieurs hôtes (distribuées) en se basant toujours sur les données d'audit. Il n'y a aucune analyse du trafic réseau. Il utilise les mêmes algorithmes qu'IDES. [MYK, 1994]

4.8.3. NADIR

NADIR (Network Anomaly Detection and Intrusion Reporter) est un système expert qui a été conçu pour le réseau ICN (Integrated Computing Network) du Laboratoire National Los Alamos. Son but est d'analyser les activités réseau des utilisateurs et d 'ICN en se basant sur les règles du système expert qui définissent la politique de sécurité et les comportements suspects. L'inconvénient majeur de ce système est qu'il ne peut être porté sur d'autres réseaux, étant donné que les protocoles réseau d'ICN ne sont pas standards. [Mykerjee. B et al, 1994],

4.8.4. GrIDS

GrIDS (Graph-Based Intrusion Detection System) a été conçu pour détecter des attaques à grande échelle. GrIDS considère les réseaux larges comme une agrégation de sous réseaux. Les données concernant l'activité des hôtes et le trafic réseau entre ces hôtes sont rassemblées dans des graphes d'activité qui révèlent la structure causale de l'activité réseau. [S. Staniford-Chen, 1996]

5. Classification des systèmes de détection d'intrusion

Plusieurs classifications des méthodes de détection d'intrusion ont été proposées, mais il n'existe toujours pas de taxonomie universellement. Dans cette partie, nous présentons une taxonomie basée sur la synthèse d'un certain nombre d'éléments existants. Nous utilisons cinq critères pour classer les IDS, comme le résume la Figure 2.4.

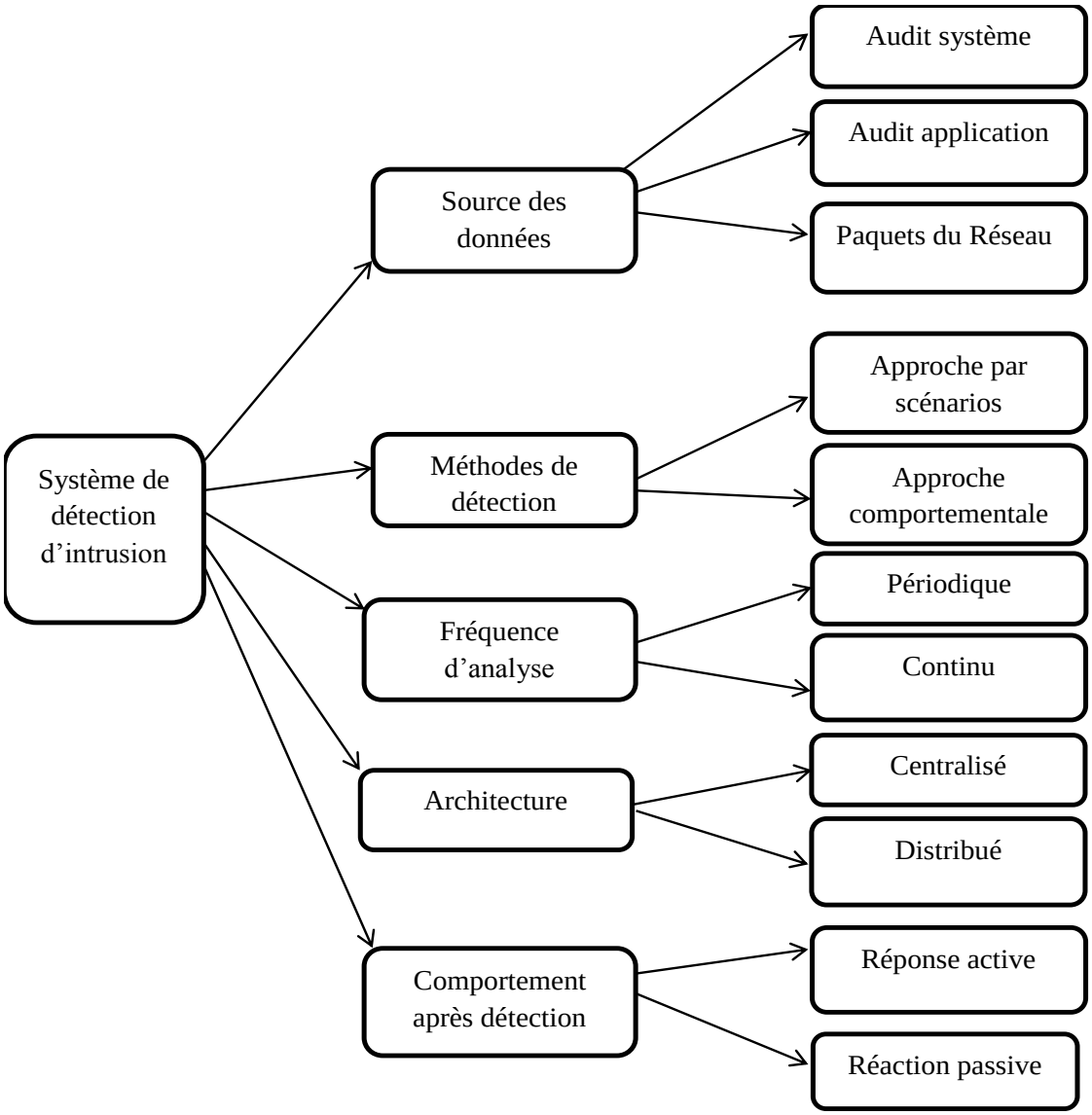

Figure 2.4 : *Classification des systèmes de détection d'intrusion. [Aleksandar Lazarevic et al, 2005]*

5.1. La source des données

Les systèmes de détection d'intrusions sont classés en fonction de l'origine des données qui seront exploitées pour détecter des actions intrusives. La source de données utilisée est une caractéristique essentielle pour classer les systèmes de détection d'intrusions. On distingue trois catégories de sources d'informations :

- Les audits système.
- Les audits applicatifs.
- Le trafic réseau.

5.1.1. Les audits système

Les audits système sont produits par le système d'exploitation d'un hôte. Ces données permettent à un IDS de contrôler et recueillir des informations sur les activités d'un utilisateur sur un hôte.

5.1.2. Les sources d'informations réseau

Ce sont des données du trafic réseau. Cette source d'informations est prometteuse, car elle permet de collecter et analyser les paquets de données circulant sur le réseau.

Les IDS qui exploitent ces sources de données sont appelées : Les IDS basés réseau « Network Based Intrusion Detection System ».

5.1.3. Les audits applicatifs

La troisième catégorie de source de données est constituée des audits applicatifs. Les données à analyser sont produites directement par une application, par exemple des fichiers logs générés par les serveurs ftp et les serveurs Web. L'avantage de cette catégorie est que les données produites sont très synthétiques, elles sont sémantiquement riches et leur volume est modéré. On note que ces types d'informations sont généralement intégrés dans les IDS basés hôte. [Hervé Debar ,2009]

5.2.Les méthodes de détection d'intrusion

Lorsqu'on parle de système de détection d'intrusion, on pense avant tout à la méthode de détection utilisée ou ce qu'on appelle la stratégie d'analyse. Dans la pratique, on distingue deux approches principales pour analyser les événements afin de détecter les attaques : L'approche à base de connaissances ou approche par signatures (misuse detection) et l'approche comportementale (anomaly detection).

5.2.1. L'approche par signatures (misuse detection) :

Cette approche consiste à chercher dans les activités des entités surveillées les empreintes ou les signatures des attaques connues. Chacune de ces signatures décrit une attaque spécifique et chaque attaque peut être détectée par un ou une séquence d'événements obtenus à partir d'un ou plusieurs capteurs (collecteur d'informations) (figure 2.5). Ces derniers permettent de classifier tous les événements d'attaques qui peuvent provenir, soit d'un hôte (exemple : fichiers audit, trace d'exécution des commandes, etc.), soit d'un réseau. La figure 2.5 montre un modèle générique d'un IDS adapté pour l'approche par signature. Cette démarche est similaire à celle des outils antivirus et présente les mêmes inconvénients que ceux-ci.

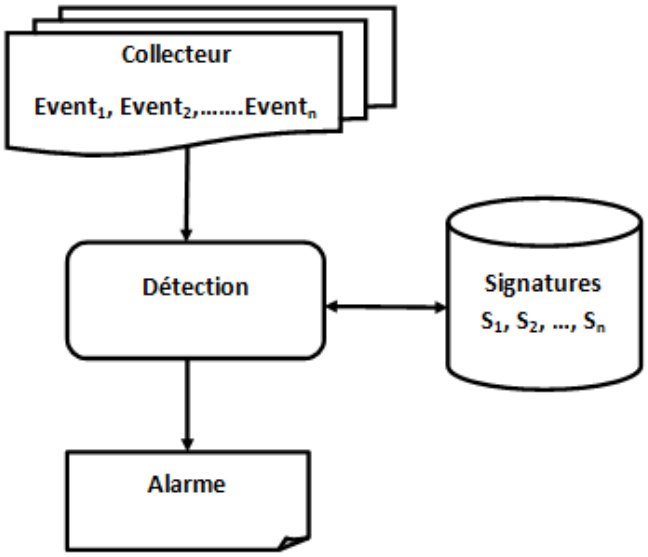

***Figure 2.5** : Modèle de détection pour l'approche par signature. [A.KARTIT et al ,2012]*

Ce qui nous amène à conclure que ce type d'IDS ne peut détecter que les attaques qu'ils ont des signatures. Ces IDS nécessitent des mises à jour régulières de leur base de signatures et leur efficacité dépend du contenu de cette base. Si les signatures sont fausses ou mal conçues, l'ensemble du système est par conséquent inefficace. Ce modèle est très facile à implémenter et à optimiser.

L'approche par signature nécessite d'avoir la connaissance des attaques auxquelles le système est exposé. Cette base de connaissance est utilisée pour détecter l'occurrence d'attaques contre le système.

- **Les Mécanismes de détection par approche de signature**

Plusieurs mécanismes ont été proposés pour localiser les signatures d'attaques dans les traces d'audit. Parmi ces mécanismes :

- **Systèmes experts** : ils utilisent un ensemble de règles d'implication "Si-alors" pour caractériser les signatures de malveillance.
- **Analyse des transitions d'états** : Les signatures d'attaques sont considérées comme des systèmes de transitions étiquetées. En démarrant d'un état initial et en analysant les séquences d'actions effectuées sur le système, nous pouvons détecter des états indésirables qui reflètent des tentatives d'intrusions.
- **Réseaux de neurones** : la flexibilité apportée par les réseaux de neuronaux permet d'analyser les données même si elles sont incomplètes ou déformées. Ils peuvent de plus permettre une analyse non-linéaire de ces données. Les réseaux de neurones permettent de faire une analyse efficace du flux d'audit en temps réel grâce à leur flexibilité et leur rapidité.

On peut utiliser les réseaux neuronaux pour filtrer et sélectionner les informations suspectes pour permettre une analyse détaillée par un système expert. On peut aussi les utiliser directement pour la détection de malveillances. Mais leur apprentissage est extrêmement délicat, et il est difficile de savoir quand un réseau est prêt pour l'utilisation.

Les réseaux de neurones sont souvent utilisés pour distribuer une population (un ensemble d'individus) en différentes classes. Pour la détection d'intrusions, la population est l'ensemble des actions effectuées sur le système. Ces actions, on peut les distribuer en deux classes : les actions malicieuses et les actions non malicieuses.

- **Reconnaissance des formes (Pattern Matching) :** avec la représentation des signatures d'attaques par des séquences abstraites d'événements et la modélisation de trafic par une séquence concrète d'actions et de voir s'il est possible de les unifier. Cette technique peut être utile pour l'identification d'intrusions qui sont proches, mais différentes.
- **Algorithmes génétiques** : on définit chaque scénario d'attaque comme un ensemble pas forcément ordonné d'événements. Lorsqu'on veut tenir compte de tous les entrelacements possibles entre ces ensembles, l'explosion combinatoire qui en résulte interdit l'usage d'algorithmes de recherche traditionnels, et les algorithmes génétiques sont d'un grand secours.

L'approche par signature possède un certain nombre des avantages et d'inconvénients.

- **Les avantages de l'analyse basée connaissance**
  - L'analyse basée connaissance est très efficace pour la détection d'attaque avec un taux très bas des alarmes de type faux positif.
  - Les alarmes générées sont significatives.
- **Les inconvénients de l'analyse basée connaissance**
  - L'analyse basée connaissance permet seulement la détection des attaques qui sont connues au préalable. Donc, la base de connaissances doit être constamment mise à jour avec les signatures de nouvelles attaques.
  - Le risque que l'attaquant peut influencer sur la détection après la reconnaissance des signatures.

5.2.2. L'approche comportementale (anomaly detection)

Cette approche consiste à modéliser le comportement normal du système ou de la partie du système qui risque d'être attaquée (détecter si un utilisateur a un comportement anormal par rapport à ses habitudes). Ce comportement est utilisé dans la phase de détection en observant si le système dévie de ce comportement normal. Si tel est le cas, on suppose qu'une attaque a eu lieu contre le système.

L'approche comportementale utilise un modèle statistique développé par Denning dans [D.dening ,1987] où elle se base sur le profil du comportement normal de l'utilisateur, compte tenu de plusieurs variables aléatoires.

Au cours de l'analyse, le système calcule un taux de déviation entre le comportement courant et le comportement passé. Si ce taux dépasse un certain seuil, le système signale un comportement inhabituel et déclare qu'il a été attaqué.

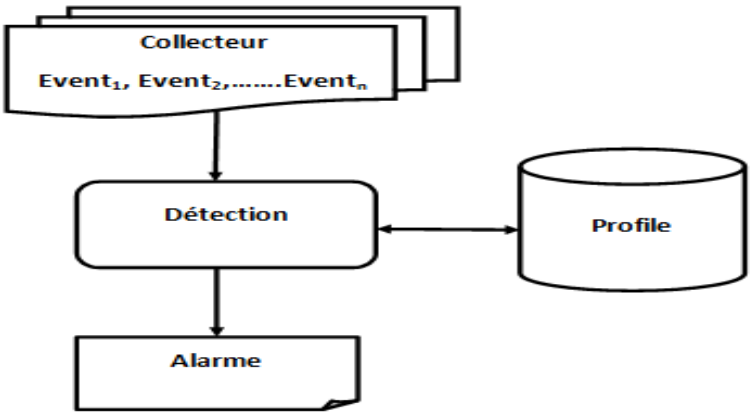

Figure 2.6 : *Modèle de détection par l'approche comportementale. [A.KARTIT et al ,2012]*

Le principal avantage de cette approche par rapport à l'approche par signatures est qu'elle est capable de détecter des attaques non encore connues.

Toutefois, la difficulté de l'approche comportementale consiste en la construction d'un modèle de comportement légitime exact et complet. Sans ces deux propriétés, la détection risque d'être sujette à :

- ✓ **Des faux positifs** : le système lance des fausses alertes des détections d'intrusion qui ne sont pas réellement des attaques.
- ✓ **Des faux négatifs :** des attaques non détectées par le système de détection d'intrusion (le système ne détecte pas l'intrusion dans le cas d'un intrus qui a un comportement normal).

➢ **Les mécanismes de détection par approche comportementale**

Il existe de nombreux algorithmes de détection d'anomalie proposés dans la littérature qui diffèrent selon les informations utilisées pour l'analyse et selon des techniques qui sont utilisées pour détecter des déviations du comportement normal. Une classification des techniques de détection des anomalies basées sur les techniques employées dans les cinq groupes suivants :

- **Méthodes statistiques :** Les méthodes statistiques surveillent le comportement de l'utilisateur ou du système en mesurant certaines variables dans le temps (par exemple, le temps de connexion et de déconnexion de chaque session).
- **Méthodes basées sur la distance :** La plupart des approches statistiques ont des limites lorsqu'elles détectent des valeurs aberrantes dans des espaces à dimensions supérieures, car il devient de plus en plus difficile et inexact d'estimer les distributions multidimensionnelles des points de données. Les approches basées sur la distance tentent de surmonter les limites des approches de détection des aberrations statistiques et elles détectent les valeurs aberrantes en calculant les distances entre les points.
- **Technique des Systèmes basés sur des règles :**Les systèmes basés sur des règles utilisés dans la détection des anomalies caractérisent le comportement normal des utilisateurs, des réseaux et/ou des systèmes informatiques par un ensemble de règles.
- **Méthodes de profilage :** Dans les méthodes de profilage, des profils de comportement normal sont construits pour différents types de trafic réseau, utilisateurs, programmes, etc., et les écarts par rapport à ceux-ci sont considérés comme des intrusions. Les méthodes de profilage varient considérablement, allant de différentes techniques d'exploration de données à diverses approches heuristiques.
- **Approches basées sur un modèle :** De nombreux chercheurs ont utilisé différents types de modèles pour caractériser le comportement normal du système surveillé. Dans les approches

basées sur le modèle, les anomalies sont détectées comme des écarts pour le modèle qui représente le comportement normal.

L'approche comportementale possède un certain nombre des avantages et d'inconvénients.

- **Les avantages de l'analyse comportementale**
  - Efficace pour détecter de nouvelles situations imprévues vulnérabilités.
  - Moins dépendant du système d'exploitation.
  - Faciliter la détection des abus de privilège
- **Les inconvénients de l'analyse comportementale**
  - Faible précision des profils en raison des événements observés.
  - Non disponible lors de la reconstruction des profils de comportement.
  - Difficile de déclencher des alertes en temps réel. [Aleksandar Lazarevic et al, 2005]

5.3. Fréquence d'analyse

En ce qui concerne les aspects temporels des IDS, nous distinguons deux groupes principaux :

5.3.1. Les IDS en temps réel (On ligne/continu) :

Tentent de détecter les intrusions en temps réel ou presque en temps réel. Ils fonctionnent sur des flux de données continues provenant de sources d'information et analysent les données pendant que les sessions sont en cours.

5.3.2. Les IDS hors ligne(Périodique) :

Effectuent une analyse des données d'audit. Cette méthode analyse périodiquement les différentes sources de données à la recherche d'une éventuelle intrusion ou une anomalie passée. [Herve Debar ,2009]

5.4. Architecture

La plupart des systèmes de détection d'intrusion sont en architecture centralisée, ils détectent les intrusions qui se produisent dans un seul système / réseau surveillé.

Actuellement ; plusieurs attaques apparaissent qui ont une architecture distribuée et les processeurs centralisés ne sont pas capables de traiter les données collectées à partir des attaques réparties en réseau ou distribuées (par exemple l'attaque DDoS).

Dans un IDS centralisée, l'analyse des données est effectuée sur un nombre fixé d'emplacements. Par contre, dans l'IDS distribuée (DIDS), l'analyse des données est effectuée sur un certain nombre d'emplacements proportionnel au nombre de systèmes disponibles en réseau. [Herv´e Debar ,2009]

5.5. Comportement après détection

La réponse des IDS aux attaques identifiées peut être passive ou active.

5.5.1. La réponse passive

Les IDS ont une réaction passive laquelle est de faire une alerte d'existence d'une intrusion (événement malveillant), sans aucune contre-mesure n'est activement appliquée pour contrecarrer l'attaque. La méthode la plus courante est celle des notifications ou bien la méthode par le biais de fenêtres pop-up ou des alertes à l'écran ou par l'enregistrement des alertes dans un fichier.

5.5.2. La réponse active :

La réponse active c'est le processus de contre-attaque .Dans ce type de réponses La réaction d'un IDS ne se limite pas à la détection d'intrusion et au lancement d'une alerte d'existence, mais la réaction de base centré autour de contre-attaque et quel traitement doit être réalisé pour stoppé les attaques. (Par exemple les bloquées).

