Déploiement d'un réseau sans fil pour des instituts de microfinance dans le cadre de la coopération au développement
Table des matières

1. Introduction ................................................. 9
   1.1. La microfinance ...................................... 9
   1.2. Aquadev ................................................. 9
   1.3. AdBanking .............................................. 10
   1.4. Centres régionaux .................................. 11

2. Description du problème .................................. 12
   2.1. Contexte .............................................. 12
   2.2. Modélisation ......................................... 13
       2.2.1. Capture de données ................................ 13
       2.2.2. Résultats de la capture ......................... 13
       2.2.3. Conclusions de l’analyse de trafic ............ 14
       2.2.4. Environnement .................................. 14

3. Solutions envisagées ......................................... 18
   3.1. Introduction ........................................... 18
   3.2. Connexion par fournisseur internet local ........... 18
   3.3. Connexion satellite .................................. 18
   3.4. Faisceaux hertziens ................................ 18
       3.4.1. Wi-Fi ............................................ 18
       3.4.2. WiMax ........................................... 19
       3.4.3. HiperLAN ....................................... 19
       3.4.4. Autres solutions radio ......................... 20
   3.5. Conclusions ........................................... 20

4. Etude du Wi-Fi .............................................. 21
   4.1. Les normes importantes .............................. 21
       4.1.1. Le standard de l’ISO : OSI ...................... 21
       4.1.2. Les standards de l’IEEE ......................... 22
           4.1.2.1. Les réseaux (IEEE 802) .................. 22
           4.1.2.2. Les réseaux sans fil (IEEE 802.11) .... 23
   4.2. Techniques de modulation ............................ 25
   4.3. Propagation d’ondes .................................. 29
       4.3.1. Onde libre ....................................... 29
       4.3.2. Pertes de puissance ............................. 31
4.3.3. Pertes sur une liaison avec ligne de vue .............................. 31
4.3.4. Réfraction dans l'atmosphère ........................................... 32
4.3.5. Diffraction et Zones de Fresnel ........................................ 33
   4.3.5.1. Le principe de Huygens ........................................... 33
   4.3.5.2. La spirale de Cornu .............................................. 34
   4.3.5.3. Les zones de Fresnel ............................................. 35
   4.3.5.4. Première zone de Fresnel ....................................... 36
   4.3.5.5. Conclusion concernant la diffraction ............................ 36
4.3.6. Réflexion ........................................................................ 37
4.3.7. Facteurs météorologiques .................................................. 37
4.4. Antennes ............................................................................. 38
   4.4.1. Antennes omnidirectionnelles ....................................... 39
   4.4.2. Antennes directionnelles .............................................. 39
   4.4.3. Fabrication artisanale .................................................. 40
4.5. Aspects électroniques .......................................................... 41
4.6. Sécurité .............................................................................. 42
   4.6.1. Contrôle d'adresses MAC .............................................. 42
   4.6.2. Le protocole WEP ....................................................... 43
   4.6.3. Les protocoles WPA et WPA2 ...................................... 43
   4.6.4. Chiffrement sur la couche réseau ................................... 44
   4.6.5. Sécurité sur la couche de transport ................................. 45
   4.6.6. Conclusions ................................................................. 46

5. Sur le terrain .......................................................................... 47
   5.1. Préparation de la mission .................................................. 47
      5.1.1. Matériel .................................................................. 47
      5.1.2. Budget de lien ......................................................... 48
      5.1.3. Financement ........................................................... 48
   5.2. Séjour sur place ............................................................... 49
   5.3. Repérage ......................................................................... 50
      5.3.1. KIST .................................................................... 50
      5.3.2. Siège Inkingi ......................................................... 50
   5.4. Préparation ...................................................................... 50
   5.5. Déploiement ................................................................. 50
   5.6. Tests de liaison .............................................................. 53
   5.7. Tests par Internet ........................................................... 56
   5.8. Fabrication locale d'antennes ........................................... 57

6. Conclusions .......................................................................... 58
   A. Les réseaux informatiques .................................................. 60
      A.1. Le modèle ISO ........................................................... 60
         A.1.1. La couche physique ................................................. 60
         A.1.2. Diffraction de données ........................................... 60
A.1.3. La couche réseau ......................................................... 61
A.1.4. La couche transport ...................................................... 61
A.1.5. La couche session ........................................................ 61
A.1.6. La couche présentation .................................................. 61
A.1.7. La couche d’interface application ..................................... 62
A.2. Le modèle TCP/IP .......................................................... 62
A.3. L’identification ............................................................. 63
A.4. Concrètement ............................................................... 64
  A.4.1. Réseau local Ethernet ................................................ 64
  A.4.2. Fonctionnement des bridges ......................................... 64
  A.4.3. Serveur Internet public .............................................. 64
  A.4.4. Redirection de port .................................................. 65
  A.4.5. Réseau privé virtuel (VPN) .......................................... 65
B. La sécurité informatique ..................................................... 66
  B.1. Les différents aspects ................................................... 66
  B.2. Outils mathématiques ................................................... 66
    B.2.1. La cryptographie symétrique ..................................... 67
    B.2.2. La cryptographie asymétrique ................................... 68
    B.2.3. les fonctions de hachage .......................................... 69
C. Sécurité des réseaux .......................................................... 70
  C.1. La couche physique ...................................................... 70
    C.1.1. Ethernet .............................................................. 70
    C.1.2. Wi-Fi ................................................................. 70
  C.2. liaison de données ...................................................... 70
    C.2.1. Ethernet .............................................................. 70
    C.2.2. Wi-Fi ................................................................. 71
  C.3. La couche réseau ......................................................... 72
  C.4. La couche transport ...................................................... 72
D. Reconstruction des flux TCP capturés ...................................... 73
E. Réalisation d’un câblage Ethernet .......................................... 76
F. Logiciels employés ............................................................ 77
  F.1. Ethereal ................................................................. 77
  F.2. nmap ................................................................. 77
  F.3. ping ................................................................. 77
  F.4. OpenSSH ............................................................ 77
  F.5. Kismet ............................................................... 78
  F.6. Airsnort ............................................................... 78
  F.7. AdBanking ............................................................. 78
  F.8. Apache .............................................................. 78
# Table des matières

- F.9. OpenSSL ......................................................... 79
- G. Rapports hebdomadaires ........................................ 81
  - G.1. Première semaine ........................................... 81
    - G.1.1. Rencontre des intervenants et formalités douanières .... 81
    - G.1.2. Lundi ..................................................... 81
    - G.1.3. Mardi ..................................................... 81
    - G.1.4. Mercredi ................................................ 82
    - G.1.5. Jeudi ..................................................... 82
    - G.1.6. Vendredi ................................................. 82
    - G.1.7. Conclusions ............................................. 84
  - G.2. Deuxième semaine ........................................... 84
    - G.2.1. Lundi ..................................................... 84
    - G.2.2. Mardi ..................................................... 85
    - G.2.3. Mercredi ................................................ 86
    - G.2.4. Jeudi ..................................................... 87
    - G.2.5. Vendredi ................................................. 87
    - G.2.6. Conclusions ............................................. 88
  - G.3. Troisième semaine ......................................... 88
    - G.3.1. Lundi ..................................................... 88
    - G.3.2. Mardi ..................................................... 88
    - G.3.3. Mercredi ................................................ 88
    - G.3.4. Jeudi ..................................................... 89
    - G.3.5. Vendredi ................................................. 89
    - G.3.6. Conclusions ............................................. 89
      - G.3.6.1. Liaison sans fil .................................. 89
      - G.3.6.2. Liaison par Internet ................................ 90
      - G.3.6.3. Module multi-agences ............................. 90
      - G.3.6.4. Tableau récapitulatif ............................. 91

5
Table des figures

2.2. capture de trafic avec pic d’activité ........................................... 14
2.3. Trafic SSH ................................................................................. 15
2.4. trafic total sans SSH en bytes/seconde ..................................... 16
2.5. Trafic total sans SSH en paquets ............................................. 16

4.1. Le modèle OSI ................................................................. 22
4.2. Les protocoles réseaux IEEE 802 .......................................... 23
4.3. Bridging de deux réseaux distants ........................................... 23
4.4. Modulations d’amplitude et de phase ..................................... 26
4.5. Diagramme I-Q ................................................................. 27
4.6. Exemples de modulations numériques ................................. 28
4.7. Densité spectrale de puissance en DSSS ................................. 29
4.8. Canaux non superposés ......................................................... 29
4.9. réflexion et réfraction ........................................................... 32
4.10. Le problème de la diffraction sur un objet pointu (knife-edge) 33
4.11. le front d’ondes vu comme une somme d’ondelettes ............. 34
4.12. La spirale de Cornu ............................................................. 34
4.14. la première zone de Fresnel ................................................ 36
4.15. la contrainte de Fresnel ....................................................... 37
4.16. un connecteur type N feemlle (châssis) ................................. 41

5.1. Les bureaux de Aquadev Central Africa à Kigali ................ 49
5.2. La tour de télécommunications du KIST ............................... 51
5.3. Vue du KIST depuis Nyamirambo ....................................... 52
5.4. Le siège d’Inkingi ............................................................... 53
5.5. Vue de la tour de télécommunications du KIST et de l’antenne Wi-Fi installée .......................................................... 53

G.1. Vues du mât installé au siège de Inkingi à Nyamirambo .... 83
G.2. Vues de l’antenne installée à Nyamirambo ............................ 83
G.3. Vues de la tour de télécommunications du KIST depuis le siège de Inkingi à Nyamirambo ........................................ 84
G.4. Alignement de l’antenne du KIST par Bonny ....................... 85
G.5. Vues de l’antenne placée sur la tour au KIST ....................... 86
Liste des tableaux

2.2. Capture de trafic sur une session ADBanking .......................... 13  
2.3. Précipitations à Kigali ..................................................... 17  

4.1. Différentes techniques de modulations numériques .................. 27  
4.2. Les différentes familles d’antennes ................................. 39  
4.3. La sécurité dans les réseaux sans fil .................................. 42  
4.4. Solutions de sécurité recommandées .................................. 46  

5.1. Budget de lien ................................................................. 48  
5.2. Budget du projet .............................................................. 49  

A.1. les 7 couches du modèle OSI ........................................... 62  
A.2. exemples de ports et des services associés .......................... 63  

B.1. Correspondances des lettres pour le code de Jules César avec n=5. 67  
B.2. Exemple de texte chiffré avec le code de César (n=5) ............ 67  

G.1. Grille de comparaison des solutions .................................... 91
Remerciements

Je tiens tout particulièrement à remercier Patrik Bikar et Cisco Systems Belgique pour leur soutien matériel, ainsi que Pr. Philippe Mathys de l’ULB pour m’avoir orienté vers les bonnes personnes et Pr. Esteban Zimanyi, Jean-Michel Dricot et Augustin Siaens pour avoir proposé et encadré ce mémoire.

Ma gratitude va aussi à toute l’équipe d’Aquadev Central Africa pour leur accueil chaleureux, et plus spécialement à Adrien Kabale, Arthur Rutembesa, Freddy Munyaburanga et Boniface qui ont beaucoup fait pour que tout se passe bien pour moi.

Mes remerciements vont également à ma famille et à mes amis (spécialement à Jasper qui s’est levé au milieu de la nuit pour faire le taxi, Jonathan et Philippe qui en faisant le facteur m’ont épargné 1600 km, à Géraldine qui m’a aidée pour le dossier de financement et tous ceux qui m’ont fait cadeau de boîtes de pringles vides). Ils ont prêté une oreille parfois attentive et toujours patiente à mes passionnants problèmes de câbles, de prises électriques et d’antennes.

Le voyage réalisé dans le cadre du présent travail/stage a été rendu possible grâce à l’intervention financière du Conseil interuniversitaire de la Communauté française de Belgique - Commission universitaire pour le Développement - Rue de Namur, 72-74, 1000 Bruxelles - http://cud.ciuf.be
1. Introduction

1.1. La microfinance

La microfinance, ou plus précisément le microcrédit, consiste en l’offre de prêts financiers à des personnes qui, en raison de leur dénuement, n’ont pas accès aux services classiques du milieu bancaire. Particulièrement dans les pays en voie de développement, le microcrédit permet à des populations très pauvres de développer des projets personnels qui assurent un revenu afin de subvenir aux besoins personnels et familiaux.

C’est au cours d’une famine au Bangladesh, en 1974, qu’un professeur d’économie américain originaire du pays, Muhammad Yunus, constata qu’un petit prêt pouvait faire une grande différence. Cependant les banques traditionnelles n’étaient pas intéressées par ce type de produit, les pauvres étant considérés comme de mauvais payeurs et donc présentant un trop grand risque. Il fonda donc, en 1976, la Grameen Bank, qui a depuis prêté près de 5000 millions de dollars à 4 millions de clients, presque exclusivement des femmes.


La principale critique du microcrédit est le taux d’intérêt très élevé réclamé par les bailleurs de fonds. C’est cependant une nécessité pour compenser les risques dus aux mauvais payeurs. De plus, certains s’inquiètent que l’assistance fournie aux programmes de microcrédit ne se fasse au détriment des programmes d’aide de première nécessité tels que la santé, l’eau et l’éducation.

Les prêts sont majoritairement établis et remboursés au nom de femmes ; cependant des études montrent que beaucoup de ces prêts sont investis en pratique et utilisés par des hommes.

L’offre de comptes d’épargne est intéressante car elle permet d’une part une sécurité financière et d’autre part l’autofinancement des prêts, indépendamment de sources externes internationales. Ces comptes épargnes locaux sont ainsi la source principale des financements de prêts dans des IMF africaines solides.

1.2. Aquadev

Aquadev[2] est une organisation non gouvernementale (ONG) fondée en 1987 dont le siège est situé en Belgique et dont l’objet s’exerce dans le domaine de la coopération au
développement, Aquadev emploie une centaine de personnes et gère des projets d’une
d’une valeur globale de plus ou moins 3 millions d’euro.
Cette ONG est active dans trois secteurs :
1. la microfinance : secteurs financier décentralisé et appui aux entreprises ;
2. la sécurité nutritionnelle : approche planificatrice et multisectorielle ;

1.3. AdBanking

L’expérience d’Aquadev dans la microfinance sur le terrain, en collaboration avec des
IMF, a amené l’ONG à constater que ces IMF étaient rarement informatisées. Cela
deviendra un problème, certains étant amenés à gérer des milliers de comptes.
AdFinance, la branche microcrédit d’Aquadev, démarrera alors le développement du
logiciel AdBanking, très bien adapté aux besoins car conçu dès le départ en étroite
collaboration avec les utilisateurs (à Ouagadougou au Burkina Faso). C’est un logiciel
de gestion transactionnelle à destination des instituts de microfinance construit sur une
plate-forme basée sur des logiciels libres\(^1\) qui a permis une nette limitation des coûts :
système d’exploitation Linux, moteur de base de données PostgreSQL, serveur Web
Apache, navigateur Mozilla Firefox, code PHP\(^2\). La licence d’utilisation d’AdBanking
est gratuite pour les IMF des Pays les Moins Avancés (PMA). Seuls les coûts d’installation
leurs sont facturés, Aquadev pouvant cependant prendre dans le cadre d’un accord de
partenariat, une partie des coûts à sa charge.
AdBanking est fortement adapté avant le déploiement dans chaque IMF selon le nombre
et le type de produits financiers proposés. Les principales fonctionnalités sont :
- la gestion des clients (enregistrement, défection et mise à jour, frais d’adhésion et
  parts sociales),
- la gestion de l’épargne (ouverture et clôture, transaction, consultation des opéра-
tions),
- la gestion du crédit (introduction de demandes, gestion des approbations et rejets,
  versement, commissions, assurances, échéances des remboursements, suivi du dos-
sier),
- la gestion des guichets (approvisionnement et délestage de caisse, saisie par lots
d’opérations effectuées sur le terrain, chèques, transactions),
- le paramétrage du système (jours fériés, utilisateurs, produits),
- la gestion du système (ouverture et fermeture d’agence, sauvegarde et restauration
de données).

\(^1\)Les logiciels libres\(^3\) présentent quatre caractéristiques : liberté d’exécuter le programme (sans li-
mite temporelle, géographique ou de domaine d’application), liberté d’étudier le fonctionnement du
programme et de l’adapter à ses besoins, liberté de redistribution et liberté d’amélioration.
\(^2\)La prochaine version devrait tourner sous Java.
1.4. Centres régionaux

L’ONG Aquadev est structurée de façon décentralisée. Ainsi il n’y a que 4 ou 5 personnes à travailler pour AdFinance à Bruxelles. La plus grande partie des intervenants, recrutés dans les populations locales, est répartie sur le terrain dans des centres régionaux d’expertise amenés à intervenir dans les pays environnants. Ils accompagnent les IMF dans leurs démarches d’informatisation à travers une approche méthodologique qui repose sur un ensemble de services. Ces derniers sont assurés via un accompagnement (mode participatif) aussi bien en amont qu’en aval du processus.

