No: 7 /2006

Université libanaise
Faculté des sciences

Université Paul Sabatier – I.R.I.T.

DEA d'Informatique

Coopération dans les sciences de traitement de l'information

Année universitaire 2005/2006

Etude des protocoles et infrastructures de sécurité dans les réseaux

Préparé par Imad Bou Akl

Responsable Zoubir Mammeri

Jury Bilal Chebaro

Ali Awada

Kablan Barbar

Mots-clés : Système embarqué - Attaques - Infrastructure critique - réseaux de capteur - WiFi - Pare feu - IDS - connectivité - VPN - ADSL - IPSEC -sécurité - QoS - Internet -Satellite

Résumé

Ce mémoire consiste à traiter la connectivité dans les infrastructures critiques en utilisant plusieurs technologies et services. Il traite encore les méthodes qui offrent un haut débit et les dispositifs et les protocoles qui assurent la sécurité contre les attaques et les menaces.

Key words : Embedded system - Attacks - critical infrastructure - sensor networks - WiFi - Firewall - IDS - connectivity - VPN - ADSL - IPSEC - Security - QoS - Internet - Satellite

Abstract

This dissertation discusses the connectivity in critical infrastructures using several technologies and services. It also treats the methods which offer high data flow as well as the devices and the protocols which ensure the safety against attacks and the threats.

Remerciements

Ce travail a été effectué au sein de l'Institut de Recherche en informatique de Toulouse.

Je remercie mon encadrant, Monsieur le professeur Zoubir Mammeri de l'Université Paul Sabatier, responsable de l'équipe ASTRE, pour ses encouragements, ses remarques constructives, pour m'avoir accueilli dans son équipe de recherche et pour avoir assurer la direction de ce stage.

Je remercie tous les membres de l'équipe ASTRE.

Je remercie Monsieur Jean-Paul Bahsoun, Professeur et Directeur du département informatique de l'IRIT et de l'UPS pour ses encouragements et ses conseils.

Je remercie Monsieur Bilal Chebaro, Docteur à l'Université libanaise, pour son encadrement durant mon stage au Liban, sa patience, ses remarques et ses conseils.

Un grand remerciement à mes parents pour leur support et leur croyance en moi.

A toute personne qui a contribué à la réalisation de ce mémoire, je dis : Merci.

* * *

Table des matières

Introduction

Chapitre 1 : Introduction à la sécurité, réseaux sans fil et systèmes embarqués

1.1 Introduction 9
1.2 Les attaques qui menacent les systèmes critiques et embarqués 10
1.2.1 Des attaques traditionnelles 10
1.2.1.1 Introduction 10
1.2.1.2 Attaques par rebond 10
1.2.1.3 Attaque par déni de service 11
1.2.1.4 La technique dite « par réflexion » 11
1.2.1.5 Attaque par usurpation d'adresse IP (IP spooffing) 11
1.2.1.6 Mot de passe devinant 11
1.2.2 Une vrai menace dans un système critique 11
1.3 Les signaux wireless et les réseaux de capteur sans fil 12
1.3.1 Introduction 12
1.3.2 Les techniques d'étalement du spectre 13
1.3.2.1 La technique de saut de fréquence 13
Etalement du spectre à séquence directe 14
1.3.3 Les réseaux de capteur sans fil 15
1.3.3.1 La norme 802.15.4 15
1.3.3.2 Topologie réseau 15
1.3.3.3 Modèle de transfert de données 15
1.4 Techniques de calcul en temps réel pour les mesures de la sécurité 15
1.4.1 Introduction 15
1.4.2 Cryptographie 16
1.4.2.1 Chiffrement symétrique 16
1.4.2.2 Chiffrement asymétrique 17
1.4.3 Condensât 17
1.4.4 Signature numérique 17
1.4.4.1 Signature numérique symétrique 17
1.4.4.2 Signataire numérique asymétrique 18
1.5. La gestion de la sécurité par des moyens en temps réel 18
1.5.1 Introduction 18
1.5.2 Gestion des moyens de protections minimums 18
1.5.3 Capacité des équipements de sécurité 19
1.5.4 Filtrage des paquets en temps réel 19
1.6 Faire confiance d'un système embarqué 19
1.6.1 Introduction 19
1.6.2 Test en ligne intégré 20
1.6.3 Le principe du modèle checking 20
1.7 L'overhead ajouté par les mécanismes de la sécurité 21
1.7.1 Introduction 21

1.7.2 IPSec 22
1.7.3 Filtre de paquet (FP) 22
1.7.4 La sécurité et la qualité de service 22

Chapitre 2 : Technologies et services pour la connectivité

2.1 Introduction 25
2.2 Les dispositifs de connectivité des réseaux 25
2.2.1 Introduction 25
2.2.2 Les avantages de l'extension d'un réseau local 25
2.2.2 Les différents dispositifs de la connectivité 26
2.3 La mise en place d'un serveur proxy 29
2.3.1 Introduction 29
2.3.2 Le principe de fonctionnement d'un proxy 30
2.3.3 Les fonctionnalités d'un serveur proxy 30
2.3.3.1 Le filtrage 30
2.3.3.2 L'authentification 30
2.5 Mettre en place des caches web distribués 30
2.6 Les protocoles TCP/IP et Internet 31
2.6.1 TCP/IP 31
2.6.1.1 Définition 31
2.6.1.2 Adressage IP 31
2.6.1.3 IPv6 32

Chapitre 3 : Connectivité dans les infrastructures critiques

3.1 Introduction 34
3.2 Un débit élevé et le technologie multiplexage en longueur d'onde 34
3.3 ADSL 35
3.3.1 Introduction 35
3.3.2 La technologie ADSL 35
3.3.3 L'offre ADSL 36
3.3.3.1 L'offre NETISSIMO I 36
3.3.3.2 L'offre NETISSIMO II 36
3.3.3.3 Les fournisseurs d'accès Internet proposant l'ADSL 36
3.3.4 Conclusion 37
3.4 VPN 37
3.4.1 Introduction 37
3.4.2 Tunnel 37
3.5 Assurer une qualité de service à la demande 38
3.5.1 Le réseau multimédia 38
3.5.1.1 Les conditions de la qualité de service 38
3.5.2 Les solutions de la QoS 39
3.5.2.1 Les routeurs de périphérie 39
3.5.2.2 Les flux différenciés de paquets 39
3.5.2.3 La notification explicite 40

3.6 Internet par satellite 40
3.6.1 Introduction 40
3.6.2 L'équipement nécessaire 41
3.6.3 Le fonctionnement 41
3.6.4 Les serveurs Proxy 41
3.6.5 Le « Push » 42
3.6.6 Les débits 42
3.6.7 L'avenir 42

Chapitre 4 : Gestion de la sécurité

4.1 Introduction 44
4.2 Les dispositifs de la sécurité 44
4.2.1 Les pare-feu 44
4.2.1.1 Définition et fonctionnement 44
4.2.1.2 Les types de firewalls 45
4.2.2 Les systèmes de détection et de prévention de l'intrusion 46
4.3 VPN 47
4.3.1 Introduction 47
4.3.2 IPSec 48
4.3.3 SSL 49
4.3.4 Utilisation de IPsec et SSL 49
4.4 Un système VPN bien administré 49

Conclusion générale

Bibliographie

Table des figures

Figure 1 : Les grandes catégories de réseaux sans fil 12
Figure 2 : Le mode Ad Hoc et le mode Infrastructure 13
Figure 3 : La technique chipping 14
Figure 4 : Principe du model-checking 21
Figure 5 : Accès au réseau local par un tunnel VPN 37
Figure 6 : Tunnel interconnectant le sous réseau A au sous réseau B 38
Figure 7 : Représentation des antennes embarquées sur un satellite 41
Figure 8 : Différentes applications VPNS 48

Introduction Générale

Généralement la présence sur Internet est devenue une réalité pour les entreprises et les différentes infrastructures et ce quelque soit leur taille ou leur nature. La disponibilité d'accès à haut débit permanent autorise chaque entreprise héberger des services Internet et à proposer à ses collaborateurs l'accès au réseau sans contraintes.

Donc l'installation de l'Internet doit prendre en compte les problématiques suivants :

- La connectivité à l'Internet et les relations avec les ISP (Internet Service Provider)
- Le routage IP et l'adressage
- La gestion et la traduction d'adresse (NAT)
- Le filtrage et le pare-feu
- Les services Internet et leur sécurisation spécifique
- La gestion du DNS
- Le partage de charge
- La sécurisation active des services face aux pannes

Les infrastructures critiques sont les installations physiques et des technologies de l'information, les réseaux, les services et les actifs qui, en cas d'arrêt ou de destruction, peuvent avoir des graves incidentes sur la santé ou la sécurité des personnes et des biens. Les infrastructures critiques englobent :

- Les installations et les réseaux dans les secteurs d'énergie (notamment les installations de production d'électricité, de pétrole et de gaz, les installations de stockage et les raffineries, les systèmes de transport et de distribution)
- Les technologies des communications et de l'information (les télécommunications, les systèmes de radio diffusion, les logiciels, le matériel informatique et les réseaux, y compris l'Internet, etc.)
- Les finances (le secteur bancaire)
- Eau (Réserves, stockage, traitement et réseaux)
- Transport (aéroports, ports, systèmes de contrôle de trafic)
- Administration (services de base, installations, réseaux d'information, actifs et principaux sites et monuments nationaux)

Pour bien assurer une bonne interactivité entre les différents équipements des infrastructures critiques, il faut offrir un très haut débit permettant de fonctionner en temps réel. Aussi, il faut comprendre une chose : le très haut débit aujourd'hui, 2.5 Gigabits/seconde, sera le débit normal d'ici quatre ans. La limitation se fait au niveau des boucles locales, compte tenu du coût envisagé d'installation des connexions. En plus, il est utile de réduire le trafic à travers le réseau critique et ainsi d'améliorer le temps de réponse.

Donc, les technologies et les infrastructures critiques liées à l'Internet sont incontournables pour fournir une bonne qualité de service. On a considéré l'Internet lui-même comme le réseau commun pour livrer tous les types de contenu. Cette vision optimiste n'a pas encore rempli toutes ses personnes, une des raisons étant que la technologie d'accès à large bande sur la boucle locale prend plus de temps pour se

déployer que prévu. Mais, là aussi, l'évolution vers des services plus interactifs est fortement attendue.

La connectivité des systèmes critiques aux réseaux doit prendre en compte des besoins et des contraintes de plus en plus variées : montée en débit en fréquence, amélioration de la qualité de service, de la sécurité et la sûreté de fonctionnement, traitement efficace des différents type de flux (données, voix, images), inter fonctionnement des différents constituants des réseaux, besoins particuliers de certains flux…

La sécurité de ces systèmes consiste à sécuriser trois classes de composants : les nœuds du réseau (routeurs, commutateurs et entités de gestion), l'infrastructure de transport et le trafic qui utilise ce réseau.

Les travaux de ce mémoire ont consisté à étudier la connectivité dans les infrastructures critiques. L'objectif est de préciser la manière à laquelle une infrastructure se connecte au réseau surtout à Internet en précisant les différents dispositifs et les technologies servant à réaliser ce but. Ainsi, on étudie les mécanismes et les protocoles permettant de sécuriser ces infrastructures contre les attaques et les menaces.

Le contexte et l'étude générale de quelques aspects font l'objet du **premier chapitre** de ce mémoire. Les types des attaques menaçant les systèmes et les infrastructures critiques sont d'abord présentés. Puis une étude générale sur l'acquisition des signaux wireless et les réseaux de capteur a été effectuée. La cryptographie comme une technique de calcul en temps réel pour assurer la sécurité a été représentée. Aussi, des contraintes ont été citées dans le but d'offrir une sécurité en temps réel dans les systèmes informatiques critiques. Les systèmes embarqués et ses caractéristiques ont été étudiés afin d'offrir la sécurité et la confiance durant leur fonctionnement.

Le **second chapitre** est consacré à la description des technologies et des services permettant de faire la connectivité d'un réseau. Les dispositifs utilisés lors de la connectivité sont tout d'abord présentés.

Au **cours du troisième chapitre** nous étudions les technologies spéciales permettant de relier une infrastructure critique au réseau. Plusieurs méthodes sont présentées pour mettre ces infrastructures sur le réseau en offrant tout entièrement la sécurité et un haut débit permettant l'interaction en temps réel. Ainsi, nous présentons la connectivité à Internet par satellite.

La réalisation et la gestion de la sécurité avec des différents dispositifs et en utilisant des protocoles sécurisés sont menées au **quatrième chapitre**.

Ce mémoire se termine par une conclusion sur les travaux présentés.

Chapitre 1
Introduction à la sécurité, réseaux sans fil et systèmes embarqués

1.1 Introduction

Le degré d'utilisation des systèmes et réseaux d'information et l'environnement des technologies de l'information dans son ensemble ont évoluée de façon spectaculaire depuis 1992. Ces évolutions offrent des avantages significatifs mais requirent également que le gouvernement, les entreprises, les autres organisations et les utilisateurs individuels qui développent, possèdent, fournissent, gèrent, maintiennent et utilisent les systèmes et réseaux d'informations, portent une bien plus grande attention à la sécurité.

La sécurité est un enjeu majeur des technologies numériques modernes. Infrastructure de télécommunication (GSM, GPRS, UMTS), réseau sans fils (bluetooth, WiFi, WiMax), Internet, systèmes d'informations, routeurs, systèmes d'exploitation, applications informatiques, toutes ces entités présentent des vulnérabilités : faille de sécurité, défaut de conception ou de configuration. Ces systèmes tombent en panne, subissent des erreurs d'utilisation et sont attaqués de l'extérieur ou de l'intérieur par des pirates, des cybercriminels. Une approche globale de la sécurité des systèmes est essentielle pour protéger la vie privée, pour réduire les vulnérabilités des grands systèmes d'informations. **[MR 06].**

L'Internet est le support d'infrastructures vitales telles que l'énergie, les transports et les activités financières et joue un rôle majeur dans la façon dont les entreprises conduisent leurs activités, dont les gouvernements assurent des services aux citoyens et aux entreprises et dont les citoyens communiquent et échangent des informations. La nature et le type des technologies constituant l'infrastructure des communications et de l'information ont également sensiblement évolué. Le nombre et la nature des dispositifs d'accès à cette infrastructure se sont multipliés et diversifiés pour englober les terminaux d'accès fixes, sans fil et mobiles et une proportion croissante des accès s'effectue par l'intermédiaire de connexions « permanentes ». Par voie de conséquence, la nature, le volume et le caractère sensible de l'information échangée ont augmenté de façon significative. Toute cette progression demande de développer une « culture de la sécurité ».
Donc, le présent concept de protection de base a pour objectif de réduire la vulnérabilité des infrastructures critiques face aux événements et accidents naturels ainsi qu'aux attentats terroristes et aux actes criminels. Dans cet objectif, le concept de base se concentre sur les mesures de protection relatives à la construction, à l'organisation, aux personnes et à la technique.