5.6. Importance du système de détection d'intrusions (IDS)

Il est important de mettre en œuvre les systèmes de détection d'intrusion dans les organisations pour les raisons suivantes :

- Se comportent comme une couche supplémentaire de protection et fournie d'autres mécanismes de sécurité.
- Détecte les intrusions et tous autres événements suspects.
- Détecte les attaques dans ses premières étapes au même temps où l'attaquant commence juste à faire une attaque de scan (analyser les ports pour déterminer les failles du réseau).
- Prépare des rapports sur les activités détectées pour l'administrateur système.
- Une technique simple pour analyser les mesures de sécurité. [Hussain Ahmad Madni Uppal et all 14]

5.7. Évaluation des systèmes de détection d'intrusions

On peut évaluer les systèmes de détection d'intrusions selon deux critères : [Aleksandar Lazarevic et al ,2005]

5.7.1. La performance : la performance d'un système de détection d'intrusions est basée sur le mécanisme de temps de réponse (temps de lancement des alertes) et le mécanisme de contre-attaque comme suit :

A. Performance horaire : La performance du temps d'un système de détection d'intrusion correspond au temps total que l'IDS doit détecter une intrusion. Ce temps comprend le temps de traitement et le temps de propagation.

- ✓ **Le temps de traitement :** dépend de la vitesse des processus de traitement de l'IDS, Il représente le taux auquel l'IDS fait la déclaration d'une intrusion. Si ce taux n'est pas suffisamment élevé, le traitement en temps réel des événements de sécurité peut ne pas être réalisable.
- ✓ **Le temps de propagation :** est le temps nécessaire pour que l'information traitée se propage à l'analyste de sécurité.

Les deux temps doivent être les plus courts possible pour permettre à l'analyste de sécurité de réagir à une attaque avant de faire beaucoup de dégâts, et d'empêcher un attaquant de modifier les informations d'audit ou de modifier l'IDS lui-même.

B. Performance de la prédiction : Dans la détection d'intrusion, la mesure de performance simple telle que la précision de la prédiction n'est pas suffisante.

Par exemple, les intrusions de réseau représentent généralement un pourcentage très faible (par exemple 1%) de l'ensemble du trafic réseau, et un IDS banal qui étiquette tout le trafic réseau normalement, peut atteindre 99% de précision.

Afin d'avoir une bonne performance de prédiction, un IDS doit satisfaire deux critères: il doit être capable d'identifier correctement les intrusions et il ne doit pas identifier une action légitime dans un environnement système comme intrusion.

Les mesures typiques pour évaluer la performance prédictive des IDS incluent le taux de détection et le taux de fausses alarmes.

- ✓ Le taux de détection : est défini comme le rapport entre le nombre d'attaques correctement détectées et le nombre total d'attaques ;

- ✓ le faux-signal d'alarme (faux positif / faux négatif) est le rapport du nombre de connexions normales incorrectement erronées en tant qu'attaques et le nombre total de Connexions normales.

Ces faux signaux sont représentés à l'aide d'une matrice de confusion qui contient des informations sur les classifications réelles et prédites réalisées par un système de classification.

Les performances de ces systèmes sont généralement évaluées en utilisant les données illustrées dans la matrice de confusion. [Nadia Boumkheld et al, 2016]

Tableau2.1 : *Matrice de confusion.*

	Classe prédite		
Classe actuelle		Classe négative (Normal) N	Classe positive (Attaque) P
	Classe négative (Normal)	Vrai négatif (VN)	Faux positif (FP)
	Classe positive (Attaque)	Faux négatif (FN)	Vrai positif (VP)

P➔ positif : signifie la présence d'une attaque

N➔ négatif : signifie qu'il n'y a pas d'attaque

VP➔ vrai positif : est le nombre de prédictions correctes des cas positifs (nombre d'intrusions correctement classées comme des intrusions).

VN➔vrai négatif : est le nombre de prédictions correctes de négatives detection (nombre d'utilisateurs légitimes correctement classés comme légitime).

FN➔ faux négatif : est le nombre de prédictions incorrectes des cas négatives (nombre des intrusions qui ne sont pas classées comme des intrusions et qui sont classées comme des utilisateurs légitimes).

FP➔ Faux posotif : est le nombre de prédictions incorrectes (nombre des utilisateurs légitimes classés incorrectement comme des intrus).

Le calcul des valeurs des éléments de classification est fait selon les formules suivantes :

- ✓ **Taux de détection = (VP / P)**

Cet élément désigne le taux de détection d'intrusions qui sont correctement identifiées.

- ✓ **Fausse alarme = (FP / N)**

Cet élément désigne la proportion des utilisateurs légitimes classés incorrectement comme des intrus.

- ✓ **Accuracy (Exactitude) = [(VP + VN)] / [(VP+VN+FN+FP)]**

Cet élément désigne que la proportion du nombre total de prédictions est-elle correcte.

- ✓ **Precision = (VP / (VP + FP))**

Cet élément désigne que la proportion des cas positifs prévus (attaques) était-elle correcte.

- ✓ **Erreur = 1-exactitude**
- ✓ **Taux de faux négatif = (FN / P)**

Cet élément désigne le taux de détection d'intrusion classés incorrectement comme des non intrus (utilisateurs légitimes).

Dans la pratique, il est très difficile d'évaluer ces deux mesures, car il n'est pas possible d'avoir une connaissance globale de toutes les attaques. Étant donné que le taux de détection et le taux de fausses alarmes sont souvent en contraste.

C. La tolérance aux pannes : Un IDS devrait être fiable, robuste et résistant aux attaques, et devrait être capable de récupérer rapidement contre les pannes et de continuer à fournir un service sécurisé.

Ceci est vrai dans le cas de très grandes attaques DoS distribuées, des attaques de débordement de tampon et de diverses attaques délibérées qui peuvent arrêter un système informatique et donc un IDS.

Ce critère est très important pour le bon fonctionnement d'un IDS, car la plupart des IDS commerciaux fonctionnent sur des systèmes d'exploitation et des réseaux vulnérables aux différents types d'attaques.

En outre, IDS devrait également être résistant aux scénarios lorsqu'un adversaire peut provoquer l'IDS à générer un grand nombre d'alarmes fausses ou trompeuses. Ces alarmes peuvent facilement avoir un impact négatif sur la disponibilité du système, et les IDS devraient être en mesure de surmonter rapidement ces obstacles.

Conclusion

Dans ce chapitre nous avons vu comment un attaquant peut compromettre un système informatique en suivant une stratégie bien définie et en utilisant des outils adaptés. Pour remédier à ces problèmes, des solutions de sécurité efficaces sont mises en œuvre par les administrateurs.

Les techniques traditionnelles de prévention des intrusions, telles que les pare-feu, le contrôle d'accès ou le cryptage, n'ont pas totalement réussi à protéger le réseau. Dans une optique d'optimisation de cette sécurisation, les systèmes de détection d'intrusions présentent un bon moyen pour garantir une sécurité maximale aux réseaux.

Nous avons discuté dans ce chapitre qu'un système de détection d'intrusion est la partie importante du système défensif de ressources d'ordinateur et de réseau. Ce système détecte les attaques et les intrusions ainsi que toutes les activités malveillantes plus précisément que n'importe quel autre système de sécurité et soulève moins d'alarmes faussement positives. Comme il s'agit d'une mesure de sécurité importante, il devient donc nécessaire pour les organisations de le mettre en œuvre.

Les plupart des IDS sont fiables, ce qui explique qu'ils sont souvent intégrés comme des solutions de sécurité. Les avantages qu'ils présentent face aux autres outils de sécurités les favorisent, mais d'un autre côté cela n'empêche pas que les meilleurs IDS présentent aussi des lacunes et quelques inconvénients.

Chapitre 3: Les Systèmes de détection d'intrusion dans le contexte des Smart Grids

Introduction

La grille intelligente s'étend en utilisant des technologies TIC avancées comprenant à la fois des réseaux câblés et sans fil, y compris le pouvoir de créer des réseaux ad hoc en cas d'urgence.

Grâce à cette extension, le réseau local (HAN) est également couvert .Cela rend le Smart grid un réseau énorme qui fonctionne simultanément dans les secteurs de l'offre (production) et de la demande (consommation).

Afin d'optimiser la production, la consommation et la distribution de l'énergie, les différents dispositifs d'un smart grid échangent quotidiennement des flux croissants d'informations. La sécurisation de ces flux de données est essentielle.

Une seule défaillance ou attaque pourrait menacer la sécurité de tout l'ensemble d'un réseau électrique intelligent. Le système de protection intelligent en Smart Grid doit non seulement compromettre l'infrastructure du réseau électrique en raison d'erreurs des utilisateurs, de pannes d'équipements et de catastrophes naturelles, mais aussi de cyberattaques délibérées, comme les employés mécontents, les espions industriels et les terroristes [Fang et al, 2012].

La cyber sécurité est considéré comme l'un des plus grands défis des SG. Les vulnérabilités peuvent permettre à un attaquant de pénétrer dans un système, d'obtenir des données privées des utilisateurs, d'accéder au logiciel de contrôle et de modifier les conditions de charge pour déstabiliser la grille de manière imprévisible.

Les réseaux traditionnels de contrôle de supervision et d'acquisition de données (SCADA) manquent d'une telle intégration et restent logiquement et physiquement séparés.

Le Smart Grid est la fusion entre les réseaux SCADA et les TIC qui améliorent la livraison d'électricité aux consommateurs avec une interruption minimale en fournissant un système d'autogestion pour accroître l'efficacité, la génération de revenus et la résilience au remplacement des infrastructures critiques vieillissantes.

Les futurs SG ouvriront de nouvelles fonctionnalités au système d'alimentation électrique actuel avec des objectifs de haute résistance aux perturbations, un contrôle total de l'alimentation électrique et de la consommation dans les réseaux de distribution et l'amélioration de l'observation du réseau à l'aide de fonctions de gestion avancées. Cela présente de nouveaux risques de sécurité abordés dans les deux questions suivantes :

- Pourquoi les Smart Grid ont besoin de protection ?
- Pourquoi les systèmes de sécurité traditionnels ne sont pas suffisants ?

Dans ce chapitre, nous commençons d'abord par présenter brièvement les besoins de sécurité des réseaux électriques intelligents .Ensuite, nous allons décrire en détail la classification des attaques qui peuvent affecter ce type de réseaux .Enfin on va parler sur l'efficacité des IDS que nous avons les détaillés dans le chapitre précédent comme des meilleurs outils de sécurisation où nous utilisons les travaux de recherches précédents pour confirmer ce choix.

1. Pourquoi les Smart Grid ont besoin de protection ?

Notre dépendance à l'électricité et la dépendance au SG pour la gestion et la distribution de l'électricité en font un atout essentiel. La perturbation de l'alimentation électrique a d'énormes conséquences et impacts sur la société. Par conséquent, la sécurité du SG devient une question importante.

L'épine dorsale de SG est ses réseaux sous-jacents qui relient les différents composants et qui permettent une communication mutuelle entre eux.

Les émergences de ces vastes réseaux multi-facettes sont plus facilement exposées aux cyberattaques.

Le HAN du côté de la demande fournit le point d'accès le plus simple pour les cyber-attaquants.

La connectivité des réseaux entre SCADA et les TIC augmente le risque d'attaque cybernétique qui devient de plus en plus grave, allant des piratages et des attaques terroristes à l'espionnage industriel.

Les vulnérabilités du système permettent à un attaquant de pirater un centre de gestion de contrôle et de manipuler les conditions de charge, de la distribution d'électricité pour endommager l'équipement, déstabiliser un SG ou bloquer l'accès au réseau.

La plupart des systèmes nécessitent des données en temps réel et toute perte peut avoir des effets négatifs sur les réseaux électriques.

Dans plus de 90% des scénarios d'attaque par cyber-attaque, l'attaquant manipule toutes les vulnérabilités bien connues et les serveurs mal configurés, les systèmes d'exploitation et les périphériques réseau.

Par exemple, en juillet 2010, le ver Stuxnet a utilisé les vulnérabilités du système d'exploitation Microsoft Windows pour attaquer un système SCADA. Il est signalé comme la première attaque de code malveillant qui a porté atteinte directement à l'infrastructure nucléaire sensible dans 45 000 réseaux mondiaux.

Les Cyber incidents comme ceux-ci nécessitent d'intégrer intrinsèquement des systèmes de sécurité cybernétique avec un IDPS sophistiqués comme une exigence fondamentale des SG futurs pour surmonter la destruction intentionnelle et les dégâts involontaires

1.1. Les besoins de sécurité pour les communications du Smart Meters

Un certain nombre de services de sécurité sont nécessaires pour sécuriser les échanges du smart meters avec le centre de contrôle. Les principaux défis de la sécurisation de ces échanges se résument dans la mise en place :

- **D'un service d'authentification** afin d'éviter les attaques d'usurpation d'identité et d'injection de faux messages. L'injection de fausses commandes de connexion par exemple peut priver d'électricité tout un quartier voire même des bâtiments publics sensibles tels que des hôpitaux, des commissariats de police etc.
- **D'un service d'intégrité** afin d'éviter les attaques de modification ; par exemple les messages contenant les mesures d'énergie consommée au niveau du HAN ont une grande importance dans le réseau smart grid et leur modification peut causer des conséquences graves sur les frais de consommations.
- **D'un service de confidentialité** afin de contrer les attaques d'écoute et d'atteinte à la vie privée. Ce service a une importance primordiale, puisqu'il permettra de rendre les messages échangés entre le Smart Meter et le centre de contrôle incompréhensibles pour tout attaquant. La mise en œuvre de ce service doit répondre aux exigences des applications temps réel du réseau Smart Grid.

  Le smart Meter est un dispositif important du Smart Grid. Il est critique de point de vue disponibilité. Un dysfonctionnement de ce composant peut causer des conséquences graves, d'où la nécessité de la mise en œuvre d'un service de disponibilité pour éviter les attaques de déni de service.

  Les communications entre le smart Meter et le centre de contrôle nécessitent la mise en œuvre de mécanismes d'anti-rejeu pour éviter le rejeu de certains messages ou commande tels que : messages de panne, messages du taux consommation, facture, commandes de coupure de courant ...etc.

2. Les attaques sur l'architecture du Smart Grid

Le déploiement des technologies de l'information et de la communication sur les réseaux d'électricité soulève plus de préoccupations concernant la sécurité du système électrique et la protection des données de consommation que par les réseaux électriques traditionnels. [Y. Xiao ,2012]

Plusieurs travaux ont été intéressés par l'identification des attaques et des menaces sur les Smart Grid, Ils les ont classés selon les différents composants du réseau Smart Grid, à savoir :

- Dispositifs
- Systèmes
- Réseaux

2.1. Les attaques sur les Dispositifs

Plusieurs types d'attaques peuvent affecter différents dispositifs (smart meter, PHEV, PMU,.. .etc) d'un réseau Smart Grid. Dans cette partie, nous allons présenter ces attaques.

2.1.1. Smart Meter (compteurs intelligents)

Le nœud malveillant peut perturber les actions normales des compteurs intelligents en effectuant plusieurs types d'attaques :

- **Des attaques de brouillage** peuvent être lancées pour empêcher le compteur intelligent de communiquer avec d'autres nœuds du réseau Smart Grid. (sous-stations distribuées, compteurs intelligents voisins, centre de contrôle)
- **L'attaque d'écoute** peut être effectuée pour détecter des informations sensibles sur l'utilisation d'énergie du consommateur (consommation d'énergie, factures d'énergie, types de périphériques électroniques domestiques ...). De même, cette attaque peut aboutir à une attaque sur la vie privée des consommateurs**.**
- **L'attaque de fausses données injectées (false data injection attack):** un attaquant peut effectuer une attaque par injection des fausses données contre les compteurs intelligents en envoyant une commande de contrôle des erreurs.
- **L'attaque de déconnexion à distance : Cette attaque fonctionne** à l'aide d'une application appelé **Remote Connect Disconnect** (RCD) qui permette aux attaquants d'effectuer une attaque de déconnexion à distance en envoyant des commandes de déconnexion pour arrêter le compteur intelligent du client. Nous pouvons noter que les attaquants peuvent également utiliser cette application pour connecter un compteur intelligent et bénéficier d'une énergie illégale. [ImenAouini and Lamia Ben Azzouz,2015]
- **L'attaque par 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). [Thien-ToanTran ,2013]
- **L'attaque de modification :** les auteurs de l'article [Rui Tan et al ,2013] 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 en réduisant leurs valeurs avec la scalingattack, ou en fournissant les anciens prix à plus de la moitié de tous les consommateurs avec le delayattack (peut être réalisée en compromettant la synchronisation de l'heure des compteurs intelligents déployés.
- **L'attaque par un accès physique :** Les compteurs intelligents sont situés à l'extérieur des maisons. Un attaquant peut avoir un accès physique à au moins un compteur intelligent .Il peut lancer une attaque compromettante à travers une IHM pour divulguer des clés et d'autres informations. Par exemple, de telles attaques sont possibles en utilisant des outils open source connu sous le nom de KillerBee. [Mohammad Hossein Yaghmaee et al ,2013]

2.1.2. Home gateway

La Home gateway reçoit les données de consommation d'énergie du compteur intelligent et l'affiche sur des outils qui sont utilisé par les consommateurs pour connecter à leur profil de consommation (par exemple, ordinateur portable, tablette, Smartphone).

La passerelle domestique (home gateway) où le compteur intelligent peut envoyer les données de consommation d'énergie à un fournisseur de services pour gérer l'utilisation de l'énergie à des fins financière (exemple : choix du prix ...).

Les communications dans cette passerelle peuvent être affectées par les attaques d'écoute et de modification. Par exemple, un nœud malveillant peut modifier les données de consommation d'énergie pour affecter les objectives de commercialisations du fournisseur de services. [ImenAouini and Lamia Ben Azzouz ,2015]

2.1.3. Phasor Measurements Units (PMU)

Les unités de mesure Phasor (PMU) sont capables de collecter des mesures sur le terrain des tensions et des quantités électriques et l'envoyer au Phasor Data Concentrator (PDC).

Un nœud malveillant peut effectuer une attaque d'usurpation d'identité sur un PMU, modifier les messages PMU qui contiennent des données de mesure d'énergie et peut également reproduire les messages en transit entre le PMU et le PDC (Phasor Data Concentrator).

Ces attaques affectent les opérations de décision critiques telles que la détection des défauts et la localisation des événements. Par exemple, lorsqu'un attaquant rejoue un ancien message qui contient des pertes de mesure d'énergie ou des pannes de ligne, les systèmes de la grille peuvent prendre une décision pour couper l'électricité dans cette zone. [ImenAouini and Lamia Ben Azzou ,2015]

2.1.4. Plug-in hybrid electric vehicle (PHEV)

Bien qu'une infrastructure de communications bidirectionnelles puisse apporter de nombreux avantages pour le Smart Grid, elle peut introduire des nouvelles vulnérabilités.

Un attaquant peut manipuler l'information de tarification en temps réel qui est communiquée par l'entreprise de service public pour les véhicules. L'attaquant peut perturber la transmission de l'information de prix d'électricité au propriétaire PHEV, entraînant la perte de l'information d'évaluation, qui est, en fait, l'une des possibles attaques de déni de service (DoS) sur le Smart Grid. De même, il est possible pour l'attaquant de manipuler les informations de tarification en injectant des valeurs de prix incorrects afin d'induire en erreur les propriétaires de véhicules hybrides rechargeables. [Yifan Li et al ,2012].

2.1.5. Remote Terminal Unit (RTU)

Les Remote Terminal Unit (RTU) sont traditionnellement utilisées pour configurer et dépanner à distance les périphériques du réseau intelligent. Cette fonctionnalité d'accès à distance peut donner lieu à des attaques qui permettent à des nœuds malveillants de prendre le contrôle des périphériques. [Fadi Aloula et al ,2012].

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 entraînera un retard ou une inhibition de l'échange de données en temps réel.