- Audits préalables à l’informatisation : examen de la situation financière et opérationnelle de l’institution afin d’évaluer sa maturité pour une éventuelle informatisation ;
- Plans d’informatisation : aider les IMF à élaborer celui-ci (aux niveaux stratégie et budget) et les accompagner dans leur recherche de financement ;
- Déploiement du logiciel AdBanking : sensibilisation / information des organes et des équipes, installation et configuration du matériel, installation du logiciel, paramétrage, reprise et numérisation des données, etc... ;
- Renforcement des capacités : appropriation du logiciel par les partenaires à travers des formations à la carte, basées sur les techniques d’apprentissage des adultes ;
- Accompagnement au changement : analyse des impacts organisationnels, mise à jour des procédures, prise en compte du facteur humain, etc... ;
- Suivi du changement : formations continues, prise en compte des demandes d’évolution, etc... ;
- Support et assistance technique de proximité assurées par les centres nationaux de compétences ;
- Capitalisation qui s’articule autour :
  - de la production et/ou de l’amélioration des outils méthodologiques propres en conceptualisant l’expérience de terrain ;
  - du suivi et de l’analyse de l’évolution des comportements des bénéficiaires de l’information des différents acteurs du secteur sur la problématique spécifique de l’informatisation des institutions de microfinance ;
  - de la mesure de l’impact des actions liées à l’offre, permettant ainsi d’améliorer l’approche et l’outil et donc, les perspectives de viabilité.
2. Description du problème

2.1. Contexte

Le succès des informatisations locales a créé une nouvelle demande d’informatisation globale des IMF. Il serait intéressant pour elles de centraliser toutes les données de toutes les agences afin de construire une vue d’ensemble de l’état de santé financier de l’institution.

Les IMF encadrées par Aquadev sont principalement localisées en milieu urbain. La plupart d’entre elles ont un réseau de plusieurs agences et une caisse centrale. La qualité des moyens de communication dans les pays dans lesquels Aquadev est active ne permet pas de connecter ces agences au siège central via des lignes louées ou via des technologies telles que l’ADSL.


Une autre possibilité a donc été envisagée par Aquadev : permettre une connexion directe des agences à la base de données située au siège central en faisant appel aux dernières technologies de réseau sans fil. Dans cette configuration les agences seraient considérées comme des guichets et les problèmes de cohérence de la base de données seraient résolus. Cela faciliterait grandement l’intégration des opérations effectuées dans les agences ainsi que leur sauvegarde. Aquadev travaille fréquemment avec le milieu académique et de nombreux étudiants ont déjà consacré leur mémoire à ces activités, que ce soit dans les domaines de l’environnement ou de la microfinance.

C’est dans ce contexte qu’Augustin Siaens, de la cellule “Outils et Stratégies”, a contacté Esteban Zimanyi, directeur du Service Informatique et Réseaux, pour lui proposer de faire travailler un étudiant sur ce projet dans le cadre d’un Mémoire de Fin d’Études.

C’est la possibilité de travailler dans le cadre de la coopération au développement qui m’a fait choisir ce mémoire, ce qui m’a permis de faire des rencontres humaines enrichissantes et de découvrir d’une manière plus concrète les problèmes rencontrés dans les pays du Tiers-monde.
2.2. MODÉLISATION

<table>
<thead>
<tr>
<th>Durée de la capture</th>
<th>37 minutes 40 secondes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Taille moyenne des paquets</td>
<td>534 octets</td>
</tr>
<tr>
<td>Débit en paquets</td>
<td>2,7 paquets/seconde</td>
</tr>
<tr>
<td>Débit en octets</td>
<td>1463 octets/seconde</td>
</tr>
<tr>
<td>Round Trip Time (temps d’aller-retour)</td>
<td>de 0,1 à 60 ms</td>
</tr>
</tbody>
</table>

Tab. 2.2.: Capture de trafic sur une session ADBanking

2.2. Modélisation du problème

Le système construit autour d’AdBanking consiste en une architecture client-serveur utilisant uniquement des requêtes HTTP\(^1\), et le but du projet est de rendre accessible le serveur web et base de données localisé au siège principal de l’IMF à des postes clients situés dans des filiales.

Grâce à la modularity offerte par l’architecture en couches des réseaux modernes (TCP/IP, OSI), cela sera possible sans aucune modification de l’infrastructure logicielle existante. En effet les requêtes HTTP se situent au niveau de la couche 7 du modèle OSI (couche application) et nous allons envisager des solutions au niveau des couches 1 et 2 (respectivement physique et liaison de données), en conservant la couche réseau IP (niveau 3) et toutes les couches supérieures. On trouvera plus loin une présentation générale (section 4.1.1 page 21), et en annexe (annexe A.1 page 60) une présentation plus détaillée des couches constituant ce modèle.

2.2.1. Capture de données

Lors d’une visite au siège de Aquadev Belgique, Augustin Siaens m’a montré la version de démonstration d’AdBanking qui tourne sur leur réseau local. Pendant environ 40 minutes il a fait le tour des fonctionnalités offertes par le logiciel : ouverture de l’agence, encodage de nouveaux clients, encodage d’opération de versement, consultation des informations de crédit, génération de divers rapports au format pdf ...

Simultanément, un enregistreur de trafic réseau\(^2\) enregistrait toutes les trames Ethernet vues par l’interface réseau de l’ordinateur. J’ai récupéré ce fichier pour l’analyser par la suite.

2.2.2. Résultats de la capture

On trouvera ci-dessous le graph de trafic entre les deux systèmes en fonction du temps :

On peut constater sur le graphique de bande passante utilisée, que quasiment tout le trafic reste sous la barre des 100 000 octets /seconde. De plus, pour tout ce trafic,

\(^1\)Protocole standardisé permettant l’utilisation de sites web.
\(^2\)Ethereal Network Protocol Analyzer (voir annexe F.1 et [5])
2.2. MODÉLISATION

CHAPITRE 2. DESCRIPTION DU PROBLÈME

Fig. 2.2.: capture de trafic avec pic d’activité

descendre la bande passante disponible à 50 000 octets / seconde ne devrait pas trop poser de problème car le trafic moyen est inférieur à cette valeur.

Par contre, on observe un pic important de trafic autour des 1000 secondes. Après analyse, ce pic correspond en fait à l’établissement d’une connexion Secure Shell\(^3\), utilisée par Augustin pour reconfigurer certains paramètres du serveur AdBanking d’Aquadev.

2.2.3. Conclusions de l’analyse de trafic

Les besoins en connectivité pour un poste peuvent être estimés à 2,5 paquets par seconde et 0,012 MBit/seconde.

Une liaison à 1MBit devrait alors permettre 80 connexions simultanées sans perte de qualité. Pour une agence équipée de 5 postes, les besoins évalués correspondent à une liaison à 0,06 MBit.

2.2.4. Environnement

C’est l’IMF Inkingi, basée à Kigali, au Rwanda, qui s’est montrée la plus enthousiaste concernant ce projet. Les tests sur le terrain se feront donc en collaboration avec eux. Elle possède une dizaine d’agences dans la capitale et une trentaine dans l’ensemble du pays.

\(^3\)SSH, pour Secure Shell Server. Protocole de communication sécurisée par cryptographie asymétrique (paires de clé publique et privée). Pour plus d’information consulter F.4 et [6].
Les conditions climatiques sont tropicales, tempérées par l’altitude moyenne élevée du Rwanda (1500 mètres à Kigali). L’Association Mondiale de Météorologie (World Meteorological Organisation) fournit sur son site un relevé annuel de pluviométrie [7]. On y relève pour le mois de février, un niveau de 100 mm.

En comparaison, en Belgique au mois de février, les précipitations moyennes sont de 53 mm.

Il y a deux saisons des pluies, une petite autour de novembre et une grande autour du mois d’avril. Seul le mois de juillet est vraiment sec. Le séjour s’effectuera au mois de février, à la fin de la petite saison sèche.

On évaluera l’impact éventuel de ces facteurs environnementaux sur le système mis en place.
Fig. 2.4.: trafic total sans SSH en bytes/seconde

Fig. 2.5.: Trafic total sans SSH en paquets
2.2. MODÉLISATION

<table>
<thead>
<tr>
<th>Mois</th>
<th>Précipitation moyenne (mm)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Janvier</td>
<td>69</td>
</tr>
<tr>
<td>Février</td>
<td>100</td>
</tr>
<tr>
<td>Mars</td>
<td>106</td>
</tr>
<tr>
<td>Avril</td>
<td>183</td>
</tr>
<tr>
<td>Mai</td>
<td>92</td>
</tr>
<tr>
<td>Juin</td>
<td>20</td>
</tr>
<tr>
<td>Juillet</td>
<td>9</td>
</tr>
<tr>
<td>Août</td>
<td>34</td>
</tr>
<tr>
<td>Septembre</td>
<td>86</td>
</tr>
<tr>
<td>Octobre</td>
<td>102</td>
</tr>
<tr>
<td>Novembre</td>
<td>127</td>
</tr>
<tr>
<td>Décembre</td>
<td>100</td>
</tr>
</tbody>
</table>

Tab. 2.3.: Précipitations à Kigali
3. **Inventaire des solutions techniques envisagées**

3.1. **Introduction**

Plusieurs facteurs ont été retenus pour l’évaluation des technologies existantes. Le coût, la portée, le débit, la résistance aux interférences, les régulations locales concernant les émissions radio, la facilité de déploiement et d’entretien et la résistance aux conditions climatiques.

3.2. **Connexion par fournisseur internet local**

L’opérateur national, RwandaTel[12], fournit des connexions Internet. Leur site web étant en construction je n’ai pu obtenir une liste des tarifs. Aquadev m’a informé du coût élevé de ce genre de solution, et de son manque de fiabilité.

Néanmoins ce secteur est en rapide évolution et une réévaluation de cette solution sera effectuée sur place.

3.3. **Connexion satellite**

Les connexions satellites sont rapides, mais extrêmement chères et asymétriques.

3.4. **Faisceaux hertziens**

3.4.1. **Wi-Fi**


Deux topologies de réseau sans fil sont possibles : *ad hoc* et *infrastructure*. En mode ad hoc, les clients sont connectés les uns aux autres directement, tandis qu’en mode infrastructure un point d’accès (AP) est utilisé et l’ensemble forme alors une cellule (Base Station Set) à laquelle est assignée un identifiant (BSSID), adresse MAC du point d’accès. Plusieurs cellules forment alors un Extended Service Set (ESS) reliées par un service de distribution (DS), auquel est assigné un identifiant ESSID, fréquemment abrévé en SSID. C’est une chaîne de caractères qui permet aux utilisateurs d’identifier le réseau formé.
3.4. FAISCEAUX HERTZIENS  

CHAPITRE 3  SOLUTIONS ENVISAGÉES

La norme 802.11 originale n’est plus utilisée actuellement. Elle permettait des liaisons à 1 ou 2 Mbps. Les normes actuelles permettent de 11 à 54 Mbps théoriques (voire 108 Mbps chez certains fabricants : 802.11b+, 802.11g+).

Cette technologie est connue principalement dans son mode infrastructure. Ainsi on trouve sur le marché de nombreux points d’accès à bas coût, permettant de connecter entre eux les différents équipements informatiques d’une habitation ou d’une entreprise et de partager une connexion internet à haut débit.

Nous envisageons ici la possibilité de créer une liaison point à point par ondes électromagnétiques en employant des ponts (bridges).

Un pont Ethernet relie deux (ou plus) réseaux physiques ethernet pour former un grand réseau logique Ethernet. Dans le standard 802.11, La fonctionnalité bridge est un sous-mode du mode infrastructure.

Une contrainte de 802.11 est la nécessité d’une liaison en ligne de vue. Tout obstacle visuel dégradera sérieusement les performances, voire rendra la liaison impossible. Il faudra donc évaluer l’environnement d’utilisation.

Les distances que l’on peut couvrir dépendent des besoins en bande passante et du matériel : avec de bonnes antennes paraboliques et des câbles de très haute qualité on peut couvrir 40 km. Un record a même été établi à 300 km avec un ballon-sonde.

La sécurité du médium n’est pas à négliger : le secteur d’activité étant le milieu bancaire il est important de garantir l’identité des intervenants ainsi que d’assurer une certaine confidentialité et une intégrité des liaisons. Une liaison radio est par nature plus facile à intercepter qu’une liaison câblée. 802.11 comprend un protocole de sécurité, appelée Wired Equivalent Privacy (WEP), qu’on pourrait traduire par Sécurité équivalente aux réseaux câblés. Nous verrons plus loin (sous-section 4.6.2) si ce protocole atteint l’ambitieux objectif annoncé.

3.4.2. WiMax

En cours de standardisation, WiMax (IEEE 802.16, [14]) offre du haut débit radio, et ce dans des rayons allant jusqu’à 50 km. Malheureusement ce genre d’équipement est hors de portée financière de notre projet, et est plutôt destiné à des opérateurs de réseaux publics de télécommunications en raison du coût de la (les) station(s) de base. Le matériel ne devrait pas arriver sur le marché avant fin 2005. De plus, de nombreux fabricants participant au forum de normalisation WiMaxForum ont déjà annoncé leur intention d’offrir du matériel implémentant des extensions propriétaires au protocole. Il existe donc quelques doutes quand à l’interopérabilité des équipements.

3.4.3. HiperLAN

Standard développé par l’institut européen des standards de télécommunication (ETSI, [15]). Cette norme est similaire au Wi-Fi. Existe en deux versions, soit 20 Mbps pour HiperLAN/1 et 54 Mbps pour HiperLAN/2.

Le succès du Wi-Fi a empêché le développement commercial de cette solution. Le matériel est difficile à obtenir.
3.4.4. Autres solutions radio

Motorola propose une gamme de produits appelée Canopy [16] qui utilisent un protocole propriétaire au fabricant. Les fréquences employées vont de 900 Mhz à 5.8 Ghz. Ce genre de matériel est plutôt destiné aux fournisseurs d’accès internet sans fil (WISP), est onéreux et permet des liaisons sans ligne de vue (NLOS, Non Line Of Sight).

3.5. Conclusions

Pour des raisons d’accessibilité du matériel et d’efficacité technique, nous choisissons la technologie Wi-Fi.

Il faudra obtenir des points d’accès, des antennes directionnelles et des câbles à faibles pertes. Pour ce faire, plusieurs dossiers de demande de sponsoring ont été introduits chez la plupart des fabricants de matériel Wi-Fi : Cisco, 3Com, DLink, Linksys, NetGear...
4. Etude plus détaillée de la technologie choisie

4.1. Les normes importantes

4.1.1. Le standard de l’ISO : OSI

Les réseaux font intervenir des technologies variées pour satisfaire des besoins différents. L’emploi simultané de toutes ces techniques pour fournir le service voulu devient rapidement très difficile. Pour y voir plus clair, et permettre l’interopérabilité des matériels des différents vendeurs, l’ISO a établi une décomposition fonctionnelle en couches de l’architecture des réseaux dans le cadre de son programme Open Systems Interconnect (OSI). Les normes de l’ISO n’ont pas rencontré le succès espéré en termes de déploiements opérationnel (en raison de leur complexité et de la difficulté de devoir tout changer en une fois), mais elles font office de modèle de référence pour situer les protocoles qu’on rencontre dans le domaine des réseaux. Le modèle OSI n’est pas parfait, ce sont principalement les couches basses qui sont utilisées. Elles sont brèvement introduites ici, le lecteur intéressé trouvera plus d’informations dans l’annexe A.1 page 60.

Un des points forts du modèle OSI est la spécification des interfaces entre les couches, chacune ayant connaissance uniquement des couches qui l’encadrent, ce qui réduit grandement la complexité de l’ensemble. Une implémentation de plusieurs couches successives du modèle OSI est souvent appelée pile, par exemple on parlera de la pile des protocoles TCP/IP.

1. La couche physique, qui spécifie toutes les propriétés électriques et physiques, permettant l’établissement de communications et la modulation de l’information ;
2. la couche liaison de données (DLL pour Data Link Layer), fournit les procédures de transfert de données, de contrôle d’erreur et parfois de retransmission (par exemple Ethernet, HDLC, Aloha) ;
3. la couche réseau, permet le transfert de messages de taille variable de la source à la destination en passant par un ou plusieurs réseaux, tout en assurant la Qualité de Service (QoS) demandée par la couche transport ;
4. la couche transport offre un service de transfert de données transparent pour les applications ;
5. la couche session ;
6. la couche présentation ;
7. la couche application.
4.1. LES NORMES IMPORTANTES  

CHAPITRE 4. ÉTUDE DU WI-FI

On fait souvent la distinction à l’intérieur de la couche liaison de données, des couches Medium Access Control (MAC) et Link Layer Control (LLC), ce qui permet de séparer clairement les procédures d’accès au médium et les procédures de contrôle des trames lorsque l’accès au médium a été établi.

4.1.2. Les standards de l’IEEE

4.1.2.1. Les réseaux (IEEE 802)

Le matériel portant le label Wi-Fi [8] respecte un ensemble de normes définies par l’Institute of Electrical and Electronics Engineers (IEEE [9]). Les normes de l’IEEE sont regroupées en une structure hiérarchique.


Ce standard présente les différentes méthodes d’interconnexion de réseaux :

1. Interconnexion au niveau physique : répéteurs et hubs ;
2. Interconnexion au niveau MAC (voir plus loin) : les bridges et les switches ;
3. Interconnexion au niveau réseau : les routeurs.
4.1. LES NORMES IMPORTANTES

CHAPITRE 4. ETUDE DU WI-FI

Fig. 4.2.: Les protocoles réseaux IEEE 802

On y définit la notion de domaine d'accès, ensemble de stations communiquant sur le même médiunm de transmission et utilisant un même protocole MAC d'établissement d'accès au bus.

On y trouve aussi la définition des ponts transparents (transparent bridging) : les bridges sont des appareils permettant l'interconnexion de réseaux, ou plus précisément, des domaines d'accès. Un bridge transparent assure la fonctionnalité de bridge sans nécessiter de changement dans le mode de fonctionnement des stations communicantes. Du point de vue de ces stations, la liaison s'établit comme si elles étaient directement sur le même domaine d'accès. Un bridge transparent travaille uniquement au niveau de la sous-couche MAC.