Aussi le temps est une dimension importante qu'il faut considérer dans les infrastructures critiques et dans les systèmes des contrôles et la prise en compte de ses contraintes intervient à tous les niveaux du cycle de vie des applications. La correction fonctionnelle repose notamment sur des approches de génie logiciel (conception de composants orientée objet ou aspect). La correction temporelle repose sur des approches propres au temps réel, notamment la spécification et la validation de contraintes de temps et la communication avec une qualité de service prédictible.

1.2 Les attaques qui menacent les systèmes critiques et embarqués

Les systèmes embarqués représentent une grande partie des objets qui nous entourent, et qui contiennent de l'informatique sans pour autant être explicite. L'informatique embarquée est présente dans des contextes très divers allant des téléphones portables aux instruments de navigation des avions.

Un système embarqué n'a pas le droit d'avoir une réaction imprévisible. Il faut pouvoir garantir une borne temporelle pour les fonctions prises en charge. Les cyber-attaques menaçant tous ces systèmes prennent diverses formes : prises de contrôle d'un système, déni de service, destruction ou vol de données …elles ont toutes une conséquence négative pour les organisations. **[GB 05]**

Les motivations des attaques peuvent être des différentes sortes :

- Obtenir un accès au système
- Voler des informations, tels que des secrets industriels ou des propriétés intellectuelles ;
- Récupérer des données critiques
- S'informer sur l'organisation
- Troubler le bon fonctionnement d'un service
- Utiliser le système de l'utilisateur comme « rebond » pour une attaque
- Utiliser les ressources du système de l'utilisateur, notamment lorsque le réseau sur lequel il est situé possède une bande passante élevée.

Un système embarqué est aussi un système mobile, et donc il peut être amené à subir souvent des pannes matérielles. Ces pannes matérielles doivent pouvoir être évitées, et lorsqu'elles arrivent, le système, s'il est autonome, doit logiquement pouvoir trouver un autre moyen d'effectuer sa tâche (si la gravité de la panne le permet).

1.2.1 Des attaques traditionnelles

1.2.1.1 Introduction

Les cyber-attaques menaçant tous ces systèmes prennent diverses formes : prises de contrôle clandestine d'un système, déni de service, destruction ou vol de données sensibles, *hacking* (piratage du réseau de télécommunication), *craking* (craquage des protections logicielles des programmes), *phreaking* (sabotage, prise de contrôle de centrales téléphonique, …). Elles ont toutes des conséquences négatives pour les organisations ou individus qui sont victimes.

1.2.1.2 Attaques par rebond

Lors d'une attaque, le pirate garde toujours à l'esprit le risque de se faire repérer, c'est la raison pour laquelle les pirates privilégient habituellement les attaques par rebond, consistant à attaquer une machine par l'intermédiaire d'une autre machine, afin de masquer les traces permettant de remonter à lui (telle que son adresse IP) et dans le but d'utiliser les ressources de la machine servant de rebond.

1.2.1.3 Attaque par déni de service

Une « attaque par déni de service » est un type d'attaque visant à rendre indisponible pendant un temps indéterminé les services ou ressources d'une organisation. Il s'agit la plupart du temps d'attaques à l'encontre des serveurs d'une entreprise, afin qu'ils ne puissent être utilisés et consultés.

Le principe des attaques par déni de service consiste à envoyer des paquets IP ou des données de taille ou de constitution inhabituelle, afin de provoquer une saturation ou un état instable des machines victimes et de les empêcher ainsi d'assurer les services réseau qu'elles proposent.

1.2.1.4 La technique dite « par réflexion »

La technique dite « attaque par réflexion » (en anglais « smurf ») est basée sur l'utilisation de serveurs de diffusion (broadcast) pour paralyser un réseau. Un serveur broadcast est un serveur capable de dupliquer un message et de l'envoyer à toutes les machines présentes sur le même réseau.

1.2.1.5 Attaque par usurpation d'adresse IP (IP spoofing)

L'usurpation d'adresse IP est une technique consistant à remplacer l'adresse IP de l'expéditeur d'un paquet IP par l'adresse IP d'une autre machine.

Cette technique permet ainsi à un pirate d'envoyer des paquets anonymement. Il ne s'agit pas pour autant d'un changement d'adresse IP, mais d'une mascarade de l'adresse IP au niveau des paquets émis.

La technique de l'usurpation d'adresse IP peut permettre à un pirate de faire passer des paquets sur un réseau sans que ceux-ci ne soient interceptés par le système de filtrage de paquets (pare-feu).

1.2.1.6 Mot de passe devinant

Il est facilement d'obtenir un programme fendant de mot de passe tel que la « fente ». Ce programme essaie simplement de deviner le mot de passe d'un compte.

1.2.2 Une vrai menace dans un système critique

Un logiciel est dit critique lorsqu'une erreur dans son déroulement peut avoir un impact sur la sécurité des personnes ou avoir de graves répercussions pour le système qu'il contrôle : c'est le cas par exemple, du contrôle-commande d'une centrale nucléaire, des commandes de vol d'un avion ou du système de pilotage d'un métro sans chauffeur.
Les erreurs peuvent néanmoins subsister et le contrôle de leur propagation dans le système n'est pas toujours assuré. En témoignant quelques exemples récents de catastrophes spectaculaires :

L'explosion du premier lanceur Ariane 5, en 1996, après quarante secondes de vol, était due à un problème de conversion de format de nombre dans le programme contrôlant le système de référence inertiel qui assure la stabilité de la fusée. Elle se traduisait par une

perte d'un demi milliard d'euros en matériel et par le risque de perte de crédibilité d'un programme de sept milliards d'euros.

En 1991, lors de la première guerre du Golfe, une imprécision numérique dans le calcul d'une horloge interne causa la mort de vingt-huit soldats américains après la défaillance d'un missile antimissile Patriot.

1.3 Les signaux wireless et les réseaux de capteur sans fil

1.3.1 Introduction

Les réseaux sans fil prennent le devant de la scène du monde des télécommunications. La gamme des réseaux sans fil normalisée ne fait que s'étendre et devrait venir concurrencer de plus en plus les réseaux sans fil en plus les réseaux de mobiles provenant du monde de télécommunications.

Plusieurs gammes de produits sont actuellement commercialisées, mais la normalisation en cours devrait introduire de nouveaux environnements. Les groupes de travail qui se chargent de cette normalisation sont l'IEEE 802.15, pour les petits réseaux personnels d'une dizaine de mètres de portée ou PAN (Personal Area Network), l'IEEE 802.11, pour les réseaux LAN (Local Area Network), IEEE 802.16 pour les réseaux MAN (Metropolitan Area Network) atteignant plus de dix kilomètres et enfin IEEE 802.22 pour les réseaux RAN (Regional Area Network), c'est-à-dire les réseaux de plusieurs centaines de kilomètres de portée. Chacune de ces gammes correspond à un usage différent, fonction de ses caractéristiques :

- vitesse de transmission,
- débit maximum,
- coût de l'infrastructure,
- coût de l'équipement connecté,
- sécurité,
- souplesse d'installation et d'usage,
- consommation électrique et autonomie.

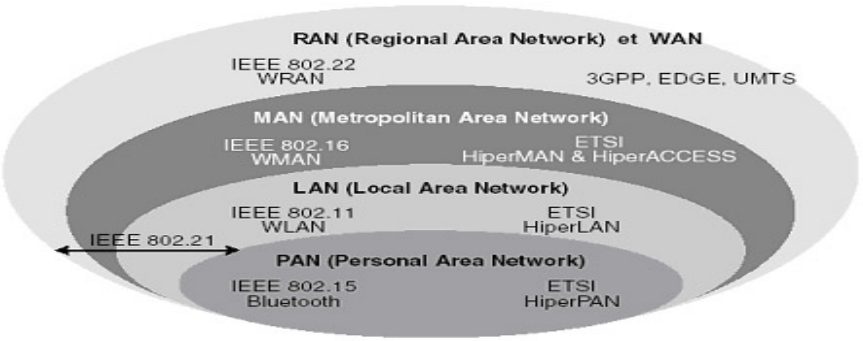

Figure 1 : Les grandes catégories de réseaux sans fil

Le protocole 802.11 de l'Institut of electrical and Electronics Engineers (IEEE), parfois nommé Wi-Fi, définit plusieurs couches physiques et une couche d'accès au médium pour les réseaux sans fil (Wireless local area networks - WLAN).
Les différentes couches physiques définissent différents codages permettant d'assurer une transmission sans fil fiable et un multiplexage de plusieurs canaux de transmission.

Le standard 802.11 définit deux modes opératoires :

- Le mode infrastructure dans lequel les clients sans fil sont connectés à un point d'accès. Il s'agit généralement du mode par défaut des cartes 802.11b.
- Le mode ad hoc dans lequel les clients sont connectés les uns aux autres sans aucun point d'accès.

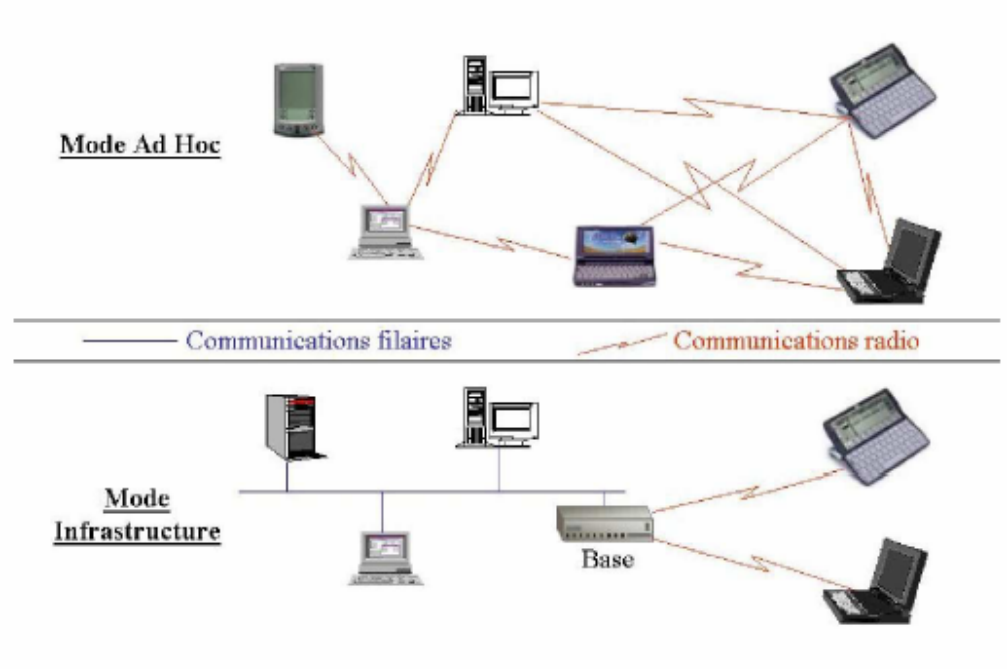

Figure 2 : Le mode Ad Hoc et le mode Infrastructure

1.3.2 Les techniques d'étalement du spectre

La norme IEEE 802.11 propose deux techniques de modulation de fréquence pour la transmission de données issues des technologies militaires. Ces techniques, appelées étalement de spectre consistent à utiliser une bande de fréquence large pour transmettre des données faibles puissances. On distingue deux types techniques d'étalement de spectre :

- La technique de l'étalement de spectre à saut de fréquence,
- La technique de l'étalement de spectre à séquence directe

1.3.2.1 La technique de saut de fréquence

La technique **FHSS** (Frequency Hopping Spread Spectrum, en français étalement de spectre par saut de fréquence ou étalement de spectre par évasion de fréquence) consiste à

découper la large bande de fréquence en un minimum de 75 canaux (hops ou sauts d'une largeur de 1MHz), puis de transmettre en utilisant une combinaison de canaux connue de toutes les stations de la cellule. Une allocation aléatoire d'une séquence de fréquence permet de multiplexer efficacement plusieurs transmissions et offre une bonne résistance aux interférences en bande, c'est-à-dire l'interférence en causées par des signaux émis dans la même bande de fréquence que le signal utile. Dans la norme 802.11, la bande de fréquence 2.4 - 2.4835 GHz permet de créer 79 canaux de 1 MHz. La transmission se fait ainsi en émettant successivement sur un canal puis sur un autre pendant une courte période de temps (d'environ 400 ms), ce qui permet à un instant donné de transmettre un signal plus facilement reconnaissable sur une fréquence donnée.

L'étalement de spectre par saut de fréquence a originalement été conçu dans un but militaire afin d'empêcher l'écoute des transmissions radio. En effet, une station ne connaissant pas la combinaison de fréquence à utiliser ne pouvait pas écouter la communication car il lui était impossible dans le temps imparti de localiser la fréquence sur laquelle le signal était émis puis de chercher la nouvelle fréquence.

Aujourd'hui les réseaux locaux utilisant cette technologie sont standards ce qui signifie que la séquence de fréquences utilisées est connue de tous, l'étalement de spectre par saut de fréquence n'assure donc plus cette fonction de sécurisation des échanges. En contrepartie, le FHSS est désormais utilisé dans le standard 802.11 de telle manière à réduire les interférences entre les transmissions des diverses stations d'une cellule.

Etalement du spectre à séquence directe

La technique **DSSS** (Direct Sequence Spread Spectrum, étalement de spectre à séquence directe) consiste à transmettre pour chaque bit une séquence ***Barker*** (parfois appelée bruit pseudo-aléatoire ou en anglais pseudo-random noise, noté PN) de bits. Ainsi chaque bit valant 1 est remplacé par une séquence de bits et chaque bit valant 0 par son complément.

La couche physique de la norme 802.11 définit une séquence de 11 bits (*10110111000*) pour représenter un 1 et son complément (*01001000111*) pour coder un 0. On appelle *chip* ou *chipping code* (en français *puce*) chaque bit encodé à l'aide de la séquence. Cette technique (appelée *chipping*) revient donc à moduler chaque bit avec la séquence *Barker*.

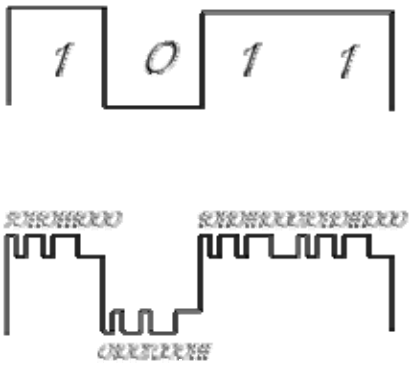

Figure 3 : La technique chipping

Grâce au *chipping*, de l'information redondante est transmise, ce qui permet d'effectuer des contrôles d'erreurs sur les transmissions, voire de la correction d'erreurs.

1.3.3 Les réseaux de capteur sans fil

Un réseau de capteur sans fil est un ensemble de capteurs variant de quelques dizaines d'éléments à plusieurs centaines, parfois plus. Les capteurs ne sont pas intégrés à une quelconque architecture pré-existante de réseau. C'est pourquoi ils communiquent à l'aide d'un réseau ad hoc sans fil.