En conséquence, les opérateurs de centres de contrôle peuvent ne pas avoir une vue complète de l'état de la du réseau électrique, ce qui entraîne une prise de décision incorrecte. [Dong Wei et al ,2011]

2.1.6. Voltage Control Device

Un attaquant peut manipuler le comportement d'un régulateur de tension par l'injection des fausses données de tension. Cette attaque peut être effectuée de façon furtive, en injectant un flux de paquets avec des petits détournements de voltage normal, les attaques peuvent ne pas être détectées par le système jusqu'à ce qu'il aboutisse à un résultat catastrophique (c'est-à-dire une panne de courant). [JianyeHao et al ,2011]

2.1.7. Sensors or Intelligent Electronic Devices (IEDs)

Les commutateurs sont utilisés pour protéger les infrastructures électriques dans les sous-stations, lorsqu'un IED détecte un état anormal (exemple : courant élevé), il envoie un message ouvrir/fermer aux commutateurs pour équilibrer la charge d'alimentation. Si un attaquant usurpe d'identité d'un IED de surveillance, il pourrait envoyer des faux messages de fermeture/ouverture pour commuter et endommager le système de protection, ce qui entraîne une perte potentielle d'alimentation pour les clients. [Wenye Wang and Zhuo Lu ,2013].

2.2. Les attaques sur les systèmes

Dans cette partie, nous allons étudier la sécurité de quelques systèmes du réseau smart grid.

2.2.1. Les systèmes de contrôle et de gestion

Un nœud malveillant peut effectuer des attaques DoS sur les systèmes de contrôle et affecter leur disponibilité. En outre, une attaque injectée par des fausses données contre les systèmes de contrôle peut affecter leurs décisions. Par exemple, l'envoi de fausses mesures d'énergie aura un impact sur les opérations de distribution et de transmission, tandis que les systèmes prendront des décisions de contrôle basées sur de fausses informations PMU.

Les cybers attaques peuvent causer des problèmes techniques majeurs au niveau du système de gestion de l'énergie (EMS) ; tels que les pannes d'électricité dans les systèmes d'alimentation par injection de données (false Data Injection Attack). Les mesures peuvent contenir des erreurs en raison de diverses raisons telles que des erreurs aléatoires, des informations de topologie incorrectes et l'injection de mauvaises données par des attaquants. En intégrant des technologies cybernétiques plus avancées dans le système de gestion de l'énergie (EMS), les cybers attaques peuvent causer des problèmes techniques majeurs tels que les pannes d'électricité dans les systèmes d'alimentation. Les attaques peuvent également être conçues pour le bénéfice financier de l'attaquant au détriment du coût net de l'électricité par le consommateur. [Mohammad Esmalifalak et al, 2013].

2.2.2. Le système de surveillance, de protection et de contrôle étendu WAMPAC

Le système WAMPAC (Wide Area Monitoring, Protection and Control) est également vulnérable à l'attaque basée sur le chronométrage (attaque DOS) alors que les applications fournissent des opérations et des performances en temps réel.

Une attaque de différent service peut être effectuée à différents niveaux de communication. Par exemple, un nœud malveillant peut lancer un blocage qui remplit le support sans fil avec des signaux de bruit et peut avoir un impact sévère sur les messages critiques. L'attaque d'écoute est capable d'endommager la disponibilité du système et le nœud légitime ne peut pas récupérer les messages.

En outre, les d'autres types d'attaques telles que la falsification et les attaques man in the middle ne peuvent être lancés que lorsque les canaux de communication complets ou partiels peuvent être bloqués. [ImenAouini and Lamia Ben Azzouz, 2015]

2.2.3. AMI (Advanced Metering Infrastructure)

Les canaux de communication utilisés par AMI pour communiquer les données entre les smart meters et les systèmes d'utilité sont également vulnérables aux cyberattaques. Les données transitant par ces canaux peuvent être interceptées et falsifiées par des intrus. [SheerazNiazLighari et al ,2014]

Dans le système AMI (communications entre les compteurs intelligents et le centre de contrôle), les messages sont livrés en multi-hop. Les attaques de Man in the Middle peuvent éventuellement être lancées et les informations sur la consommation d'énergie peuvent être modifiées avant de transmettre les messages. En outre, en écoutant sur le canal de communication sans fil, un attaquant pourrait obtenir des informations échangées entre le compteur intelligent et le centre de contrôle. [ImenAouini and Lamia Ben Azzouz, 2015]

2.2.4. Outage Management System (OMS)

La gestion automatisée de la panne nécessite des compteurs intelligents pour envoyer les informations de panne. L'utilitaire utilise les informations telles que l'heure et l'emplacement de la panne du message pour restaurer l'alimentation en temps réduit.

Une interruption de cette fonction affecte directement la résilience opérationnelle de la grille en retardant la récupération et la restauration de l'alimentation des clients finaux.

Un attaquant peut usurper l'identité d'un Smart Meter et envoyer un message de panne, encore il peut modifier le message envoyé (Message modification and false data injection attack) pour influer la résilience de la grille. [Anas AlMajali et al ,2012].

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.

2.3. Les attaques sur les réseaux

Les Smart Grids sont connectés et contrôlés à l'aide des réseaux de communication. Dans cette partie nous avons choisi la classification des attaques qui peuvent être menées sur ce réseau, en deux catégories.

- Attaques sur les protocoles de routages utilisés.
- Attaques sur les protocoles de communication utilisés.

2.3.1. Les attaques sur les protocoles de routage

Parmi les protocoles de routage qui peuvent être utilisés dans les réseaux NAN on cite :

a. **RPL :** 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 récoltées jusqu'au DODAG root (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 des réseaux de faible puissance et avec perte (RPL) définie par l'IETF (Internet Engineering Task Force). Il a été conçu afin de prendre en charge les exigences spécifiques de ces réseaux.
   - Le protocole de routage RPL pour IoT (Internet of Things[1]) peut être affecté par les attaques de transfert sélectif (Selective Forwarding Attacks) : les nœuds malicieux essaient d'arrêter les paquets dans le réseau en refusant de transférer ou d'annuler les messages qui les passages. Avec ces attaques il est possible de lancer des attaques DoS où les nœuds malveillants transfèrent sélectivement les paquets. Cette attaque vise principalement à perturber les chemins de routage. Par exemple, un attaquant peut transmettre tous les messages de contrôle RPL et déposer le reste du trafic. Cette attaque a des conséquences plus sévères lorsqu'elle est couplée à d'autres attaques, par exemple

[1] **Internet of thing :** L'Internet des objets (IoT) est un concept reflétant un ensemble connecté de n'importe qui, n'importe quand, n'importe quel service, et n'importe quel réseau. Elle est une mégatence dans les technologies de nouvelle génération qui peuvent avoir une incidence sur l'ensemble du spectre des entreprises et peut être considérée comme l'interconnexion d'objets et de dispositifs intelligents identifiables de manière unique dans l'infrastructure Internet d'aujourd'hui avec des avantages étendus. Ainsi qu'elle fournit des solutions appropriées pour une large gamme d'applications. Est décrit comme un facilitateur qui relie des objets transparents autour de l'environnement et effectue une sorte d'échange de messages entre eux.

les attaques sinkhole (Un noeud malveillant annonce un chemin de routage avantageux artificiel et attire de nombreux nœuds voisins pour acheminer le trafic à travers celui-ci). [Linus Wallgren et al ,2013]

b. MTE : Le protocole de Transmission de Minimum énergétique (MTE) reprend le protocole DSR (Dynamic Source Routing) de base (sans les caches) et assigne à chacun des liens un poids qui est fonction de l'énergie nécessaire pour transmettre un paquet sur cette voie. Le routage se fait selon les routes de plus faible poids, en agrégeant l'ensemble des liaisons constitutif d'un chemin. [Alaoui Nabih ,2013]

2.3.2. Les attaques sur les protocoles de communication

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 (qui devient l'attaque DoS primaire dans les réseaux smart grid, en particulier dans les systèmes de distribution et de transport).

Dans cette partie, nous allons étudier la sécurité des protocoles ZigBee, DNP3**.**

a. ZigBee

ZigBee a 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 le contenu de la mémoire de cette dernière dans un support, puis il peut trouver la clé. Encore Zigbee peut être affecté par les attaques de type Dos. [Jan Durech and Maria Franekova ,2014]

b. DNP3

Les auteurs de l'article [Zhuo Lu et al ,2010] ont évalué quantitativement l'impact des attaques de déni de service (DoS) sur un réseau expérimental de sous-stations électriques avec DNP3 (Distributed Network Protocol), c'est un protocole de communication largement utilisé dans les systèmes électriques d'aujourd'hui .Ils ont montré que les longs paquets DNP3 sont plus vulnérables aux attaques DoS que les paquets courts DNP3.

2.4. Récapitulatif des attaques sur l'architecture Smart Grid

Un récapitulatif des attaques qui peuvent être menées sur le réseau Smart Grid est représenté dans la figure 3.1.

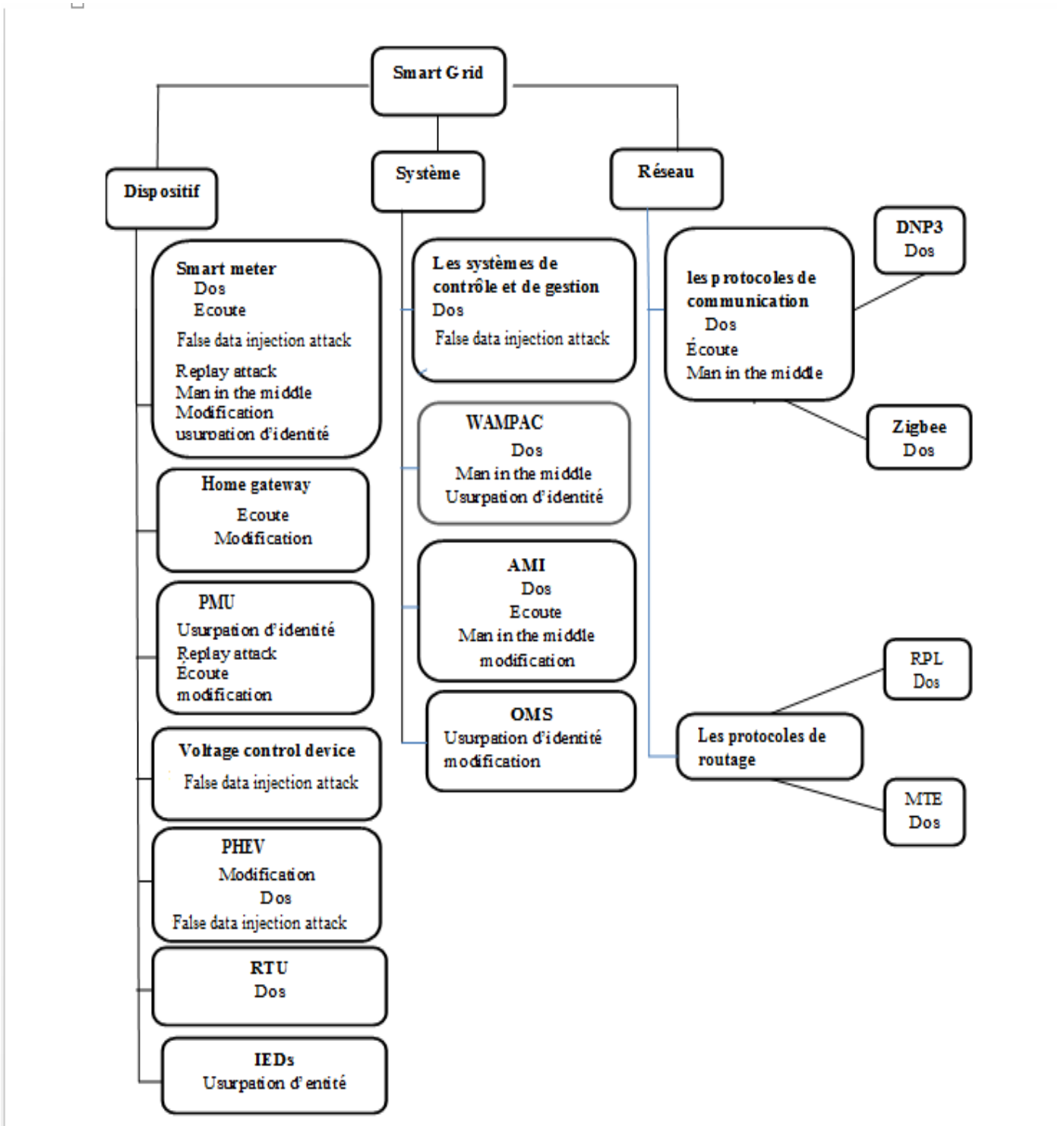

Figure 3.1 : *Un récapitulatif des attaques qui peuvent être menées sur le réseau Smart Grid.*

3. Pourquoi les systèmes de sécurité traditionnels ne sont-ils pas suffisants ?

La sécurité du réseau électrique intelligent présente de nouveaux défis pour l'industrie et les chercheurs, au-delà des problèmes de sécurité traditionnels des réseaux SCADA et TIC, car :

- La plupart des systèmes de contrôle existants sont conçus pour fonctionner dans des réseaux indépendants non connectés, bien que dans les réseaux electrique intélligents toute la technologie devienne numérique.
- SG contient inévitablement des systèmes existants qui ne peuvent être mis à jour, corrigés ou protégés par des techniques traditionnelles de sécurité des TIC. Les systèmes et les périphériques existants avec des ressources informatiques limitées n'ont peu de sécurité.
- SG se compose de technologies de réseau et de protocoles hétérogènes (tels que ProfiBus, ModBus et DNP).
- Les réseaux de SG sont massifs et peuvent potentiellement s'élargir à des milliards de nœuds de réseau.
- Le réseau électrique déployé dans tous les futurs SG devrait répondre aux nouvelles exigences des systèmes entièrement automatisés et de la communication de données en termes de nouveaux protocoles de communication, de charge, de retard, de bande passante et de débit.
- Les réseaux SG sont très flexibles en termes de taille et d'application, et ils pourraient être le moyen potentiel d'intrusion et d'attaque sur le réseau.
- Les réseaux SG sont très sensibles et essentiels, et les intrusions peuvent entraîner une énorme quantité de perte pour les hôtes ou les utilisateurs du réseau. Les réseaux SG devraient être protégés contre de nouvelles intrusions dont les intrus hybrides sont les attaques les plus difficiles pour les systèmes de sécurité traditionnels.
- Tout système de sécurité dans le SG ne doit pas entraver la disponibilité ou la sécurité du système d'alimentation dans toutes les conditions d'utilisation normales et d'urgence, telles que le verrouillage d'un système après beaucoup de tentatives de connexion avec un mot de passe incorrect.

L'une des meilleures façons de protéger un SG, autre que par des mesures extrêmes, est de fournir un IDS intelligent, où il effectue une détection des activités malveillantes et empêche les dégâts plus graves des systèmes protégés en temps réel.

4. Les travaux connexes

4.1. Les Travaux connexes concernant les Smart Grid

Le réseau électrique intelligent utilise les technologies de l'information et de la communication (TIC) pour améliorer la production et la distribution de l'électricité. Il s'appuie sur les communications bidirectionnelles et l'automatisation pour améliorer notablement le rendement énergétique.

Cependant, il reste un problème au niveau de la compatibilité entre les divers systèmes de compteurs intelligents, qui limite leur adoption à grande échelle. Les opérateurs de réseaux électriques et autres acteurs ne peuvent garantir le fonctionnement harmonieux de systèmes et d'équipements venant de différents constructeurs.

La Commission européenne soutient de nombreux projets de recherche et développement (R&D) sur les technologies de Smart grids parmi eux, on peut citer : [w9]

4.1.1. Le projet ADDRESS« Active Distribution network with full integration of Demand and distributed energy RESourceS »

Le projet ADDRESS est un projet européen de R&D relevant du 7éme PCRD ; il été lancé en juin 2008, piloté par EnelDistribuzione[2] et financés par la Commission européenne. [w13]

Ce projet vise à concevoir et développer des solutions techniques et commerciales pour permettre une gestion intelligente des consommations d'électricité. L'objectif est d'améliorer l'efficacité, la sécurité et la qualité de l'approvisionnement électrique, dans un contexte de production électrique d'origine renouvelable croissante.

L'approche proposée s'appuie sur la participation des clients résidentiels et professionnels et sur le développement de nouvelles technologies de gestion des consommations électriques.

Parmi les nombreuses dimensions du Projet ADDRESS, nous citons :

- Le fonctionnement du réseau selon un nouveau scénario, avec l'implication des consommateurs, du système «intelligent» et des entreprises de distribution ;
- Les aspects socio-économiques pour comprendre les exigences des consommateurs et chercher les solutions les plus adéquates ;
- Les télécommunications pour étudier et définir une architecture de communication qui rende possible l'interaction en temps réel entre les clients et les différents sujets du marché ;
- Les systèmes de mesure et de gestion des «électroménagers intelligents», des systèmes de production électrique domestique.

[2]**EnelDistribuzione (ED) :** est l'activation d'une des plus grandes compagnies de surveillance de la qualité d'énergie dans le monde.

4.1.2. Le projet OPEN NODE

Le projet OpenNode été lancé en janvier 2010 ans, il est piloté par Atos Origin[3], dans le but de développer des standards de communication favorisant le développement de l'intelligence et la communication autour du poste de distribution publique dans une approche pré normative. [w12]

L'industrie énergétique européenne est confrontée à trois défis majeurs :

- L'intégration accrue des ressources énergétiques renouvelables et fluctuantes pour atteindre les objectifs climatiques ;
- Augmentation de l'intelligence », en particulier dans le réseau de distribution d'électricité pour répondre aux besoins de capacités croissantes.
- La diversification des parties prenantes en séparant le réseau d'opérations, l'approvisionnement en énergie, les services de comptage et les services auxiliaires ...etc.

Dans le projet OpenNode, le travail se concentre particulièrement sur les parties intérieures du réseau de distribution pour répondre aux trois principaux défis décrits, à savoir sur la recherche et le développement d':

- Un nœud de sous-station secondaire ouvert (SSN) qui est considéré comme un composant de contrôle essentiel de la future grille de distribution intelligente ;
- Un Middleware pour coupler le SSN avec les systèmes Utilities pour l'opération de grille et d'utilité ;
- Une architecture de communication modulaire basée sur des protocoles de communication normalisés pour accorder la flexibilité requise par la diversification des parties prenantes et pour faire face aux systèmes embarqués massivement distribués dans le réseau de distribution.

4.1.3. Le projet OPEN METER «Open Public Extended Network Metering»

En 2011, Le projet OPEN METER, financé par l'unité européenne dans le septième programme-cadre de recherche et développement (7éme PCRD). Il est piloté par Iberdrola, il vise à développer des standards de communication favorisant le développement de services associés au déploiement des compteurs intelligents. Son objectif principal était de rédiger un ensemble complet de normes ouvertes et publiques afin de bâtir une nouvelle infrastructure compatible avec plusieurs systèmes de compteurs intelligents.

Le projet a commencé par analyser les besoins du marché et les problèmes de réglementation, puis a évalué les technologies et les normes, en place ou nouvelles. Il a ensuite identifié et comblé les manques de connaissances et testé les solutions conçues, puis rédigé les normes nécessaires et les a proposées aux organismes de normalisation concernés.

[3]Atos Origin, société internationale de services informatiques, annonce la création d'un centre de services nearshore à Casablanca destiné à ses clients francophones. Ce nouveau centre va permettre d'accélérer de façon significative le développement des activités nearshore du groupe Atos Origin au Maroc.

L'acronyme OPEN METER résume la philosophie du projet : [w10]

- **Open** : Le projet basé sur des normes ouvertes et des solutions non-propriétaires, résultant d'un ensemble de normes ouvertes
- **Public** : les résultats doivent être mis à la disposition de toutes les parties prenantes
- **Extended** : va au-delà de la mesure de l'utilité et permet de fournir de nouveaux services énergétiques
- **Network** : les appareils de mesure deviennent des nœuds de réseaux de télécommunications.