Fig. 4.3.: Bridging de deux réseaux distants

La norme 802.2 définit un protocole de contrôle de lien (Link Layer Control, LLC) qui vérifie la bonne réception des trames, permet la retransmission de trames en cas de pertes, et un contrôle de flux, et ce en modes connecté ou non.

4.1.2.2. Les réseaux sans fil (IEEE 802.11)

Les normes 802.11 (Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications [11],[48]) définissent les méthodes d'accès au médiunm de communica- tion (couche MAC), ainsi que les spécifications de la couche physique (couche PHY), pour les réseaux sans fil. C’est cet ensemble de normes qui nous intéresse particulièrement ici.
Les réseaux sans fil présentent quelques différences fondamentales avec leurs homologues câblés :
- l’adresse de destination sur un réseau sans fil n’est pas équivalente à la localisation physique du destinataire ;
- il est impossible de déterminer une frontière du médium de communication au-delà de laquelle on peut être sûr qu’aucune station ne peut recevoir de messages du réseau ;
- les couches physiques 802.11 ne sont pas protégées des messages provenant de l’extérieur ;
- le médium est nettement moins fiable ;
- les topologies sont dynamiques ;
- les réseaux sans-fil ne présentent pas la propriété importante de connectivité complète : c’est-à-dire que l’hypothèse classique que toute station peut entendre toutes les autres stations est invalide ici ;
- les propriétés de propagation varient temporellement et sont asymétriques.

On définit des blocs de bases, les Basic Service Sets (BSS), dans lesquels les stations sont en connectivité totale. Ce qui amène à la configuration la plus simple, celle de BSS indépendants (IBSS). Ce type de fonctionnement est possible dès que deux stations peuvent communiquer correctement, et comme cette configuration est disponible sans préparation on l’appelle réseau ad hoc.

L’autre mode de fonctionnement permet de relier des BSS grâce à un service de distribution (DS, Distribution System). On remarquera que le système de distribution peut utiliser un autre médium de communication que les Base Stations. Dans chaque BSS, une station joue le rôle de point d’accès (Access Point, AP), faisant aussi partie du service de distribution.

La combinaison des BSS et des DS permet d’établir des réseaux de taille et de complexité arbitraire ; cette construction est appelée ensemble de services étendus (Extended Service Set, ESS). Cet ESS est défini uniquement aux niveaux PHY / MAC et donc la couche LLC ne voit aucune différence entre un ESS et un IBSS.

L’interconnexion avec des réseaux câblés se fait par l’intermédiaire d’un dernier composant architectural : le portail (portal). C’est par le portail que les messages peuvent passer d’un réseau à l’autre. Cette fonctionnalité logique peut être implantée dans une station faisant aussi office de point d’accès (AP), ayant accès au service de distribution (DS).

Voici une brève description des révisions de la norme 802.11 :
- 802.11b : Higher-speed Physical Layer Extension in the 2.4 Ghz Band[40], porte le débit brut de 2 Mbit/s à 11 Mbit/s, mais en conservant le même mécanisme d’accès au médium (CSMA/CA) qui gaspille de la bande passante, ramenant le débit net maximal à 5.9 Mbit/s en TCP, ce qui fait moins de 1 MB/s. La technique de modulation est DSSS.
- 802.11a : High-speed physical layer in the 5Ghz Band[39], permet d’utiliser la bande des 5Ghz, moins encombrée que celle des 2.4 Ghz et donc moins sujette aux interférences. Par contre la portée est légèrement moindre. Le débit brut total maximal est de 54 Mbit/s, ce qui permet d’atteindre un débit net supérieur à 20 Mbit/s (à peu
près 3 MBytes/s). Le multiplexage employé est OFDM (Orthogonal Frequency Division Multiplexing), et plusieurs méthodes de modulations numériques sont proposées en fonction de la qualité de la liaison (BPSK, QPSK, 16-QAM, 64-QAM).

- 802.11g : Further Higher-Speed Physical Layer Extension[41], porte le débit brut dans la bande des 2.4 Ghz à 54 Mbit/s et le débit net à 24.7 Mbit/s, une performance donc équivalente à 802.11a. Ce protocole est entièrement compatible avec 802.11b, mais en pratique une station 802.11b dégraderait fortement les performances d'un réseau de type g.
- 802.11n : le groupe de travail 802.11n a été formé en janvier 2004 et a pour objectif de porter le débit net à plus de 100 Mbit/s, soit 5 fois plus rapide que 802.11a/g et 20 fois meilleur que 802.11b. Deux standards sont en compétition, WWiSE (Broadcom) et TGn Sync (Intel, Philips). La norme devrait être prête fin 2006. Elle apporte des avancées comme MIMO (multiple-input multiple-output) OFDM, permettant le multiplexage spatial.
- 802.11h : révision de la norme IEEE 802.11a pour améliorer le contrôle de puissance d'émission.
- 802.11i : Medium Access Control (MAC) Security Enhancements, apporte des améliorations au niveau de la sécurité (voir plus loin).
- 802.11p : Wireless Access for the Vehicular Environment (WAVE), devrait permettre un accès réseau sans fil pour les véhicules comme les ambulances et les voitures.

Les problèmes de sécurité ont bien sûr été adressés dans ces normes. La première version proposait le protocole WEP (Wired Equivalent Privacy). Le but de ce protocole était de rendre les réseaux sans-fil aussi sûr que les réseaux câblés.

Il a été mis à jour par la suite avec le standard 802.11i, connu par le grand public sous deux noms commerciaux : WPA pour une pré-version et WPA2 pour la version finale.

Ces protocoles sont envisagés plus en détail dans la section 4.6 concernant la sécurité.

4.2. Techniques de modulation

La modulation est un déplacement en fréquence du signal à transmettre ([17],[29],[18]). C'est une opération non-linaire. On dira qu'une modulation est une opération mathématique faisant correspondre à un signal f son signal modulé. Cette opération est une modulation si et seulement si son inverse est unique, c'est-à-dire qu'à un signal modulé correspond un et un seul signal démodulé. On peut moduler en amplitude, en phase ou en fréquence.

Quasiment tous les systèmes de télécommunications emploient des modulateurs / démodulateurs, l'exception la plus notable étant le téléphone qui transmet directement le signal électrique du micro en bande de base (de 300 Hz à 3,4 KHz, soit une bande passante de 3,1 KHz) sur la ligne de transmission.

Un système de modulation en bande étroite (narrow band) est caractérisé par le rapport de la fréquence de modulation à la bande occupée autour de cette fréquence, très inférieur à l'unité. On module le signal sur un court intervalle de fréquences autour de la fréquence de transmission (exemples : AM, FM, PM).
On attribue alors des canaux différents à des communications différentes. C’est le Frequency Division Multiple Access (FDMA) qui permet plusieurs accès au médium par l’emploi de fréquences différentes. L’exemple le plus connu est la radio FM.

Ce type de transmission est insuffisant pour les réseaux locaux informatiques sans fils. Ceux-ci ont les contraintes suivantes :

- partage de la bande passante entre les différentes stations d’une même cellule ;
- propagation par chemins multiples d’une onde radio (phénomène d’écho).

Ces dernières années des techniques de modulation numériques ont remplacé les anciennes technologies analogiques dans le domaine :

- QPSK : Quadratic Phase Shift Keying ;
- FSK : Frequency Shift Keying ;
- MSK : Minimum Shift Keying ;
- QAM : Quadrature Amplitude Modulation.

On représente facilement le signal dans un diagramme polaire où la porteuse sert de référence de phase et d’amplitude.

Fig. 4.4 : Modulations d’amplitude et de phase

En modulation numérique on définit une constellation de \(2^n\) points dans le diagramme polaire, ce qui permet de transmettre \(n\) bits en une fois. Cela nécessite un changement simultané de la phase et de l’amplitude, une opération difficile et complexe avec des modulateurs de phase et d’amplitude. C’est pourquoi on utilise des modulateurs I/Q : on ajoute un repère cartésien sur le diagramme polaire, l’axe horizontal est appelé I et est associé à la référence de phase de la porteuse, et l’axe vertical est l’axe Q, perpendiculaire à I. Cette décomposition du signal en composantes orthogonales a un grand avantage : ces composantes sont indépendantes l’une de l’autre. On module chacune de ces composantes et on les additionne à la sortie pour créer le signal à émettre.

En modulation, les signaux émis sont des symboles et représentent les bits à transmettre. Un symbole représente plusieurs bits. Le débit de symbole se calcule facilement :

\[ \text{Débit en symbole} = \frac{n}{T} \]

où \(n\) est le nombre de bits par symbole et \(T\) est la durée de chaque symbole.

26
4.2. TECHNIQUES DE MODULATION

![Diagramme I-Q](image)

**FIG. 4.5.: Diagramme I-Q**

<table>
<thead>
<tr>
<th>Technique de modulation</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSK, GMSK</td>
<td>GSM</td>
</tr>
<tr>
<td>BPSK</td>
<td>modems câble</td>
</tr>
<tr>
<td>QPSK, 1/2DQPSK</td>
<td>satellite, CDMA, modems câble</td>
</tr>
<tr>
<td>QPSK</td>
<td>CDMA, satellite</td>
</tr>
<tr>
<td>FSK, GFSK</td>
<td>DECT, sécurité publique</td>
</tr>
<tr>
<td>8, 16 VSB</td>
<td>télévision numérique américaine</td>
</tr>
<tr>
<td>8 PSK</td>
<td>satellites, avions</td>
</tr>
<tr>
<td>16 QAM</td>
<td>radio numérique micro-ondes, modems</td>
</tr>
<tr>
<td>32 QAM</td>
<td>DVB-T</td>
</tr>
<tr>
<td>64 QAM</td>
<td>modems, boîtiers télévision set-top</td>
</tr>
<tr>
<td>256 QAM</td>
<td>Modems, vidéo numérique</td>
</tr>
</tbody>
</table>

**Tab. 4.1.: Différentes techniques de modulations numériques**

C’est le taux de bits divisé par le nombre de bits transmis par symbole. En Binary Phase Shift Keying (BPSK), un symbole représente un bit et les deux sont égaux. En Quadratic Phase Shift Keying, chaque symbole est codé par 2 bits et le taux de symbole vaut la moitié du taux de bits. On parle souvent de baud au lieu de symbole, ce sont des synonymes. Si on arrive à augmenter le nombre de bits par symbole il est possible de réduire la bande passante utilisée pour transmettre le même taux de bits. C’est le but des techniques de modulation numérique.

En PSK, on module donc en définissant plusieurs valeurs de phase possibles et l’amplitude ne change pas.

En FSK (Frequency Shift Keying), plusieurs fréquences sont possibles pour la portée et l’amplitude n’est pas non plus modifiée. Dans le cas le plus simple on attribue une fréquence pour un 1 et une autre pour un 0. Un changement de fréquence correspond à un changement de phase, et les démodulateurs I/Q détecteront ce changement très facilement lorsque cette variation est de \((2N + 1)\frac{\pi}{2}\) radian, soit un multiple de 90 degrés.
Lorsque la modulation est de +90 degrés on parle de Minimum Shift Keying (MSK), la méthode de modulation la plus efficace pour les FSK.

En Quadrature Amplitude Modulation la phase et l’amplitude sont modifiées simultanément. Par exemple en 16-QAM on utilise 4 valeurs possibles de I et 4 valeurs pour Q, soit une constellation de 16 points, avec un taux de symboles égal au quart du taux de bits. On atteint actuellement 256-QAM, mais l’augmentation de la taille de la constellation rend les signaux plus sensibles au bruit : le taux d’erreur (Bit Error Rate, BER) augmente plus rapidement avec les interférences.

La couche physique de la norme 802.11 introduit trois méthodes de transmission pour limiter les interférences : étalonnée de spectre par évasion/saut de fréquence (Frequency Hopping Spread Spectrum ou FHSS), étalonnée de spectre à séquence directe (Direct Sequence Spread Spectrum ou DSSS) et infrarouge.

La norme infrarouge n’a apparemment jamais été utilisée.

FHSS est un système initialement conçu par les militaires. Les participants à la connexion changent régulièrement de fréquence porteuse, dans un temps suffisamment court pour que toute écoute soit irréalisable, le temps de repérage de la nouvelle fréquence étant trop grand (première utilisation durant la crise des missiles de Cuba). Dans le standard cet aspect sécuritaire n’existe pas vu que la séquence est une information publique et commune à tous les appareils à la norme. Le procédé est utilisé uniquement pour la meilleure immunité au bruit dû à l’étalonnage du spectre.

Les produits à la norme 802.11 utilisent en pratique BPSK et QPSK en combinaison avec DSSS (Direct Sequence Spread Spectrum), une technique de protection contre les interférences et les échos. Avec DSSS, le signal est multiplié par un code de bruit pseudo-aléatoire (Pseudo Random Noise Code, PNcode). Un PNcode est une séquence de chips (terme utilisé pour éviter la confusion avec les bits du signal de données). La bande passante est donc multipliée par la longueur du PNcode. Ce signal combiné est ensuite modulé sur la porteuse. Cette modulation d’un signal à fréquence élevée a pour conséquence l’augmentation de la bande passante utilisée. L’information est étalée sur une plus large bande et le signal émis ressemble à du bruit. Au récepteur, il suffit de combiner le signal reçu avec la même porteuse modulée avec le PNcode.

La puissance restant la même, la densité spatiale de puissance diminue. Cette technique permet de mieux résister au bruit lorsqu’il est concentré sur une fréquence, grâce
à la redondance d’information apportée par le PNcode.
802.11 utilise toujours le même code (la séquence Barker de longueur 11), et de ce fait permet le fonctionnement simultané de seulement trois réseaux, chacun occupant un canal de 24 Mhz.

Fig. 4.7.: Densité spectrale de puissance en DSSS

Fig. 4.8.: Canaux non superposés

La révision 802.11b implémente CCK (Complementary Code Keying [30]) comme séquence PNcode, ce qui a pour conséquence de permettre une forte amélioration du débit car plusieurs séquences sont possibles et la longueur est augmentée, ce qui augmente aussi le “spreading factor” ou facteur d’étalonnage. En d’autres termes, on augmente l’étalonnage et les bénéfices qu’on en retire en sont d’autant améliorés.
Le standard 802.11a utilise la modulation COFDM (Coded Orthogonal Frequency Division Multiplexing), où plusieurs portées sont employées simultanément.

4.3. Propagation d’ondes

4.3.1. Onde libre

À première vue, la propagation d’ondes radio paraît proche de la propagation de la lumière : les signaux radio et lumineux sont tous des ondes électromagnétiques (Heinrich Hertz, 1887). Mais la grande différence en fréquence fait que plusieurs facteurs environnementaux ont une importance toute autre que pour la lumière visible (dont la fréquence varie entre 380 THz et 750 THz).
4.3. PROPAGATION D’ONDES

Une onde électromagnétique est caractérisée par trois grandeurs : son intensité (ou amplitude), sa fréquence (déterminant la couleur dans le cas particulier de la lumière) et sa polarité (non perçue habituellement par les humains).

Une onde radio est une onde transverse électromagnétique (TEM) composée de deux champs perpendiculaires oscillant en phase, l’un étant magnétique et l’autre électrique. De plus, ces deux champs sont perpendiculaires à la direction de propagation de l’onde [27, 20].

L’onde est atténuée lors de sa propagation selon une loi de carré inverse (le champ électrique décroit linéairement et la puissance est fonction du carré du champ électrique : \( P = \frac{E^2}{r} \)).

On parle fréquemment de la source isotropique en propagation d’ondes ; c’est une vue de l’esprit, car irréalisable concrètement, qui considère comme source d’ondes une sphère ponctuelle émettant de manière égale dans toutes les directions. On compare souvent les antennes réalisées à cette antenne idéale de référence.

Soit un émetteur de puissance \( P_t \) utilisant une antenne isotropique, rayonnant donc également en toute direction. La densité de flux spectral s’exprime comme le rapport entre la puissance émise et la surface à une distance \( d \) :

\[
s = \frac{P_t}{4\pi d^2}
\]

et la puissance reçue à l’émetteur est simplement :

\[
Pr = s \times A_R
\]

\( A_R \) étant la surface de réception, valeur établie pour l’antenne isotropique idéale à :

\[
A_r = \frac{\lambda^2}{4\pi}
\]

La perte de puissance sur le chemin s’exprime par le rapport des puissances émise et reçue, et on travaille en fréquence plutôt qu’en longueur d’onde. On obtient au final :

\[
\frac{P_t}{P_r} = \frac{P_t (4\pi)^2 d^2}{P_r \lambda^2} = \left( \frac{4\pi}{\lambda} \right)^2 f^2 d^2,
\]

puissance délivrée à une charge \( L \) à une distance \( d \). La perte de puissance sur le chemin (path loss) entre antennes isotropiques s’exprime :

\[
L_{dB} = 10 \log \left( \frac{P_t}{P_L} \right) = 20 \log d + 20 \log F_{\text{MHz}} + k,
\]

avec \( k=27.55 \) si \( d \) est en mètres ou \( k=32.4 \) pour \( d \) en kilomètres.

Dans ces conditions, doubler la distance revient donc à une perte de 6 dB (plus précisément 20log2 dB). La distance est exprimée en kilomètres et la fréquence en Hertz.

La polarisation d’une onde électromagnétique est par définition, la direction du champ électrique. En pratique on polarise les ondes soit verticalement soit horizontalement, selon la façon dont sont disposées les antennes. Une polarisation croisée occasionne une perte de 20 à 30 dB, il conviendra donc de toujours placer les antennes avec la même polarité. On verra plus loin si le choix de l’une ou l’autre polarisation s’avère plus intéressant.
4.3. PROPAGATION D’ONDES

4.3.2. Pertes de puissance

Le problème rencontré ici est de déterminer la puissance du signal au niveau du récepteur ([36, 27]). Pour que la liaison soit utilisable il faut que le taux d’erreur (on parle en télécommunications de *Bit Error Rate*, ou BER) soit inférieur à un certain taux. Cela est équivalent à imposer un taux minimum de rapport signal-bruit (*Signal-Noise Ratio* ou SNR), exprimé en décibel.