Parmi les applications concernant les réseaux de capteurs, on distingue :

- Supervision de l'état du l'air, du sol
- Détection du séisme
- Surveillance militaire
- Ailes d'avion

1.3.3.1 La norme 802.15.4

La norme IEEE 802.15.4 a été spécialement en fonction des caractéristiques des réseaux de capteurs, un faible débit et une faible consommation électrique. Elle décrit le fonctionnement de la couche physique, et de la couche MAC.

1.3.3.2 Topologie réseau

Deux topologies sont supportées par le protocole 802.15.4. La topologie en étoile et la topologie point à point. Dans la topologie en étoile, les communications s'établissent directement entre le nœud central (coordinateur) et les capteurs, le coordinateur étant le nœud qui initie et gère les communications dans le réseau.
La topologie point à point se rapproche alors plus de mode de communication tel qu'il est structuré dans le réseau ad hoc. La topologie point à point nécessite l'utilisation d'un protocole de routage (routage mech, ad hoc…etc.)

1.3.3.3 Modèle de transfert de données

La norme IEEE 802.15.4 définit trois modèles transactionnels possibles :

- Transfert de données du coordinateur vers un nœud du réseau.
- Transfert de données d'un nœud de réseau vers le coordinateur.
- Transfert de données de deux nœuds du réseau entre eux.

Dans le cas d'une topologie en étoile, seules les deux premiers transactions sont possibles car les échanges se font exclusivement.

1.4 Techniques de calcul en temps réel pour les mesures de la sécurité

1.4.1 Introduction

La première étape dans l'évaluation de la sécurité est, bien évidement, la compréhension de la notion de « sécurité ». À ce jour, on en connait deux définitions majeurs.

La première, au sens de la théorie de l'information, a été initialement évoquée par Shannon. Elle concerne l'information sur le texte clair contenu dans le texte chiffré : un shéma de chiffrement est parfaitement sûr si le texte chiffré ne contient aucune information au sujet du texte clair correspondant. Dans le cadre d'un schéma de chiffrement symétrique, il a été démontré que la sécurité parfaite n'est atteinte que si la clef utilisée est aussi longue que le message. Cette condition a une sérieuse limite en pratique.

La deuxième approche, au sens de la théorie de la complexité, est actuellement utilisée dans l'analyse des schémas de chiffrement. Elle ne s'intéresse pas au contenu du texte chiffré mais met l'accent sur la « difficulté » d'extraire de l'information sur le texte clair à partir du texte chiffré. Cette difficulté est considérée au sens de la complexité et elle est souvent comparée à la difficulté d'un problème bien défini : la factorisation, par exemple.

1.4.2 Cryptographie

La cryptographie ou chiffrement est le processus de transcription d'une information intelligible en une information inintelligible par l'application de conventions secrètes dont l'effet est réversible. La loi française définit les prestations de cryptologie comme : « toutes prestations visant à transformer à l'aide de conventions secrètes des informations ou signaux clairs en information ou signaux inintelligibles pour des tiers, ou à réaliser l'opération inverse, grâce à des moyens, matériels ou logiciels conçus à cet effet »

Il existe deux grands types de cryptographie :

- La cryptographie symétrique : la même clé (le code secret) est utilisée pour encrypter et décrypter l'information. Le problème de cette méthode est qu'il faut trouver le moyen de transmettre de manière sécurisée la clé à son correspondant.
- La cryptographie asymétrique : ce n'est pas la même clé qui crypte et qui décrypte les messages. L'utilisateur possède une clé privée et une clé publique. Il distribue sa clé publique et garde secrète sa clé privée. Dans ce type d'application, tout le monde peut lui écrire en utilisant la clé publique, mais seul l'utilisateur destinataire pourra décrypter et donc lire le message avec sa clé privée. La cryptographie permet ici d'assurer la confidentialité des données transitant sur un réseau : les données sont uniquement portées à la connaissance des personnes autorisées. Une autre paire de clés sera utilisée pour s'assurer de l'identité de l'émetteur d'un message : c'est la question de l'authentification. L'utilisateur crypte avec sa clé privée son message. Tout le monde peut décrypter le message avec la clé publique correspondant à l'expéditeur ainsi identifié.

1.4.2.1 Chiffrement symétrique

La même clé est utilisée pour chiffrer et déchiffrer. Le principal avantage du chiffrement symétrique est une grande vitesse de chiffrement obtenue par une réalisation en circuits intégrés. Le principal inconvénient est la difficulté de partager la même clé par deux entités distantes. En effet, cette clé devra être générée par une entité puis transportée vers l'autre entité, ce qui impose un transport très sécurisé.
Parmi les clés de chiffrement symétrique, les plus connus sont DES et AES. La taille des clés est souvent comprise entre 40 bits et 256 bits.

Fonctions pseudo-aléatoires
Pour la catégorie de chiffrement la plus fréquemment étudiée en cryptographie symétrique – le chiffrement par bloc – la propriété désirée est que le chiffrement soit une permutation (super) pseudo aléatoire. Une permutation pseudo aléatoire. Une permutation pseudo aléatoire est une fonction pseudo aléatoire où la fonction est une permutation. La notion pseudo de permutation super pseudo-aléatoire est une extension de permutation pseudo aléatoire où l'attaquant peut accéder non seulement à la permutation mais aussi à son inverse. Ces derniers seront, à leur tour, utilisées comme primitives pour d'autres applications (chiffrement de données à travers des modes d'opérations, code d'authentification de message…).

1.4.2.2 Chiffrement asymétrique

Dans le chiffrement asymétrique, les clés de chiffrement et de déchiffrement sont différentes. Une des clés appelée clé secrète, est mémorisée et utilisée par une entité. L'autre clé, appelée clé publique, est distribuée à toutes les autres entités. La clé publique porte bien son nom car sa distribution peut ne pas être confidentielle (c'est l'avantage du chiffrement asymétrique) mais son authentification reste nécessaire. La clé publique est utilisée en général lors du chiffrement et la clé privée pour le déchiffrement. Comme seule l'entité possédant la clé privée peur déchiffrer, la confidentialité de l'échange est assurée.
L'inconvénient est que ces algorithmes utilisent des fonctions mathématiques complexes qui ne peuvent être réalisés sur des circuits intégrés. Le débit de ce type de chiffrement sera donc très faible.
Parmi les algorithmes de chiffrement asymétrique, le plus connu est RSA. La taille de chiffrement asymétrique est souvent comprise entre 512 et 2048 bits.

1.4.3 Condensât

Le condensât est défini comme une fonction mathématique dont le paramètre d'entrée peut être de grande taille et dont le résultat est de taille très réduite. Le calcul du condensât doit être rapide et il doit être impossible de calculer le paramètre d'entrée à partir du résultat. La dernière propriété du condensât est que deux paramètres d'entrées identiques à un bit près doivent fournir deux résultats tout à fait différents.

1.4.4 Signature numérique

La signature numérique permet d'assurer à la fois l'origine et l'intégrité du message. De manière semblable au chiffrement, il existe deux classes de signatures, l'une symétrique (utilisation d'une clé partagée entre la source et la destination d'un message), l'autre asymétrique (utilisation d'une paire de clés par entité).

1.4.4.1 Signature numérique symétrique

La signature symétrique utilise le concept de condensât en combinaison avec une clé partagé : le signataire du document calcule le résultat du condensât sur la concaténation du message à signer et de la clé partagée et il envoie au destinataire le message et le résultat du condensât : le destinataire calcule le condensât sur la concaténation du

message reçu et de la clé partagée et vérifie si le condensât calculé est identique au condensât reçu. Si c'est le cas, cela signifie que le message n'a pas été modifié (service d'intégrité) et que l'origine du message est bien le signataire (car seuls le signataire est le destinataire possèdent le secret partagé).

1.4.4.2 Signataire numérique asymétrique

La signature asymétrique utilise le concept de condensât en combinaison avec la clé privée du signataire. Pour le signataire du document, l'opération est effectuée en trois phases :

- Calcul du résultat du message chiffré à signer
- Chiffrement du résultat du condensât avec sa clé privée
- Envoi du message et du condensât chiffré au destinataire

Trois opérations sont également effectuées par le destinataire :

- Calcul du résultat du condensât du message reçu
- Déchiffrement du condensât reçu avec la clé oblique du signataire

Vérification de l'identité du condensât calculé et du condensât déchiffré. Si cette identité est vérifiée, cela signifie que le message n'a pas été modifié et que l'origine du message est bien le signataire, car seul le signataire possède la clé privée pour signer le condensât.

1.5. La gestion de la sécurité par des moyens en temps réel

1.5.1 Introduction

La sécurité des systèmes informations est généralement bâtie sur 3 briques de bases :

- La protection
- La détection
- La réaction

Jusqu'à maintenant les efforts, en terme de sécurité, étaient mis sur la brique traditionnelle « Protection » (le pare feu, l'antivirus, le système d'authentification).

Dans les applications critiques, le temps est une dimension importante qui met des contraintes en temps réel sur les différentes mesures de la sécurité. Notre objectif sera donc de préciser ses différentes contraintes afin de mettre une politique de la sécurité respectant le temps dans les systèmes temps réel.

1.5.2 Gestion des moyens de protections minimums

On sait que les dispositifs de la sécurité (pare-feu…) sont placés pour protéger les systèmes contre les attaques et les menaces qui peuvent perturber le fonctionnement des applications. Lors du fonctionnement, ces dispositifs peuvent ajouter un délai qui met en danger les applications et les systèmes qui fonctionnent en temps réel. Donc, il ne faut pas les installer ou de les configurer une fois par toutes, une solution consiste par exemple :

- Valider régulièrement la validation de vos pare-feux
  - Pour être efficace, vos pare-feux ont été configurés au moment de leur mise en place en ligne avec vos politiques de sécurité.

  - Pour rester efficace, leur configuration doit être testée périodiquement et les alertes générées contrôlées et corrélées.
  - Pour mieux maîtriser ces changements et affiner la configuration de vos pare-feux dans le but de réduire le temps, vous devez connaître les flux applicatifs pour filtrer et analyser les paquets concernant ces flux seulement.
- Valider la mise à jour corrective régulièrement et tester périodiquement les vulnérabilités de tous les composants logiciels de votre système d'information.
- Veiller à l'activation permanente de vos anti-virus.

1.5.3 Capacité des équipements de sécurité

Pour gagner le temps, il faut que les firewalls et tous les équipements de sécurité soient conçus pour ne pas ralentir le trafic de votre réseau et que leurs capacités leur permettent de traiter les paquets de données le plus rapidement possible.

1.5.4 Filtrage des paquets en temps réel

Le filtrage des paquets est peut être l'aspect le plus important de la sécurité informatique proactive et efficace. Dans les systèmes temps réel, cet aspect nécessite le développement d'un nouveau filtre de paquets qui emploie des structures des données et des algorithmes optimisés pour réaliser une bonne performance pour le filtrage des paquets et la translation d'adresse.

1.6 Faire confiance à un système embarqué

1.6.1 Introduction

Un système embarqué est un système complexe qui intègre du logiciel et du matériel conçus ensemble afin de fournir des fonctionnalités données. Le système matériel et l'application (logiciel) sont intimement liés et immergés dans le matériel et ne sont pas aussi discernables comme dans un environnement de travail classique de type ordinateur de bureau. Un système embarqué est autonome et ne possède pas des entrées/sorties standards tels qu'un clavier ou un écran d'ordinateur.

La sûreté de fonctionnement d'un système logiciel/matériel embarqué et temps réel est la propriété qui permet à ses utilisateurs de placer une confiance justifiée dans le service qu'il délivre et dans le temps de réaction qui doit être prévisible. Mettre en place une équipe pour préparer la procédure de validation des logiciels, proposer des règles rigoureuses pour cette qualification et assurer que les spécifications, les vérifications et les tests des logiciels sont nécessaires pour fonctionner les systèmes embarqués.

L'obtention d'un système Logiciel/Matériel sûr de fonctionnement passe par l'utilisation combinée d'un ensemble de méthodes que l'on peut classer comme suit :

- **prévention des fautes** : comment empêcher, par construction, l'occurrence ou l'introduction des fautes.
- **Tolérance aux fautes** : comment fournir, par redondance, un service conforme à la spécification en dépit des fautes.

- **Elimination des fautes** : comment minimiser par vérification, la présence des fautes.
- **Prévisions des fautes** : comment estimer, par évaluer, la présence, la création, et les conséquences des fautes.
- Prévention des fautes et élimination des fautes peuvent être vues comme constituent l'**évitement des fautes :** comment tendre vers un système exempt de fautes.
- l'**obtention de la sûreté de fonctionnement** : comment procurer au système l'aptitude à délivrer un service conforme à la spécification.
- Élimination des fautes et prévision des fautes peuvent être regroupées dans la **validation de la sûreté de fonctionnement** : comment avoir confiance dans l'aptitude du système à délivrer un service conforme au service spécifié.

1.6.2 Test en ligne intégré

L'objectif visé est de s'affranchir de l'influence des fautes pour ainsi contribuer à l'amélioration de la sécurité et la sûreté de fonctionnement des systèmes conçus et fabriqués.
Différentes méthodes peuvent être conjointement utilisées pour atteindre cet objectif. On distingue :

- La prévention des défaillances qui vise la réduction de la probabilité d'occurrences de fautes : elle implique une analyse des mécanismes des différents modes de défaillance pour en réduire les lois de dégradation qui les gouvernent.
- La tolérance aux fautes qui concerne la réduction de la sensibilité de la fonction implémentée aux fautes.
- La prévision qui implique la surveillance du système. Elle regroupe les opérations de détection et de localisation de fautes afin de décider d'une action compensatrice de sorte que le processus puisse continuer à remplir la mission qui lui a été confiée, malgré la présence des défauts mis en évidence.
  La décision d'intervention ou de reconfiguration est prise lorsqu'il y a évidence expérimentale d'un défaut imminent. **[ES 05]**

1.6.3 Le principe du modèle checking

La vérification par modèle-checking consiste à vérifier les propriétés souhaitées d'un système sur une traduction mathématique de celui ci. Son principe est illustré dans la figure suivante :

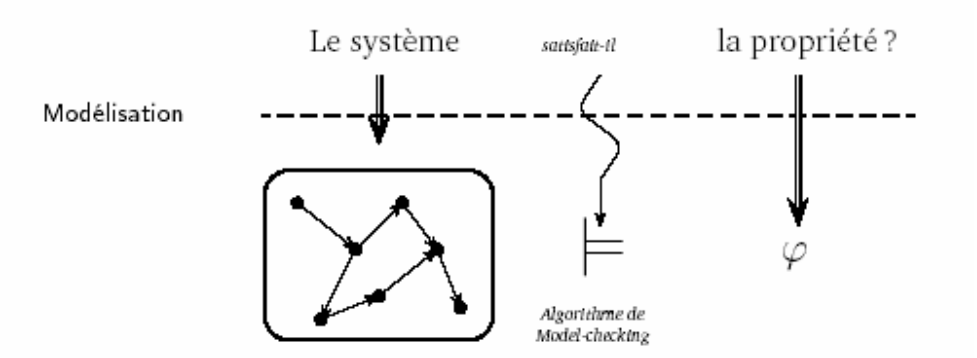

Figure 4 : Principe du model-checking

Afin de vérifier un système, le concepteur doit :

- Réaliser un modèle du système qu'il souhaite vérifier. Cette tâche est délicate puisque, la plupart du temps, le système est décrit en langue naturelle ou sous forme de programme incompatible avec le formalisme des programmes et il est alors nécessaire de traduire, le plus souvent à la main, cette description.
- Spécifier formellement, par exemple dans un langage logique, les propriétés attendues du système. Nous donnons quelques exemples de propriétés :
  - **Le système peut-il se bloquer ?**
  - **Après une panne, le signal d'alarme se déclenche-t-il ?**

.