Les objectifs scientifiques et techniques spécifiques du projet OPEN METER qui ont mené à la réalisation de son objectif principal étaient les suivants :

- Fournir une sélection et une compréhension commune pour l'utilisation des normes ouvertes de communication ouvertes adaptées à l'assistance AMI.
- Proposer des recommandations pour les modifications ou les extensions aux normes de communication de données existantes (adaptées aux IAM) adoptées par les organismes de normalisation. Cela devrait conduire à un ensemble harmonisé de normes qui couvrent les besoins de l'AMI.
- Effectuer les activités de recherche et de développement nécessaires pour combler les lacunes existantes en matière de connaissances afin d'avoir des définitions et des spécifications des nouvelles normes et technologies de communication pour les canaux de communication et/ou les nouvelles technologies où les normes n'existent pas encore ou ne répondre pas aux besoins de l'AMI.
- Proposer des procédures de test de conformité et des scénarios de test pour la mise en œuvre de normes de communication de données nouvelles et existantes qui prennent en charge l'AMI et testent les premières implémentations du système en fonction des résultats du projet.
- Sensibiliser les parties prenantes de l'AMI (à savoir les services publics, les opérateurs de réseaux de distribution, les associations, les organismes de normalisation, les utilisateurs finaux, les administrations publiques nationales et européennes, les régulateurs, les développeurs, les fournisseurs et les testeurs).
- Pour lancer et soutenir le processus officiel de normalisation du nouvel ensemble de normes sélectionné et spécifié pour les AMI.

4.1.4. Le projet SmartHouse/SmartGrid

Le projet **SmartHouse/SmartGrid** cherche à faire interagir des maisons intelligentes avec les réseaux intelligents dans le but d'améliorer l'efficacité énergétique. Il était lancé en février 2011.

À l'heure actuelle, les technologies de la maison intelligente et de l'énergie intelligente traitent les maisons et bureaux comme des entités séparées, ce qui a tendance à limiter l'efficacité énergétique.

Le projet SmartHouse/SmartGrid vise à créer un environnement dans lequel des maisons intelligentes pourront être agrégées et permettra la communication, l'interaction et la négociation des consommateurs avec les services énergétiques dans le réseau local d'énergie.

La technologie SmartHouse/SmartGrid repose sur l'utilisation des standards ouverts disponibles dans les secteurs des TIC et de l'énergie, en utilisant des capacités de communication et d'informatique qui sont déjà largement répandues dans les environnements domestiques et de travail traditionnel. [w11]

4.1.5. Le projet SMILE « Smart Ideas to Link Energie »

Le projet SMILE déposé le 17 juillet 2015.Il est porté par les Conseils régionaux de Bretagne et des Pays de la Loire, ainsi que neuf syndicats départementaux d'énergie.

Les objectifs principaux de déploiement de ce projet sont : [w14]

- Intégrer massivement les énergies de sources renouvelables et améliorer leur insertion sur les marchés et les réseaux par une meilleure prévisibilité, l'association à des flexibilités et la disponibilité en période de pointe ;
- Maîtriser les demandes d'électricité et l'adéquation consommation/production, en développant des solutions de flexibilité et de pilotage de la demande ;
- Développer une interconnexion des plates-formes d'échanges et d'analyse des flux de données énergétiques d'origines très diverses ;
- Intégrer les véhicules électriques dans le panel des solutions de mobilité durable, au travers de réseaux de bornes de recharge, plus intelligentes et flexibles et en utilisant des productions renouvelables ;
- Sécuriser les réseaux numériques associés aux réseaux électriques tout au long de la chaîne de valeur en mettant en place des outils de test et de labellisation de cyber-sécurité et d'interopérabilité ;
- Valider les modèles économiques et la viabilité des technologies et services qui ont vocation à être déployés plus largement ensuite par des analyses coûts/bénéfices et des mises à l'échelle.

4.1.6. Le projet des compteurs communicants Linky

La pose des compteurs communicants Linky a commencé le 1er décembre 2015 pour un objectif de remplacer 90 % des anciens compteurs dans 35 millions de foyers en France d'ici à 2021.

Ces compteurs intelligents peuvent recevoir des ordres et envoyer des données sans l'intervention physique d'un technicien.

Linky est le compteur communicant d'électricité, installé par le gestionnaire de réseaux Enedis (ex ERDF). Il est un compteur paramétrable à distance et communicant, capable de stocker et véhiculer de l'information vers le gestionnaire de réseaux (ERDF) et les fournisseurs d'énergie (EDF).

Il facilite l'installation des moyens de production d'énergies renouvelables (photovoltaïque, éolien) en permettant l'utilisation d'un compteur unique qui enregistre à la fois les index de production et de consommation chez les particuliers producteurs d'électricité, un compteur Linky remplacera donc les deux compteurs actuellement installés,

La possibilité de développer de nouvelles offres et de nouveaux services adaptés aux attentes et besoins des clients, sans pour autant remettre en cause les offres ou tarifs actuels. Ces compteurs offrent plusieurs services comme le suivi de consommation en temps réel sur un site Internet dédié et le relevé automatique des consommations électriques.

4.2. Travaux concernant la sécurité des SG

4.2.1. Le projet SESAM Grids

SESAM Grids est un projet de R&D pour renforcer et garantir la sécurité des smart grids. Il est lancé en décembre 2012 par ENGIE Ineo en partenariat avec l'Ecole Centrale Supélec, le CEA List et Trialog, il est piloté par CofelyIneo pour garantir la fiabilité des réseaux électriques intelligents en les modélisant puis en simulant des défaillances et des attaques afin de renforcer leur sûreté et leur sécurité, grâce à l'élaboration d'une nouvelle norme de sécurité.

L'objectif principale de ce projet et d'assurer la sûreté de fonctionnement et la sécurité des smart grid et garantir ainsi la fiabilité du réseau électrique.

La première étape du projet consiste à modéliser un micro grid générique et à identifier ses défaillances potentielles, ainsi que les points de faiblesses pouvant être utilisés par des assaillants (agissant en interne ou en externe du sous-système).

La seconde étape utilise le modèle générique afin de simuler des défaillances et des attaques informatiques, celles-ci permettront de tester les réactions du réseau et proposer des solutions d'amélioration pour renforcer la sécurité du réseau électrique dans son ensemble. [w 15]

4.3. Travaux concernant l'IDS dans le contexte des SG

Étant donné que le premier modèle de détection d'intrusion a été développé par Dorothy Denning [D.denning, 1986] chez SRI Intemational, de nombreux systèmes de détection d'intrusion (IDS) ont été proposés à la fois dans la recherche et le monde industriel.

4.3.1. Un modèle d'IDS basé sur le protocole WirelessHART

En 2008, [T. Roosta et al, 2008], les auteurs de cet article proposent un modèle d'IDS basé sur le protocole WirelessHART, pour surveiller et protéger les systèmes de contrôle des processus sans fil. L'architecture hybride se compose d'un composant central qui collecte régulièrement des informations à partir de capteurs de champ distribués. Un ensemble de 8 règles de détection fonctionnant sur les couches physiques, de liaison de données et de routage couvre les menaces, y compris le brouillage du signal, le compromis du nœud et la modification des paquets.

4.3.2. Architecture « Cumulative Attestation Kernel »

En 2009, [M.LeMay, Carl A. Gunter; 2009], les auteurs de cet article présentent une architecture appelée cumulative Attestation Kernel pour résoudre le problème de la vérification sécurisée des mises à jour du microprogramme dans les systèmes embarqués tels que les compteurs intelligents. Le système est conçu pour être efficace en termes de coût, de puissance, de calcul et de mémoire. Un prototype est mis en œuvre pour démontrer la faisabilité de la solution ainsi que pour prouver formellement qu'il répond aux exigences d'attestation à distance.

4.3.3. Approche d'authentification

En 2011, [Depeng Li et al, 2011] ont proposé une approche d'authentification efficace et robuste pour légaliser l'agrégation de données avec moins d'opérations de signature et de vérification. Ils ont utilisé l'algorithme MST (Minimum SpanningTree) pour construire un arbre couvrant l'ensemble du réseau NAN pour faire l'agrégation des signatures des Smart Meters. Chaque Smart Meter envoie sa signature à son père, puis chaque nœud fait la multiplication des signatures de ces fils et l'envoi à son père, jusqu'à l'arriver au nœud racine.

Les réalisateurs de cette approche ont était intéressé à l'authentification. Cependant, le Smart Grid contient une multitude d'applications, qui peut être sujette de plusieurs types d'attaque touchant la disponibilité, la confidentialité, la non-répudiation et l'authentification.

4.3.4. Approche d'agrégation de données multidimentionnelles

En 2012, les auteurs de l'article [Lu et al, 2012] ont proposé une architecture qui traite toutes les données de mesure dans son ensemble plutôt que séparément. Ils ont proposé un schéma EPPA (**E**fficient and **P**rivacy **P**reserving **A**grégation). L'EPPA est une approche d'agrégation de données multidimensionnelles basées sur le crypto système homomorphe[4] de Paillier (homomorphic Paillier crypto system) qui permet d'assurer la confidentialité du trafic de l'application Meter Reading.

Les auteurs de cet article ont proposé un schéma d'agrégation efficace et sécurisé, pour les communications sécurisées en smart grids, qui se compose principalement des quatre parties suivantes : l'initialisation du système, la génération de rapports d'utilisateurs, l'agrégation des rapports sur la protection de la vie privée et la lecture et la réponse sécurisées des rapports.

Par rapport aux méthodes traditionnelles d'agrégation de données unidimensionnelles, l'EPPA peut considérablement réduire les coûts de calcul et améliorer considérablement l'efficacité de la communication, en satisfaisant les exigences en temps réel de collecte de données à haute fréquence dans les communications sur les smart grids.

[4]**Un système homomorphe :** Le système de chiffrement homomorphe est un crypto système permettant de faire des calculs sur les données chiffrées.

L'analyse de sécurité démontre la solidité de sécurité et la capacité de préservation de la vie privée et l'analyse de performance pour montrer l'amélioration de l'efficacité.

4.3.5. IDS pour l'infrastructure de mesure avancée AMI

L'AMI peut faire l'objet de nombreuses menaces, par exemple le vol d'énergie (par un consommateur illégitime); le compteur intelligent compromettant (pour obtenir un accès non autorisé au réseau), le déni de service (c'est-à-dire le brouillage des canaux de réseau), ce qui peut causer des problèmes majeurs tels que l'instabilité du réseau, les pannes de courant et la fuite de l'information du client, c'est pourquoi la sécurité de l'AMI est d'une importance primordiale. À cet égard, de nombreuses contributions ont été faites pour sécuriser l'AMI.

En 2011, les auteurs de l'article [P. Jokar et al ,2011] ont développé un système de détection d'intrusion basé sur les spécifications pour le réseau de la zone de résidentiel (HAN, qui est un sous-système au sein d'AMI responsable sur le transfert des données entre les compteurs intelligents et les appareils électriques ménagers). Puisque, le réseau d'habitation (HAN) est l'un des sous-systèmes les plus vulnérables dans les smart grids, en raison de son environnement physiquement peu sécurisé.

Ils ont considéré la technologie ZigBee pour la communication à l'intérieur du HAN. La conception d'IDS cible les couches de contrôle d'accès physique et moyen (MAC) de la technologie ZigBee (la technologie dominante dans le futur HAN) et définit son comportement normal à partir des spécifications extraites de la norme IEEE 802.15.4 (norme ZigBee).

4.3.6. IDS pour le sous réseau NAN

Etant donné que le sous réseau NAN (la partie qui relie les compteurs intelligents aux concentrateurs de données) comprend des applications telles que la mesure intelligente (smart metering) et la réponse à la demande (demande réponse) requises pour transmettre les données d'un grand nombre de clients à un concentrateur de données / sous-station ou vice versa.

Ces applications nécessitent des débits de données élevés et une couverture étendue, et peuvent être implémentées à l'aide de réseaux de réseau WiFi, des réseaux de maille Zigbee, WiMAX, PLC, etc.

En 2012, les auteurs de l'article [M. A. Faisal et al, 2012] proposent un IDS pour l'AMI, qui comprend trois IDS locaux placés dans des compteurs intelligents, des concentrateurs de données (DC) et une prise en charge AMI. L'IDS s'appuie sur l'exploration de données en cours d'exécution pour détecter la présence d'attaques dans le réseau.

Ces chercheurs développent un IDS dédié à une partie de l'AMI qui est le réseau de la zone de voisinage NAN et qui vise à détecter les activités malveillantes dans cette zone causées par des attaques de Blackhole en utilisant une approche d'exploration de données.

L'IDS dans ce cas est installée au niveau du collecteur de données. Il est considéré comme une boîte noire qui est placée à côté du collecteur de données afin de ne pas épuiser la capacité de courant continu (en intégrant la fonction IDS à l'intérieur de DC).

Le DC et l'IDS communiquent entre eux comme suit :

- ✓ DC envoie le flux de trafic qu'il envoie / reçoit à / des compteurs intelligents à l'IDS.
- ✓ L'IDS analyse le trafic et décide de la présence ou de l'absence de l'attaque de blackhole. Si l'attaque est détectée, l'IDS identifie les nœuds malveillants et déclenche une alarme pour informer un niveau supérieur (utilitaire par exemple), qui prend les actions appropriées contre les nœuds malveillants (compteurs intelligents ou collecteur de données).

Ce système de détection d'intrusion basé sur l'approche d'anomalie (anomaly detection) qui détecte les activités malveillantes comme des écarts par rapport au comportement statistiquement normal du système. Il est centralisé et il regroupe toutes les informations recueillies et envoyées par le collecteur de données qui requiert une grande capacité de calcul et de mémoire.

L'algorithme de classification utilisé dans cet IDS est le Naïve Bayes[5] classifier. En dépit de leurs hypothèses trop simplifiées. Les classificateurs Bayes naïfs ont bien fonctionné dans de nombreuses situations réelles, telles que la classification des documents et le filtrage des spams. Ils nécessitent également une petite quantité de données de formation pour estimer les paramètres nécessaires et ils peuvent être extrêmement rapides par rapport à des méthodes plus sophistiquées.

4.3.7. IDS contre l'attaque BlachHole

En 2016, les auteurs de l'article [Nadia Boumkheld et al ,2016] implémentent un IDS contre l'attaque Blackhole qui représente une dangereuse attaque DOS qui déstabilise le réseau smart grid. Les résultats qu'ils ont montrés prouvent l'efficacité de cet IDS dans la détection d'attaques.

Ce système de sécurité utilise des techniques d'exploration de données pour la détection d'une attaque de déni de service (DOS) dans une grille intelligente, l'attaque Blackhole. Il est centralisé et regroupe toutes les informations recueillies et envoyées par le collecteur de données qui requiert une grande capacité de calcul et de mémoire.

[5]**Naive Bayes** est un simple classificateur probabiliste basé sur l'application du théorème de Bayes avec l'hypothèse «naïve» d'indépendance entre chaque paire de fonctionnalités.

Conclusion

Étant donné que le réseau smart grid est une hybridation du système d'alimentation et d'un réseau de communication, par conséquent, il faut détecter les intrusions qui ciblent le système d'alimentation physique et/ou le réseau de communication. La combinaison de ces problèmes se réfère à l'aspect cyber physique de la grille intelligente qui considère la partie hard dans cette dernière.

En outre, l'étude du cyber sécurité dans les réseaux électrique intelligents couvre également les cybers vulnérabilités de ces dispositifs physiques qui comprennent à la fois des composants matériels et logiciels.

Puisque,ces smart grids sont des réseaux qui se composent d'un ensemble des nœuds interconnecté selon une telle infrastructure, l'infrastructure de communication omniprésente déployée à l'intérieur du ce dernier en fait une cible à différents types d'attaques, c'est pourquoi la sécurité est un élément essentiel dans la construction d'une grille robuste.

L'IDS est la solution performante pour la résolution des problèmes de protection, il est décisif de choisir une topologie de communication efficace et une norme de communication adaptables ainsi qu'un algorithme de classification d'attaque robuste.

Par exemple d'une part, pour obtenir une topologie fiable pour la communication, le choix de la topologie du réseau de maillage sans fil est la meilleure. Ainsi que l'utilisation des normes adaptées à cette topologie comme la norme Zigbee, parce qu'elle est une norme de réseau à faible coût et à faible puissance qui peut être largement déployée. [Yichi Zhang et al ,2011]

D'autre part, il faut utiliser des protocoles de routage sécurisés pour assurer une protection maximale contre les différentes menaces. Ainsi que L'une des exigences des IDS proposés dans le contexte des smart grids est la capacité de détecter et classifier les attaques grâce à l'utilisation des algorithmes de classification robustes. À cet égard, de nombreux travaux de recherche ont été faits pour sécuriser ces réseaux électriques intelligents ; Et c'est ce que nous avons examiné dans ce chapitre.

Partie II : Contribution

Chapitre 4

Introduction

De nos jours, l'informatique est partout. Toutes les données les plus importantes sont informatisées. Il est donc impératif que celles-ci soient protégées.

Notre dépendance à l'électricité et la dépendance au Smart Grid pour la gestion et la distribution de l'électricité en fond un atout essentiel .la perturbation de l'alimentation électrique à d'énormes conséquences sur tout le réseau et la société. Par conséquent, la sécurité de ces réseaux électriques intelligents représente un grand défi.

L'informatique évolue, les applications sont de plus en plus complexes et les délais laissés aux programmeurs et aux administrateurs sont souvent très courts. Les risques de failles applicatives sont donc très importants et peuvent être dangereux pour les applications répandues.

La sécurité contre les attaques distantes augmente, notamment grâce aux dispositifs réseau plus puissants (tels que les pare-feu intelligents), en revanche les attaques locales sont encore très efficaces : ARP Spoofing, le vol de session, ... restent souvent possible.

Compte tenu la sensibilité des smart grids contre les intrusions et pour remédier aux points critiques qui peuvent être affecté par les différents menaces de ce type. Et étant donné que les attaques distribué sont parmi les plus attaques dangereuse qui mettent la sécurité de ce type de réseaux en danger et qui la menacée.

Dans notre cas d'étude (smart grid), Les attaques distribuées seront toujours redoutables si la plupart des points critiques ne sont pas protégées. Ce qui nous amène à notre deuxième partie à poser la question de comment détecter et prévenir ces attaques qui sont considéré également comme les attaques les plus dangereuses qui font peser une forte menace pour les réseaux électrique intelligents; Ce qui oblige à les détecter et les prévenir en temps réel et l'empêcher à atteindre ces objectif.

Plusieurs études ont abordé le problème de la détection d'intrusion et les différentes techniques/ méthodes de détection fiable pour établir un IDS performent, robuste et résistant aux attaques ; Et qui atteint des bons résultats de sécurisation .Cet IDS qui devrait être capable de récupérer rapidement contre les pannes et de continuer à fournir un service sécurisé.

Dans notre proposition nous avons choisi d'établir un système de détection d'intrusion discret qui analyse les paquets collectées à partir des capteurs placés dans les points critiques de smart grid.

1. Description de Proposition

Notre objectif principal est de présenter le problème de la détection d'intrusions dans les réseaux de données (Cas de Smart Grid) et de proposer des outils permettant de se prémunir de ces dernières. On parle alors des systèmes de détection d'intrusions IDS.

La plupart du temps, ces percées ont le travail d'une intention malveillante. Et le fait que cet outil de sécurisation eux-mêmes est vulnérable à être ciblé, on propose qu'il soit discret (placées d'une façon cachée) pour qu'il ne soit pas susceptible aux attaques. Car si un pirate détecte la présence d'un IDS, il peut le désactiver ; ou mieux encore, générer de fausses attaques pendant qu'il commettra son forfait tranquillement. Donc nous avons proposé dans ce chapitre un modèle architectural qui présente notre idée, Comme il est illustré dans la figure 4.1.