On a déjà déterminé la perte de signal sur une propagation d’onde en espace libre sur une distance équivalente.

Dans un système réel il faut aussi prendre en compte les pertes dues aux câbles et les gains d’antenne. Cela conduit à l’équation du bilan de puissance :

\[ P_r = P_t - L_{dB} + G_t + G_r - L_t - L_r \]

où
- \( P_t \) est la puissance à l’émetteur,
- \( L_{dB} \) la perte de transmission en propagation libre entre antennes isotropiques,
- \( G_t \) le gain de l’antenne d’émission,
- \( G_r \) le gain de l’antenne de réception,
- \( L_t \) et \( L_r \) les pertes sur les câbles d’antenne à l’émetteur et au récepteur.

Puis les différents facteurs physiques pouvant causer des écarts à ce modèle simplifié seront pris en compte : diffraction, réfraction et réflexion.

4.3.3. Pertes sur une liaison avec ligne de vue

Dans la plupart des cas, la liaison visuelle est synonyme de liaison radio. On parle de Line Of Sight (LOS). L’horizon radio va plus loin que l’horizon visuel, il est possible d’avoir une LOS radio sans LOS optique. Ceci est dû au chemin courbé emprunté par les ondes radio dans l’atmosphère.

La liaison LOS ne garantit pas l’équivalence de propagation avec l’onde libre. En effet, trois facteurs supplémentaires sont à prendre en compte :

1. la réflexion sur des objets proches ou lointains du chemin direct,
2. la réfraction dans l’atmosphère,
3. la diffraction.

Lorsque l’onde rencontre un milieu plus dense selon un certain *angle d’incidence*, et est réfléchie selon exactement le même angle, on parle de réflexion.

La réfraction se manifeste lorsque l’onde incidente pénètre dans une région de densité différente, ce qui cause des changements de vitesse et de direction. L’importance de la variation dépend du rapport des densités des deux milieux. Dans le cas des ondes radio les deux milieux peuvent être des couches d’air présentant des différences de densité.

Ces deux phénomènes peuvent donc coexister.

La diffraction est un cas particulier d’interférence ondulatoire. Lorsqu’une onde rencontre un obstacle partiel ou latéral dont la dimension n’est pas trop grande par rapport à la longueur d’onde, l’intensité du signal n’est pas nulle derrière l’obstacle. Ce thème sera développé plus en détail par la suite.
4.3.4. Réfraction dans l’atmosphère

Les ondes radio se propageant à proximité de la surface terrestre ne suivent pas des lignes droites mais empruntent des chemins légèrement courbés. Ce phénomène est causé par l’index de réfraction de l’atmosphère, qui diminue de façon monotone avec l’altitude. Cet effet est plus important au niveau des fréquences radio qu’aux fréquences observables par l’œil, ce qui fait que la ligne d’horizon optique est plus proche de l’observateur que la ligne d’horizon radio. LOS Radio n’implique donc pas LOS optique. Un artifice utilisé pour tenir compte de cet effet est l’emploi de cartes terrestres modifiées avec un “rayon terrestre de 4/3” : si les cartes sont reprojétées en supposant un rayon terrestre “radio” égal à quatre tiers du rayon terrestre réel, les ondes radio suivent alors des lignes droites et il est facile de déterminer l’horizon radio.

Lors de l’emploi de cette technique il ne faudra bien sûr jamais oublier que cet horizon radio calculé est un maximum théorique. Par exemple, les conditions météo peuvent considérablement modifier le radio LOS car l’indice de réfraction varie alors fortement. Dans le cas appelé superréfraction le radio LOS est repoussé plus loin, ce qui peut permettre dans un cas extrême, le ducting, la propagation du signal à des distances extrêmement grandes. Ce cas étant peu fréquent on ne peut pas s’y fier et il n’a pas vraiment d’intérêt pratique. L’autre cas, plus problématique, est la subréfraction. Là, l’horizon radio
est réduit, et les chemins empruntés par les ondes radio rencontrent plus facilement les obstacles éventuels. Il n'y a plus de trajectoire en "saut de puce". La perte sur le chemin augmente et peut conduire jusqu'à une mise hors service du lien.

Les solutions commerciales évaluent statistiquement ces risques pour en tenir compte lors du calcul du budget de lien. Nous n'entrerons pas dans de telles sophistications et retiendrons qu'il est nécessaire de prévoir une marge dans le calcul du budget de lien. L'évaluation de la solution sur le terrain permettra d'effectuer des mesures de la variation de la qualité du lien.

4.3.5. Diffraction et Zones de Fresnel

![Diagram of Diffraction](image)

**Fig. 4.10.** Le problème de la diffraction sur un objet pointu (knife-edge)

4.3.5.1. Le principe de Huygens

Huygens s'est intéressé à la propagation des ondes. Ses expériences le menèrent à la conclusion suivante : chaque point d'un front d'onde doit être considéré comme la source d'une onde secondaire, nommée *ondelette*, et un nouveau front d'onde est construit en sommant toutes les contributions individuelles des ondelettes provenant du front d'onde précédent.

Les ondelettes ne rayonnent pas également dans toutes les directions : leur amplitude dans une direction donnée est proportionnelle à $(1 + \cos \alpha)$ où $\alpha$ est l’angle entre cette direction et la direction de propagation du front d'onde. L’amplitude est donc maximale dans la direction de propagation et nulle dans le sens opposé.
4.3. PROPAGATION D'ONDES

4.3.5.2. La spirale de Cornu

C’est l’outil nécessaire à la modélisation de la rencontre du front d’onde avec un obstacle.

Lorsqu’il n’y a pas d’obstacle toutes les ondelettes contribuent à la construction du nouveau front d’onde en tous ses points et le vecteur résultant relie les points X et Y.

Au sommet de l’obstacle les contributions des ondelettes provenant d’en-dessous de
l’obstacle sont bloquées par celui-ci et seules les ondelettes supérieures contribuent à la construction du nouveau front. Sur la spirale de Cornu le vecteur résultant est facilement observable : il relie les points origine et Y, et correspond donc à la moitié de ce qui aurait été observé dans le cas de la propagation libre d’obstacle. C’est une atténuation de 6 dB en amplitudes.


**FIG. 4.13:** Effet d’un obstacle pointu sur l’amplitude du front d’onde

---

### 4.3.5.3. Les zones de Fresnel

Nous avons développé une certaine compréhension de la diffraction. Cela nous permet d’introduire le concept de zone de Fresnel. C’est le volume déterminé par un ellipsoïde construit avec les deux antennes prises pour ses centres. Il existe n zones de Fresnel telles que leur surface est déterminée par le chemin \( ACB \), dont la longueur est telle qu’elle respecte la relation suivante : \( \text{longueur}(ACB) = \frac{n}{2} \text{longueur}(AB) \).

Dans la plupart des cas il suffit de s’intéresser à la première zone de Fresnel \((n = 1)\).

Un chemin radio est dit libre en première zone de Fresnel (first Fresnel zone clearance) si aucun obstacle capable de diffraction n’est compris dans l’ellipsoïde correspondante.

Cela se traduit en termes de perte de puissance grâce à l’ellipsoïde de Cornu : la spirale supérieure est intacte et nous nous trouvons sur un point après l’extrémité inférieure, sur
le chemin qui remonte. Le vecteur résultant est proche de l’amplitude en propagation libre.
En pratique il est nécessaire d’obtenir 60% de l’espace de la première zone de Fresnel libre, pour que les pertes soient proches de celles calculées en espace libre.

4.3.5.4. Première zone de Fresnel
La distance \( h \) entre le chemin direct et le point le plus proche de l’obstacle, située dans le plan perpendiculaire à la direction de propagation, doit respecter la contrainte suivante :

\[
h \geq 17.3 \sqrt{\frac{d_1 d_2}{f(d_1 + d_2)}}
\]

avec \( d_1 \) et \( d_2 \) les distances en km du sommet de l’obstacle aux antennes, \( f \) la fréquence de transmission en GHz et \( h \) est exprimée en mètres.
Cette formule est une approximation et n’est pas valable pour des obstacles proches des antennes.

4.3.5.5. Conclusion concernant la diffraction
Le problème des zones de Fresnel peut sembler d’un intérêt très théorique au premier abord. Mais il se trouve que nous nous sommes basés sur une hypothèse optimiste : nous avons supposé que la longueur de l’obstacle était petite devant la longueur d’onde du signal. C’est l’hypothèse \textit{knife-edge}.
Dans la plupart des cas l’objet présentera une surface arrondie comme le sommet d’une colline, ou plate comme le toit d’un building. Avec ce type d’objets en contact tangent avec la première zone de Fresnel, la perte sera bien plus que 6 dB. Elle approchera plutôt les 20 dB !
De plus, il ne faut pas oublier que la zone de Fresnel est un ellipsoïde tridimensionnel et non une simple ellipse. Il faudra dès lors tenir compte aussi des façades des immeubles.
4.3.6. Réflexion

Malgré toutes ces précautions, les pertes peuvent encore différer sensiblement des résultats des calculs théoriques précédents. Ceci est alors dû à la réflexion des ondes sur le sol, particulièrement sur des surfaces planes. Ce problème n’est donc pas particulièrement important en ville où les constructions diverses et les arbres constituent une surface assez irrégulière (à l’exception des façades d’immeubles). Par contre les étendues d’eau forment un très bon réflecteur.

La polarisation du signal peut jouer un rôle : l’onde réfléchie est d’amplitude plus petite pour un signal polarisé verticalement, mais cela n’est vrai que lorsque l’angle d’incidence est relativement important (remarque : en transmissions radio on mesure habituellement l’angle d’incidence depuis la tangente à la surface, contrairement à l’optique, dans quel cas on prend la normale comme référence).

On retiendra simplement que pour de courtes distances et en milieu rural la polarisation verticale du signal permettra de diminuer sensiblement les pertes par rapport à une polarisation horizontale.

Dès que les distances deviennent relativement importantes la différence n’est plus significative et la réflexion est toujours un problème. Il convient alors de placer les antennes de manière à ce que le point de réflexion soit situé sur une zone non spéculaire.

En ville, la polarisation horizontale sera plus intéressante car elle est verticale relativement aux surfaces des grands bâtiments, et donc limite la réreflectivité. Il sera dès lors intéressant de l’essayer si de telles constructions sont présentes.

4.3.7. Facteurs météorologiques

On a déjà envisagé les effets sur la réfraction de la météo, causant les phénomènes de superréfraction, subréfraction et ducting.
4.4. **ANTENNES**

La pluie et le brouillard ne deviennent gênants qu’à des fréquences élevées, de l’ordre des micro-ondes. Le brouillard commence à être gênant vers les 30 Ghz (atténuation de 1 dB ou plus), ainsi que la neige (qui ne devrait pas être un problème au Rwanda).

De fortes pluies peuvent causer des pertes de l’ordre de 1 dB au kilomètre à partir de 10 Ghz.

Donc un lien Wi-Fi, utilisant une bande de fréquences entre 2.4 et 2.5 Ghz (ou 5 Ghz pour du Wi-Fi 5), ne devrait pas être affecté.

4.4. **Antennes**

Une antenne est un ensemble de conducteurs électriques conçus pour rayonner un champ électromagnétique en réponse à une force électromotrice alternative et un courant électrique alternatif associé qui lui sont appliqués [20, 34].

De même, si une antenne est placée dans un champ électromagnétique, ce champ va induire un courant alternatif et une force électromotrice entre ses extrémités.

Les antennes sont généralement conçues pour fonctionner sur une gamme de fréquences rapprochées, autour de la fréquence de résonance de l’antenne.

Les autres paramètres importants sont l’impédance, le gain, le diagramme de rayonnement (radiation pattern) et la polarisation.

Dans un système de radiocommunications (radio, câble d’antenne, antenne, espace libre), l’onde peut rencontrer des variations d’impédance à l’interface entre les composants. Une partie de l’onde va être réfléchie à la source et forme alors une onde stationnaire dans le câble d’antenne. L’impédance est une grandeur électrique (de valeur complexe) liée à la longueur électrique de l’antenne à la fréquence d’utilisation. On peut procéder à des adaptations d’impédance, et l’impédance peut être choisie de façon à minimiser l’énergie perdue aux interfaces.

Le gain est une grandeur scalaire, qui permet de comparer une antenne avec une antenne de référence (souvent l’antenne isotrope). Le gain est associé à une direction. L’ensemble des valeurs du gain permet de tracer le diagramme de rayonnement (radiation pattern). Lorsqu’on parle du gain d’une antenne on parle en réalité de la valeur du gain dans la direction où cette antenne rayonne le plus.

L’antenne la plus simple est le dipôle, aussi appelée parfois antenne Hertz car Heinrich Hertz l’a utilisée dans ses expériences. Il suffit de se munir de deux conducteurs électriques, qui seront les éléments rayonnants de l’antenne, tels que chacun mesure un quart de la longueur d’onde du signal à émettre. Les deux éléments sont placés sur une même droite et le signal sera alors isotope dans un plan perpendiculaire à cette droite. Cette antenne est intéressante pour sa simplicité et sa propriété d’isotropisme dans un plan. Par contre dans la direction de l’axe il y a des zéros. Nous n’entrerons pas plus en détail dans le fonctionnement des antennes. Nous en savons suffisamment maintenant que pour pouvoir évaluer les différentes options techniques.

Il existe sur le marché deux grandes catégories d’antennes : les antennes passives et les antennes actives. Ces dernières permettent généralement de meilleurs gains mais elles présentent le désavantage de nécessiter une alimentation électrique. Elles sont aussi plus
4.4. ANTENNES

complexes ce qui fait augmenter les prix. Il y a donc en tout quatre possibilités, en combinant les propriétés de directionnalité et de fonctionnement électrique.

4.4.1. Antennes omnidirectionnelles

Elles sont intéressantes dans le cas de liaisons point à multipoint (point-to-multipoint), par exemple lorsqu’il existe un point ayant ligne de vue sur plusieurs sites à relier et qu’il est possible d’y installer une antenne. Sinon, ce type d’antenne gaspille l’énergie du signal en la rayonnant dans toutes les directions et offre un point d’accès à d’éventuels attaquants.

4.4.2. Antennes directionnelles

Les antennes actives présentent le problème de nécessiter une alimentation électrique, qu’il faut placer à l’extérieur. Cela suppose une sécurisation des lieux (vols de câbles électriques) et une protection contre les intempéries, particulièrement durant la saison des pluies.

Il reste alors deux types d’antennes passives, les antennes Yagi, en forme de rateau, et les antennes paraboliques. Ces dernières présentent des gains plus importants et existent en deux versions sur le marché : le réflecteur peut être “en dur” comme pour une antenne satellite classique, ou en grille métallique ce qui diminue le poids de l’antenne et sa prise au vent. On remarquera encore qu’il existe des versions démontables des déflecteurs ce qui facilite alors le transport.

39
4.4. Fabrication artisanale

De nombreuses personnes ont fabriqué des antennes Wi-Fi à très bas coût en utilisant des matériaux de récupération [13, 34, 20]. La documentation à ce sujet est abondante sur Internet mais les sources de qualité sont rares. La plupart présentent des résultats empiriques sans réelle procédure systématique d’évaluation. La proposition la plus simple consiste en la fabrication d’un guide d’onde circulaire. Intuitivement, un guide d’onde est un tube métallique mis à la masse, dans lequel un élément rayonnant est placé. L’onde émise est alors guidée par cet assemblage et si les dimensions sont bien choisies toute la puissance du signal va être concentrée dans la direction de l’ouverture du guide d’onde (une des deux sections du guide étant fermée). Il est difficile de trouver une analyse théorique des guides d’ondes circulaires. Cependant j’ai trouvé des valeurs qui sont censées être idéales pour un tel guide d’onde, mais je n’ai pas pu obtenir de solides justifications théoriques. À titre informel, je les ai incluses dans ce mémoire car elles pourraient servir de point de départ pour une évaluation de cette solution.

Les deux contraintes initiales sont les suivantes :

- Le diamètre du guide d’onde doit être suffisamment grand que pour pouvoir permettre la propagation en mode TE11 à la fréquence la plus basse du signal émis (=> diamètre > 73.177 mm).
- Il doit aussi empêcher la propagation d’onde en mode TM01 à la fréquence la plus haute (=> diamètre < 92.796 mm).

Il faut maintenant déterminer le diamètre idéal entre ces deux bornes, en sachant qu’avec une augmentation du diamètre du guide d’onde :

- le faisceau devient plus étroit (meilleur gain) ;
- l’aperture augmente, cédant que la surface de capture d’un signal s’agrandit et donc que la réceptivité augmente ;

La longueur d’onde dans le guide est un paramètre du guide d’onde. Elle varie selon la fréquence d’émission et le diamètre du guide. Autour de 76 mm elle varie beaucoup pour des fréquences d’émission entre 2400 et 2480 Mhz, par contre pour un diamètre de 90 mm elle varie peu, ce qui signifie que le placement de l’émetteur, déterminé par cette longueur d’onde, sera correct pour toutes les fréquences de travail.

Un diamètre intéressant serait donc de 92 mm. Toutes les autres dimensions caractéristiques vont s’en déduire.

Longueur : 492 mm,
emplacement de l’émetteur depuis le fond du guide : 49.22 mm,
dimension de l’émetteur : 30.685 mm.