L'avantage essentiel du modèle-checking sur les méthodes fondées sur le test et la simulation est l'exhaustivité : une propriété valide sur le modèle le sera dans absolument toutes les situations alors qu'un scénario réel de fonctionnement a pu être oublié dans une procédure de test. Par ailleurs, lorsqu'une propriété n'est pas vérifiée dans un modèle ; les outils existants fournissent une trace d'exécution du modèle démontrant que la propriété n'est pas satisfaite. Il est plus facile de déterminer l'origine de l'erreur et de la corriger.

1.7 L'overhead ajouté par les mécanismes de la sécurité

1.7.1 Introduction

La sécurité des réseaux depuis quelques années, a vu son importance s'accroître au point de devenir une priorité. Des outils automatisés de plus en plus complexes, des virus attaquent les réseaux et menacent en permanence l'intégrité des systèmes d'information.
Les mécanismes de la sécurité deviennent fortement consommatrices de temps. Donc, il faut améliorer la gestion de la sécurité pour garantir la qualité de service surtout dans les applications temps réel. Il s'agit en fait de la qualité du transport des informations dans le sens où les données arrivent avec un délai de transmission contrôlé. Par exemple, pour la visioconférence, la qualité de service est nécessaire pour éviter d'avoir des mauvaises transmissions.
Donc en assurant la sécurité, il faut prendre en compte plusieurs paramètres et de les gérer d'une manière qui respecte la QoS. Parmi celles-ci on retrouve :

- Le délai : différents délais peuvent être pris en compte. Dans ce cas, on s'intéresse au délai de transport, c'est-à-dire le temps total passé au niveau des composants actifs du réseau (switch, firewall, etc…) ;
- La latence : la somme de tous les délais, dans une direction, dans une communication en temps réel. Une limite de 75 millisecondes est tolérable. Au-delà, la communication est dégradée ou de faible qualité.
- La variance (jitter) : la variation de la latence. Le maximum toléré est de 20 millisecondes.

1.7.2 IPSec

IPSec est un protocole destiné à fournir différents services de sécurité. Son intérêt principal reste sans contexte son mode dut de tunneling, c'est-à-dire d'encapsulation d'IP qui lui permet entre autres choses de créer des réseaux privés virtuels (ou VPN en anglais).

Il ne faut pas négliger les aspects pratiques tels que la charge processeur due au chiffrement, le débit théorique possible, l'overhead induit et donc le débit effectif…
De plus IPSec n'est pas le seul protocole permettant d'établir des tunnels, il en existe d'autres comme les « point-à-point » tel que L2TP, L2F ou encore PPTP qui peut induire un overhead non négligeable.

1.7.3 Filtre de paquet (FP)

Le filtrage des paquets est peut être l'aspect le plus important de la sécurité informatique proactive et efficace.

Un filtre des paquets contrôle les paquets atteignant l'une de ses interfaces et prend une décision basée sur des règles en fonction duquel il acheminera ou n'acheminera pas ceux via une autre interface jusqu'à destination.

Chaque paquet est comparé à l'ensemble des règles de filtrage. L'ensemble des règles se compose d'une liste associée de règles. Chaque règle contient un ensemble de paramètres définissant l'ensemble de paquets pour lesquels la règle s'applique. Les paramètres peuvent être les suivants : l'adresse source ou l'adresse destination, le protocole, le numéro de port, etc. Pour un paquet correspondant à la règle, on réalise la transmission ou le blocage de ce dernier.

Dans les systèmes temps réel, il faut développer un nouveau filtre des paquets qui emploie des structures des données et des algorithmes optimisés pour réaliser une bonne performance pour le filtrage des paquets.

1.7.4 La sécurité et la qualité de service

La phase de la réalisation de la sécurité dans une application temps réel avec les mécanismes cités nécessite le développement d'une structure matériel et l'intégration du logiciel sur cette structure. Cette phase doit conduire à un système de sécurité conforme

aux objectifs, c'est-à-dire répondant aux spécifications du problème et en particulier garantir un comportement temporel satisfaisant.

Pour garantir les contraintes temporelles avec un délai minimum, il faut non seulement écrire des algorithmes de traitement dont on sait évaluer un temps maximal d'exécution, mais également maîtriser les caractéristiques des dispositifs qui les exécute

Lorsque les traitements sont importants et que les contraintes temporelles sont très strictes, l'exécution de ces traitements nécessite l'utilisation de **machines parallèles**.

Un des buts principaux dans de développement des dispositifs fonctionnant avec des processus parallélisés est de réduire les frais généraux présentés par les mécanismes de la sécurité. Le temps de traitement est un facteur très important et qui doit être minimisé. Beaucoup d'architectures essayent de réduire ces frais généraux en réduisant en minimum le moment réel pour le traitement y compris le délai. Donc, il faut présenter une architecture pour garantir la QoS.

Pour réaliser la sécurité qui garantie la QoS, un traitement parallélisé dans les équipements de la sécurité est l'une des solutions efficaces. La gestion des processus est nécessaire pour offrir un meilleur temps d'exécution. Nous voulons dire aussi qu'un paquet doit être livré de sa source à sa destination dans une date limitée même s'il passe par les dispositifs de la sécurité.

Il est difficile d'offrir une sécurité avec une grande vitesse. En effet, les dispositifs de la sécurité comme le firewall sont forcés d'analyser des milliers des paquets qui passent dans le réseau ce qui augmente le délai. Donc, il faut considérer les aspects qui servent à garantir la QoS.

Les équipements de transport qui assurent la sécurité dans un système temps réel doivent être assez intelligents pour identifier et stopper tous les menaces et les attaques en respectant la qualité de service surtout en termes de délai et de latence. Donc, la politique de la sécurité doit être en relation avec la politique de la QoS.

Chapitre 2
Technologies et services pour la connectivité

2.1 Introduction

Pour se connecter à Internet, il faut une connexion fiable et permanente, permettant l'utilisation des technologies actuelles, comme l'ADSL, une leased line et câble, avec une largeur de bande minimale de 128Kpbs… pour garantir la fiabilité, il est souhaitable de pouvoir utiliser les scénarios de back-up nécessaire. Nous pensons à l'ISDN ou à une autre technologie. Les réseaux physiquement différents (ISDN, leased line, ADSL) doivent pouvoir être connectés, le serveur de communication se chargeant du routing entre ces différents réseaux.

2.2 Les dispositifs de connectivité des réseaux

2.2.1 Introduction

Les dispositifs de connectivité sont des matériels ou des logiciels qui permettent de prolonger, de segmenter ou de raccorder des réseaux (locaux ou étendus). Les dispositifs de connectivité permettent par exemple d'étendre un réseau local.

2.2.2 Les avantages de l'extension d'un réseau local

L'avantage principal, c'est la nécessité. Les besoins ont augmenté, le trafic explose et met en danger la pérennité du réseau existant.

Un réseau local est une structure évolutive, qui change en fonction des besoins et du degré de son utilisation. Tous les réseaux locaux sont amenés à devenir insuffisant à mesure que le trafic devient de plus en plus important.

Chaque topologie réseau a ses propres limites. Parfois, il ne suffit pas de rajouter des postes sur le réseau existant, et le réseau doit évoluer

- Le débit maximum du câble est presque atteint
- Les délais d'attente deviennent insupportables
- Les activités réseau se développent
- L'apparition de nouveaux besoins
- Le partage de nouvelles ressources
- Le travail en réseau
- La messagerie Intranet
- Les applications réseaux
- Le GROUPWARE
- Les bases de données
- L'accès à Internet
- Le nombre des collaborateurs augmente
- Le nombre de postes augmente
- Les serveurs
- Les stations
- Les imprimantes
- Le nombre de sites augmente

2.2.2 Les différents dispositifs de la connectivité

Les différents dispositifs de connectivité sont les suivants :

- **Les répéteurs**
- **Les ponts**
- **Les routeurs**
- **Les ponts-routeurs**
- **Les passerelles**

Les répéteurs : Les répéteurs régénèrent le signal électrique qui se dégrade à mesure qu'il parcourt le câble (c'est l'affaiblissement ou l'atténuation du signal). Selon le type de câble, la distance maximum est différente. Le répéteur permet au signal de parcourir une distance plus grande (dans les deux sens). Ainsi, le répéteur permet d'étendre un réseau au-delà de ses limites, il permet d'accroître la longueur du câble et le nombre de nœuds.

Certains répéteurs peuvent passer les paquets d'un support à un autre, comme par exemple d'un brin de coaxial fin vers de la fibre optique. Le répéteur peut être multi câble.

Le répéteur agit au niveau de la couche physique du modèle OSI, c'est à dire qu'il réceptionne chaque paquet qui lui arrive, le régénère et le réexpédie de l'autre coté du câble. Les paquets ne sont pas filtrés, ni routés, ni traduit dans un autre protocole. De part et d'autre du répéteur, la méthode d'accès au réseau et le protocole doivent être strictement les mêmes. Un répéteur ne segmente pas un réseau et ne diminue jamais le trafic. Au contraire, les problèmes de saturation du trafic, les tempêtes de diffusions générales (Broadcast Storm), se communiquent sur tout le réseau…

Un répéteur se situe toujours entre deux segments et seulement deux. Toutefois, quand le répéteur dispose de plusieurs ports, c'est un répéteur multi ports et il fait office de concentrateur.

Il ne faut pas utiliser de répéteur dans certaines conditions :

- Le trafic réseau est très important, le problème persistera…
- Les segments du réseau utilisent des méthodes d'accès différentes…
- Les protocoles réseau sont différents
- Les paquets doivent être filtrés et/ou routés…

Les ponts : Les ponts (Bridges) permettent de prolonger et de segmenter un réseau, d'augmenter le nombre de postes (le nombre de nœuds), de réduire les goulets d'étranglement, de router les paquets, de relier des supports différents. Les ponts permettent de relier ou de segmenter deux réseaux qui utilisent le même protocole. La segmentation permet d'isoler le trafic sur chaque segment, et parfois cela facilite la localisation d'un problème. Les ponts sont souvent utilisés pour des protocoles réseaux qui ne peuvent pas être routés.

Les ponts agissent au niveau de la couche liaison du modèle OSI (les ponts n'accèdent pas aux couches supérieures, ils ne font pas la différence entre des protocoles différents,

et donc, tous les protocoles traversent les ponts). La couche LIAISON peut être divisée en deux sous-couches, la sous-couche LLC et la sous-couche MAC. Les ponts travaillent au niveau de la sous-couche MAC qui reconnaît les adresses MAC des cartes réseaux (l'adresse Mac de chaque carte réseau, de chaque nœud du réseau, est une adresse unique dans le monde entier…). Les ponts sont parfois appelés des « ponts de couche MAC ».

Les ponts possèdent une mémoire dans la quelle ils stockent les informations de la table de routage. Au démarrage, la table de routage d'un pont est vide. Les ponts construisent une table de routage en examinant les adresses sources des paquets qui lui parviennent. Ainsi, au fur et à mesure du trafic, les ponts accumulent les informations sur les stations émettrices :

- L'adresse MAC de chaque nœud
- Le segment auquel elles appartiennent, c'est à dire le port du pont auquel est relié le câble du segment en question

Quand un paquet arrive sur un pont, celui-ci vérifie si l'adresse source de l'expéditeur figure dans sa table de routage, si ce n'est pas le cas, le pont l'y inscrit. Ensuite, le pont vérifie si l'adresse cible du destinataire figure dans sa table de routage, si c'est le cas, alors il achemine le paquet vers le segment (le port) auquel appartient le destinataire (sauf, si c'est le même segment que l'expéditeur), si ce n'est pas le cas, le pont transfert le paquet vers tous les autres segments, vers tous ses ports (le pont devra attendre que le destinataire émette à son tour…).

Les routeurs : Les routeurs (Routers, Gateway) permettent de prolonger et de segmenter un réseau, d'augmenter le nombre de postes (le nombre de nœuds), de réduire les goulets d'étranglement, de router le paquets, de relier des supports différents, de relier des segments qui utilisent des méthodes d'accès au réseau différentes, ou des protocoles routables différents.

Les routeurs sont souvent utilisés pour interconnecter plusieurs réseaux entre eux ; les interconnexions des réseaux proposent plusieurs chemins possibles pour que deux stations communiquent. Les routeurs permettent de « router » les paquets d'un réseau vers un autre, tout en considérant que le chemin le plus court n'est pas forcément le plus rapide.

Les routeurs travaillent au niveau de la couche RESEAU du modèle OSI. Lorsqu'un paquet est transmis à un autre routeur, les adresses réseaux de la source et de la cible sont recréées, et éventuellement traduites, c'est ce qui permet à un routeur de transmettre les paquets d'un segment Ethernet vers un segment Token Ring par exemple.
La table de routage d'un routeur conserve les informations de routage qui le concerne directement, c'est à dire les informations des matériels adjacents (ordinateurs ou routeurs) qui sont installés sur les segments auxquels il est lui-même raccordé. Un routeur ne communique pas avec les ordinateurs qui sont situés au-delà d'un autre routeur. Les routeurs partagent leurs informations de routage avec les autres routeurs du réseau. Les informations de routage permettent aux routeurs de déterminer la route optimale :

- **Les adresses réseaux** des ordinateurs placés sur les segments adjacents

- **Les masques de sous réseaux des autres segments**, les plages d'adresse qui sont gérées par les routeurs adjacents
- **Les chemins possibles** pour acheminer un paquet vers un des routeurs du réseau
- **Le nombre de sauts de routeurs** pour arriver à tel ou tel segment

Les routeurs ne laissent pas passer les messages de diffusion générale (Broadcast), ils ne laissent passer que les protocoles routables. Les routeurs ne laissent passer que les paquets dont les adresses sont connues. Les routeurs peuvent servir de barrière de sécurité entre les segments d'un réseau. Les routeurs permettent de prévenir les saturations de diffusion.