Ils existent plusieurs méthodes pour cacher un IDS ; dans notre proposition nous choisit la méthode de chiffrement ou bien de cryptage pour masquer l'accès à ce dernier ainsi que pour essayer de camoufler son existence dans le réseau (par exemple on crypte son adresse IP à l'aide de plusieurs outils de chiffrement).

Ce système de détection d'intrusion discret analyse le trafic des paquets circulés qui sont collectés à partir des capteurs de concentration de données ; ces derniers sont placés dans les points critiques de smart grid (les points de transmission d'informations)

1.1. Les Points Critiques de réseaux smart grid

Lépine dorsal des smart grids est ces réseaux sous-jacents qui relient les différents composants et qui permettent une communication mutuelle entre eux. Les émergences de ces vastes réseaux multifacettes sont plus facilement exposées aux cyber-attaques, ce qui les rendre très sensibles face à ces derniers.

1.1.1. Le réseau HAN

Le réseau d'habitation HAN du côté de la demande fournit le point d'accès le plus simple pour les cyber-attaques. C'est l'un des sous-réseaux les plus vulnérables dans les smart grids, en raison de son environnement physiquement peu sécurisé.

a. Les smart meters :

Les smart meters qui sont placés dans ce sous réseaux et qui représente les dispositifs les plus important dans le réseau Smart Grid. Ils ont critique de point de vue disponibilité. Un dysfonctionnement de ce composant peut causer des conséquences graves, d'où la nécessité de la mise en œuvre d'un service de disponibilité pour éviter les différentes attaques.

b. Les home gateway :

La passerelle domestique (home gateway) où le compteur intelligent peut envoyer les données de consommation d'énergie à un fournisseur de services pour gérer l'utilisation de l'énergie à des fins financière. Donc Les communications dans cette passerelle peuvent être affectées par des attaques.

Cette passerelle reçoit les données de consommation d'énergie du compteur intelligent et l'affiche sur des outils qui sont utilisé par les consommateurs pour connecter à leur profil de consommation.

1.1.2. La partie AMI

L'infrastructure de mesure avancée (AMI) est un composant essentiel de la grille électrique intelligente et peut être conçue comme une pièce jointe pour fournir une communication bidirectionnelle du domaine utilisateur au domaine de l'utilité. Elle est utilisée pour assurer une communication automatisée bidirectionnelle entre les clients (compteurs intelligents) et les fournisseurs. L'AMI peut faire l'objet de nombreuses menaces ; ce qui peut causer des problèmes majeurs tels que l'instabilité du réseau, les pannes de courant et la fuite de l'information du client, c'est pourquoi la sécurité de l'AMI est d'une importance primordiale. À cet égard, de nombreuses contributions ont été faites pour sécuriser l'AMI.

1.1.3. Le réseaux NAN

Le NAN couvre et gère les communications entre les compteurs intelligents dans une zone géographique spécifique .Il connecte plusieurs HAN à des points d'accès locaux qui sont des concentrateurs de données. Ces concentrateurs ont la responsabilité d'accumuler des données provenant de diverses lectures de compteurs à différents moments de la journée.

Ce sous réseaux permet aux périphériques dans une petite zone, comme un quartier de communiquer entre eux. Par exemple, tous les compteurs intelligents dans un quartier peuvent communiquer entre eux à l'aide d'un routeur pour former un maillage interconnecté de périphériques intelligents. Donc tout un point de communication risque d'être attaqué.

Par exemple un nœud malveillant peut effectuer une attaque d'usurpation d'identité sur un PMU, modifier les messages PMU qui contiennent des données de mesure d'énergie et peut également reproduire les messages en transit entre le PMU et les différents concentrateurs de données.

1.1.4. Le Réseau WAN

Le WAN ou le sous réseau à grande surface forme l'épine dorsale du réseau de communication, pour connecter des petits réseaux hautement distribués. Il permet de connecter les réseaux du Smart Grid au centre de contrôle. Ainsi qu'il permet aux périphériques dans une grande zone géographique de communiquer entre eux.

Ce sous réseaux est très sensibles face aux attaques, car toute une intrusion au niveau de ce dernier peut déstabilisera l'ensemble de smart grid.

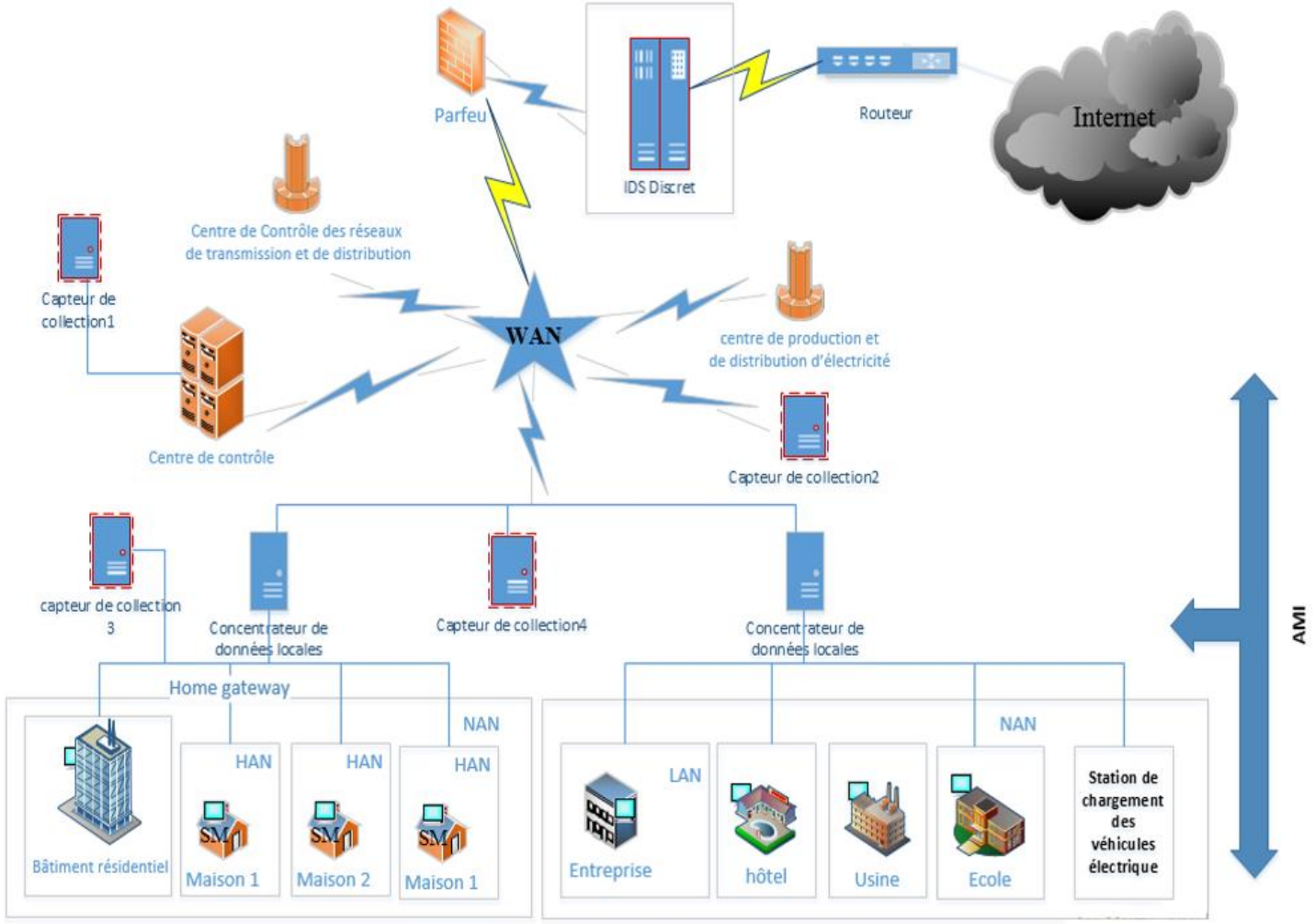

Figure 4.1 : *Proposition architectural d'un IDS Discret dans le contexte des Smart Grids .*

1.2. IDS Choisi

L'idée de notre proposition et d'établir un système de détection d'intrusions de type Réseaux (N-IDS) au niveau de tous les point sensible de réseau étudié dans notre mémoire.

Parmi les caractéristique des N-IDS, qu'ils assurent la sécurité au niveau du réseau Ces systèmes sont principalement déployés sur un point stratégique dans l'infrastructure réseau. Ils sont responsables sur surveillance du trafic réseau passant par des segments de ce réseau.

Ils peuvent capturer et analyser des données pour détecter des attaques connues ou des activités illégales .On peut les appelés par "snifers-paquets", car ils captent et collectent les données sous forme des paquets Internet passant par des moyens de communication.

2. Expérimentation

2.1. L'approche de détection choisie

Étant donné qu'ils existent différents méthodes de détection d'intrusion utilisée par ce type de système de sécurisation .qui l'on peut les classées en deux catégories comme il est détaillé dans le second chapitre : la catégorie de la détection en utilisant l'approche par signature (missus detection) et l'autre de la détection comportementale (anomaly detection).

Nous avons choisi dans ce chapitre de faire le test de détection en utilisant l'approche par signature qui consiste à chercher dans les activités des entités surveillées les motifs ou les signatures des attaques connues.

Tel que ces signatures représente un modèle une attaque spécifique et chaque attaque peut être détectée par un ou une séquence d'événements obtenus à partir d'un ou plusieurs capteurs qui sont responsables sur la classification des événements d'attaques qui peuvent provenir ; soit d'un hôte, soit d'un réseau.

- **Les avantages de l'approche basé signature**
  - Peu de possibilités d'erreur de détection
  - Extrêmement fiable
  - Facile à programmer et à implémenter

➢ **Les Inconvénients de l'approche basé signature**

L'inconvénient majeur de la détection d'intrusions basé sur la méthode par signature est qu'elle nécessite des mise à jours fréquente parce qu'elle ne peut pas reconnaitre les modèle des intrusions non enregistrés dans la base de signature.

2.2. L'environnement de développement (Le logiciel weka)

Weka c'est l'acronyme de **W**aikato **E**nvironment for **K**nowledge **A**nalysis) ; est un ensemble d'outils permettant de manipuler et d'analyser des fichiers de données, implémentant la plupart des algorithmes d'intelligence artificielle, entre autres, les arbres de d´décision et les réseaux de neurones. Il est ´écrit en java, disponible sur le web. [w25]

L'intérêt de Weka dans le cadre du cours d'Apprentissage est multiple car :

- Pouvoir mettre en œuvre les algorithmes ´étudies en cours en grandeur nature, sans devoir réécrire tout le code correspondant ;
- Comprendre et utiliser intelligemment les différentes sorties de ces algorithmes ;
- Pouvoir programmer des agents intelligents en un temps raisonnable, pour des tâches non triviaux ;
- Evaluer les performances d'un algorithme ;
- Comparer les performances de deux algorithmes ;
- Etudier le rôle des paramètres d'un algorithme ;
- Combiner plusieurs algorithmes ;
- Eventuellement définir un nouvel algorithme.

2.3. La méthode de classification choisie

On essaye de faire le test avec différentes méthode de classification et nous choisissons l'arbre décisionnel comme le meilleur qui nous donne des bons résultats de détection.

2.3.1. La méthode d'Arbre de décision

Un arbre de décision est une méthode de classification sous forme d'un arbre dans lequel chaque nœud représente un choix entre un certain nombre de solutions alternatives, et chaque nœud feuille représente une classification ou une décision. [Adrien Haccoun , 2012]

Elle a été utilisée comme classificateurs pour de nombreux domaines. Pour plusieurs de ces domaines, les arbres produits par la méthode C4.5[1] et ils sont petits et précis, ayant pour résultat des classificateurs rapides et fiables. Ces propriétés font des arbres de décision un outil valable et populaire pour la classification.

- **Les avantages de la méthode d'arbre de décision**
  - Les arbres de décision représentent une méthode très efficace d'apprentissage supervisé ;
  - L'arbre décisionnel est un classificateur fiable, simple, petit et rapide.

2.3.2. La technique liée à la méthode de classification

a. L'algorithme C4.5(J48) :

L'algorithme J48 implante la méthode C4.5 dans le cadre de l'apprentissage supervisé. Cet algorithme permet la génération d'un arbre de décision, élagué ou non. Cette méthode a pour but global de générer un arbre de décision simple (et petit) capable de classifier les nouvelles instances. À partir de l'ensemble d'apprentissage, C4.5 extrait la régularité de règles à partir d'instances et construit un arbre de décision qui classifiera les instances avec un certain degré d'erreur tolérée. Il prend en compte les attributs numériques ainsi que les valeurs manquantes. [w26]

[1] La méthode d'élagage de C4.5 : cette méthode conçue par Quinlan (1986) basé sur l'estimation du taux d'erreur de chaque sous arbre, et remplace le sous arbre avec un nœud feuille si l'erreur estimée de la feuille est très basse.

➢ **Fonctionnement d'algorithme J48 :**

- Pour une instance donnée, les nœuds de l'arbre de décision sont utilisés pour tester les valeurs d'attribut. Suivre une branche ou une autre d'un nœud donné dépend des résultats du test effectué au niveau du dit nœud.
- À la fin du parcours de l'arbre de décision de la racine à une feuille selon les valeurs d'un problème donné, la classification trouvée à la feuille est la classification prédite du problème.
- Pour la construction des sous arbres, C4.5 utilise le taux de gain d'information[2] IGR (**I**nformation **G**ain Rate) pour chacun des attributs possibles qui pourraient potentiellement être utilisés pour diviser les données. [w26]
- L'attribut avec le plus grand IGR est choisi comme racine d'un sous arbre. Bien qu'IGR soit une métrique qui prend une décision locale par opposition à une décision globalement optimale, l'attribut sélectionné est souvent le plus discriminatoire.

Remarque : Cette méthode de construction de sous arbres est appliquée récursivement jusqu'à ce que l'arbre résultant classifie entièrement toutes les instances d'apprentissage.

2.3.3. L'attaque choisie pour le Test

Etant de donnée que les attaques par déni de service (DOS les plus dangereuses qui menacent la sécurité des smart grids et qu'elles peuvent subir le système ou le réseau et le rendre inefficace dans quelques instants .à partir de ce point nous avons choisi de faire le test en utilisant les modèle de paquet de ce type d'attaque.

a. Exemple d'attaque par déni de service distribué (DDOS) : Le SYN flood

➢ **Définition**

C'est une technique d'attaque informatique visant à endommager un serveur. Le SYN flood est une forme d'attaque informatique visant à provoquer un déni de services, elle est destinée à rendre un réseau complètement indisponible. Cette technique d'attaque s'applique

[2] L'IGR : est une heuristique qui évalue la capacité d'un attribut de réduire l'aspect aléatoire dans des instances non classifiées.

dans le cadre d'un protocole TCP (Transmission Control Protocol) et vise principalement à submerger le serveur cible d'une tonne de requêtes SYN (Synchronized).[w27]

Le protocole TCP est un protocole de transport de paquets de données permettant d'obtenir une liaison de données fiable entre deux machines. Lorsque deux machines, qu'on appellera "Machine1' et "Machine2" dans cet exemple, veulent effectuer un échange de données à l'aide du protocole TCP, elles doivent établir une connexion. Celle-ci s'effectue en trois étapes, illustrées dans la figure 4.2 appelées « poignée de main en trois temps » (ou three-way handshake). Schématiquement, le processus se déroule ainsi :

- Machine1 envoie un paquet de type SYN à Machine2 contenant (entre autres) un numéro de séquence aléatoire ;
- Machine2 reçoit ce paquet, enregistre en mémoire une trace de cette connexion en la marquant comme étant « semi-ouverte » et envoie un paquet SYN-ACK d'acquittement à Machine1 ;

Machine1 reçoit ce paquet SYN-ACK et émet vers Machine2 un paquet d'acquittement ACK; les deux hôtes ont ainsi chacun reçu un acquittement de la part de l'autre machine, la communication est établie.

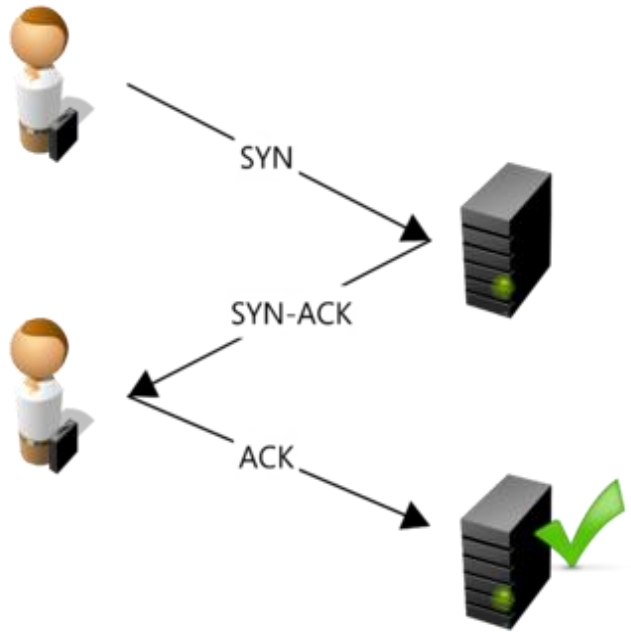

Figure 4.2 : *schéma d'une connexion normale. [w27]*

➢ **L'usage malveillant d'une connexion TCP**

Un client malintentionné peut brûler la troisième étape et ne pas répondre par un message ACK. Le serveur met ainsi du temps avant de libérer les ressources préalablement destinées au client et générer un temps d'attente.

Il peut également arriver qu'en refusant de répondre par un message ACK, un client malveillant profite de la troisième étape pour surcharger les ressources du serveur et de l'empêcher d'accepter de nouvelles requêtes, de manière à pouvoir provoquer un déni de services. Après le SYN ACK, la connexion est semi-ouverte et consomme d'importantes ressources (mémoire, temps, processeurs) et qu'en ce moment précis il est possible de surcharger les ressources du serveur cible en générant plusieurs requêtes incomplètes de ce type.[w27]

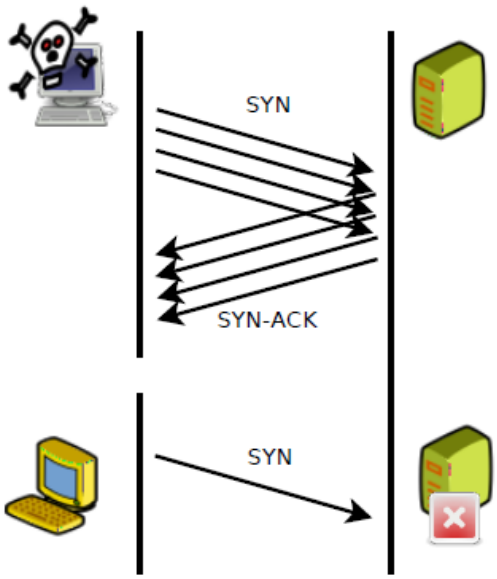

Figure 4.3 : *Schéma d'attaque de type SYN flooding. [w27]*

2.3.4. Les données choisies pour le Test de détection

KDD 99 : est un ensemble de données (Data set) devenu la base de données la plus utilisée pour l'évaluation des systèmes de détection d'intrusion depuis 2009. Il a été préparé par Stolfo en 2000.

Cet ensemble doté de deux sous-ensembles de données ; un d'apprentissage <<KDD training data set >> qui se compose d'environ 4,9 millions d'enregistrement de connexion dont chacun contient 41 caractéristique ainsi qu'une étiquette qui indique le type de connexion normal ou une attaque (le type spécifique d'attaque).

Les attaques simulées appartiennent à quatre catégories des attaques de déni de service, DOS (elle bien détaillée dans le second chapitre), R2L, L2R, Probe.