Il faudrait donc réaliser un tube métallique respectant ces dimensions, fermé d’un côté. Un trou à 30.685 mm du fond, dans la partie cylindrique du guide, doit être percé pour y insérer le châssis d’un connecteur type N sur lequel on viendra plus tard visser le câble d’antenne avec connecteur type N (fréquemment utilisé). Sur la partie du châssis venant se loger à l’intérieur du guide d’onde il faut souder une tige qui servira d’émetteur sur l’âme du connecteur, de taille 30.7 mm.
4.5. Aspects électroniques

Un bridge Wi-Fi est un boîtier électronique permettant sur un côté d’être relié à un réseau Ethernet classique par un connecteur RJ-45, et qui émet un signal électromagnétique respectant la norme Wi-Fi sur un connecteur d’antenne.

Les différents bridges Wi-Fi accessibles sur le marché se différencient selon les critères suivants :
- puissance d’émission ;
- sensibilité à la réception ;
- respects des différentes normes Wi-Fi : actuellement a, b et g ;
- matériel prévu pour un fonctionnement en intérieur (indoor) ou en extérieur (outdoor).

Différentes réglementations sont d’applications de par le monde au niveau des puissances d’émission. En Europe la norme ETSI (European Telecommunications Institute) est d’application et la limite vaut 50 mw EIRP (Effective Isotropic Radiated Power). Cette norme est en vigueur dans de nombreux pays d’Afrique. Les États-Unis ont fixé la limite de la puissance d’émission à 100 mw.

Il existe deux types de bridges : ceux conçus pour un fonctionnement à l’intérieur (indoor) et ceux conçus pour un fonctionnement à l’extérieur (outdoor).
4.6. SÉCURITÉ

<table>
<thead>
<tr>
<th>Couche</th>
<th>Technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>4. Transport</td>
<td>SSL/TLS ou tunnels SSH</td>
</tr>
<tr>
<td>3. Réseau</td>
<td>IPSEC</td>
</tr>
<tr>
<td>2. Liaison de données</td>
<td>Filtrage MAC, WEP, WPA, WPA2</td>
</tr>
<tr>
<td>1. Physique</td>
<td>aucune</td>
</tr>
</tbody>
</table>

TAB. 4.3.: La sécurité dans les réseaux sans fil

4.6. Aspects informatiques et sécurité

Un matériel à la norme Wi-Fi peut nécessiter pour établir une connexion, plusieurs paramètres [38, 11].

Les points d’accès Wi-Fi publics diffusent publiquement (broadcast) le nom de leur réseau (SSID). Il est donc très facile de les détecter dès qu’on est à portée de signal. Établir une connexion peut être une autre affaire : divers systèmes de sécurité, placés à différentes couches du modèle OSI, peuvent compliquer la chose. Pour une description plus détaillée de l’architecture OSI, de la sécurité informatique et de la sécurité des réseaux, consulter les annexes A page 60 et B page 66.

La sécurité est un aspect important dans ce projet, les données transmises étant relativement sensibles : les clients de ces instituts de microfinance se comptent par milliers.

On envisage dans cette section les différents mécanismes de contrôles disponibles, en partant des couches les plus basses du modèle OSI pour terminer par des techniques de plus haut niveau :
- le contrôle d’adresses MAC, WEP, WPA et WPA2 sont des technique de couche 2 (liaison de données) ;
- Le protocole IPsec fonctionne sur la couche 3, de réseau ;
- Le chiffrement SSL/TLS est une technique de couche 4 (transport).

4.6.1. Contrôle d’adresses MAC

Un contrôle à première vue très simple et très efficace est le contrôle d’adresse physique. Une adresse physique de carte réseau est un numéro d’identification unique au monde programmé par le fabricant avant la sortie de l’usine de la carte. Lorsqu’un client tente de se connecter, le point d’accès vérifie si l’adresse physique du lien est dans la liste des adresses autorisées par l’administrateur.

Si elle n’y est pas la demande de connexion est ignorée.

Ce système est intéressant mais pose deux problèmes. Il n’est pas très souple, car l’ajout d’un client nécessite la reconfiguration du point d’accès par l’administrateur. Et plus important, une carte Wi-Fi peut mentir sur son adresse physique, c’est-à-dire qu’elle peut très facilement être reprogrammée avec n’importe quel autre numéro. Il suffira dès lors à l’attaquant de connaître une adresse physique autorisée pour se faire passer pour elle (technique d’attaque connue sous le nom de *spoofing* et existant depuis longtemps en Ethernet câblé), et si le trafic du réseau n’est pas chiffré les adresses physiques autorisées sont rapidement identifiées.
4.6. SÉCURITÉ

4.6.2. Le protocole WEP

L’identification est une des fonctions de base de la sécurité informatique. Elle permet à des systèmes informatiques dialoguant entre eux de s’assurer de l’identité de leur(s) interlocuteur(s).

L’intégrité va souvent de pair, et permet à des systèmes informatiques de s’assurer que le ou les messages reçus n’ont pas été modifiés en cours de transmission.

La cryptographie symétrique est un concept très ancien. Elle est basée sur le principe d’un secret partagé, qu’on appelle la clé secrète. Le code de Jules César en est un exemple célèbre de plus de 2000 ans, où il suffit de décaler toutes les lettres du texte clair d’un certain même nombre de positions dans l’alphabet pour chiffrer le message, et de procéder à la transposition inverse pour retrouver le texte.

La connaissance de la clé secrète fait office de garantie de l’identité du correspondant, dès que le secret est connu d’un autre il n’y a plus aucune sécurité.

Le problème principal de la sécurité par clé secrète est le transfert confidentiel de ces clés, qui nécessite un canal sûr de transmission.

La technologie Wireless Equivalent Privacy (WEP) est le premier standard de sécurité conçu pour protéger les liaisons Wi-Fi. Elle utilise des clés secrètes partagées (PreShared Keys, PSK). Elle souffre donc d’abord du problème de partage des clés : l’utilisateur doit recevoir par un canal confidentiel cette clé et l’introduire dans son système informatique. Dès que la sécurité d’un des systèmes connaissant la clé est compromise, toutes les communications peuvent être interceptées.


Des agents américains du Federal Bureau of Investigation [21] ont effectué une démonstration publique d’attaque d’un réseau WEP, réussissant en trois minutes à retrouver les clés cryptographiques utilisées, grâce à des logiciels librement disponibles sur Internet (par exemple, aircrack¹).

4.6.3. Les protocoles WPA et WPA2

Conscient de ces problèmes, les fabricants décidèrent de réagir rapidement. Ils créèrent une norme nommée WPA (Wi-Fi Protected Access) reprenant une grande partie de la norme 802.11i, pas encore prête à l’époque. Deux modes de fonctionnement sont possibles, l’un avec un serveur d’authentification qui permet de distribuer périodiquement de nouvelles clés de chiffrement aux utilisateurs authentifiés (mode appelé WPA-Enterprise), l’autre (appelé WPA-Personal) fonctionne avec des clés pré-partagées (pre-shared keys), le mécanisme utilisé par WEP. Les données sont toujours chiffrées avec le code RC4,

¹http://www.cr0.net :8040/code/network/
mais cette fois-ci avec un vecteur d'initialisation plus grand (48 bits) et en combinaison avec un protocole de changement de clés automatique (Temporal Key Integrity Protocol, TKIP). Cela permet alors de parer aux attaques mises en place contre WEP.

Malheureusement, ce mode de fonctionnement présente lui aussi des faiblesses [23] : bien qu'il soit prévu dans le standard de définir autant de phrases de passe que de stations, en pratique la plupart des points d'accès utilisent une seule phrase de passe pour tout le réseau. Ce qui permet à n'importe quelle station ayant accès au réseau d'espionner ses voisines. Plus grave, une phrase de passe ne garantit un niveau raisonnable de sécurité qu'à partir de 20 caractères. La plupart des utilisateurs ne prendront pas cette peine et se limiteront à un mot.

La fonctionnalité d'intégrité de WEP devait elle aussi être remplacée : basée sur un code de vérification cyclique (Cyclic Redundancy Check), il était possible de modifier le message et de recalculer un CRC correct sans connaître la clé de chiffrement WEP.

Le protocole Message Integrity Check (MIC, aussi appelé l'algorithme Michael) a été mis en place, et fait appel à la clé secrète pour déterminer l'intégrité du message. Un compteur de messages a été ajouté, permettant aussi de se protéger contre les attaques par rejet (replay attacks) où une conversation entre deux hôtes qui a été enregistrée par un adversaire peut être réémise par celui-ci en se faisant passer pour un des deux hôtes, sans connaître la clé de chiffrement.

La mise en place de WPA en tant que sous-ensemble des fonctionnalités de 802.11i s'est faite pour deux raisons : d'abord, le développement de 802.11i pris beaucoup plus de temps que prévu (4 ans au final) alors que les soucis face à l'insécurité de WEP augmentaient de jour en jour, et ensuite parce que WPA utilise uniquement des mécanismes compatibles avec les matériels implémentant déjà WEP, c'est-à-dire qu'il était possible de mettre à jour les anciens matériels par la diffusion d'un nouveau firmware (logiciel embarqué sur le matériel). En règle générale seuls les matériels d'avant 2003 ont besoin d'être remplacés.

Malheureusement l'algorithme MIC n'est pas sans défaut : c'est simplement la meilleure solution qui pouvait être mise au point et permettre la compatibilité avec les appareils déjà sur le marché. Lors de l'utilisation de WPA il conviendra donc de veiller à utiliser de longues phrases de passe, et encore mieux, d'employer des chaînes de caractères hexadécimaux aléatoires.

WPA2 est la certification attribuée par le consortium Wi-Fi Alliance au matériel implémentant IEEE 802.11i. L'algorithme MIC y est remplacé par un autre type de Message Authentication Code (MAC) censé apporter une meilleure sécurité.

4.6.4. Chiffrement sur la couche réseau

IPsec est un standard de sécurisation du protocole IP [31, 32, 42], obligatoire dans la version 6 de celui-ci et optionnel dans sa version 4 (version actuelle utilisée sur Internet).

Il permet de chiffrer et d'autentifier tous les paquets IP. Il comprend d'une part des protocoles de chiffrement des communications (AH, et surtout ESP qui est le plus utilisé) et d'autre part des protocoles d'échanges de clés (IKE).

Un grand avantage de IPsec est qu'il permet de protéger indifféremment tous les types
de paquets (que le protocole de transport soit TCP ou UDP) et permet donc de sécuriser d’un coup tous les types de trafic.

Malheureusement sa mise en place n’est pas des plus simples. Le standard est trop complexe et peu clair : en pratique AH est rarement utilisé. Le principe de base de IPsec est la mise en place de *Security Associations* (SA) entre les systèmes communicants. Une SA détermine les paramètres d’une communication dans un sens (adresse source, adresse destination, protocole, algorithme, clé secrète, identifiant). Il faut donc deux SA pour que les communications entre deux stations soient sécurisés dans les deux sens.

En résumé, IPsec nécessite une bonne connaissance des mécanismes de sécurité, et sa mise en place n’est pas triviale. Par contre ce standard, lorsqu’il est correctement implémenté, offre un bon niveau de protection.

### 4.6.5. Sécurité sur la couche de transport

La société Netscape a mis au point en 1996 le protocole SSL 3 (Secure Socket Layer [25]) pour favoriser le commerce électronique. Dans son utilisation habituelle SSL permet de rendre confidentiel le trafic entre des clients et un serveur web, et de prouver l’identité du serveur aux clients. Mais SSL permet aussi d’authentifier les deux parties. Le standard TLS (Transport Layer Security [22]) s’est largement inspiré de SSL 3.

C’est une technologie dont la fiabilité n’est plus à prouver, très modulaire, et permettant donc l’emploi de nombreux algorithmes de chiffrement. Sa mise en place n’est pas triviale mais dans son mode le plus simple, authentifiant uniquement le serveur, elle réduit la complexité : les clients ne doivent pas être configurés individuellement pour pouvoir accéder au système. On trouvera en annexe des explications plus détaillées concernant la configuration de TLS.

Un autre mécanisme de sécurité est possible à ce niveau, c’est la mise en place d’un tunnel SSH. SSH (Secure Shell) a été initialement conçu comme remplacement sécurisé des applications telnet, rsh, rcp, qui permettaient d’exécuter des commandes sur une machine distante. Cependant SSH offre aussi d’autres fonctionnalités, comme les tunnels. Cette technique peut être utilisée dans la problématique qui nous intéresse : les clients peuvent créer un tunnel SSH vers le serveur, et toutes les données passant par le tunnel seront alors chiffrées. Le tunnel est associé sur la machine cliente à un numéro de port local, et à une adresse IP et un numéro de port sur la machine distante. Les clients, après avoir établi le tunnel, utilisent leur navigateur internet pour se connecter localement sur le port associé au tunnel (en pratique cela correspondra à l’adresse : http://127.0.0.1 ou plus simplement http://127.0.0.1). Le tunnel détectera la demande de connexion, chifférera les messages et les transmettra à l’autre extrémité du tunnel. Là, le message sera adressé à l’adresse de destination du tunnel. Dans le cas le plus simple ce sera aussi http://127.0.0.1, qui est une adresse spéciale identifiant la machine même (adresse dite de loopback). La réponse du serveur à cette connexion qui pour lui, semblera provenir d’un navigateur internet s’exécutant localement, sera retransmise par le tunnel au client. Il suffit alors de rajouter un pare-feu (firewall) sur le serveur, interdisant les connexions au service web autrement que depuis l’adresse de loopback 127.0.0.1, pour protéger efficacement le serveur.
4.6. SÉCURITÉ

<table>
<thead>
<tr>
<th>Couche</th>
<th>Technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>4. Transport</td>
<td>SSL/TLS</td>
</tr>
<tr>
<td>3. Réseau</td>
<td>-</td>
</tr>
<tr>
<td>2. Liaison de données</td>
<td>Filtrage MAC et WPA/WPA2 (avec des phrases de passe longues)</td>
</tr>
<tr>
<td>1. Physique</td>
<td>-</td>
</tr>
</tbody>
</table>

Tab. 4.4.: Solutions de sécurité recommandées

Le mécanisme SSH est efficace, et présente l’avantage de ne pas devoir toucher à la configuration du serveur web lui-même. Mais cela nécessite une reconfiguration des clients.

4.6.6. Conclusions

Il faut se rappeler que la sécurité est toujours un compromis, et il convient de se poser les questions suivantes [26] :
- Que veut-on sécuriser ?
- Quel degré de complexité est acceptable ?
- Système distribué ou centralisé ?
- Le niveau du système qui est sécurisé peut-il être contourné par une attaque à un autre niveau ?

En effet, un système parfaitement sûr n’existe pas, et un système très sûr peut être cher et compliqué. Les règles de bonne pratique nous proposent de multiplier les niveaux de sécurité, de minimiser les mécanismes “boîte noire” en lesquels il faut être aveuglément confiant, de simplifier l’usage du système et d’éduquer les utilisateurs du système.

Dans le cadre du problème qui nous intéresse, on souhaite sécuriser un système de télécommunications sans fil. Il s’agit d’empêcher les écoutes intempestives (confidentialité), de s’assurer qu’on est bien en communication avec le bon interlocuteur (authentification) et que le message n’a pas été corrompu (intégrité).

Le but étant de pouvoir déployer cette solution chez des clients qui n’ont pas forcément des connaissances approfondies en informatique, mais se positionner plus en tant qu’utilisateurs, la simplicité d’usage prend ici une grande importance.

La mise en place d’un filtrage MAC est facile dans le cas de liaisons point-to-point, elle peut aussi être envisagée dans le cas de point-to-multipoint.

Les protocoles WPA, ou mieux, WPA2 sont fortement recommandés, dans leur version Personal car celle-ci est plus simple à administrer (pas besoin de serveur d’authentification).

Le protocole IPsec est intéressant mais trop lourd à mettre en place. Peut-être que d’ici quelques années, avec l’adoption massive de IPv6, cette solution deviendra plus intéressante.

Le protocole TLS semble, lui, indispensable. Il allie simplicité d’emploi et robustesse. De plus il permet de sécuriser aussi bien le trafic radio que le trafic sur câble Ethernet (qui est sujet à d’autres types d’attaque).
5. Déploiement sur le terrain

5.1. Préparation de la mission

Comme je pars en échange Erasmus au second semestre et que la rentrée dans mon université d’accueil est fixée au 7 mars, je suis disponible tout le mois de février et c’est naturellement cette période qui est choisie pour mon départ. Le voyage durera trois semaines et me permettra de rencontrer les intervenants d’Aquadev Central Africa, une équipe dynamique d’une petite dizaine de personnes. J’aurai l’occasion de familiariser les responsables techniques avec les technologies sans-fil et de les sensibiliser aux aspects sécuritaires. Nous mettrons en place ensemble un système de télécommunications et évaluerons la performance obtenue, puis, si la mission se déroule bien, nous tenterons d’accomplir des objectifs secondaires tels que la mise en place de liaison par l’Internet en utilisant un fournisseur d’accès local et le réseau téléphonique de RwandaTel.

On trouvera en annexe ( G on page 81) les trois rapports de stage hebdomadaires réalisés sur le terrain pour le compte de l’ONG Aquadev.

5.1.1. Matériel

Je prépare avec Augustin Siaens des dossiers de demande de sponsoring chez tous les fabricants de matériel Wi-Fi représentés en Belgique. Malheureusement aucune de ces tentatives n’aboutit et nous nous retrouvons fin octobre toujours sans matériel.