Les protocoles routables **:**

- DECnet
- IP
- IPX
- OSI
- DDP (Apple Talk)

Les protocoles non routables :

- NetBEUI de MICROSOFT

Les ponts-routeurs : Les ponts-routeurs (Brouter en anglais) sont une combinaison des fonctionnalités d'un pont et d'un routeur. Les ponts-routeurs routent les protocoles routables et font un pont en or pour les protocoles non routables.

Les ponts-routeurs facilitent la gestion du trafic d'un réseau quand celui-ci est composé à la fois de ponts et de routeurs.

Les passerelles : Les passerelles (Gateway) permettent la communication entre réseaux d'architectures différentes. Les passerelles interconnectent les réseaux hétérogènes multi fournisseurs. Les passerelles sont souvent utilisées pour relier un réseau d'ordinateurs personnels à un réseau de mini ordinateurs ou à un réseau de grands systèmes (ce qui permet aux utilisateurs d'accéder aux ressources d'un grand système par exemple).

Une passerelle est toujours spécifique aux deux architectures qu'elle permet de réunir. Une passerelle peut agir **sur toutes les couches du modèle OSI**.

La passerelle reformate les paquets, les données entrantes sont « dépouillées » de leur pile de protocole (désencapsulées) et « rhabillées » (réencapsulées) avec l'autre pile de protocole. **La passerelle remplace une pile de protocole par une autre**. Les passerelles sont des traducteurs de protocoles. Les passerelles sont souvent utilisées pour les réseaux qui ne disposent pas de TCP/IP (par exemple, les réseaux NetWare qui fonctionnent sous SPX/IPX et qui veulent avoir un accès à Internet).

Les caractéristiques des dispositifs de connectivité					
	Répéteur	**Pont**	**Routeur**	**Pont-routeur**	**Passerelles**
Régénération	OUI	OUI	OUI	OUI	OUI
Prolonger	OUI	OUI	OUI	OUI	OUI
Les nœuds	OUI	OUI	OUI	OUI	OUI
Les supports	Multi câbles	Multi câbles	Multi câbles	Multi câbles	Multi câbles
Multi ports	Concentrateur	OUI	OUI	OUI	OUI
Broadcast	OUI	OUI	NON	OUI et NON	NON
Segmenter	NON	OUI	OUI	OUI	OUI
Filtrer	NON	OUI	OUI	OUI	OUI
Router	NON	NON	OUI	NON et OUI	OUI
Traduire	NON	NON	OUI	OUI	OUI
Couche OSI	1. Physique	2. LIAISON	3. RESEAU	2. et 3.	1. à 7.
Chemins	Un seul	Un seul	Plusieurs	Plusieurs	Plusieurs
Adresses		@ MAC	@ réseau		
Méthode d'accès	La même	La même	CSMA/CD et le jeton		Plusieurs
Protocoles	Un seul	Un seul	Routables		Plusieurs
Architecture réseaux	La même	La même	Ethernet et Token Ring		Spécifiques
Topologie	Bus	Dorsale	Maillage	Maillage	Maillage
Utilisation	Rallonger	Regrouper	Optimiser	Simplifier	Traduire

2.3 La mise en place d'un serveur proxy

2.3.1 Introduction

Un serveur proxy est à l'origine d'une machine faisant fonction d'intermédiaire entre les ordinateurs d'un réseau local et Internet.

La plupart du temps le serveur proxy est utilisé pour le web, il s'agit donc d'un proxy HTTP, toutefois il peut exister des serveurs proxy pour chaque protocole applicatif (FTP, ...).

2.3.2 Le principe de fonctionnement d'un proxy

Le principe de fonctionnement basique d'un serveur proxy est assez simple, il s'agit d'un serveur «mandaté» par une application pour effectuer une requête sur Internet à sa place. Ainsi, lorsqu'un utilisateur se connecte à Internet à l'aide d'une application cliente configurée pour utiliser un serveur proxy, celle-ci va se connecter en premier lieu au serveur proxy et lui donner sa requête. Le serveur proxy va alors se connecter au serveur que l'application cliente cherche à joindre et lui transmettre la requête. Le serveur va ensuite donner sa réponse au proxy, qui va à son la transmettre tour à l'application cliente.

2.3.3 Les fonctionnalités d'un serveur proxy

Désormais, avec l'utilisation de TCP/IP au sein des réseaux locaux, le rôle de relais du serveur proxy est directement assuré par les passerelles et les routeurs. Pour autant, les serveurs proxy sont toujours d'actualité grâce à certaines autres fonctionnalités.

2.3.3.1 Le filtrage

D'autre part, grâce à l'utilisation d'un proxy on assure un suivi des connexions (en anglais tracking) via la constitution de fourneaux d'activité (logs) on enregistre systématiquement les requêtes des utilisateurs lors de leurs demandes de connexion à Internet.

Il est ainsi possible de filtrer les connexions à Internet en analysant d'une part les requêtes des clients, d'autre part les réponses des serveurs. Lorsque le filtrage est réalisé en comparant la requête du client à une liste de requête réalisé, on parle d'une liste blanche, lorsqu'il s'agit d'une liste des sites interdits on parle de liste noire. Enfin l'analyse des réponses des serveurs conformément à une liste de critères est appelé filtrage de contenu.

2.3.3.2 L'authentification

Dans la mesure où le proxy est l'intermédiaire indispensable des utilisateurs du réseau interne pour accéder à des ressources externes, il est parfois possible de l'utiliser pour authentifier les utilisateurs, c'est à dire de leur demander de s'identifier à l'aide d'un nom d'utilisateur et d'un mot de passe par exemple. Il est ainsi aisé de donner l'accès aux ressources externes aux seules personnes autorisées à le faire et de pouvoir enregistré dans les fichiers journaux des accès identifiés.

2.5 Mettre en place des caches web distribués

Les caches web ont été créés pour remédier en partie au problème de surcharge des serveurs web et de congestion des réseaux Internet. Ces caches stockent les documents demandés récemment par les utilisateurs afin de réduire le chemin à parcourir pour récupérer à nouveau ces documents lors d'une prochaine demande. Leur utilisation permet donc de réduire le trafic à travers l'Internet et ainsi d'améliorer le temps de réponse au client. Mais ces caches n'ont pas encore atteint un niveau de performance satisfaisant, et connaissent quelques défauts d'organisation. Un même document est

dupliqué sur plusieurs sites, ce qui pose inévitablement le problème de la cohérence des différentes versions de ce document.

Pour améliorer leur efficacité, l'Institut Eurécom a étudié l'organisation des caches reliés par des liens à très haut débit, et a développé un système de caches physiquement distribués sur plusieurs sites mais apparaissant logiquement comme un seul grand cache. Avec les caches distribués, une seule copie d'un document est présente dans l'ensemble de tous les caches, ce qui permet d'assurer la cohérence des informations présentes dans le réseau, d'utiliser l'espace disque des caches d'une manière plus efficace et d'assurer des temps de réponse extrêmement faibles.

2.6 Les protocoles TCP/IP et Internet

2.6.1 TCP/IP

2.6.1.1 Définition

Le nom TCP/IP se réfère à un ensemble de protocoles de communications de données. Cet ensemble tire son nom des deux protocoles les plus importants : le Transmission Control Protocol et le Internet Protocol.

Le protocole TCP/IP devient le fondement d'Internet, le langage qui permet aux machines du monde entier de communiquer entre elles. Internet devient le terme officiel pour désigner non pas un réseau mais une collection de tous ces réseaux utilisant le protocole IP.

Le succès de TCP/IP s'est vite étendu au reste du monde à cause des facteurs suivants:

- TCP/IP est l'outil idéal pour interconnecter du matériel hétéroclite
- C'est un standard ouvert
- Il est utilisable librement
- il est indispensable des couches physiques de hardware. Il tourne à l'heure actuelle sur des supports Ethernet, Token Ring, du X25 et virtuellement tout type de media physique
- Il dispose d'un schéma d'adressage unique identifiant chaque périphérique de manière univoque.

2.6.1.2 Adressage IP

Chaque interface Internet est identifiable par une adresse Internet codée sur 32 bits. Une adresse Internet Protocole est constituée de quatre nombres de 0 à 255 et séparée par un point comme ceci : 194.78.19.32. Cela donne également 32 bits ou quatre octets qu'on représente quelquefois de manière hexadécimale comme suit 0x9A0B3CFF.

Binary Format	Dotted Decimal Notation
11000000 10101000 00000011 00011000	192.168.3.24

Chaque machine reliée à Internet dispose d'une telle adresse unique. Dans cette unique Internet, il faut encore distinguer deux parties, l'identifiant de réseau et le numéro d'hôte. Une adresse IP est composée de deux parties:

- Le numéro du réseau
- le numéro de machine sur ce réseau

2.6.1.3 IPv6

La répartition d'adresse réseau en classe commence déjà à poser de sérieux problèmes. Avec la numérotation actuelle baptisée IPv4, il n'est possible d'adresser que 2 100 000 réseaux ou un total de 3 720 000 000.

Un deuxième problème est la saturation des tables de routage qui croissent plus vite que la technologie des mémoires propres à les contenir.

Ce sera la norme IPv6 avec des adresses IP codées sur 128 bits qui sera retenue pour pallier ces deux problèmes. Fin 1994, l'Internet Engineering Task Force s'est mis d'accord sur la norme IP Next Generation alias IPv6. IPv6 supportera jusqu'à 1 milliard de réseaux. IPv6 apporte plusieurs améliorations à la norme IPv4.

- IPv6 est prévu pour coexister avec IPv4
- Un réseau IPv6 peut supporter un nombre illimité d'hôtes.
- Une adresse IPv6 peut contenir une adresse IPv4.
- L'adresse est représenté comme huit valeurs hexadécimales de 16 bits séparés par des doubles points du type 5D54:352A:1235:B357:8283:2CDE:C00D:FCB2. Des groupes de zéros contigus peuvent être représentés par un double "::" comme suit: CF76:0:0:0:0:0:0:27 devenant CF76::27. Une adresse IPv4 de type d.d.d.d devient automatiquement x:x:x:x:d.d.d.d
- 0:0:0:0:0:0:0:0 devient une "unspecified address"
- L'adresse loopback n'est plus 127.0.0.1 mais 0:0:0:0:0:0:0:1
- Le header a été simplifié pour réduire la bande passante requise par le protocole.

La grande nouveauté est l'intégration de manière native des protocoles IPsec (IP security) dans IPv6 et non plus sur certaines configurations seulement comme c'était le cas avec IPv4. Cela représente une véritable avancée, en effet, lorsqu'IPv6 sera en place, tout un chacun pourra disposer de fonctions de sécurité grâce à IPsec. La sécurisation de VPNs (Virtual Private Network) lors de l'interconnexion de sites en est un exemple intéressant. Un autre avantage de ce choix est la compatibilité avec les applications tournant sous IPv4 qui est toujours largement utilisé et qui offre également l'accès à IPsec mais de manière optionnelle.

Chapitre 3
Connectivité dans les infrastructures critiques

3.1 Introduction

On trouve aujourd'hui des gros systèmes critiques informatique dans les domaines de l'aéronautique, aérospatiale, du contrôle du procédé industrielle, de supervision de centrales nucléaire, voire de gestion de salles de marché ou de télémédecine. Pour ces exemples, une des caractéristiques est que le système informatique se voit confier d'une grande responsabilité en termes de vie humaine, de conséquence sur l'environnement. On parle alors des systèmes critiques, qui sont alors soumis à des contraintes de fiabilité et de sécurité.

La prise de contrôle d'infrastructures critiques semble être un des objectifs du cyberterrorisme, la preuve en est la recrudescence de scans (tests de systèmes informatiques pour découvrir leurs vulnérabilités afin de pouvoir les pénétrer ultérieurement) dirigés sur des ordinateurs d'organisations gérant des infrastructures critiques (eau, électricité, transport).

Les réseaux convergent aujourd'hui vers une architecture commune exploitant le protocole Internet. Ce protocole conçu pour le transport asynchrone des données informatiques n'a cependant pas été prévu pour des applications présentant des contraintes des contraintes temps réel. Les défauts rencontrés sur les réseaux IP (délai, gigue, perte des paquets et variation de la bande passante) ne pourront être surmontés sans une rénovation profonde de l'architecture et son adaptation aux nouvelles applications téléphonie, audio, vidéo à la demande
Le problème qui se pose : comment faire la connectivité des infrastructures critiques pour assurer un bon fonctionnement en respectant les contraintes du temps et de la qualité de service et en augmentant la sécurité pour lutter contres les attaques et les menaces ?

3.2 Un débit élevé et le technologie multiplexage en longueur d'onde

Pour réaliser une performance, il faut relier des routeurs nouvelles générations ou gigarouteurs, par des canaux de transmission optiques haut débit en exploitant la technologie dite multiplexage en longueur d'onde, qui permet d'utiliser plusieurs canaux, ou longueur d'onde en parallèle dans la fibre optique. Avec cette architecture, on peut atteindre un débit potentiel de 40 Gigabits par seconde en cœur du réseau. **[FT 01]**

Grâce à cette capacité en débit exceptionnel, le réseau permet de :

- Favoriser l'enseignement à distance
- Développer les techniques nécessaires à l'apprentissage du geste médical à distance
- Atteindre les potentialités attendues du calcul informatique distribué.
- Permettre la sauvegarde en ligne de très grosses bases de données.

Tout en assurant une excellente qualité de service et en qualifiant le comportement du réseau à des applications très haut débit.

Pour atteindre ce débit, il faut utiliser la technologie dite multiplexage de longueur d'onde (utilisée par France Télécom avec le réseau VTHD). Celle-ci permet d'utiliser

simultanément plusieurs longueurs d'onde pour faire circuler des informations en parallèle dans une même fibre optique. Un des attraits majeurs de cette technologie est de permettre l'accroissement progressif des capacités de transmission d'une fibre par ajout progressif de longueurs d'onde supplémentaires. Mais le débit de transfert des informations ne dépend pas seulement de la fibre optique mais aussi des routeurs et des cartes interfaces entre fibres et routeurs (pour le réseau VTHD, France Télécom n'a donc pas eu besoin d'installer de nouvelles fibres optiques : elle a simplement installé sur son réseau un matériel de dernier génération, des giga routeurs capables, via un laser, d'expédier sur une fibre une quantité colossale d'information , de l'ordre de 2,5 Gbits/s par longueur d'onde).

Avec cette technologie, on peut élaborer les garanties de qualité de service pour répondre aux attentes en termes de **sécurité** et de **fiabilité**.

3.3 ADSL

3.3.1 Introduction

On va présenter de manière synthétique les équipements et services à mettre en œuvre afin d'assurer la sécurité et la confidentialité des données de l'entreprise qui souhaite connecter au réseau local à Internet via une ligne ADSL.

L'ADSL représente actuellement la meilleur méthode d'accès à Internet pour une entreprise désirant fournir un accès relativement haut débit à ses utilisateurs. L'ADSL se positionne comme la technologie idéale pour connecter un réseau local à Internet.