Cet ensemble de données est sous forme de fichiers.csv préconfiguré afin de faciliter son intégration dans l'environnement de développement (weka) (Figure 4.4).ces fichiers contient un ensemble d'attributs qui désigne le modèle des paquets qui sont considérer comme attaques ou des paquets normaux. Comme il est représenté dans les deux figures 4.5 et 4.6.

Ces attributs désignent le contenu du format des parquets transférés,il sont classés comme suit : (duration ; protocol_type ; service ; flag ; src_bytes ; dst_bytes ; land ; wrong_fragment ; urgent ; hot ; num_failed_logins ; logged_in ; num_compromised ; root_shell ; su_attempted ; num_root ; num_file_creations; num_shells; num_access_files ; is_guest_login ; count; srv_count ; serror_rate ; srv_serror_rate ; rerror_rate ; srv_rerror_rate ; same_srv_rate ; diff_srv_rate ; srv_diff_host_rate ; dst_host_count ; dst_host_srv_count ; dst_host_same_srv_rate ; dst_host_diff_srv_rate ; dst_host_same_src_port_rate; dst_host_srv_diff_host_rate ; dst_host_serror_rate; dst_host_srv_serror_rate ; dst_host_rerror_rate ; dst_host_srv_rerror_rate; label).

Dans notre proposition nous avons choisi de reconfigurer cet « data set », on prendre en considération sauf que les modèles d'attaque DOS supposant qu'elle est la plus dangereuse pour notre cas d'étude.

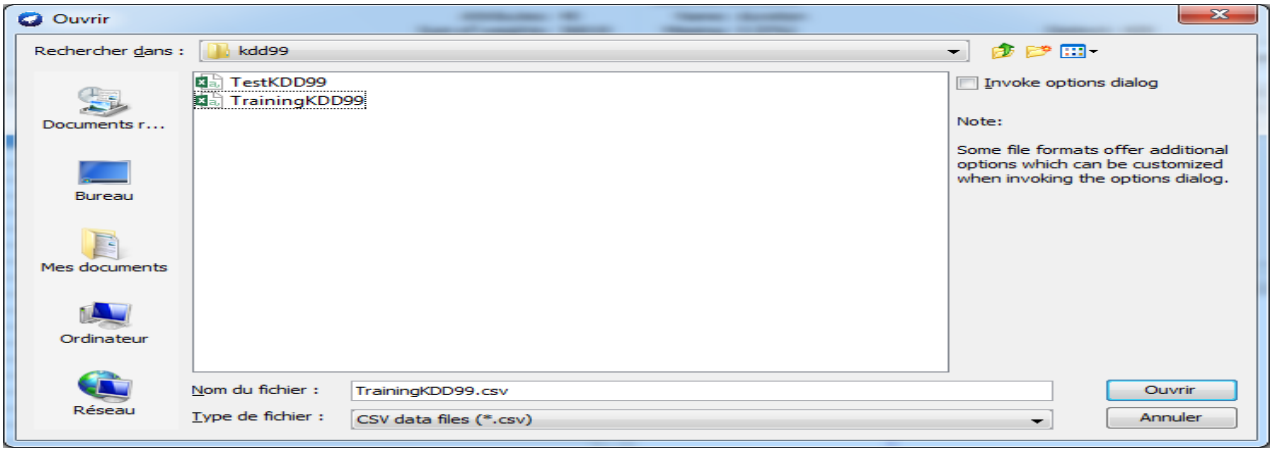

Figure 4.4 : *Capturassions des data-set KDD99.*

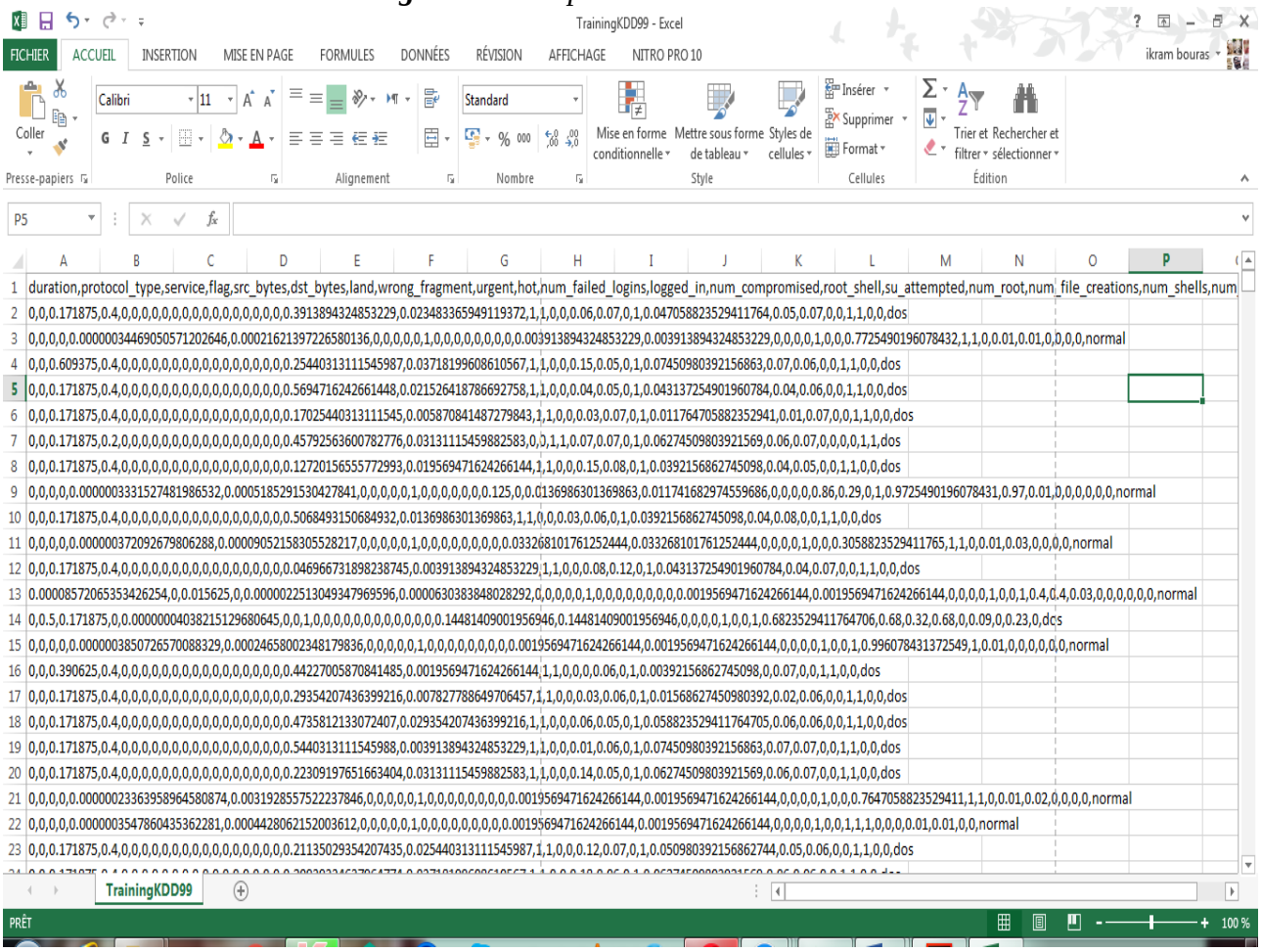

Figure 4.5 : *Représentation du format des paquets d'apprentissage (kdd99).*

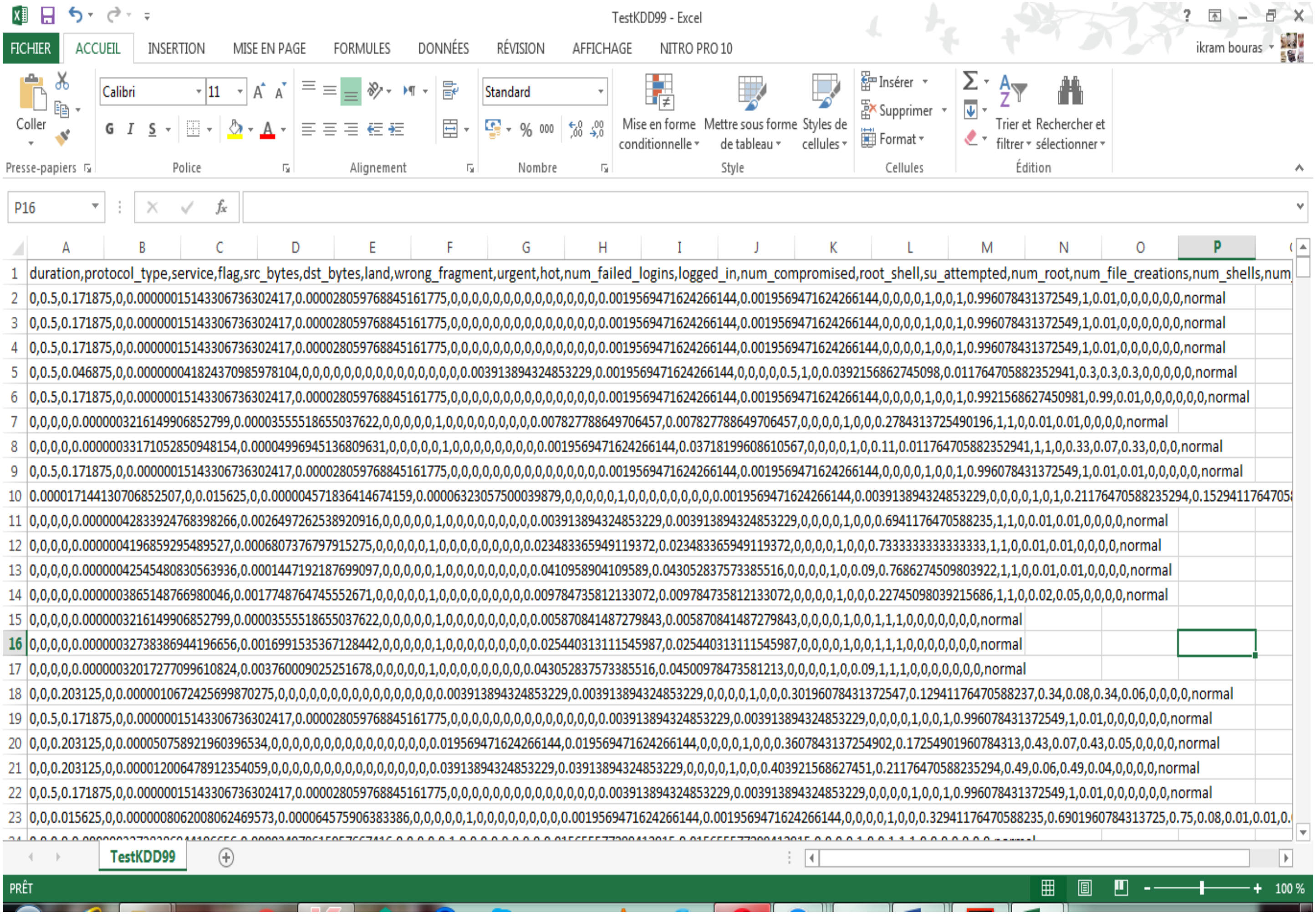

Figure 4.6 : *Représentation du format des paquets de test (kdd99).*

2.3.5. Les Caractéristiques du Pc Utilisé pour le test de détection

Tableau4.1 : *Caractéristique d'ordinateur Utilisé pour le test de détection*

Fabricant	Hewlett-Packard (HP 650
processeur	Intel (R)Core(TM) i3-2338M CPU@2,20 GHz 2,20GHz
RAM	4Go
système d'exploitation	Windows 7 Edition Integrale(32 bits) Service pack 1

2.3.6. Les Résultats Obtenus

Etant donné que l'efficacité des smart grids basé sur la communication en temps réel. Avec l'envoi massifs des demandes d'authentification, il sera détecté qu'une attaque DOS est entrain de cibler le réseau électrique intelligent (détection d'intrusions)

Par exemple lorsqu'on fait le test avec le fichier d'apprentissage « TrainingKDD99.csv » qui contient les motifs des attaque DOS ainsi que les paquets normaux (Le fichier d'apprentissage « Training-KDD99 » contient 12000 paquets de type normal et 24819 paquets de type Dos. Et le fichier de test « Test-KDD99 » contient 60593 paquets normaux et 229853 paquets de type Dos.).On obtient les résultats de détection illustrés dans les deux figures 4.8 et 4.9 sous forme de graphes ainsi que sous forme de taux de détection résultant l'exécution de la méthode de classification utilisé (l'arbre de décision) comme il est représenté dans les trois figures 4.7.

En Utilisant la méthode de classification avec la technique d'arbre décisionnel (algorithme J48) et en commence le test qui confirme dans les résultats (graphes + taux de détection d'intrusions), la présence des attaque DOS avec un taux de détection d'intrusions égale à 97%.

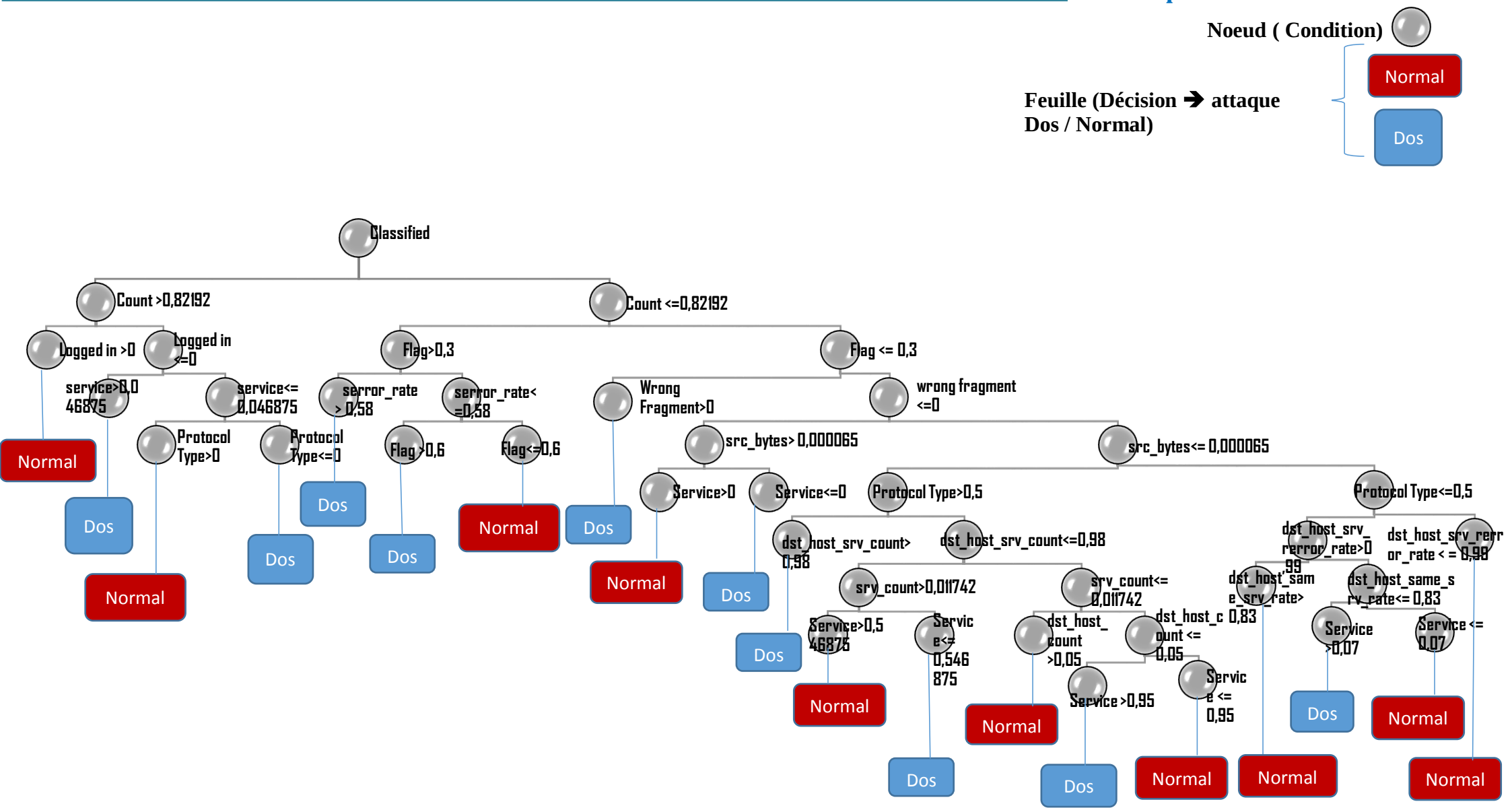

Figure 4.7 : *l'arbre de décision qui résulte l'exécution de l'algorithme j48.*

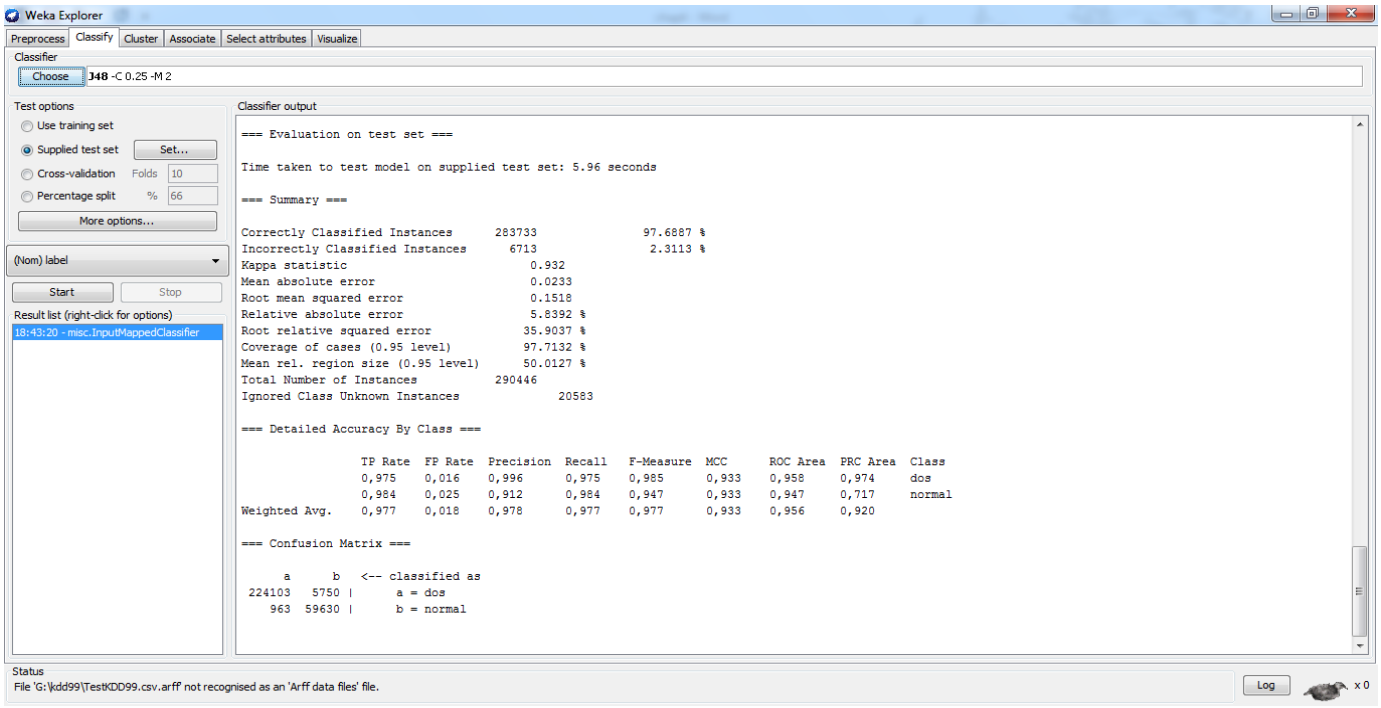

Figure 4.8 *: Les résultats de test de détection Obtenu lors de la détection d'une attaque DOS*