Je contacte alors le Professeur Pierre Mathys pour lui demander s’il ne connaîtrait pas des ingénieurs travaillant dans l’une de ces entreprises, ce qui pourrait faciliter les contacts. Il me présente Patrik Bikar, ingénieur civil des télécommunications, qui travaille chez Cisco Systems Belgium. Celui-ci est enthousiasmé par le projet et grâce à lui nous obtenons quelque temps plus tard trois bridgends Cisco Aironet AIRBR340.

Manque alors des antennes et des câbles. Augustin, puis moi, nous présentons à des réunions du Réseau Citoyen, un groupe d’habitants de Bruxelles passionnés par les réseaux sans fil et les services qu’ils peuvent rendre à la société. Ceux-ci ont longuement expérimenté la fabrication d’antennes mais nous conseillent de nous adresser à Stefan Lambrechts, de Wireless Antwerpen, chez qui ils se fournissent en antennes.

Je me rend alors à Anvers pour acheter au nom d’Aquadev deux antennes paraboliques Pacific Wireless d’un gain de 24 dBi, ainsi que trois câbles d’antennes de 3m de long. La taille de ces antennes fut gênante pour le transport en avion, c’est un facteur à prendre en considération lorsqu’on doit transporter soi-même de telles antennes. La version avec réflecteur démontable aurait été beaucoup plus pratique, mais malheureusement elle était introuvable en Belgique.
5.1. PRÉPARATION DE LA MISSION

Tab. 5.1.: Budget de lien

<table>
<thead>
<tr>
<th>Type</th>
<th>Symbole</th>
<th>Puissance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Puissance d'émission</td>
<td>$P_t$</td>
<td>17 dB</td>
</tr>
<tr>
<td>Perte de propagation (onde libre)</td>
<td>$L_{dB}$</td>
<td>-95 dB</td>
</tr>
<tr>
<td>gain d'antenne à l'émission</td>
<td>$G_t$</td>
<td>+24 dB</td>
</tr>
<tr>
<td>gain d'antenne à la réception</td>
<td>$G_r$</td>
<td>+24 dB</td>
</tr>
<tr>
<td>perte dans le câble à l'émission</td>
<td>$L_t$</td>
<td>-0.66 dB</td>
</tr>
<tr>
<td>perte dans le câble à la réception</td>
<td>$L_r$</td>
<td>-0.66 dB</td>
</tr>
<tr>
<td>Puissance reçue</td>
<td>$P_r$</td>
<td>-31.2 dB</td>
</tr>
</tbody>
</table>

La longueur des câbles d'antennes fut difficile à choisir, par manque d’informations concernant la géographie des lieux. En effet il fallait faire un compromis entre facilité d’installation (plus le câble est grand plus on est souple pour le placement du bridge) et budget de lien (plus le câble est long plus les pertes dans le câble sont grandes). Finalement il s’est avéré que contrairement à ce qu’on m’avait dit, la qualité des câbles était telle que les pertes dues à ceux-ci étaient quasiment négligeables.

5.1.2. Budget de lien

On a déjà vu précédemment (section 4.3.2 page 31) la formule de budget de lien :

$$P_r = P_t - L_{dB} + G_t + G_r - L_t - L_r$$

Les bridges fournis par Cisco Systems Belgium ont une puissance d’émission de 50 mW, soit 17 dBm (les dBm sont des décibels où la puissance est exprimée en mW).

Les câbles font 0.22 dB/m et ont une longueur de 3 mètres, ce qui fait 0.66 dB de perte dans les câbles de chaque côté.

La distance des sites à relier sur le terrain est estimée à 2 km, et la perte en propagation d’onde libre est donc évaluée à 94,34 dB qu’on arrondit à 95 dB.

On a donc : $P_r = 17 - 95 + 24 + 24 - 2*0.66 = -31.2$ dB.

Les spécifications techniques des bridges Cisco Aironet AIRBR340 nous apprennent que la sensibilité à la réception est de -84 dB à 11 Mbps, nous disposons donc d’une large marge de 53 dB. Cependant cette marge peut être vite entamée si les antennes sont mal placées relativement à l’ellipsoïde de Fresnel.

5.1.3. Financement

Aquadev finance l’achat des antennes et des câbles, et après étude de notre dossier la Commission Universitaire au Développement sélectionne le projet pour financer les frais du vol en avion aller-retour. Mon logement sur place est pris en charge par Aquadev, ainsi que les autres coûts afférents au projet pouvant survenir sur place (matériel supplémentaire...).
5.2. SÉJOUR SUR PLACE

<table>
<thead>
<tr>
<th>Type</th>
<th>quantité</th>
<th>prix unitaire (en €)</th>
<th>total (en €)</th>
<th>Prise en charge</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bridges AirBr340</td>
<td>3</td>
<td>400</td>
<td>1600</td>
<td>Cisco Systems</td>
</tr>
<tr>
<td>Vol A-R Bruxelles-Kigali</td>
<td>1</td>
<td>1214</td>
<td>1214</td>
<td>CUD</td>
</tr>
<tr>
<td>Antenne PacWireless 24dB</td>
<td>2</td>
<td>95</td>
<td>190</td>
<td>Aquadev</td>
</tr>
<tr>
<td>3 mètres câble H-500</td>
<td>3</td>
<td>18</td>
<td>54</td>
<td>Aquadev</td>
</tr>
<tr>
<td>Logement à Kigali</td>
<td>21j</td>
<td>9</td>
<td>189</td>
<td>Aquadev</td>
</tr>
<tr>
<td>Visa</td>
<td>1</td>
<td>62</td>
<td>62</td>
<td>Aquadev</td>
</tr>
<tr>
<td>Rallonge électrique (20m)</td>
<td>1</td>
<td>34</td>
<td>34</td>
<td>Aquadev</td>
</tr>
<tr>
<td>Câble Ethernet (100m) + connecteurs</td>
<td>1</td>
<td>30</td>
<td>30</td>
<td>Aquadev</td>
</tr>
<tr>
<td>Agences de douane au Rwanda</td>
<td>1</td>
<td>136</td>
<td>136</td>
<td>Aquadev</td>
</tr>
<tr>
<td>Douane belge</td>
<td>1</td>
<td>40</td>
<td>40</td>
<td>Aquadev</td>
</tr>
<tr>
<td>Boîtier pour bridge</td>
<td>1</td>
<td>20</td>
<td>20</td>
<td>Aquadev</td>
</tr>
<tr>
<td>Frais médicaux (vaccins+prophylaxie)</td>
<td>1</td>
<td>150</td>
<td>150</td>
<td>Jérôme / Mutuelle</td>
</tr>
<tr>
<td>Frais personnels sur place</td>
<td>1</td>
<td>200</td>
<td>200</td>
<td>Jérôme</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td></td>
<td>3919€</td>
<td></td>
</tr>
</tbody>
</table>

Tab. 5.2.: Budget du projet

Fig. 5.1.: Les bureaux de Aquadev Central Africa à Kigali

5.2. Séjour sur place

Dès mon arrivée à l’aéroport de Kigali en fin de journée (samedi 5 février), Adrien Kabale, directeur de Aquadev Central Africa, vient à ma rencontre à la récupération des bagages pour m’aider à passer la douane. Les antennes restent bloquées mais l’électronique ressort avec nous. Arthur, le responsable informatique, est aussi présent. Nous nous dirigeons vers mon logement situé à l’étage au-dessus des bureaux installés dans une ancienne villa, dans le quartier de la présidence (Kakiro).

J’ai droit à une visite guidée de Kigali le lendemain, et je rencontre le reste de l’équipe le lundi matin.
5.3. Repérage des sites sélectionnés

5.3.1. Kigali Institute of Science, Technology and Management (KIST)

Le KIST est l'école d'ingénieurs de la capitale. L'IMF Inkingi gère l'argent des étudiants sur le campus avec sa première agence informatisée. Non loin des guichets se trouve une petite tour de télécommunications sur laquelle sont déjà fixées plusieurs antennes. C'est cette tour qui est visible depuis le siège d'Inkingi. Cependant de grands arbres sont proches de la tour, et il faudra donc monter relativement haut pour établir une bonne liaison. Mais le KIST étant situé en haut d'une colline il ne devrait pas y avoir d'autres problèmes.

5.3.2. Siège Inkingi

Le siège d’Inkingi est installé dans un immeuble de trois étages situé dans le quartier Swahili. Ce quartier est constitué d’habitations au niveau du sol, la plupart sans étage, et la surface est celle d’une plaine en légère pente. Les conditions sont idéales pour placer une antenne.

Malheureusement l’informatisation du siège a pris du retard et leurs guichets utilisent toujours le papier. Le projet est en avance de quelques mois. De plus le responsable de Inkingi qui était intéressé par le projet ne travaille plus là et son successeur montre moins d’intérêt.

Tout cela ne nous empêchera pas d’effectuer une démonstration de l’accès à distance.

5.4. Préparation du matériel

Après la sortie en douane des antennes le mardi (8 février) suivant mon arrivée nous réalisons un test rapide du système dans les bureaux. Tout fonctionne parfaitement, le matériel ne semble pas avoir souffert du voyage.

Les câbles d’antennes ne mesurant que trois mètres il est nécessaire de placer un bridge à l’extérieur. Or les bridges dont nous disposons n’ont pas été conçus pour cela. Malgré les températures tropicales les pluies sont fréquentes au Rwanda. Il nous faut donc concevoir un boîtier de protection pour le bridge, en m’inspirant de ce que les gens du Réseau Citoyen m’ont montré à Bruxelles. Un artisan nous fabrique un boîtier métallique dans lequel placer le bridge.

5.5. Déploiement du matériel

Nous décidons de fixer d’abord l’antenne du KIST car c’est la moins accessible, puis d’ajuster celle du siège de Inkingi.

En arrivant au KIST nous avons une mauvaise surprise : l'accord qui avait été donné à Arthur ne venait pas de la personne faisant autorité en la matière. Il nous faudra plusieurs jours pour réussir à rencontrer les différents intervenants dans le processus de décision.
Fig. 5.2 : La tour de télécommunications du KIST
Fig. 5.3.: Vue du KIST depuis Nyamirambo
5.6. **TESTS DE LIAISON**  

CHAPITRE 5. **SUR LE TERRAIN**

En parallèle, Arthur, Bonny un stagiaire du KIST chez Aquadev et moi-même installons déjà l’antenne de Nyamirambo. Le site est facilement accessible et il suffit de placer un mât sur le balcon du bâtiment.

**Fig. 5.4.** Le siège d’INKINGI

Après avoir obtenu l’autorisation d’accès à la tour j’y monte pour évaluer la hauteur nécessaire où placer l’antenne. Malheureusement des arbres qui m’étaient invisibles jusque là sont dans le chemin et il faudra monter plus haut que prévu.

L’antenne est fixée entre dix et quinze mètres de haut et nous posons les câbles nécessaires pour l’alimentation électrique et la connexion au réseau Ethernet local du guichet. Les tests effectués montrent que le matériel installé au KIST fonctionne parfaitement.

**Fig. 5.5.** Vue de la tour de télécommunications du KIST et de l’antenne Wi-Fi installée.

5.6. **Évaluation de la qualité de la liaison**

Nous nous rendons à Nyamirambo pour activer le matériel que nous y avions laissé. Tout marché du premier coup, il a suffit d’allumer le bridge. Des transfert de fichiers nous
permettent d’évaluer la liaison à plus de 400 kB/s efficaces (soit 3,1 Mbps). Le logiciel AdBanking est facilement accessible et on croirait être aux guichets du KIST.

Arthur effectue une démonstration à destination des responsables d’Inkingi.

Au niveau de la sécurité, je constate à l’aide d’un scanner de port (port scanner, nmap) que deux possibilités existent au niveau de la connexion au serveur web.


```
POST /login/main_login.php HTTP/1.1
Host : 192.168.0.1
User-Agent : Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.7)
   Gecko/20041013 Firefox/0.9.3 (Ubuntu)
Accept :
text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,
text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Language : en-us,en;q=0.5
Accept-Encoding : gzip,deflate
Accept-Charset : ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive : 300
Connection : keep-alive
Cookie : PHPSESSID=5e5fd185231c10dd8e9671bab7099c2b
Content-Type : application/x-www-form-urlencoded
Content-Length : 68

login=demo&pwe=dép&prochain_ecran=login_check&enterButton=ValiderHTTP/1.1
200 OK
```

```
Date : Tue, 15 Feb 2005 13:22:44 GMT
Server : Apache/1.3.23 (Unix) (Red-Hat/Linux) mod_ssl/2.8.7 OpenSSL/0.9.6b
DAV/1.0.3 PHP/4.2.0 mod_perl/1.26
X-Powered-By : PHP/4.2.0
Expires : Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control : no-store, no-cache, must-revalidate, post-check=0,
pre-check=0
Pragma : no-cache
Connection : close
Transfer-Encoding : chunked
Content-Type : text/html
48c
```

<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd"><html>

54
5.6. TESTS DE LIAISON  

La deuxième possibilité est l'utilisation du service HTTPS sur port 443, qui place HTTP sur un canal de transmission SSL/TLS. Il suffit pour cela d'accéder au serveur par l'adresse https://192.168.0.1 au lieu de l'adresse habituelle http://192.168.0.1. Une capture de trafic réalisée dans cette situation montre que la procédure d'identification avec le serveur est alors chiffrée ; il n'est plus possible de récupérer les noms d'utilisateur et mots de passe transitant sur le réseau. Mais les pages web ne sont pas toutes chiffrées : la connexion repasse en mode non-sécurisé sur port 80. C'est probablement causé par des références dans le code HTML de AdBanking vers des pages en mode HTTP. Si c'est bien la cause du problème cela devrait être relativement facile à corriger.

Consulter pour plus d'explications au niveau de la sécurité l'annexe relative à ce sujet.
5.7. Tentative de connexion par Internet

Encouragés par le succès de la technologie mise en œuvre, Arthur et moi commençons le lendemain les préparatifs de tests pour une liaison par Internet. Le responsable de l'IMF Coopedu, informatisé depuis près d'un an, est approché pour lui présenter notre idée.

Plusieurs possibilités s'offrent à nous :
- connexion directe du serveur à Internet ;
- redirection de port ;
- réseau privé virtuel.

La connexion directe est la plus simple et la plus évidente. Le serveur dispose alors d'une adresse IP publique et il suffit de s'y connecter par Internet comme on le ferait sur le réseau local. Cette méthode pose le problème d'exposer directement le serveur aux attaquants sur Internet.

La deuxième solution suppose que le réseau local du serveur soit relié à Internet par un routeur. Il reste alors à configurer ce routeur pour rediriger les demandes de connexion sur port 80 (HTTP) sur le réseau local au serveur AdBanking. Ainsi seul le service web du serveur est exposé sur Internet.

La troisième solution consiste à configurer le routeur et les systèmes clients pour créer un tunnel sur Internet. Les machines s'adressent alors les unes les autres par des adresses numériques privées et leurs tables de routage associent les adresses privées de l'autre réseau au tunnel. Cela permet alors d'accéder à toutes les machines du réseau, et à tous leurs services.

Cette dernière solution est lourde à mettre en œuvre (configuration des deux côtés) mais représente qualitativement un équivalent virtuel de la liaison par antennes.

Nous passons plus de temps qu'initialement prévu à la préparation de ces essais. En effet il est nécessaire de télécharger un logiciel\(^1\) permettant d’assurer la redirection de

\(^1\)Nous avons choisi WinGate ( http://www.wingate.com ).
ports sous Windows, ce système d'exploitation ne permettant pas cela par défaut. Le fichier étant assez volumineux nous n'avons pas réussi à le télécharger sur la liaison ISDN du bureau Aquadev Central Africa et avons dû passer par un cybercafé.

Finalement le test d'accès au serveur AdBanking d'Aquadev réussit très bien et le test chez Coopedu est tout aussi concluant. Cependant la vitesse des connexions Internet disponibles limite fortement l'utilité du système : dès que plusieurs clients se connecteront au serveur les temps de réponse vont ralentir. Si une connexion téléphonique est acceptable par client, au niveau du serveur ce n'est pas acceptable pour une utilisation à grande échelle (cinq postes seraient sans doute un maximum pour un serveur connecté par téléphone).

5.8. Fabrication locale d'antennes

Il est possible de fabriquer soi-même un guide d'onde. Ce n'est pas une antenne à proprement parler mais un tel montage permet cependant de concentrer l'énergie rayonnée par une antenne, en l'occurrence un simple bout de fil métallique, dans une direction donnée, un peu comme une antenne parabolique.

L'antenne est constituée par un connecteur d'antenne type N femelle auquel on soude une tige de 3,1 cm.

Le guide d'ondes circulaire a la forme d'un cylindre ouvert à une extrémité. Le diamètre optimal est inférieur à 92,796 mm et la longueur associée vaut 485,724 mm. L'émetteur doit être fixé à 48,572 mm du fond fermé. La longueur de l'élément rayonnant (l'antenne à proprement parler) est idéalement de 30,685 mm.

En pratique on visera un diamètre de 9 cm, une longueur de 50 cm et un émetteur à 4,8 cm du fond de 3,1 cm de haut, ce qui donne une certaine marge d'erreur. Les dimensions les plus critiques sont le diamètre du guide d'onde et la longueur de l'antenne (le fil métallique).

Par manque de temps et surtout de matériel, les connecteurs d'antenne type N femelle étant rares au Rwanda, nous n'avons pu tester cette solution et la comparer aux antennes Pacific Wireless utilisées. Elle était pourtant intéressante, car la fabrication locale d'un guide d'onde dans un atelier de travail du fer n'aurait pas coûté grand-chose.