L'interconnexion d'un réseau local avec un réseau public doit s'effectuer dans le respect de certaines règles, notamment au niveau de la sécurité et de la confidentialité.

3.3.2 La technologie ADSL

Le principal intérêt des technologies ADSL, est de réutiliser les câblages cuivre existants. Autant dire tout de site que la totalité des lignes téléphoniques déployées en France par l'opérateur nationale est éligible. De plus ces lignes téléphoniques peuvent être utilisées simultanément pour le transport de la voie et pour le transport des données.

En effet, pour être transportée sur une ligne téléphonique la voie n'utilise qu'une bande passante de quelques dizaines de kilohertz correspond en fait à la bande passante de la voie humaine, ce qui laisse une grande partie de la bande passante du câble inemployé. Cette bande passante inemployée que les technologies xDSL en général et l'ADSL en particulier utilisent.

Ainsi une ligne téléphonique normale peut-elle être transformée ligne en ADSL par la simple adjonction d'un filtre séparateur qui se charge de transporter la voie humaine vers le périphérique habituel, et le reste des données vers le périphérique jouant le rôle de modem ADSL.

3.3.3 L'offre ADSL

L'offre ASDSL de l'opérateur national comporte plusieurs niveaux de performance. Deux solutions proposées correspondant à des besoins en bande passante différents. Ces offres s'appellent commercialement NETISSIMO I et NETISSIMO II.

3.3.3.1 L'offre NETISSIMO I

Ciblé à l'origine pour les particuliers, cette offre permet un débit de 500 Kbps en voie descendante (c'est-à-dire lorsque vous consultez des documents sur Internet ou que vous envoyez des emails) et de 128 Kbps en voie ascendante (c'est-à-dire lorsque vous envoyez des informations sur Internet ou que vous envoyer un email). Cette offre ne permet pas d'interconnecter un réseau local, mais une poste seul.

Dans cette offre le modem est connecté directement entre le filtre ADSL et l'ordinateur se connectant à l'Internet.

3.3.3.2 L'offre NETISSIMO II

Taillé pour interconnecter un réseau local, l'offre NETISSIMO II offre un débit de 1000 Kbps en voie descendante (c'est-à-dire lorsque vous consultez des documents sur Internet ou que vous envoyez des emails) et de 256 Kbps en voie ascendante (c'est-à-dire lorsque vous envoyez des informations sur Internet ou que vous envoyer un email).

Dans cette offre, la seule différence avec NETISSIMO II est qu'au lieu de connecter un ordinateur derrière le modem ADSL, on connecte un dispositif réseau appelé routeur qui est lui-même connecté au réseau local. Il est également fortement recommandé d'ajouter tous les dispositifs nécessaires afin d'assurer la sécurité et la confidentialité des données du réseau local. Ces dispositifs sont généralement concentrés au goulot d'étranglement que constitue l'accès vers Internet. On les appelle des FireWalls.

3.3.3.3 Les fournisseurs d'accès Internet proposant l'ADSL

Après avoir fait installé la ligne ADSL avec son filtre, son modem et éventuellement son routeur et son firewall, il faut encore avant de pouvoir utiliser sa ligne ouvrir un abonnement auprès d'un fournisseur d'accès à Internet (FAI).

Les abonnements ont un coût différent en fonction de si l'on a opté pour une ligne NETISSIMO I ou pour une ligne NETISSIMO II. Les autres éléments pouvant influer sur le coût de l'abonnement au FAI sont principalement la demande d'une adresse IP fixe plutôt qu'une adresse IP dynamique attribué par votre FAI pour une durée finie, et qui peut changer une fois ce délai dépassé. L'intérêt d'obtenir une adresse IP fixe auprès de votre FAI tient surtout si vous souhaitez utiliser votre ligne Internet pour les besoins suivants :

- Mettre à disposition sur le réseau Internet un serveur fournissant de l'information (serveur web, serveur de messagerie, ect.) se trouvant dans vos locaux.
- Permettre à des personnes distantes d'accéder à votre système d'une manière sécurisée, authentifiée, et cryptée par le biais du mécanisme appelé VPN. (virtual private network), réseau privé virtuelle en français. **[AD 01]**

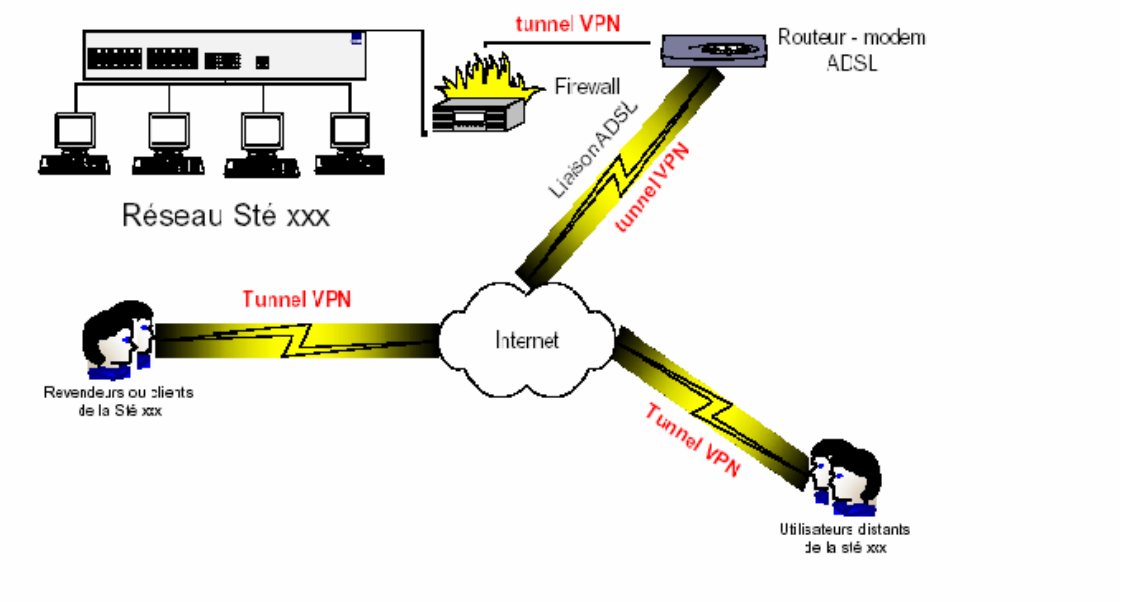

Figure 5 : Accès au réseau local par un tunnel VPN

3.3.4 Conclusion

Pour s'interconnecter de manière permanent et à haut débit au réseau Internet, les solutions ADSL restent le plus fiables et d'un moindre coût.

3.4 VPN

3.4.1 Introduction

Le but d'un réseau virtuel (VPN) est de «fournir aux utilisateurs et administrateurs du système d'administration des conditions d'exploitation, d'utilisation et de sécurité à travers un système public identique à celle disponible sur un réseau privée. En d'autres termes, on veut regrouper des réseaux privés, séparé par un réseau public (Internet) en donnant l'illusion pour l'utilisateur qu'ils ne sont pas séparés, et tout en gardant l'aspect sécurisé qui était assuré par la coupure logique au réseau Internet.

Un VPN est une technologie réseau qui crée un tunnel chiffré entre une machine sur Internet dotée d'une adresse IP quelconque et une passerelle d'accès d'un réseau privé. La machine distante se voie dotée lors de l'établissement du tunnel d'une adresse supplémentaire appartenant au réseau privé qu'elle cherche à atteindre.

3.4.2 Tunnel

Le tunnel est une composante indispensable des VPN ; la problématique est la suivante : on va relier deux réseaux privés qui sont séparés par un réseau public (Internet), de façon transparente pour l'utilisateur. L'utilisateur utilisera ainsi des interfaces réseaux virtuels et aura l'illusion de discuter directement avec le réseau qui se trouve, en fait de l'autre côté d'Internet. La solution technique utilisée, dans la plupart des cas, pour mettre en oeuvre des tunnels est l'encapsulation de protocoles.

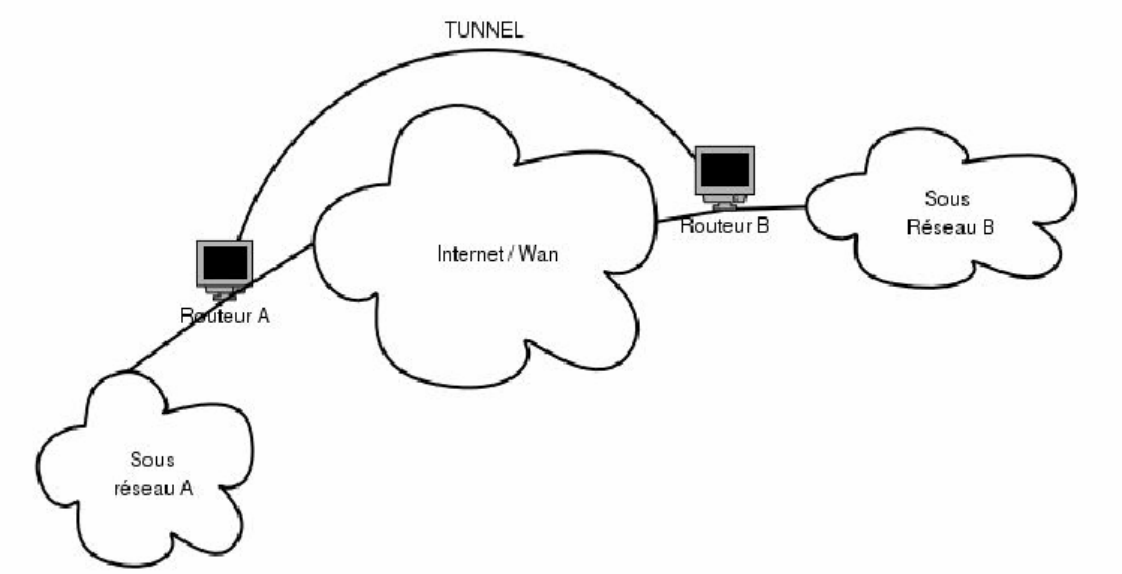

Figure 6 : Tunnel interconnectant le sous réseau A au sous réseau B

3.5 Assurer une qualité de service à la demande

Les réseaux convergent aujourd'hui vers une architecture commune exploitant le protocole Internet. Ce protocole conçu pour le transport asynchrone de données informatiques n'a cependant pas été prévu pour des applications présentant des contraintes temps réel. Les défauts rencontrés sur les réseaux IP (délai, gigue, perte des paquets et variation de la bande passante) ne pourrant pas être surmontés sans une rénovation profonde de l'architecture et son adaptation aux nouvelles applications téléphonie, audio, vidéo à la demande

Avec l'explosion du trafic Internet et son évolution vers un réseau commercial multiservice, les utilisateurs d'Internet sont devenus des clients avec des exigences fortes en matière de qualité de service. Or l'architecture actuelle du réseau est limitée dans la mesure où tous les paquets d'information sont traités de la même manière. Un réseau ayant un débit élevé permet d'assurer une excellente qualité de service avec des modèles de service adaptés aux besoins de nouvelles applications.

3.5.1 Le réseau multimédia

L'Internet multimédia qui intégrera voix, données et images dans une même architecture doit évoluer pour être capable de répondre aux nouveaux défis et de garder en même temps ses principes fondamentaux à savoir la simplicité, la robustesse et l'universalité.

3.5.1.1 Les conditions de la qualité de service

- L'augmentation de la QoS : Pour résoudre le problème de la qualité de service de l'Internet, la recette pourrait être d'abord d'augmenter la bande passante pour améliorer les performances.
- La puissance du processeur : Pour commuter des paquets à des vitesses se chiffrant en térabits par seconde ou mettre en œuvre des algorithmes de routage et

de gestion de priorité sophistiquée, il faut disposer des puissances de calcul à la mesure des objectifs et des ambitions. La puissance de traitement semble donc comme la bande passante, quasi infini.

- L'adaptation en temps réel : Une large part du délai et de la gigue lors de transmission de voix sur IP est due à l'inadéquation des terminaux aux applications audio temps réel. L'électronique conversion analogue digitale (A/D), les systèmes d'exploitation, les cartes son, ont été conçus pour des applications traditionnelles et non pas pour le temps réel. Les interfaces réseaux et les modems sont étudiés pour des paquets de données de grande taille et non pas pour des petits paquets de voix. De nouvelles technologies d'accès large bande réseaux par câble (xDSL) ou sans fils doivent améliorer ces conditions.
- Les stratégies de bout en bout : Le réseau Internet est « stupide » et se contente de router les paquets individuellement sans notion de contexte ou de QoS alors que les terminaux sont intelligents et corrigent les défauts de transmission dans le cas de service à débit constant (noté par CBR, Constant Bit Rate).
- Les stratégies réseau : Les premières tentatives de modification du fonctionnement ont d'imiter les mécanismes de QoS implantés déjà dans les réseaux ATM. Le groupe qui a travaillé entre 94 et 97 a produit le protocole de réservation de ressources RSVP. Ce protocole est apparu très vite non efficace. D'autres stratégies plus simples fondées sur des indices de priorité indiquant la classe de service du paquet représentent aujourd'hui l'avenir du réseau. Les recherches dans le domaine de la QoS sont destinées aux VPN qui ne remplaceront vraiment les liaisons spécialisées que lorsqu'ils seront capables de garantir des spécifications strictes de QoS.
- L'introduction de la complexité dans le réseau : L'implémentation de mécanismes de QoS dans le réseau aura des répercutions importantes sur l'évolution des équipements. La mise à jour ultérieure ainsi que les services futurs devront être compatibles avec les mécanismes implantés déjà dans les machines. L'introduction de la complexité doit être réversible.

3.5.2 Les solutions de la QoS

3.5.2.1 Les routeurs de périphérie

Le routeur moyen perd une partie de ses prérogatives au profit de nouveaux équipements d'extrémité, le routeur de périphérie qui sert de port d'entrée au sous réseau. C'est ce routeur qui calcule le chemin de routage qui affecte un indice de priorité au paquet et qui effectue éventuellement un contrôle d'accès.

3.5.2.2 Les flux différenciés de paquets

L'introduction de mécanismes de ressources des classes de services (notées CoS) représente une évolution certaine vers d'avantage d'intelligence. Les routeurs de l'Internet classique « best effort » traitent tous les paquets de la même manière. Les routeurs de l'Internet multimédia savent trier les paquets en fonction de leur indice CoS et leur apporter un traitement différencié.

Les paquets subissent des contraintes de temps réel et seront servis en priorité et orientés vers des files d'attente garantissant la bande passante nécessaire. De même, en cas de

congestion seront sacrifiés en premier les paquets d'application peu sensibles aux pertes. Ce que le routeur perd d'un côté (le calcul du routage), il le gagne de l'autre en se dotant de capacité de discernement et de traitement différencié des paquets.

3.5.2.3 La notification explicite

Une évolution prochaine pourrait introduire un mécanisme de notification explicite par laquelle un noeud informerait la source d'un état de congestion naissante, du montant de ressources disponibles à un instant donné ou de sa capacité à accepter et à traiter les paquets de priorité élevée.