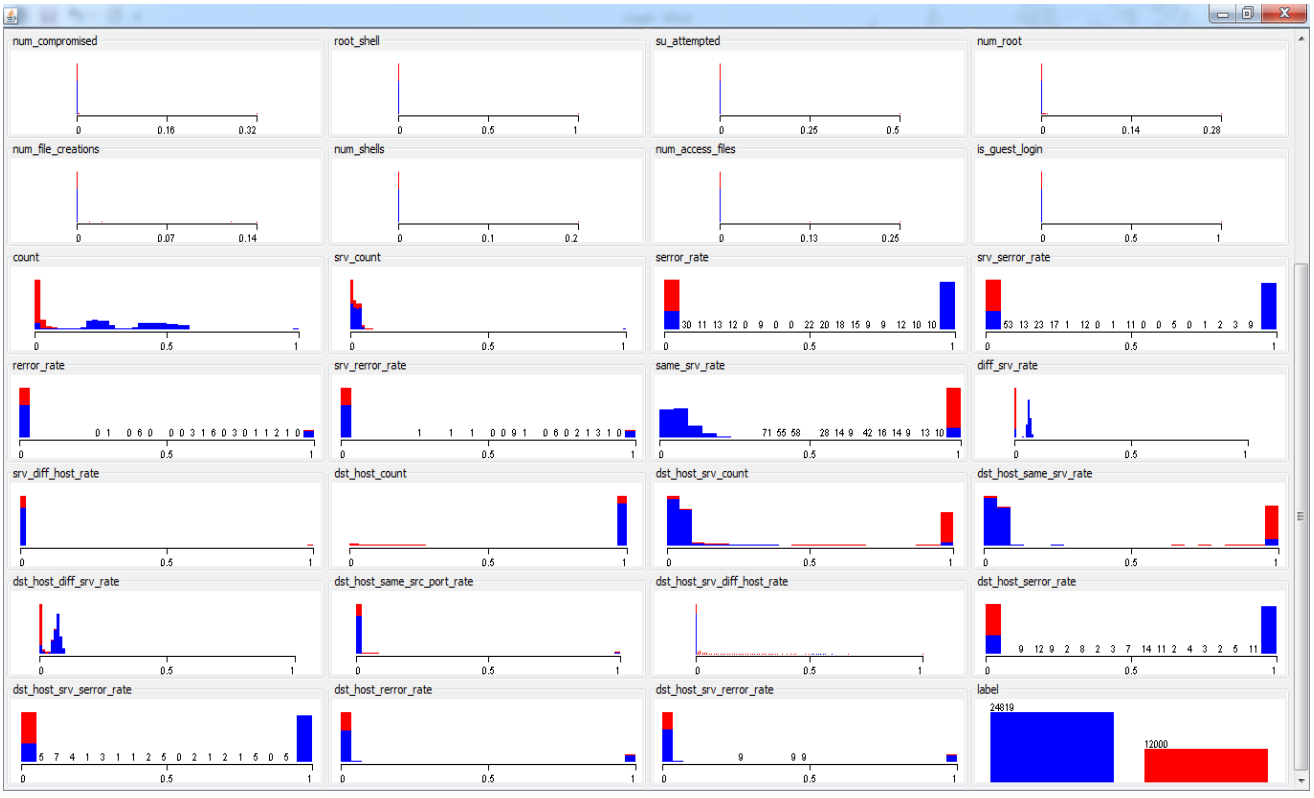

Figure 4.9 *: Les résultats sous forme de graphe qui représente la classification d'un paquet normal en rouge ou d'un paquet malveillant en bleu (attaque DOS).*

➢ L'évaluation de test :

Les performances de ce test sont généralement évaluées en utilisant les données illustrées dans la matrice de confusion.

Tableau4.2 : *Matrice de confusion Résultant le test de détection*

	Classe prédite		
Classe actuelle		Classe négative (Normal) N	Classe positive (DOS) P
	Classe négative (Normal)	VN=224103	FP=5750
	Classe positive (DOS)	FN=963	VP=59630

Selon les résultats obtenus le test de détection donne les valeurs d'évaluation suivante :

P➔ positif : signifie la présence d'une attaque ➔ p=24819 paquets

N➔ négatif : signifie qu'il n'y a pas d'attaque ➔ N=12000 paquets

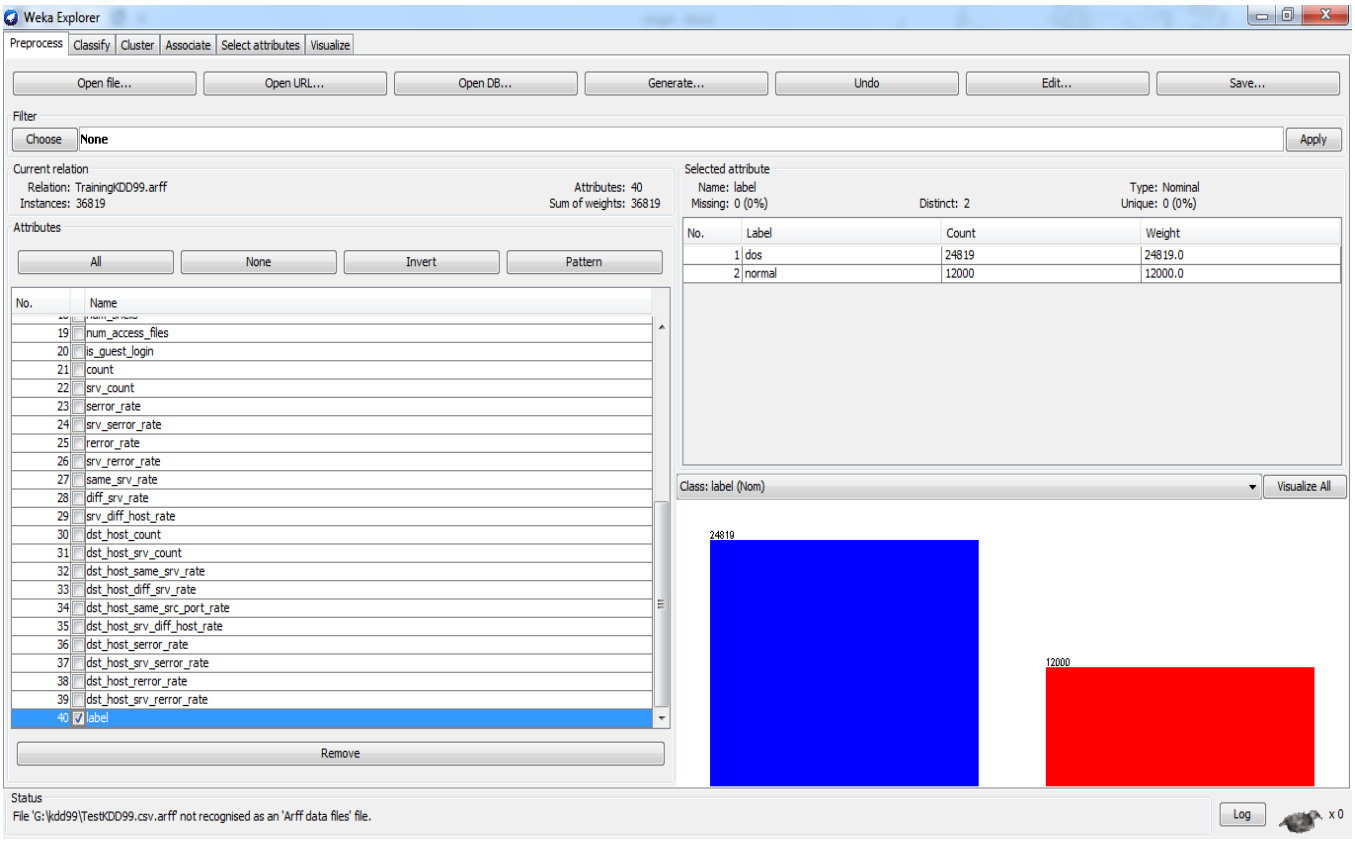

Figure 4.10 : *le résultat de nombre de paquets détectés comme des paquets normaux ou des DOS.*

VP➔ vrai positif : est le nombre de prédictions correctes des cas positifs (nombre d'intrusions correctement classées comme des intrusions).

VN➔vrai négatif : est le nombre de prédictions correctes de négatives détections (nombre d'utilisateurs légitimes correctement classés comme légitime).

FN➔ faux négatif : est le nombre de prédictions incorrectes des cas négatives (nombre des intrusions qui ne sont pas classées comme des intrusions et qui sont classées comme des utilisateurs légitimes).

FP➔ Faux positif : est le nombre de prédictions incorrectes (nombre des utilisateurs légitimes classés incorrectement comme des intrus).

Les métriques traditionnelles de classification comprennent le taux d'exactitude et le taux d'erreur de la classification [ahmed ahmim, 2014], elles sont définies comme suit :

- ✓ **Accuracy (Exactitude) = [(VP+VN)/ (VP+VN+FP+FN)] (0 ,97688727)**
- ✓ **Erreur = 1-exactitude (0,02311273)**
- ✓ **Precision = (VP / (VP + FP)) (0,91205262)**

Conclusion

L'efficacité d'un Tel système se relèvera par sa capacité à détecter et à prévenir les nouveaux Type d'attaques, et de faire bien protéger contre eux.

Le choix d'une méthode de détection classificatrice nous a poussées à choisir un algorithme assez connu pour effectuer cette tâche. Il s'agit de l'algorithme J48 qui est appliqué suivant d'un arbre décisionnel. Une fois qu'on a détaillé son fonctionnement, nous avons eu l'idée de stocker les traces des intrusions par ce dernier, nous poussant ainsi à réfléchir sur la manière à réaliser une base de données et par la suite une interface pour l'exploiter.

Conclusion Générale

Conclusion générale

L'informatisation progressive des réseaux d'électricité par les technologies ***smart grids*** est en cours de développement. Où le déploiement de ces technologies de réseaux électrique intelligents vise surtout à automatiser les équipements sur le réseau, à bâtir une infrastructure de mesurage avancé et à réduire les pointes de demande d'électricité.

Durant notre analyse des travaux à propos des smart grids, ont ses biens familiarisés avec ce domaine de recherche et qui reste un sujet d'actualité qui préoccupe de plus en plus.

Ces systèmes font également apparaître de nouveaux problèmes de sécurité : sécurité matérielle des équipements, comme les compteurs ; cyber sécurité des systèmes informatiques, de communication, d'acheminement et de traitement des données, notamment ; confidentialité des données ; ou encore stockage des téraoctets de données que ces nouveaux compteurs et infrastructures produisent.

L'efficacité d'un tel système se relèvera par sa capacité à détecter et à prévenir les nouveaux type d'attaques et de faire bien protéger contre eux .A travers ce travail nous avons consacré une grande partie de notre étude à la recherche des algorithmes et des méthodes de détection ; en essayant de trouver les plus efficaces qui assure l'analyse des flux en temps réel. Le choix d'une méthode de détection classificatrice nous a poussées à choisir un algorithme assez connu pour effectuer cette tâche. Il s'agit de l'algorithme J48 qui est appliqué suivant d'un arbre décisionnel. Une fois qu'on a détaillé son fonctionnement, nous avons eu l'idée de stocker les traces des intrusions par ce dernier, nous poussant ainsi à réfléchir sur la manière à réaliser une base de données et par la suite une interface pour l'exploiter.

L'application de cette technique de décision peut être réalisée pour des futurs travaux dans le cadre de développement d'un IDS Hybride qui combine entre l'utilisation des deux approches en utilisant la technique des outils statistiques combiné à la méthode de classification .

Annexes

Annexe I : Dictionnaire

Vocabulaire et définitions :

TIC : Acronyme de « technologies de l'information et de la communication ». Qui représentent un Ensemble des techniques (technologies informatiques) et des équipements informatiques permettant de communiquer à distance par voie électronique ; pour traiter, modifier et échanger des informations (des données numérisées). La naissance des TIC est due notamment à la convergence de l'informatique, des télécommunications et de l'audiovisuel.
Norme : Est un ensemble de règles communes relatives aux caractéristiques d'un produit ou service et à son mode de fabrication et de commercialisation.
Réseau : Est un ensemble des nœuds interconnecté entre eux selon une telle architecture (Topologie).
Infrastructure : Est un ensemble d'éléments interconnectés qui fournissent le cadre pour supporter la totalité de la structure **.** (Wan, NAN, HAN)
Les protocoles de communications : définit l'ensemble des règles qui précisent les modalités de fonctionnement d'une communication entre deux ordinateurs.
Les protocoles de routages : Un protocole de routage est un ensemble de processus, d'algorithme et de messages standardisés utilisé pour échanger, entre routeurs, des informations sur ce que l'on va appeler des réseaux, des routes ou encore des préfixes. Ces protocoles permettent de choisir, pour chaque destination possible, le « meilleur chemin ».
Les protocoles de sécurité : Ensemble de règles régissant le comportement d'individus pour répondre aux besoins d'une application (paiement en ligne, vote électronique, authentification d'individus, etc.)
TCP : Acronyme de « Transmission Control Protocol » est un protocole de transport fiable, en mode connecté, documenté dans la RFC 793 de l'IETF. Dans le modèle TCP/IP, TCP est situé au niveau de la couche de transport. Les applications transmettent des flux de données sur une connexion réseau, et TCP découpe le flux d'octets en segments, dont la taille dépend de la MTU du réseau sous-jacent (couche liaison de données).
IP : Acronyme de « Internet Protocol » est une famille de protocoles de communication de réseau informatique conçus pour et utilisés par Internet. Les protocoles IP sont au niveau 3 dans le modèle OSI. Les protocoles IP s'intègrent dans la suite des protocoles Internet et permettent un service d'adressage unique pour l'ensemble des terminaux connectés. [A.KARTIT et al ,2012]
Smart grid : Ensemble des technologies d'informations couplées à une infrastructure de réseau électrique, de manière à optimiser la production, le transport, la distribution et la consommation d'électricité. L'objectif visé étant l'efficacité énergétique pour réduire notre impact environnemental.
Smart meter : Un smart meter est un composant d'un smart grid, il s''agit d'un compteur énergétique (électrique en général) capable de suivre en détail, et souvent en temps réel, la consommation électrique d'un bâtiment, d'une entreprise ou d'un foyer. Ce compteur intelligent est en outre communicant et transmet par différents canaux (courant porteur, Internet, téléphone) les informations recueillies. Il est un périphérique compatible Internet qui mesure la consommation d'énergie d'une maison.
Le réseau de backhaul : Ensemble connecte le contrôle / les opérations de l'utilité, y compris l'entreprise AMI, avec le réseau étendu (WAN), les réseaux de sous-stations de distribution, les DER, le réseau de zone de terrain (FAN), les points d'accès à la distribution NAN, etc.

Annexe I : Dictionnaire

AMI : acronyme de **« A**dvanced **M**etering **I**nfrastructure **»**.C'est l'infrastructure de communication pour les compteurs intelligents. Ou ce qu'on appelle l'infrastructure de comptage évoluée. C'est l'ensemble formé par des compteurs communicants et les systèmes de communication et d'information centralisés correspondants pour pour assurer une communication automatisée bidirectionnelle entre les clients (compteurs intélligents) et les fournisseurs.

AMR : acronyme de **« Automatic Meter Reading(AMR) »** .L'AMR est connu aussi sous le nom de Smart Meter Measurements [Kenneth_C._Budka et al ,2014].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.

AMM (Advanced **M**eter **M**anagement**)**

Actionneur : Partie d'une machine ou d'un système de commande à distance qui permet de convertir l'énergie reçue en travail utile pour exécuter les tâches d'un système automatisé.

Capteur : C'est un appareil qui détecte un phénomène (lumière, chaleur, contact etc…) Détection avec contact (le capteur doit entrer en contact physique avec un phénomène pour le détecter). Détection sans contact (le capteur détecte le phénomène à proximité de celui-ci).

SCADA : Acronyme de **« S**upervisory **C**ontrol **a**nd **D**ata **A**cquisition **»** ;sont des systèmes de contrôle et de gestion ;ils ont un rôle primordial dans le réseau smart grid .Ils sont connus sous le nom de systèmes SCADA ; ce dernier est reliés aux capteurs et aux actionneurs via un réseau complexe de dispositifs comprenant :

- **Des processeurs frontaux FEP (Front End Processors) :** Ces processeurs s'appelle aussi les frontaux de télécommunication, ils représentent un type de processeurs qui assurent toutes les taches de télécommunication en périphérie d'un ordinateur central. Ils fournissent une passerelle à partir des protocoles et des supports propriétaires utilisés par le réseau de capteurs au système informatique général qui exécute le système SCADA.

- **Des dispositifs électroniques intelligents IED (I**ntelligent **E**lectronic **De**vices**) :** Les IED sont de très petits systèmes informatiques dédiés qui se connectent directement aux capteurs et aux actionneurs et les contrôlent.(capteur / actionneur intelligent qui contient les informations nécessaires pour acquérir des données, communiquer avec d'autres appareils et effectuer des traitements et des contrôles locaux. Un IED peut combiner un capteur d'entrée analogique, une sortie analogique, des capacités de commande de bas niveau, un système de communication et une mémoire de programme dans un seul appareil).

- **Des unités des terminaux distantes (RTU(Remote Terminal Units)) :** Une RTU se connecte à un ou plusieurs IED et consolide leur collecte et contrôle de données fournissant une passerelle entre l'IED et le système SCADA ou MTU.

- **Des contrôleurs logiques programmables PLC :** acronyme de « **P**rogrammable **L**ogic **C**ontrollers ». Les PLC fournissent une interface plus directe entre le capteur ou l'actionneur au système SCADA englobant la fonctionnalité de l'IED et de la RTU dans un seul dispositif.

Annexe I : Dictionnaire

• **Des unités de terminal maître (MTU (Master Terminal Units)) :** Les MTU se connectent à plusieurs RTU, consolidant le contrôle et le trafic de données des RTU vers le système SCADA.
• **Des centres de commande de moteur (MCC (Motor Control Centers)) :** Les MCC sont des systèmes informatiques dédiés qui contrôlent les performances d'un moteur électrique.
• **Des concentrateur de données PDC(Phasor Data Concentrator):** Plate-forme d'analyse des données de mesure des PMU d'un sous-réseau en vue d'un diagnostic précis et rapide et une prise de décision visant à contrôler l'état du réseau électrique.
• **Des Unités de Mesure PMU (Phasor Measurements Units)** : Sont des dispositifs électronique permettant de mesurer dans le plan complexe, des signaux de courant et de tension, de manière synchrone avec le GPS. La finalité recherchée est une meilleure connaissance du réseau électrique en temps réel.
Les PMUs sont placés sur les lignes de transmission. Ils contribuent à créer une capture instantanée de l'état du réseau électrique (mesure du voltage). Ils sont capables de recueillir des mesures sur les tensions et les grandeurs électriques et les envoyer au PDC qui lit les données à partir de plusieurs PMU puis les fusionne en un seul message. Ce message sera communiqué au domaine des opérations.
Distribution Management System (DMS) : est un système informatique d'utilité capable de collecter, organiser, afficher et analyser les informations sur le système de distribution électrique en temps réel ou en temps réel. Un DMS permet également aux opérateurs de planifier et d'exécuter des opérations complexes du système de distribution afin d'accroître l'efficacité du système, d'optimiser les flux de puissance et d'éviter les surcharges.
Système de gestion de l'énergie (EMS) : acronyme de **E**nergy **M**anagement **S**ystem **;** est un système d'outils utilisé pour surveiller, contrôler et optimiser la génération, la livraison et / ou la consommation d'énergie.
Ressource énergétique distribuée (DER) : source d'énergie électrique qui n'est pas directement reliée à un système de transmission de puissance en vrac. Les DER comprennent à la fois des générateurs et des technologies de stockage d'énergie.
Outage Management System (OMS) : La gestion automatisée de panne (**O**utage **M**anagement) 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.
Le systéme WAMPAC: Acronyme de "**W**ide **A**rea **M**onitoring, **P**rotection **A**nd **C**ontrol " .Ce système échange les données de transmission avec d'autres systèmes de contrôle pour fournir des fonctions de surveillance et d'alarme en temps réel et assurer la transmission efficace de l'énergie, la production et l'agrégation dans la grille électrique .
DNP3 (Distributed Network Protocol) : c'est un protocole de communication largement utilisé par les services publics d'électricité. Ils ont utilisé iperf (un générateur de trafic réseau) pour occuper le canal de communication, ce qui réduit la disponibilité du réseau.