\footnote{Cette situation a changé avec Windows XP Service Pack 2 qui intègre un Firewall permettant la redirection de port. Cependant aucune des machines que j'ai utilisées au Rwanda ne disposait de cette version de Windows.}
6. Conclusions

Excepté la fabrication d’antenne sur place, que j’avais proposée personnellement, les objectifs du déplacement sur le terrain ont tous été remplis. Le projet est un succès pour les responsables de l’ONG car il a permis de familiariser les informaticiens locaux avec ce genre de technologies, et permettra de choisir en connaissance de cause les techniques qui seront amenées à être déployées sur le terrain.

Je reviendrai encore une fois sur les situations où la technologie Wi-Fi est intéressante : liaison en ligne de vue dégagée, et respect des conditions de Fresnel, combinée avec une inadéquation de l’offre des fournisseurs d’accès à l’Internet. De manière empirique on emploiera des mâts et on s’assurera qu’il n’y a ni arbres ni bâtiments proches de la position de l’antenne. La qualité de la liaison permet de plus d’envisager l’utilisation d’applications annexes, et ce de manière très sécurisée si WPA2 est implémenté : serveur de fichiers, partage de connexion Internet, VoIP (Voice over IP, téléconférences).

Il faudra toutefois se renseigner au préalable au niveau administratif : l’installation d’antennes Wi-Fi et la mise en place de liaisons radio est souvent réglementée et des frais supplémentaires sont à prévoir.

J’espère avoir suffisamment attiré l’attention sur la problématique de la sécurité. Il est certain qu’une bonne politique de sécurité nécessite du temps et de l’énergie, et que cela peut paraître un gaspillage de moyens. Mais il est tout aussi certain que l’incident le moins génant est celui qui n’arrive pas. Mieux vaut donc prévenir que guérir, surtout dans un secteur où la confidentialité et la sécurité ont beaucoup d’importance pour les clients. Si un incident grave survenait et devenait connu du public l’IMF concernée pourrait rencontrer de sérieuses difficultés quand à son avenir. L’état actuel de sécurité des systèmes informatiques déployés pourrait être facilement amélioré par l’utilisation d’une technologie appropriée (SSL/TLS), ne nécessitant pas énormément de travail.

Le secteur des télécommunications est toujours en plein essor technologique : les accès rapides à l’Internet, facturés au mois et non plus au temps d’utilisation, commencent à se mettre en place (ADSL à Kigali). La norme IEEE 802.16, plus connue sous le nom de WiMax, devrait faire son apparition sur le marché mondial d’ici un an. Des essais du matériel sur le terrain se font déjà actuellement aux États-Unis. Ce système permet de couvrir de larges étendues grâce à un réseau de stations de base, de manière similaire aux réseaux GSM. Cela pourrait apporter une couverture Internet aux pays en voie de développement car un tel réseau est moins cher qu’un déploiement national d’ADSL, cette dernière technologie restant surtout réservée aux grandes villes.

Ces technologies permettraient une connexion à l’Internet à un prix moindre qu’actuellement. Les problèmes de sécurité resteraient à peu près les mêmes et à ce titre, ce mémoire devrait toujours être d’actualité car il présente des technologies de chiffrement permettant de sécuriser des liaisons par l’Internet (comme cela a été fait temporairement
CHAPITRE 6. CONCLUSIONS

avec l’IMF Coopedu par modem téléphonique).

D’un point de vue plus personnel je suis très content d’avoir choisi ce projet, et des résultats obtenus. J’ai rencontré beaucoup de gens d’horizons différents, que ce soit en Afrique ou en Belgique, et j’ai souvent été amené à devoir trouver des solutions par moi-même à des problèmes pratiques, que ce soit au niveau du financement, du transport des antennes, ou des négociations avec les administrations (rwandaise et belge).

Je crois que ce projet m’a apporté beaucoup d’expérience en termes de gestion de projet, et ce sans délaisser le côté technique. J’ai une connaissance nettement meilleure des ondes radio et des communications sans fil numériques qu’auparavant, ce qui sort peut-être un peu du cadre strict des études d’ingénieur informaticien, mais m’intéresse beaucoup. Et l’aspect sécurité et configuration des réseaux m’a ramené sur un terrain plus familier.

La coopération avec Aquadev s’est très bien déroulée, il faut savoir travailler de façon autonome mais cela n’est pas forcément un inconvénient. La liberté d’action qui en découle m’a responsabilisé vis-à-vis du projet et m’a motivé. Je recommande donc à tout(e) autre étudiant(e) ce genre de sujet si l’occasion venait à se représenter, ce qui n’est pas impossible d’après les échos que j’en ai eu chez Aquadev.
A. Les réseaux informatiques

Ce qu'on appelle réseaux informatiques forme un ensemble assez vaste, faisant intervenir des technologies différentes à plusieurs niveaux. C'est pourquoi, afin d'y voir plus clair, le standard OSI (Open Standard Institute) fut développé. Il définit 7 couches, chacune communicant avec sa ou ses voisines immédiates. Une couche fournit des services bien définis à la couche qui lui est immédiatement supérieure et fait appel aux services fournis par la couche inférieure.

Ainsi on peut changer complètement la façon dont on fournit un certain service dans une couche sans devoir toucher aux autres couches tant que la manière dont le service est fourni reste la même : par exemple lors de l'utilisation d'un ascenseur l'utilisateur appuie sur le bouton correspondant à l'étage où il souhaite se rendre, et cette interface est la même quelle que soit le moteur faisant fonctionner l'ensemble.

Le modèle OSI est cependant plus un modèle de réflexion qu'une réalité pratique.

On utilise fréquemment le modèle TCP/IP qu'on peut faire correspondre à certaines couches du modèle OSI.

Les couches les plus importantes sont les plus basses.

A.1. Le modèle ISO

A.1.1. La couche physique

La couche physique définit toutes les propriétés physiques (électriques, magnétiques et mécaniques) des matériels employés. Ainsi les câbles Ethernet et leurs connecteurs font partie de la couche physique. Elle définit aussi par exemple la modulation des informations, c'est-à-dire la manière dont sont converties en signaux physiques les valeurs binaires logiques.

C'est à ce niveau qu'opèrent les répéteurs et les hubs.

A.1.2. Diffraction de données

Elle permet de transmettre des données d'un équipement réseau à un autre et offre des mécanismes de détection et de correction d'erreur : contrôle d'accès au canal de communication (protocole Medium Access Control, MAC) dans le cas des réseaux Ethernet, ce qui permet à chaque station connectée sur le réseau d'obtenir un temps de parole, et contrôle d'erreur avec retransmission du ou des messages erronés (protocole Link Layer Control, LLC, toujours dans le cas des réseaux Ethernet).

On constatera dans l'exemple ci-dessus que la couche transport correspond dans ce cas à deux protocoles. (Il n'y a donc pas toujours une correspondance univoque protocole
A.1. LE MODÈLE ISO

ANNEXE A. LES RÉSEAUX INFORMATIQUES


Chaque équipement dispose d’une adresse définie au moment de la fabrication, qu’on
appelle l’adresse physique.

C’est à ce niveau qu’opèrent les switches et les bridges.

A.1.3. La couche réseau

La couche réseau permet le bon acheminement des messages d’un point du réseau à un
autre. C’est donc principalement le routage et l’adressage des systèmes qui sont concernés
ici 1. Les protocoles les plus connus sont Internet Protocol (IPv4 ou IPv6), ICMP, et en
ce qui concerne le routage : BGP, EIGRP, RIP et OSPF. L’adressage est logique et choisi
par l’administrateur. De plus il est hiérarchique : on peut grouper les adresses logiques
en adresses de réseaux.

Les périphériques fonctionnant à cette couche-ci sont les routeurs ; ils aiguillent les
paquets de données sur ce qu’ils estiment être le meilleur chemin vers leur destination.

A.1.4. La couche transport

Cette couche fournit le service de transmission de données selon une qualité de service
garantie. Ainsi le protocole IPv4 définit deux mécanismes de transport selon la qualité
souhaitée. Le premier, Transmission Control Protocol ou TCP, permet le transfert de
données avec accusés de réception et tentatives de retransmission en cas de perte de
données. C’est un service orienté connexion. L’autre possibilité est le User Datagram
Protocol, optimisé pour la vitesse de transfert et ne contrôlant pas la bonne réception,
sans retransmission de paquets. Cela est utilisé notamment pour beaucoup d’applications
multimédia (Vidéo, Audio).

A.1.5. La couche session

Mécanisme de contrôle de la couche transport : permet la mise en place, la surveillance
et l’arrêt d’une connexion de transport comme TCP.

Mécanismes permettant aux applications complexes d’établir, de contrôler, de redém-
marrer et d’arrêter des sessions application. Par exemple la connexion et l’identification
d’un utilisateur sur un réseau d’entreprise permet par la suite aux applications démarrées
par l’utilisateur d’accéder à certaines ressources du réseau. Le protocole le plus employé
est Common Internet File System / Server Message Block (CIFS/SMB) qui est utilisé
sur les domaines Microsoft Windows.

Il existe aussi Kerberos.

A.1.6. La couche présentation

Elle se charge de convertir les formats de données employés par une machine en formats
compréhensibles par le ou les interlocuteurs. Un des plus connus est MIME (Multipart

1Les autres fonctionnalités de couche 3 sont la segmentation et la déssegmentation, le contrôle de flux
et le contrôle d’erreur.
Internet Message Extension) permettant l’envoi de fichiers par email entre ordinateurs sous Windows, MacOS ou Unix. En pratique cependant c’est bien souvent l’application qui se charge elle-même de la conversion si nécessaire.

A.1.7. La couche d’interface application

Cette couche est la dernière du modèle OSI, et beaucoup de protocoles en font partie : HTTP pour la consultation de sites web, POP3/IMAP pour la réception de messages électroniques et SMTP pour l’envoi, mais aussi SSH, DNS, FTP, SNMP...

Toutes les applications qui implémentent un de ces protocoles peuvent alors dialoguer entre elles et exploiter les fonctionnalités fournies par eux. La plupart des protocoles sont basés sur un modèle client-serveur mais il existe des protocoles d’égal à égal (peer to peer) où aucune machine du réseau n’est privilégiée : BitTorrent permet notamment le transfert rapide de gros fichiers très demandés, Skype permet la téléphonie sur Internet, GnomeMeeting la vidéoconférence...

A.2. Le modèle TCP/IP

On parle de pile de protocoles ou encore de pile réseau lorsqu’un ensemble de protocoles assurent les fonctions d’une partie des couches du modèle OSI. Le protocole IPv4 assure par exemple les services de couche 3 et 4, indépendamment des couches 1 et 2. C’est cette indépendance du matériel qui a permis le succès considérable du réseau Internet.

Le but au moment de la conception était d’établir des protocoles qui permettraient l’interfonctionnement de réseaux existants, utilisant tous déjà des protocoles fermés. Le modèle OSI était en cours de développement simultanément.

Le Protocole Internet (IP) définit une série de protocoles. On citera notamment ICMP (Internet Control Message Protocol) pour le contrôle de flux et DHCP (Dynamic Host Control Protocol) pour la configuration automatique des paramètres réseaux au niveau 3, et TCP et UDP dont on a déjà parlé pour le niveau 4.

Ensuite toute une série de protocoles, qui ne font pas à strictement parler du protocole IP, furent définis pour fournir des services aux applications. Ce sont les protocoles cités au niveau 7. Ainsi l’ensemble des protocoles utilisés pour accéder aux ressources de l’Internet correspondent aux couches 3 à 7 du modèle OSI.
A.3. L’identification sur les réseaux

Chaque couche peut présenter des mécanismes d’identification. Le mécanisme le plus connu est l’adressage IP : chaque machine connectée au réseau dispose d’une adresse numérique codée sur 4 octets, unique sur le réseau. Lorsque cette adresse est unique au monde elle est dite publique ; sinon elle est dite privée. Une adresse IP est un mécanisme d’identification de couche 3 (couche réseau).

Au niveau inférieur (couche 1 et 2) le système habituel est Ethernet. Les stations disposent chacune d’une adresse physique\(^2\) théoriquement unique\(^3\) codée sur 24 octets. Le protocole MAC (Medium Access Control) permet d’établir la correspondance.

Plus haut, au niveau transport un mécanisme de ports est mis en œuvre. Les ports sont des numéros allant de 1 à 65535 permettant d’établir autant de communications dans chaque transport\(^4\).

Ce mécanisme de ports permet donc à plusieurs applications de se partager toute liaison de télécommunication disponible au système informatique, et de communiquer simultanément. C’est grâce à cela qu’il est possible de recevoir des emails tout en naviguant sur le web et en téléchargeant des fichiers. Certains ports sont associés à des services célèbres.

Une communication IP est donc déterminée par les port et adresse utilisés sur chacune des deux machines. Les ports de 1 à 1024 sont réservés à des services serveur (ils sont dits privilégiés et sont souvent réservés d’accès à l’administrateur) ; les applications clientes correspondantes (par exemple un navigateur web) utilisent n’importe quel port libre supérieur à 1024.

\(^2\) souvent appelée MAC address.

\(^3\) il est possible de les reconfigurer logiciellement.

\(^4\) Il est donc théoriquement possible d’établir simultanément 65535 connexions TCP en même temps que 65535 transports UDP (UDP n’établit pas à proprement parler de connexion).
A.4. Application de ces principes au projet

A.4.1. Réseau local Ethernet

Décrit dans la norme IEEE 802.3, Ethernet est un standard qui définit des couches de bas niveau 1 et 2 de manière à rendre interopérables les matériels réseaux de différents fabricants. C’est ce qui explique en partie le succès d’Ethernet : la certitude de pouvoir utiliser ensemble des matériels de différents fabricants.

A.4.2. Fonctionnement des bridges

Un bridge est un équipement réseau électronique capable d’être connecté simultanément sur deux réseaux respectants des normes de couche 2 différentes.

Le principe d’un bridge Ethernet - Wi-Fi est de recevoir des paquets sur ses deux interfaces, d’analyser la couche 2 du paquet correspondant à l’interface de réception et de réécouter une couche 2 avec les protocoles adaptés à l’autre interface, puis d’émeter ce paquet sur cette autre interface. Ainsi on ne touche pas aux niveaux plus élevés et ceux-ci ne peuvent pas remarquer cette manipulation. Le système est donc transparent et d’une grande facilité de mise en œuvre du point de vue informatique : il suffit de correctement configurer les deux interfaces du bridge sur chacun des réseaux, et parfois cela peut même être fait de manière automatique.

A.4.3. Serveur Internet public

Un serveur est un système informatique sur lequel tourne un ou plusieurs logiciels implémentant la partie serveur d’un protocole applicatif (couché 7). Par exemple un serveur HTTP est un logiciel pouvant répondre de manière appropriée aux messages qu’envoient les navigateurs web (Internet Explorer, Mozilla Firefox...).

Un serveur Internet public dispose d’une adresse publique sur le réseau Internet. Il existe en effet deux types d’adresses. Les adresses publiques sont uniques \(^5\) tandis que les adresses privées sont souvent utilisées sur des réseaux d’entreprises ou de particuliers pour des machines non destinées à être exposées directement à Internet.

Lors d’une connexion à Internet par un fournisseur d’accès une adresse IP publique est temporairement attribuée à la machine. Cette adresse peut très bien changer à la connexion suivante. Dans le cadre de notre projet il faut une méthode pour pouvoir accéder de façon transparente au serveur. C’est possible par l’utilisation d’un service de DNS dynamique\(^6\). Un petit programme contacte un serveur DNS lors de l’établissement de la connexion à Internet pour communiquer la nouvelle adresse IP. Ce mécanisme est aussi utilisé dans les situations suivantes.

\(^5\)Et distribuées par un organisme officiel, le IANA.
A.4.4. Redirection de port

Nous avons vu dans le paragraphe consacré à l'identification sur les réseaux qu'à un programme en cours d'exécution communiquant par le réseau correspondent un ou plusieurs ports.

AdBanking est un logiciel qui utilise le serveur web Apache. Le port utilisé est donc tout naturellement le port HTTP (80). Lorsque les utilisateurs veulent accéder à AdBanking ils introduisent dans leur navigateur web l'adresse IP numérique du serveur (par exemple http://192.168.0.1) et une tentative de connexion est automatiquement établie sur le port 80 de la machine sélectionnée.

Si nous voulons protéger le serveur web de tentatives d'attaques, ou utiliser une connexion internet existante déjà partagée sur le réseau local par un matériel spécialisé (soit un ordinateur dédié à cette tâche soit un routeur électronique), il faut utiliser la redirection de port pour rendre le serveur accessible. En effet celui-ci dispose alors d'une adresse IP privée, injoignable au travers d'Internet. Le routeur partageant la connexion Internet établit des tables de correspondances et permet ainsi de réécrire les paquets IP qu'il voit passer. On va l'utiliser pour rediriger les tentatives de connexions sur son adresse publique au port HTTP vers le serveur AdBanking local.

Pour la sécurité on activera convenablement la fonctionnalité SSL permettant un service HTTPS (443/tcp) à la place de HTTP.

A.4.5. Réseau privé virtuel (VPN)

Cette technologie met en place des liaisons de données sécurisées sur Internet, sortes de tunnels indéchiffrables aux observateurs extérieurs grâce à des techniques de cryptographie. Les ordinateurs ayant accès à ces liaisons sécurisées les modélisent comme des cartes réseaux physiques virtuelles, avec leurs adresses IP propres. C'est un mécanisme mis en place dans les couches 3 et 4, les couches supérieures ne subissent pas de modification et l'utilisateur a l'équivalent d'une liaison câblée privée avec les autres systèmes informatiques participant au réseau privé virtuel.