3.6 Internet par satellite

3.6.1 Introduction

Les télécommunications par satellites permettent de repousser les limites de la transmission de données par voie terrestre. De plus, la transmission de données s'effectue par liaison directe assurant ainsi un service homogène et ceci quelque soit la position de l'utilisateur. Télévision, radio, Internet et multimédia, communications d'entreprise et services de communication mobiles, le satellite peut être utilisé pour un large éventail d'application, dont la coexistence peur être particulièrement avantageuse. En effet, TV, radio, Internet et multimédia peuvent être combinés en une seule offre, ce qui permet de réduire les coûts des équipements et des services. A ces avantages, il peut être rajouté d'autres atouts comme une qualité de service exceptionnelle, une rentabilité appréciable ou une large capacité de transmission.

Les informations entre la terre et le satellite sont transmises par ondes électromagnétiques. Au fur et à mesure, ces ondes se propagent le long du trajet radioélectrique (Terre/satellite) et subissent un affaiblissement (pour un trajet de 36 000 kilomètres correspond à peu près à la distance entre un point de la terre et un satellite géostationnaire, l'intensité d'une onde radio de 100 W à l'émission n'est plus qu'un 1/ (2.10^{14}) Watt par mètre carré à la réception). La principale fonction des antennes utilisées dans les systèmes de télécommunications par satellite est de compenser la perte de puissance du signal qui se produit lors de son émission du sol vers l'espace (et vice versa). Les antennes spatiales installées au bord des satellites géostationnaires peuvent émettre, recevoir, ou les deux à la fois. La conception d'une antenne dépend des exigences de la mission, lesquelles deviennent de plus en plus complexes. Elles sont caractérisées par le nombre de zones de services, la bande passante, la réutilisation des fréquences, la connectivité des canaux entre les zones de service, la flexibilité et la tenue en puissance. Pour répondre à de nombreuses applications, le satellite embarque une multitude d'aériens comme le montre la Figure ci dessous**. [RG 03]**

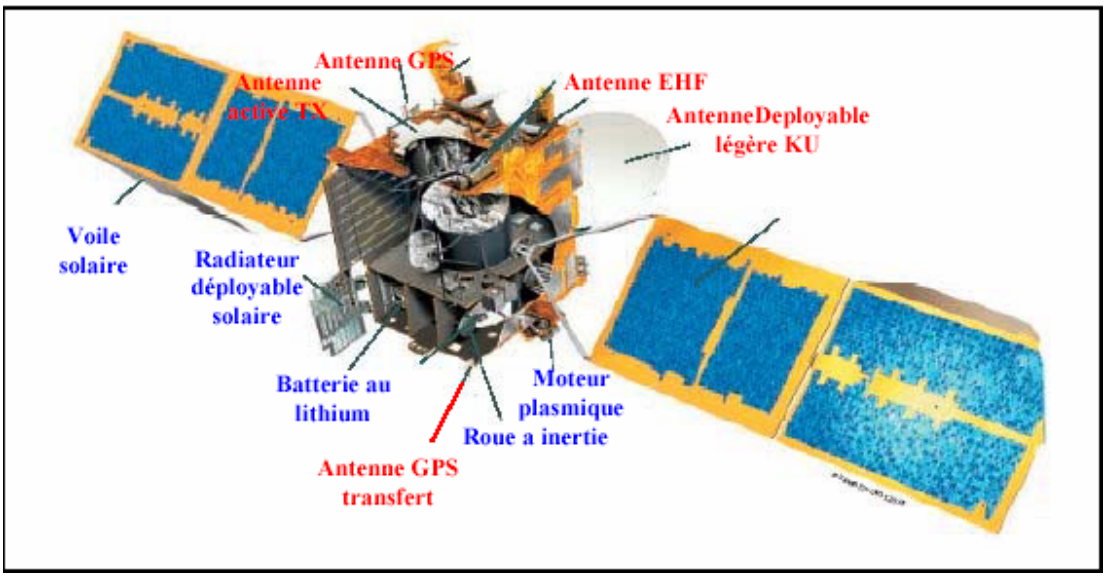

Figure 7 : Représentation des antennes embarquées sur un satellite

L'Internet par satellite devient plus en plus un besoin et même une nécessité avec la démocratisation des WebTV, des «Streaming» de plus en plus gourmand en bande passante et des sites web toujours plus riche en contenu multimédia.

3.6.2 L'équipement nécessaire

Bien que des expérimentations soient actuellement menées sur la transmission de données bidirectionnelle entre un PC et un satellite, le matériel le plus fréquemment utilisé dans le cadre d'une utilisation résidentielle reste la carte de réception DVB-MPEG-2 et le modem téléphonique pour la remontée des requêtes vers les serveurs du fournisseur d'accès. Il existe maintenant une large gamme de cartes offrant plus ou moins de fonctionnalité.

3.6.3 Le fonctionnement

Le principe de fonctionnement de l'Internet par satellite est simple. A l'inverse de la connexion par modem téléphone standard, vous n'avez qu'un « interlocuteur »: les serveurs Proxy de votre fournisseur d'accès situé à la station d'émission (appelée aussi « station d'Uplink »). En effet, là ou un internaute utilisant une connexion par modem entrera en contact avec différents serveurs disséminés sur le réseau mondial Internet, un internaute communiqué par satellite ne communiquera qu'avec un seul serveur qui est chargé de récupérer les demandes de l'abonné et de lui retransmettre le résultat de ses requêtes par la voie des aires. Inconvénient en cas de panne du serveur de la station d'émission. La fiabilité du matériel du fournisseur d'accès devient alors un élément non négligeable.

3.6.4 Les serveurs Proxy

Les serveurs Proxy sont les serveurs chargés de « surfer » à la place de l'internaute. Ces serveurs appelés aussi « cache », récupèrent les fichiers et données demandées par un

abonné. Les données ainsi récoltées sont ensuite transmises à différentes machines dont la tâche et de les encapsuler en DVB-MPEG-2 avec un code d'identification unique afin que seul l'abonné ait effectué la requête reçue son fichier. Bien souvent, l'adresse MAC de la carte de réception DVB-MPEG-2 est utilisée pour identifier l'abonné.

3.6.5 Le « Push »

Autre possibilité intéressante de la réception de données par satellite vers un micro-ordinateur : le PUSH de données. Ce mode de réception rejoint complètement l'utilisation d'un satellite de façon « normale ». L'intérêt de l'utilisation d'un satellite est la possibilité de toucher des millions d'utilisateurs (ou spectateurs) en un seul envoi de données. A l'inverse, en utilisation « point à point » (principe de base de l'Internet), le service du satellite ne sera utilisé que pour une seule personne isolée. Le mode PUSH peut donc être utilisé pour émettre des données intéressant un large public. On peut donc imaginer l'envoi de certaines de sites Internet vers tous les postes d'un groupe d'abonnés ayant les mêmes centres d'intérêt. Par ailleurs, l'utilisateur n'a plus besoin d'effectuer des requêtes sur les serveurs Proxy de son fournisseur d'accès et par conséquent, n'a même plus besoin de se connecter à l'Internet pour recevoir des données.

3.6.6 Les débits

Sur un satellite, un transpondeur dispose d'une capacité de 34 Mb, ce qui correspond à une connexion Internet à très haut débit souvent utilisés par les fournisseurs d'accès Internet terrestre ou de grandes sociétés nécessitant des haut débits pour l'échange de données entre différents sites éloignés. Cette bande passante est alors partagée par le nombre d'abonnés utilisant simultanément les services de son fournisseur d'accès. En heure de pointe, cette bande passante peut être mise à mal si chaque abonné dispose lui même d'un matériel de réception et d'émission à haut débit.

En théorie, une carte de réception DVB MPEG-2 accepte jusqu'à 45 MB par seconde! Un abonné pourrait alors consommer l'intégralité de la bande passante à lui tout seul... Le fournisseur d'accès limite alors le débit maximum par utilisateur en effectuant différents réglages à la station d'émission.

3.6.7 L'avenir

Des sociétés préparent plus ou moins discrètement des services d'accès Internet par satellite pour le grand public dont les lancements commerciaux sont prévus pour les mois à venir. Mais l'échec de certains pionniers a la matière de prouver qu'il n'est pas facile de proposer des services d'accès Internet par satellite en point à point en utilisant une technologie étudiée pour de la diffusion de masse, autrement dit : le multi-point.

Chapitre 4
Gestion de la sécurité

4.1 Introduction

Il faut assurer la sécurité des infrastructures critiques lors de la connexion. Les systèmes de commande et l'acquisition de données embarqués dans les infrastructures critiques sont menacés par des attaques externes. Une architecture sécurisée est nécessaire lors de l'établissement de la connectivité.

Il faut mettre en application des architectures plus bloquées et des technologies de sécurité, par exemple, en segmentant le réseau par des pare-feu robustes, utilisant l'authentification forte, mettant en application les programmes efficaces de gestion de la sécurité qui incluent la sécurité de tous les systèmes de commande.

Une solution aux problèmes de la sécurité est le firewall. Ce dispositif dispose de règles lui permettant de savoir comment réagir en fonction des données qui transitent par lui.
Par exemple, s'il détecte un paquet en provenance d'Internet qui possède une adresse IP correspondant à une adresse du réseau local (cas de figure ou quelqu'un essayerait de pénétrer sur le réseau local depuis l'extérieur en falsifiant l'adresse source afin de faire croire qu'il est non pas sur Internet, mais sur le réseau local), le firewall rejettera le paquet détectant une anomalie.

Parmi les autres fonctionnalités potentielles d'un firewall, on notera la possibilité de mettre en place des tunnels VPN. Les VPN (Virtual Private Network) ou réseaux privés virtuelles en français, permettant d'établir un tunnel de données cryptés et authentifiés entre un utilisateur distant et le réseau local tout en passant par l'Internet.

4.2 Les dispositifs de la sécurité

4.2.1 Les pare-feu

4.2.1.1 Définition et fonctionnement

Un pare-feu (*firewall*, en anglais) est un dispositif matériel et/ou logiciel qui implémente la fonction de sécurité de contrôle d'accès. Un pare-feu est donc un dispositif pour filtrer les accès, les paquets IP, les flux entrant et sortant d'un système. Un pare-feu est installé en coupure sur un réseau lorsqu'il sert de passerelle filtrante pour un domaine à la frontière d'un périmètre fermé. Un pare feu est un système permettant de filtrer les paquets de données échangés avec le réseau, il s'agit aussi d'une passerelle filtrante comportant au minimum les interfaces réseaux suivante:

- Une interface pour le réseau à protéger (réseau interne).
- Une interface pour le réseau externe.

Un pare-feu met en vigueur une politique de sécurité qui laisse passer, ou arrête les trames ou les paquets d'information selon cette politique. Il peut donc autoriser ou empêcher des communications selon leur origine, leur destination ou leur contenu. Dans la pratique, un pare-feu lit et analyse chacun des paquets qui arrivent. Après analyse, il décide du passage ou de l'arrêt selon l'adresse IP de l'émetteur, du récepteur, selon le

type de transport (TCP ou UDP) et le numéro de port, en relation avec le type d'application réseau.

Quand la politique de sécurité ne concerne que les couches basses, la seule analyse du paquet permet d'autoriser, de rejeter ou d'ignorer le paquet.

Quand la politique décrit des règles de sécurité qui mettent en jeu le transport fiable, les sessions ou les applications, le pare feu doit connaître l'état momentané de la connexion et doit garder en mémoire de nombreux paquets pendant un certain temps de façon qu'il puisse décider de l'autorisation ou du rejet des paquets.

Les pare-feu ont des limitations : ils doivent être très puissants en termes de ressources pour ne pas ralentir le trafic, dans un sens ou dans un autre, puisqu'ils ont en coupure sur le réseau. Ils ne doivent pas être court-circuités par d'autres passerelles ou des modems connectés directement à l'extérieur. Ils sont des « bastions », c'est-à-dire des cibles pour les attaquants qui peuvent les assaillir pour saturer leur ressource.

Un pare-feu doit posséder un système de journalisation (.log) sophistiqué a posteriori tous les faits importants qui jalonnent la vie de cette passerelle filtrante : tentatives d'intrusion, événements anormaux, attaques par saturation, par balayage.

Un pare feu est en général architecturé de telle manière que l'on puisse distinguer physiquement les communications avec l'extérieur, celles avec le réseau à protéger et enfin celles qui sont déviées vers une zone tampon de parking, souvent appelée zone démilitarisée (DMZ en anglais), c'est dans cette zone qu'on place le site web, ouvert à l'Internet, à l'abri d'un pare-feu, mais nettement séparé du réseau interne à protéger.

Il convient d'ailleurs de dire ici qu'il n'existe aucun système de sécurité qui soit infaillible à 100%. Tout logiciel, qu'il soit de type *firewall* ou de type chiffrement d'information peut être «cassé». Mais il suffit que les besoins financiers à mettre en œuvre pour ce faire soient supérieurs à la valeur marchande estimée des informations en notre possession pour que le système soit considéré comme fiable. **[OA 97]**

4.2.1.2 Les types de firewalls

Packet filter : Le packet filter, comme son nom l'indique, filtre les paquets dans les deux sens. Pour ce faire, il utilise des fonctions de routage interne classiques. Ce sont des protections efficaces, mais pas toujours suffisantes. Certaines attaques complexes peuvent déjouer les règles.

Screening router : Evite le IP spooffing en vérifiant que les adresses d'origine des paquets qui arrivent sur chaque interface sont cohérentes et il n'y a pas de mascarade. Exemple: un paquet qui a une adresse de votre réseau interne et qui vient de l'extérieur est un Spoofed Packet. Il faut le jeter et prévenir le plus vite l'administrateur qu'il y a eu tentative d'attaque.

4.2.2 Les systèmes de détection et de prévention de l'intrusion

Un système de détection d'intrusion (IDS en anglais), est un dispositif matériel et/ou logiciel de surveillance qui permet de détecter en temps réel et de façon continue des tentatives d'intrusion en temps réel, dans un SI ou dans un ordinateur seul, de présenter des alertes à l'administrateur, voire pour certains IDS plus sophistiqué, de neutraliser ces pénétrations éventuelles et de prendre en compte ces intrusions afin de sécuriser davantage le système agressé.

Un IDS réagit en cas d'anomalie, à condition que le système puisse bien identifier les intrus externes ou internes qui ont un comportement anormal, en déclenchant un avertissement, une alerte, en analysant éventuellement cette intrusion pour empêcher qu'elle ne se reproduise, ou en paralysant même l'intrusion.

Un IDS est un capteur informatique qui écoute de manière furtive le trafic sur un système, vérifie, filtre et repère les activités anormales ou suspects, ce qui permet ultérieurement de décider d'action de prévention. Sur un réseau, l'IDS est souvent réparti dans tous les emplacements stratégiques du réseau.