Annexe I : Dictionnaire

Bibliographie

Bibliographie

[A. B. M. S Ali, 2013] :(A. B. M. Shawkat Ali,"Smart Grid", 2013).

[abdojell, 2011] : (abdojell, digiSchool Documents,"Reseau electrique de distributionet de repartion ",2011).

[Aleksandar Lazarevic et al, 2005]: (INTRUSION DETECTION: A SURVEY Aleksandar Lazarevic, Vipin Kumar, Jaideep Srivastava Computer Science Department, and University of Minnesotaù).

[A.KARTIT et al, 2012] :(A. KARTIT, SAIDI, BEZZAZI, EL MARRAKI, RADI ; "A NEW APPROACH TO INTRUSION DETECTION SYSTEM" ; Laboratoire de Recherche en Informatique et Télécommunications, Faculty of Sciences, University of Mohammed V, Rabat,Technology, Journal of Theoretical and Applied Information Technology ,2012).

[Ahmad Usman, Sajjad Haider Shami; 2013] :(Ahmad Usman and Sajjad Haider Shami. Evolution of communication technologies for smart grid applications. Renewable and Sustainable Energy Reviews, 2013).

[Anas AlMajali et al, 2012]: (Anas AlMajali, Arun Viswanathan, and Clifford Neuman. Analyzing resiliency of the smart grid communication architectures under cyber-attack. In CSET, 2012).

[Alaoui Nabih, 2013]: (Alaoui Nabih. Cooperative Communications In Mobile Ad hoc NETworks. PhD thesis, Limoges, 2013).

[Ahmim ahmed , 2014]: (Ahmim Ahmed, Système de détection d'intrusion Adaptatif et distribué , These de doctorat, 2014).

[Adrien Haccoun ,2012] : (Adrien Haccoun , MASTER ISI, Comparaison de méthodes de classifications, URL :https://www.lri.fr/~antoine/Courses/Master-ISI/ISI 10/Projets_2012/Projet_DM.pdf , ,2012)

[Burgermeister, D.et Krier,J ;2006] : (Burgermeister, D.et Krier, J.Les systemes de détection d'intrusion , Juillet 2006).

[Brigitte Ulmann ,2004] : (Brigitte Ulmann, « Cisco et la sécurité », Novembre 2004).

[B.-H. Elias, 2013]:(Elias , Bou-Harb; Claude , Fachkha; Makan , Pourzandi; Mourad , Debbabi; Chadi , Assi;"CYBER SECURITY FOR SMART GRID - COMMUNICATIONS: PART 2- Communication Security for Smart Grids Distribution Networks";IEEE Communications Magazine;Concordia University;January 2013)

Dejun Yang, Student Member, IEEE"Smart Grid – The New and Improved Power Grid: A Survey", (ETP SmartGrid – European Technology Platform), EEGI (European electricity grid initiative), IEEE, 2012)

[David, Jonathan ; 2006] : (David Burgermeister et Jonathan Krier, « Les Systèmes de Détection d'Intrusions », Juillet 2006 ; URL :https://repo.zenksecurity.com/Protocoles_reseaux_securisation/Les%20systemes%20de%20detection%20d%20intrusions.pdf).

[David Burgermeister et Jonathan Krier 06] : ([Burgermeister, D.et Krier,J 06] Burgermeister, D.et Krier, J.Les systemes de détection d'intrusion.Juillet 2006).

[Dong Wei et al, 2011]: (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, 2011).

[Depeng Li et al, 2011]: (Depeng Li, Zeyar Aung, John R Williams, and Abel Sanchez. Efficient authentication scheme for data aggregation in smart grid with fault tolerance and fault diagnosis. In Innovative Smart Grid Technologies (ISGT), 2012 IEEE PES. IEEE, 2012).

[F. Bao et al, 2012]: (F. Bao, P. Samarati, and J. Zhou. Applied Cryptography and Network Security: 10th International Conference, ACNS 2012, Singapore, June 26-29, 2012, Proceedings.Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2012).

[Fadi Aloula et al , 2012]: (Fadi Aloula, AR Al-Alia, Rami Al-Dalkya, Mamoun Al-Mardinia, and Wassim El-Hajj. Smart grid security: Threats, vulnerabilities and solutions. International Journal of Smart Grid and Clean Energy, 2012).

[Guy Pujolle ,2008] : (Guy Pujolle, « Les réseaux », Eyrolles ; 2008).

[Hervé Debar et al, 2000] : (Hervé Debar, Marc Dacier ET Andreas Wespi ; "A Revised Taxonomy for Intrusion-Detection Systems – Annales des Télécommunications " ; 2000).

[Hussain Ahmad Madni Uppal et al , 2014] : (Hussain Ahmad Madni Uppal1, Memoona Javed and M.J. Arshad ;"An Overview of Intrusion Detection System (IDS) along with its Commonly Used Techniques and Classifications " ;Department of Computer Science and Engineering, UET, Lahore, Pakistan;2014)

[IEEE Standards Association et al]: (IEEE guide for smart grid interoperability of energy technology and information technology operation with the electric power system (eps), end-use applications, and loads. IEEE Std 2030, 2011)

[Ishtiaq Rouf et al, 2012]: (Ishtiaq Rouf, Hossen Mustafa, Miao Xu, Wenyuan Xu, Rob Miller, and Marco Gruteser. Neighborhood watch: security and privacy analysis of automatic meter reading systems. In Proceedings of the 2012 ACM conference on Computer and Communications security, 2012).

[Imen Aouini, Lamia Ben Azzouz; 2015]: (Imen Aouini and Lamia Ben Azzouz;" Smart meter: Applications, security issues and challenges", 2015).

[J.L. LILIEN, 2006] : (J.L. LILIEN,"Transport et Distribution de l'Energie Electrique", Cours donné à l'Institut d'Electricité Montefiore, Université de Liège ,2006)

[Jianye Hao et al, 2014]: (Jianye Hao, Eunsuk Kang, Daniel Jackson, and Jun Sun. Adaptive defending strategy for smart grid attacks. In Proceedings of the 2nd Workshop on Smart Energy Grid Security, 2014).

[Jan Durech, Maria Franekova; 2014]: (Jan Durech and Maria Franekova. Security attacks to zigbee technology and their practical realization. In Applied Machine Intelligence and Informatics (SAMI), 2014 IEEE 12th International Symposium on, pages 345–349. IEEE, 2014).

[Kenneth_C._Budka et al, 2014] :(K.C. Budka, J.G. Deshpande, and M. Thottan. Communication Networks for Smart Grids: Making Smart Grid Real. Computer Communications and Networks. Springer-Verlag, 2014).

[Khaleel Ahmad1et al , 2011]: (Khaleel Ahmad, Shikha Verma,Nitesh Kumar and Jayant Shekhar;" Classification of Internet Security Attacks"; CSE/IT Dept. S.I.T.E., Swami Vivekananda Subharti UniversityMeerut, Uttar Pradesh, India1;2011).

[KE Martin et al, 2005]: (KE Martin, D Hamai, MG Adamiak, S Anderson, M Begovic, G Benmouyal, G Brunello, J Burger, JY Cai, B Dickerson, et al. " Exploring the ieee standard c37. 118–2005 synchrophasors for power systems. Power Delivery", IEEE Transactions on , 2008).

[Linus Wallgren et al 2013]: (Linus Wallgren, Shahid Raza, and Thiemo Voigt. Routing attacks and countermeasures in the rpl-based internet of things. International Journal of Distributed Sensor Networks, 2013)

[Lu et al, 2012]: (Rongxing Lu, Rongxing Lu, Xiaodong Lin. and Xuemin Sherman Shen. EPPA : An Efficient and Privacy-Preserving Aggregation Scheme for Secure Smart Grid Communications, 2012).

[Murat Kuzlu et al, 2014] :(Murat Kuzlu, Manisa Pipattanasomporn, and Saifur Rahman. Communication network requirements for major smart grid applications in han, nan and wan. Computer Networks, 2014).

[MYK, 1994]: (Mykerjee. B & Heberlein. L.T & Levitt .K.N « Network Intrusion Detection », IEEE Network, 1994).

[Mohammad Hossein Yaghmaee et al, 2013]: (Mohammad Hossein Yaghmaee, Qurban Ali Frugh, and Malihe Bahekmat ; " Monitoring approach for detection compromise attacks in smart meter", 2013).

[Mohammad Esmalifalak et al, 2013]: (Mohammad Esmalifalak, Ge Shi, Zhu Han, and Lingyang Song. Bad data injection attack and defense in electricity market using game theory study. Smart Grid, 2013).

[M. A. Faisal et al ,2012] :(M. A. Faisal, Z. Aung, J. R.Williams, and A. Sanchez, "Securing Advanced Metering Infrastructure Using Intrusion Detection System with Data Stream Mining," Pacific Asia Workshop, PAISI 2012, Kuala Lumpur, Malaysia Proceedings, 2012).

[NC Batista et al ,2013] :(NC Batista, R Melício, JCO Matias, and JPS Catalão. Photovoltaic and wind energy systems monitoring and building/home energy management using zigbee devices within a smart grid. Energy, 2013).

[NC Batista et al, 2012]: (NC Batista, Rui Melicio, JCO Matias, and Joao PS Catalao. "Zigbee wireless area network for home automation and energy management: Field trials and installation approaches. In Innovative Smart Grid Technologies (ISGT Europe) ", 3rd IEEE PES International Conference and Exhibition on, 2012).

[Nadia Boumkheld et al,2016] : (Intrusion Detection System for the Detection of Blackhole Attacks in a Smart Grid Nadia Boumkheld , Mounir Ghogho, and Mohammed El Koutbi ENSIAS, Morocco .Université Internationale de Rabat (UIR), Morocco;2016).

[Philippe Biondi, 2001] : (Philippe Biondi ; « Architecture expérimentale pour la détection d'intrusions dans un système informatique » ; philippe.biondi@ ;2001).

[Phung Khac ,2005] : (Phung Khac ; « La sécurité dans les réseaux hauts débit » ; Mai 2005).

[P.jokar et al ,2011] :(P. Jokar, H. Nicanfar, V. C. M. Leung, "Specification-based Intrusion Detection for Home Area Networks in Smart Grids," , 2011).

[Patel et al, 2013] :(Patel, A., Celestino, J., & Myrup, J. (2013). Computer Standards & Interfaces An intelligent collaborative Intrusion Detection and Prevention System for Smart Grid environments. Computer Standards & Interfaces, 2013).

[Q GAO et al, 2008]: (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 , 2008).

[Rui Tan et, 2013] : (Rui Tan, Varun Badrinath Krishna, David KY Yau, and Zbigniew Kalbarczyk ; “ Impact of integrity attacks on real-time pricing in smart grids”; In Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, 2013).

[S.Shekara, 2011]: (Shekara, S., Reddy, S., Wang, L., & Devabhaktuni, V. (2011). Smart meters for power grid: Challenges, issues, advantages and status. Renewable and Sustainable Energy Reviews, 2011)

[S.salinas, 2013] :(Salinas, S., Li, M., Li, P., & Fu, Y. (2013). Dynamic Energy Management for the Smart Grid, 2013)

[Shengrong Bu et al, 2011]: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 (GreenCom , IEEE , 2011).

[STA, 1997]: (S. Staniford-Chen, « GrIDS Outline Design Document ». GrIDS Project Home Page at UC Davis’sComputer Science Department, URL: http://olympus.cs.ucdavis.edu/arpa/grids/design.html , 1997).

[Sheeraz Niaz et al ,2014]: (Sheeraz Niaz Lighari, Dil Muhammad Akbar Hussain, Asad Ali Shaikh, and Bogi Jensen;” Attacks and their defenses for advanced metering infrastructure”; In Ultra-Modern Telecommunications and Control Systems and Workshops (ICUMT); 2014 6th International Congress on, pages 148–151. IEEE; 2014).

[Tarek Khalifa et al, 2011] (Tarek Khalifa, Kshirasagar Naik, and Amiya Nayak. A survey of communication Protocols for automatic meter reading applications. Communications Surveys & Tutorials, IEEE, 13(2): 168–182, 2011).

[Thomas Basso, Richard DeBlasio; 2011] :(Thomas Basso and Richard DeBlasio. Ieee smart grid series of standards ieee 2030 (interoperability) and ieee 1547 (interconnection) status. Grid-Interop, pages 5–8, 2011).

[Thien-Toan Tran et al ,2013]: (Thien-Toan Tran, Oh-Soon Shin, and Jong-Ho Lee; “Detection of replay attacks in smart grid systems”; In Computing, Management and Telecommunications (Com-ManTel); 2013 International Conference on, pages 298–302. IEEE; 2013).

[Viardin ,2006] : (Viardin,A ; « Un petit guide pour la sécurité » ;Février 2006).

[W.wang et al, 2011]: (Wang, W., Xu, Y., & Khanna, M. (2011). A survey on the communication architectures in smart grid, 55, 3604–3629. http://doi.org/10.1016/j.comnet.2011.07.010)

[Wayes Tushar et al ,2012]:'Wayes Tushar, Jian Zhang, David B Smith, H Vincent Poor, Glenn Platt, and Salman Durrani. An efficient energy curtailment scheme for outage management in smart grid. In Global Communications Conference (GLOBECOM), IEEE, 2012).

[Wenye Wang, Zhuo Lu; 2013]: (Wenye Wang and Zhuo Lu; "Cyber security in the smart grid: Survey and challenges"; Computer Networks; 2013).

[Xi Fang et al, 2011]: **(**Xi Fang, IEEEStudent Member IEEE, Satyajayant Misra, Member S, IEEE, Guoliang Xue ;"Smart Grid-the new and improved power Grid : A survey"; IEEE;2011)

[Ye.Yan et al, 2012]: (Yan, Y., Qian, Y., Sharif, H., & Tipper, D;" A Survey on Cyber Security for Smart Grid Communications"; 2012)

[Yasir Arafat et al, 2014]: (Yasir Arafat, Lina Bertling Tjernberg, and Per-Anders Gustafsson. Remote switching of multiple smart meters and steps to check the effect on the grid's power Quality. In T&D Conference and Exposition, 2014 IEEE PES, IEEE, 2014).

[Yichi Zhang et al ,2011]: (Zhang, Y., Wang, L., Sun, W., Ii, R. C. G., & Alam, M. Distributed Intrusion Detection System in a Multi-Layer Network Architecture of Smart Grids,2011).

[Y. Xiao, 2012]: (Y. Xiao. Communication and Networking in Smart Grids. Taylor & Francis; 2012).

[Yifan Li et al, 2012]: (Yifan Li, RanWang, PingWang, Dusit Niyato,Walid Saad, and Zhu Han." Resilient phev charging policies under price information attacks. In Smart Grid Communications (SmartGridComm)", 2012 IEEE Third International Conference on, IEEE; 2012).

[Zhuo Lu et al: 2010]: (Zhuo Lu, Xiang Lu, Wenye Wang, and Cliff Wang. "Review and evaluation of security threats on the communication networks in the smart grid. In MILITARY COMMUNICATIONS CONFERENCE" ; IEEE ; 2010).

➢ Références WEB

[w1]	(URL :https://commons.wikimedia.org/wiki/File:Electricity_Grid_Schematic_English.sg).
[w2]	(Angela Berger,Smart Grids Austria Technology roadmap ,2015, URL:www.smartgrids.at).
[w3]	(Réseau intelligent (Smart Grid), connaissance des energies, URL:http://www.connaissancedesenergies.org/fiche-pedagogique/reseau-intelligent-smart-grid , mise à jour le 14 avril 2015).
[w4]	(smartgrids cre ,URL: http://www.smartgrids cre.fr/index.php?p=comprendre-les-smart-grids).
[w5]	(smartgrids ,URL: https://energie2020.fr/wp-content/uploads/2014/10/smartgrids_savoir_faire_francais_.pdf , 2014).
[w6]	(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.)
[w7]	(Grid, C. S., & Group, C. (2012). CEN-CENELEC-ETSI Smart Grid Coordination Group Smart Grid Reference Architecture Contents, (November). URL: https://ec.europa.eu/energy/sites/ener/files/documents/xpert_group1_reference_architecture.pdf)
[w8]	(William Beaucardet, Réseau intelligent (Smart Grid), Laboratoire d'essai pour tester des composants de smart grids (©EDF-), URL :http://www.connaissancedesenergies.org/fiche-pedagogique/reseau-intelligent-smart-grid, mis à jour e 14 avril 2015)
[w9]	(URL : http://www.smartgrids-cre.fr/index.php?p=europe-introduction)
[w10]	(URL : http://cordis.europa.eu/result/rcn/90264_fr.html)
[w11]	(URL : http://cordis.europa.eu/project/rcn/87374_fr.html)
[w12]	(URL: http://cordis.europa.eu/project/rcn/93771_en.html)
[w13]	(URL: http://www.enel.fr/address.aspx)
[w 14]	(URL: http://www.smartgrids-cre.fr/index.php?p=smile-bretagne)
[w 15]	(URL : http://www.cea.fr/presse/Pages/actualites-communiques/ntic/SESAM-Grids,-un-projet-de-RD-pour-renforcer-la-securite-des-smart-grids.aspx)
[w16]	(Titre : PODCAST NOLIMITSECU : LES SYSTÈMES SCADA ET LEUR SÉCURITÉ,Editer par MICKAEL DORIGNY, URL:https://www.information-security.fr/podcast-nolimitsecu-systemes-scada securite/,31/07/2015)
[w17]	(Titre : SCADA, Editer par Margaret Rouse , URL : http://www.lemagit.fr/definition/SCADA , mise à jour en février 2016)
[w18]	(Titre : Les systèmes de supervision scada, Editer par automationsense , URL:http://www.automation-sense.com/blog/automatisme/les-systemes-de supervision-scada.html , 17/02/2016)
[w19]	(Titre : SYSTÈME SCADA, URL : https://www.meteocontrol.com/fr/industrial-line/scada-center/)
[w20]	(Titre article/ SCADA Systems , Editer par Anshul Thakur https://www.engineersgarage.com/articles/scada-systems)

[w21]	(Titre d'Article/ SCADA Systems , Editer par Anshul Thakur URL: https://www.engineersgarage.com/articles/scada-systems)
[w22]	(Titre : Protection des systèmes SCADA et ICS : un enjeu vital, Editer par : Par Arnaud Kopp ,URL : http://www.itpro.fr/a/protection-systemes-scada-et-ics-un-enjeu-vital/ Protection des systèmes SCADA et ICS : un enjeu vital , 23/03/2015)
[w23]	(Titre Les 10 principales défaillances des systèmes Scada selon Lexsi , Editer par : Christophe Lagane, URL : http://www.silicon.fr/10-principales-defaillances systemes-scada-selon-lexsi-121545.html,10 juillet 2015, 9:00)
[w24]	(Titre: A Survey of Research in Supervisory Control and Data Acquisition (SCADA) Editer par: Sidney C Smith / Army Research Laboratory September 2014)
[w25]	URL :http://www.fil.univ-lille1.fr/~decomite/ue/APE/tp/tp1/weka2009.pdf
[w26]	http://abdelhamid-djeffal.net/web_documents/coursad.pdf
[w27]	http://igm.univmlv.fr/~dr/XPOSE2013/panoramas_des_attaques_reseaux/attaques_historiques.html