Les techniques sont différentes selon que l'IDS inspecte un réseau ou que l'IDS contrôle l'activité d'une machine (hôte, serveur).

- Sur un réseau, il y a en général plusieurs sondes qui analysent de concert, les attaques en amont d'un pare-feu ou d'un serveur.
- Sur un système hôte, les IDS sont incarnés par des démons ou des applications standards furtives qui analysent des fichiers de journalisation et examinent certains paquets issus du réseau.

Il existe deux grandes familles distinctes d'IDS:

- Les N-IDS (Network Based Intrusion Detection system), ils assurent la sécurité au niveau du réseau.
- Les H-IDS (Host Based Intrusion Detection system), ils assurent la sécurité au niveau des hôtes.

Un N-IDS nécessite un matériel dédié et constitue un système capable de contrôler les paquets circulant sur un ou plusieurs liens réseau dans le but de découvrir si un acte malveillant ou anormal a lieu.

Le H-IDS réside sur un hôte particulier et la gamme de ces logiciels couvre donc une grande partie des systèmes d'exploitation tels que Windows, Linux, ect...
Le H-IDS se comporte comme un démon ou un service standard sur un système hôte. Traditionnellement, le H-IDS analyse des informations particulières dans les journaux de logs (syslogs, messages, lastlogs...) et aussi capture les paquets réseaux entrant/sortant de l'hôte pour y déceler des signaux d'intrusion (Déni de services, Backdoors, chevaux de troie...).

4.3 VPN

4.3.1 Introduction

Les entreprises et les organisations possèdent en général plusieurs sites géographiques qui travaillent conjointement en permanence. Dans chaque site géographique, les utilisateurs sont connectés ensemble grâce à un réseau local. Ces réseaux locaux sont souvent connectés via Internet. En outre, certains utilisateurs peuvent vouloir se connecter aux réseaux de l'entreprise en étant à l'extérieur chez un client ou en déplacement.
Il existait autrefois des liaisons physiques spécialisées, qui sont maintenant abandonnées au profit de liaisons logiques.
Un réseau virtuel privé (*Virtual Private Network,* en anglais d'où l'abréviation VPN) consiste en fabrication d'un tunnel logique qui sera contracté par les communications de l'entreprise, lesquelles seront véhiculées dans cette tranchée numérique construite sur un réseau fréquenté par d'autres usagers. Dans la pratique, il s'agit d'un artifice, car les données vont utiliser un chemin ordinaire, emprunté par tout le monde, mais ces données chiffrées et tagguées seront sécurisées, à l'image du transport de containers plombés sur une route. Le caractère privé du réseau est donc complètement virtuel puisqu'il ne s'agit pas de liaison physique spécialisée. Le caractère privé est créé par un protocole cryptographique (IPSec ou PPTP). Un VPN est donc une communication sécurisée entre deux points d'un réseau public, d'où l'expression de tunnel.

Un VPN fournit un service fonctionnellement équivalent à un réseau privé, en utilisant les ressources partagées d'un réseau public. Les réseaux VPN Internet sont utilisés dans plusieurs types d'application : Intranet étendus, Extranet, accès distants. Des tunnels empruntent le réseau Internet et assurent une sécurité robuste des échanges de données : authentification forte des équipements VPN source et destination, intégrité et confidentialité des données échangées.

VPN fournit aux utilisateurs et administrateurs du système d'information des conditions d'exploitation, d'utilisation et de sécurité à travers un réseau public identiques à celles disponibles sur le réseau privé. Parmi les protocoles VPN les plus utilisés, on peut citer : VPN IPSec et VPN SSL

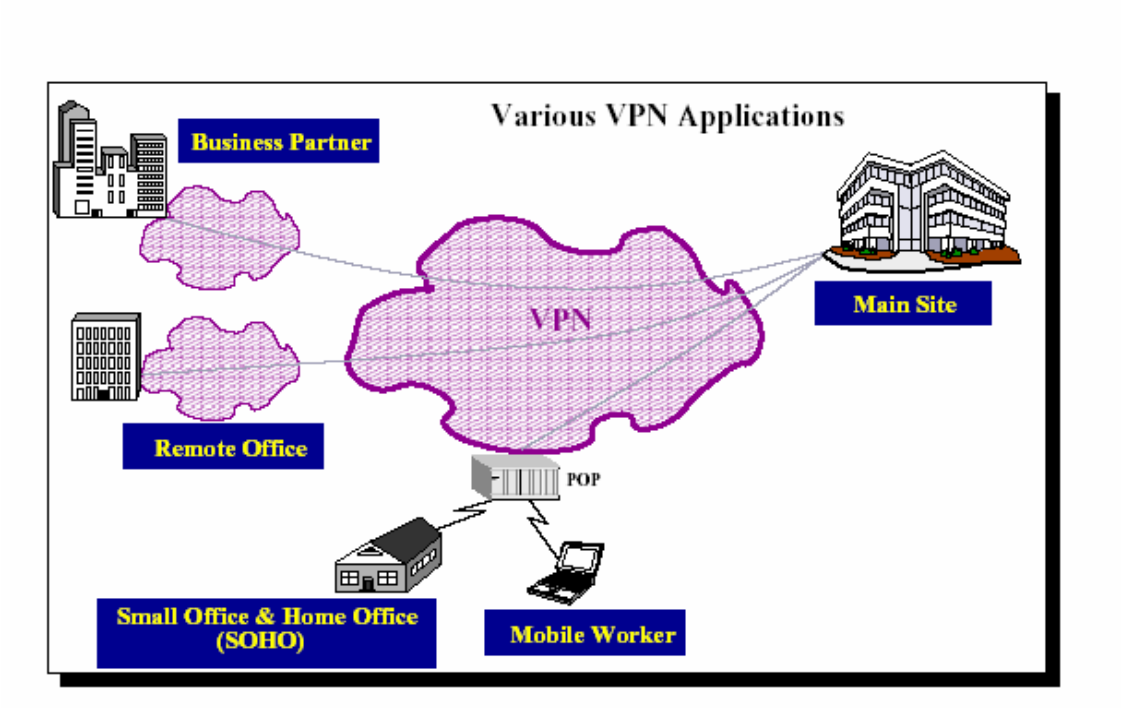

Figure 8 : Différents applications VPNS

4.3.2 IPSec

IPSec est un protocole destiné à fournir différents services de sécurité. Son intérêt principal reste sans contexte son mode de tunneling, c'est-à-dire d'encapsulation d'IP qui lui permet entre autres choses de créer des réseaux privés virtuels (ou VPN en anglais).

Citons quelques propriétés générales des tunnels destinées aux VPNs :

- Les données transitant sont chiffrées (confidentialité) et protégées (intégrité)
- Les 2 extrémités sont authentifiées
- Les adresses sources et destination sont chiffrées

Il ne faut pas négliger les aspects pratiques tels que la charge processeur dû au chiffrement, le débit théorique possible, l'overhead induit et donc le débit effectif…
De plus IPSec n'est pas le seul protocole permettant d'établir des tunnels, il en existe d'autres comme les « point-à-point » tel que L2TP, L2F ou encore PPTP qui peut induire un overhead non négligeable.

IPSec est un protocole au niveau de la couche réseau qui offre :

- Intégrité des paquets : les paquets sont protégés de sorte que tous les changements pendant leur transmission aient pu être détectés.
- Confidentialité des paquets : les paquets sont chiffrés avant d'être transmis sur les réseaux.

- Authentification d'origine des paquets : les paquets sont protégés pour s'assurer qu'ils sont envoyés par l'expéditeur souhaité.

4.3.3 SSL

SSL (Secure Sockets Layers) est un procédé de sécurisation des transactions effectuées via Internet. Il repose sur un procédé de cryptographie par clef publique afin de garantir la sécurité de la transmission de données sur Internet. Son principe consiste à établir un canal de communication sécurisé entre deux machines (un client et un serveur) après une étape d'authentification.

Le système SSL est indépendant du protocole utilisé, ce qui signifie qu'il peut aussi bien sécuriser des transactions faites sur le Web par le protocole HTTP que des connexions via le protocole FTP, POP ou IMAP. En effet, SSL agit telle une couche supplémentaire, permettant d'assurer la sécurité des données, situées entre la couche application et la couche transport (protocole TCP par exemple).

4.3.4 Utilisation de IPsec et SSL

IPsec et SSL sont les protocoles de sécurité les plus utilisés sur internet. Néanmoins ces deux protocoles présentent de grandes différences :

- Niveaux d'opérations : IPsec est un protocole de niveau réseau tandis que SSL est un protocole de niveau applicatif. Cette différence est le point de divergence essentiel.
- Périmètre sécurisé : opérant à deux niveaux différents, SSL offre des services de sécurité limités à TCP tandis que IPsec supporte n'importe quel trafic, TCP, UDP ou autre. De même SSL sécurise une application donnée tandis qu'IPsec sécurise plusieurs applications simultanément.
- Support d'installation : Un grand avantage de SSL est l'absence de logiciel supplémentaire côté client, un grand nombre de navigateurs supportant nativement HTTPS (hTTP sur SSL). A l'inverse IPsec requiert à ce jour le déploiement de logiciels spécifiques.

D'un point de vue sécurité, il n'y pas une grande différence entre SSL et IPsec qui partagent les mêmes algorithmes. Etablir un VPN SSL ou un VPN IPsec dépend alors essentiellement des besoins des utilisateurs.

4.4 Un système VPN bien administré

Trois points clés pour réussir l'administration d'un VPN, sont: la sécurité, l'administration et le dynamisme. Le déploiement de réseaux privés sur des infrastructures partagées voire publiques comme Internet nécessite des précautions impératives pour protéger les systèmes connectés à l'infrastructure partagées et les échanges qui vont prendre place sur cette infrastructure. Les solutions retenues s'appuient sur plusieurs protocoles de sécurité, tel que L2TP, PPTP ou encore IPsec. IPsec, une suite de protocoles de sécurité définie par l'IETF, est le protocole utilisé dans notre approche grâce à ces avantages sur les autres protocoles.

D'autres part, l'étude d'une solution VPN, nécessite une bonne maîtrise de l'architecture du réseau à modifier ou à construire. L'administration est un élément clé au déploiement des VPNs et tout particulièrement tout ce qu'il concerne les services de groupes de communications. La mise en place d'une solution bien administrée est reliée avec les points suivants :

- Politique: le système d'administration doit avoir le pouvoir de convertir les politiques de configuration à des règles appliquées sur les passerelles VPNs. La sécurité et l'atténuation des attaques sont aussi basées sur les politiques.
- Configuration : l'approvisionnement et la configuration des équipements VPN doivent être fait d'une manière automatisée et appliquée sur les passerelles VPNs.
- Déploiement rentable : dans un système administré, il faut avoir un mécanisme pour envoyer, déployer, et mettre à jour les fichiers de configuration.
- Connaissance des topologies VPNs: plusieurs types de topologie doivent être supportés. On distingue les VPN maillés et les VPN en étoile qui correspond respectivement à des topologies de liaisons virtuelles entre sites de type n vers m (réseau maillé) soit de type n vers 1 (réseau en étoile).
- Surveillance : l'environnement sécurisé doit être mise sous contrôle et sous surveillance. Une automatisation de la supervision et de l'administration des équipements VPN installés sur les sites des utilisateurs finales.

En général, l'administration est avant tout une problématique de connectivité réseau et d'infrastructure IP. Certains problèmes spécifiques liés à la technologie utilisée compliquent la mise en œuvre, par exemple, la diffusion des fichiers de configuration IPsec bien cohérents entre les différents équipements VPN distribués sur l'Internet.

Conclusion générale

Au cours de cette étude, nous avons présenté différentes méthodes et technologies pour connecter une infrastructure au réseau et l'intérêt d'utiliser des lignes de communication spéciales (ADSL, VPN, ect…) et des protocoles afin de réaliser la sécurité et d'offrir un haut débit nécessaire pour le fonctionnement en temps réel. Les travaux de recherche dans ce domaine ont pour objectif d'étudier les différents points qui servent à réaliser la connectivité des infrastructures critiques.

Les principales étapes d'une étude d'une recherche appliquée à la connectivité ont été abordées au cours de ce mémoire.

Tout d'abord, une étude générale sur quelques aspects a été proposée dans le chapitre 1 afin de mettre en évidence les besoins de protection des réseaux contre les attaques et offrant un haut débit et une interaction acceptable. La sécurité en générale a été étudiée aussi en mettant l'accent sur les dispositifs nécessaires et en utilisant la cryptographie comme technique de calcul en temps réel.

Le chapitre 3 traite la connectivité dans les infrastructures critiques par l'utilisation des méthodes efficaces et des technologies sécurisées et fonctionnant en temps réel. La connectivité à Internet par satellite a été traitée comme un exemple d'infrastructure critique.

Dans le chapitre 4, la gestion de la sécurité a été présentée. Les différentes étapes liées à la conception et la réalisation de cet objectif ont été traitées.

Plusieurs perspectives peuvent être avancées à l'issue de cette étude. La gestion de la sécurité en respectant la qualité de service serait une première amélioration. Aussi, la proposition des architectures matérielles pour sécuriser les systèmes embarqués serait un deuxième point.

Bibliographie

[DD 04] Damien DEVILLE- « Un système d'exploitation temps réel extensible pour carte à microprocesseur »- Thèse de doctorat, Université des sciences et technologies de Lille, décembre 2004.

[ES 05] Emmanuel SIMEU – « Test et surveillance intégrés des systèmes embarqués »- Diplôme d'habilitation à diriger des recherches, université Joseph Fourrier de Grenoble, le 22 septembre 2005.

[OA 97] Olivier Andrieu-« Internet guide de connexion »- Eyrolles, 3ème édition 1997-ISBN : 2-212-08928-7

[UIT 03] Union internationale des télécommunications- « Le rapport essentiel sur la téléphonie IP ».

[LC 05] Lina AL-CHAAL- « Dynamic and Easily Manageable Approach for Secure IP VPN Environments » Thèse de doctorat, institut national polytechnique de Grenoble, le 2 février 2005.

[RG 03] Régis CHANTALAT- « Optimisation d'un réflecteur spatial a Couverture cellulaire par l'utilisation d'une bande interdite électromagnétique multisources. »- Thèse de doctorat, université de Limoges, novembre 2003.

[FT 01] France Télécom- « Réseau VTHD, l'Internet vraiment très haut débit »-, paris, le 9 mai 2001.

[GB 05] Gilles BROUSSILLON- « AUTONOMIC COMPUTING », Etude d'approfondissement, Master 2, Génie informatique, Université Joseph Fourrier, Grenoble, Novembre 2005.

[MR 06] Michel RIGUIDEL- « La sécurité des réseaux et des systèmes », Paris, 2005-2006.

[AD 01] Alain DESEINE- « Accéder à Internet via ADSL », janvier 2001.

Nous vous suggérons de visiter:

www.commentcamarche.fr : Un site informatique offrant des informations utiles surtout des cours sur le réseau.