Cependant cette technologie est lourde à mettre en place, les outils cryptographiques sont complexes à manier et la sécurité du système est alors rapidement compromise.

---

*Celles-ci prennent bien souvent la forme de connexions sur tous les ports disponibles afin de déterminer la présence d'autres services, peut-être plus vulnérables, afin d'en exploiter les failles de sécurité éventuelles.*
B. La sécurité informatique

La sécurité informatique [26] est un sujet suscitant beaucoup d’intérêt. L’utilisation de l’Internet pour accomplir des actes bancaires tels le commerce électronique et le home banking en est une bonne raison. Mais d’autres besoins existent : citons par exemple les signatures numériques, l’identification (à ce sujet Bill Gates a annoncé à Bruxelles que son logiciel MSN Messenger permettra l’identification des utilisateurs grâce à la carte d’identité belge électronique), la protection de la vie privée (chiffrement des emails)...

B.1. Les différents aspects

La sécurité informatique est un domaine de l’informatique qui propose des techniques pour répondre à plusieurs besoins fondamentaux :

1. la confidentialité
2. l’identification
3. l’intégrité

Pour illustrer ces notions on emploiera par la suite les personnages classiques des scénarios de sécurité informatique : Alice et Bob sont les utilisateurs ou plus généralement les systèmes informatiques qui tentent légitimement d’entrer en communication, Oscar est le personnage qui tente de profiter des failles de sécurité.

La confidentialité, c’est la garantie que seuls Alice et Bob ont accès aux messages échangés. En d’autres mots, Oscar ne doit pas avoir accès aux messages échangés.

L’identification, c’est la garantie pour Alice que le message qu’elle a reçu provient bien de Bob (et réciproquement). Ainsi Oscar ne peut ni se faire passer pour Alice auprès de Bob ni pour Bob auprès d’Alice.

L’intégrité, c’est la garantie que les messages échangés entre Alice et Bob n’ont pas été modifiés en cours de route. Donc l’intégrité permet de détecter toute tentative par Oscar de modifier les messages échangés entre Alice et Bob.

L’intégrité va souvent de pair avec la confidentialité.

Nous voulons établir ces trois fonctionnalités de sécurité dans le système mis en place.

B.2. Outils mathématiques

La cryptographie est le domaine des mathématiques qui fournit les outils nécessaires à la sécurité informatique. Nous n’entrerons pas en profondeur dans le sujet ; cette section se veut un aide-mémoire rapide permettant de comprendre de quoi l’on parle.
B.2.1. La cryptographie symétrique

C'est la forme la plus ancienne de cryptographie. L'exemple le plus célèbre est probablement le code de Jules César. Ce militaire romain devait parfois envoyer des messages par plusieurs porteurs sur de longues distances. Les messages risquaient d'être interceptés par les porteurs eux-mêmes ou par un ennemi capturant le porteur. La confidentialité était donc nécessaire.

Tab. B.1: Correspondances des lettres pour le code de Jules César avec n=5.

<table>
<thead>
<tr>
<th>en clair</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
<th>f</th>
<th>g</th>
<th>h</th>
<th>i</th>
<th>j</th>
<th>k</th>
<th>l</th>
<th>m</th>
</tr>
</thead>
<tbody>
<tr>
<td>chiffré</td>
<td>v</td>
<td>w</td>
<td>x</td>
<td>y</td>
<td>z</td>
<td>a</td>
<td>b</td>
<td>c</td>
<td>d</td>
<td>e</td>
<td>f</td>
<td>g</td>
<td>h</td>
</tr>
<tr>
<td>en clair</td>
<td>n</td>
<td>o</td>
<td>p</td>
<td>q</td>
<td>r</td>
<td>s</td>
<td>t</td>
<td>u</td>
<td>v</td>
<td>w</td>
<td>x</td>
<td>y</td>
<td>z</td>
</tr>
</tbody>
</table>

| chiffré | i | j | k | l | m | n | o | p | q | r | s | t | u |

Jules César utilisa alors un code très simple : la transposition. À chaque lettre du texte en clair on fait correspondre la lettre de l’alphabet qui la suit de n positions. La confidentialité du message repose sur la connaissance de ce nombre n, qu’on appelle de manière générale une clé secrète. Tant qu’Alice et Bob sont les seuls à connaître la clé secrète, le message dispose d’une certaine confidentialité car ils sont les seuls à pouvoir lire le message. Comme ils sont les seuls à connaître la clé cela apporte de facto la preuve de l’identité des intervenants. Si le message venait à être modifié par Oscar, modifiant une ou plusieurs lettres au hasard du texte chiffré, Alice ou Bob le constaterait en déchiffrant le message car il y aurait des fautes d’orthographe (en supposant que le message n’en contenait pas au départ).

Tab. B.2: Exemple de texte chiffré avec le code de César (n=5).

<table>
<thead>
<tr>
<th>Ce texte est très mal protégé.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Xz ozsoz zno omzn hvg kmjozbx.</td>
</tr>
</tbody>
</table>

En pratique le code César est très facile à casser et n’apporte presqu’aucune sécurité face au premier cryptanalyste amateur venu, mais il fournit néanmoins une bonne illustration de la cryptographie symétrique.

En effet nous avons vu que dans le code employé par Jules César les fonctions de sécurité reposaient sur le principe de la confidentialité d’une clé secrète (un nombre) connue par Alice et Bob mais pas par Oscar.

Ceci explique le terme symétrique : les deux correspondants disposent des mêmes informations pour communiquer de manière sécurisée.

L’avantage principal des systèmes de cryptographie à clé secrète est la rapidité de calcul, et le désavantage principal est le problème de la communication sécurisée de la ou des clés secrètes. En effet si l’on dispose d’un canal fiable pour la distribution des clés alors pourquoi mettre en place un cryptosystème ?

Pour terminer on citera quelques exemples modernes d’utilisation de cryptographie symétrique : les algorithmes DES (Data Encryption Standard), 3DES (Triple DES) et
maintenant AES (Advanced Encryption Standard) sont les standards successifs de sécurité recommandés par le gouvernement américain. DES fut mis au point par IBM (et amélioré par la NSA, National Security Agency) et AES est son successeur, choisi parmi plusieurs algorithmes concurrents. C'est la solution belge Rijndael qui fut choisie pour son élégance et sa simplicité mathématiques, sa rapidité de calcul et ses grandes capacités d'évolution. 3DES est employé quotidiennement par des dizaines de millions de personnes sans le savoir, car c'est le standard actuel des banques.

### B.2.2. La cryptographie asymétrique

C'est pour remédier au problème du transport des clés secrètes que cette technique est employée. Elle permet l'échange d'informations privées sur un canal de communication non sécurisé.

Chaque intervenant génère ce qu'on appelle une paire de clés privée et publique. Chacun garde sa clé privée et ne la communique à personne. La clé publique est comme son nom l'indique accessible à tout un chacun (y compris Oscar) sur le canal de communication non sécurisé (par exemple Internet).

Lorsqu'Alice veut envoyer un message confidentiel à Bob elle emploie la clé publique de celui-ci. L'algorithme génère alors un message incompréhensible, que Bob est le seul à pouvoir déchiffrer, et ce grâce à sa clé privée. L'intégrité du message est garantie\(^1\) car si le texte chiffre est modifié alors Bob ne peut pas déchiffrer le message. La fraude est ainsi détectée.

Il est très simple de rajouter la preuve de l'identité d'Alice à ce message, en utilisant la clé privée de celle-ci en plus de la clé publique de Bob lors du chiffrement. Bob, pour déchiffrer le texte, utilisera alors la clé publique d'Alice et sa propre clé privée. Si le déchiffrement réussit alors Bob est sûr que le message qu'il a devant lui a bien été émis par Alice et n'a pas été modifié en cours de route.

Conceptuellement c'est comme si Alice distribuait des cadenas (ouverts) qui fonctionnent tous avec la même clé, qu'elle est la seule à posséder. Lorsque Bob lui envoie un message il ferme la boîte contenant le message avec le cadenas. Ainsi seule Alice peut l'ouvrir.

Le mécanisme de signature est la situation inverse : Bob possède une grande quantité de cadenas à combinaison chiffrée qu'il conserve précieusement chez lui et donne la combinaison permettant de les ouvrir à tout le monde. En supposant que personne d'autre ne peut fabriquer des cadenas utilisant sa même combinaison, toute boîte fermée avec un cadenas à chiffre qui s'ouvre avec le code public de Bob est donc signée par Bob.

Quelques algorithmes couramment utilisés de la cryptographie asymétrique : RSA, DSA et Diffie-Hellman.

---

\(^1\)En pratique on utilisera toutefois un mécanisme spécialisé : les fonctions de hachage. Voir plus loin pour plus d'information.
B.2. OUTILS MATHÉMATIQUES  ANNEXE B. LA SÉCURITÉ INFORMATIQUE

B.2.3. les fonctions de hachage

Les fonctions de hachage sont un outil mathématique fort pratique dans la sécurité informatique. Une fonction est une relation entre deux ensembles, faisant correspondre à tout élément du premier une image dans le deuxième.

Les fonctions de hachage correspondent à des entrées de longueur quelconque (sans aucune limite supérieure de taille) des sorties de longueur fixe. Les fonctions de hachage utilisées en cryptographie sont choisies de telle manière qu’à deux entrées qui se ressemblent beaucoup elles font correspondre deux images totalement différentes, et que la connaissance d’une image ne permet pas facilement de retrouver le message initial\(^2\) ni un autre message qui aurait la même image\(^3\).

Elles sont très utilisées dans l’identification par mot de passe : ainsi les systèmes informatiques modernes ne stockent plus depuis longtemps les mots de passe en clair sur disque dur. Au lieu de cela, ils utilisent le mot de passe choisi pour générer un code de hachage qui peut être connu de tous sans danger. Et la procédure d’identification demande à l’utilisateur d’entrer son mot de passe, qu’elle utilise pour calculer un code de hachage comme précédemment, puis compare celui-ci avec le code de hachage de référence. S’ils concordent c’est que l’utilisateur a bien entré le bon mot de passe.

Ainsi il n’est pas possible aux administrateurs système de connaître les mots de passe de leurs utilisateurs.

\(^2\)propriété dite de préimage.
\(^3\)propriété de la seconde préimage.
C. La sécurité dans les réseaux informatiques

Nous avons vu les différentes fonctionnalités de sécurité que nous désirons implemen-
ter : la confidentialité, l'authentification et l'intégrité. Nous avons vu de quelle façon on
découpe l'architecture des réseaux. Cette section étudie les possibilités de sécurisation de
des établissements bancaires, il est difficile de se connecter frauduleusement au système
physique.

C.1. La couche physique

C.1.1. Ethernet

Ce système, basé sur un câblage électrique, est par nature bien adapté aux problèmes
de sécurité. En effet il permet de limiter facilement la diffusion spatiale de l'information.
Il est théoriquement possible d'écouter un câble Ethernet en plaçant un autre câble côté
côte mais cela sort de la problématique envisagée ici. Si le bâtiment est relativement
bien sécurisé, ce qui est déjà le cas avec les instituts de microfinance vu que ce sont
des établissements bancaires, il est difficile de se connecter frauduleusement au système
physique.

C.1.2. Wi-Fi

Par sa nature ondulatoire la diffusion d'informations par ondes radio n'est pas spa-
tialement limitée. Plus le matériel d'écoute sera sensible plus loin l'attaquant pourra être
placé.
Il existe cependant deux grandes catégories d'antennes : les antennes omnidirection-
nelles et les antennes directionnelles. Les secondes concentrent la plus grande partie de
l'énergie du signal émis dans une direction particulière, ce qui le rend légèrement plus
difficile d'accès. Mais plus on s'éloigne de l'antenne et plus le faisceau devient large, et
il n'existe pas d'antennes totalement unidirectionnelles : il y a toujours plusieurs pics de
rayonnement et on ne peut pas consacrer exactement toute l'énergie dans un seul pic.
Les liaisons radio sont donc intrinsèquement moins sécurisées que les liaisons câblées.

C.2. liaison de données

C.2.1. Ethernet

Les câbles sont reliés à un système électronique qui redistribue l'information. Il en
existe deux types : les hubs qui à la réception d'une trame sur une interface se contentent
de réémettre celle-ci sur toutes les autres interfaces (et opèrent donc en couche 1), et les switches (de couche 2) qui établissent des listes dynamiques des adresses physiques des machines connectées sur chacun des ports, afin de réémettre une trame reçue uniquement sur l’interface où c’est nécessaire.

L’emploi de switches au lieu de hubs augmente la confidentialité en limitant l’accès par les utilisateurs à des informations destinées aux autres. Cependant la plupart des switches ne résistent pas à des attaques dites de spoofing, lorsqu’un attaquant émettant des trames Ethernet particulières réussit à tromper le switch dans la construction des listes d’adresses. Il est alors possible de recevoir les trames destinées à la machine dont on a simulé l’adresse, ou aussi de noyer le switch sous un trafic trop élevé ce qui empêche le bon fonctionnement du réseau\(^1\).

Il n’y a donc pas vraiment de mécanismes de sécurité propres à la couche transport d’Ethernet. On retiendra cependant qu’il est plus intéressant d’employer des switches plutôt que des bridges, aussi bien d’un point de vue confidentialité qu’au niveau de l’efficacité.

C.2.2. Wi-Fi

Les concepteurs de la norme 802.11b étaient conscients des problèmes de sécurité causés par la couche physique du système. Pour y remédier ils développèrent un protocole particulier de sécurité, dénommé Wired Equivalent Privacy (WEP) dont le but était comme son nom l’indique d’assurer une sécurité équivalente à celle d’une liaison câblée en Ethernet.

WEP est un système de cryptographie symétrique, avec le problème administratif de la distribution sécurisée des clés que cela comporte. Les clés peuvent être de différentes longueurs : 32, 64 ou 128 bits. Malheureusement les algorithmes développés comportent des failles mathématiques qui rendent la plupart des clés possibles très fragiles. Il existe de nombreux logiciels qui après une heure de capture de trafic peuvent analyser les paquets captés et en déduire la clé secrète! Cela ne réussit pas toujours, c’est fonction des paquets reçus. Mais plus le nombre de paquets capturés est grand et plus la probabilité de succès augmente.

C’est pourquoi de nouvelles normes ont été introduites : Wireless Protected Access (WPA) basée sur une version intermédiaire du standard IEEE 802.11i alors en cours d’élaboration et WPA2, respectant le standard IEEE 802.11i final et utilisant AES (WEP et WPA utilisent RC4).

Signalons aussi la possibilité de mise en place d’une liste blanche (on parle plutôt de white-listing) comprenant les adresses Ethernet des périphériques autorisés dans le réseau. Toute autre adresse Ethernet sera alors ignorée. Mais comme pour Ethernet il est très facile de modifier\(^2\) l’adresse physique d’un périphérique Wi-Fi.

---
\(^1\)On parle alors d’attaque par déni de service (Denial of Service, DoS)

\(^2\)Par exemple grâce à l’utilitaire macchanger sous Linux ou smac (non testé) sous Windows.
C.3. La couche réseau


Il y a deux modes de fonctionnement : tunnel et encapsulation. Dans le premier mode le paquet reçoit d'abord son en-tête IP, puis l'ensemble est chiffré et emballé dans un nouveau paquet IP. Cela permet de créer des tunnels sur un réseau non sécurisé en laissant percevoir un minimum d'informations aux attaquants. C'est idéal pour la mise en place d'un VPN.

Le deuxième mode est plus classique. Seule la partie données du paquet IP est chiffrée et l'en-tête est accessible à tous, ce qui permet le bon routage du paquet jusqu'à destination.

C.4. La couche transport

Les protocoles Secure Sockets Layer / SSL 3 et leur successeur Transport Layer Security / TLS 1 permettent de sécuriser des protocoles de couche applicative, que ce soit l'email ou le web. C'est dans ce dernier cas que nous nous y intéressons ici. En configurant convenablement le serveur web, toutes les communications avec le site web / serveur de base de données peuvent être chiffrées et le serveur web peut être authentifié. Ce mécanisme est relativement simple à mettre en place, bien documenté car il existe depuis longtemps et réputé sûr. De nombreux sites de commerce électronique l'utilisent pour les systèmes de paiement en ligne.

Cette technique est documentée dans l'annexe F.9 page 79.
D. Reconstruction des flux TCP capturés

La première capture effectuée depuis le siège de Inkingi à Niamirambo a enregistré le trafic échangé lorsqu’une session AdBanking est établie. On trouvera ci-dessous un extrait de la reconstruction du dialogue entre les machines.

POST /login/main_login.php HTTP/1.1
Host : 192.168.0.1
User-Agent : Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.7)
Gecko/20041013 Firefox/0.9.3 (Ubuntu)
Accept : text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Language : en-us,en;q=0.5
Accept-Encoding : gzip,deflate
Accept-Charset : ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive : 300
Connection : keep-alive
Cookie : PHPSESSID=5e5fd185231c10dd8e9671bab7099c2b
Content-Type : application/x-www-form-urlencoded
Content-Length : 68
login=demo&pwd=public&prochain_ecran=login_check&enterButton=Valid erHTTP/1.1 200 OK
Date : Tue, 15 Feb 2005 13:22:44 GMT
Server : Apache/1.3.23 (Unix) (Red-Hat/Linux) mod_ssl/2.8.7
OpenSSL/0.9.6b DAV/1.0.3 PHP/4.2.0 modperl/1.26
X-Powered-By : PHP/4.2.0
Expires : Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control : no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma : no-cache
Connection : close
Transfer-Encoding : chunked
Content-Type : text/html
48c
<DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
La ligne mise en évidence contient le nom d’utilisateur et le mot de passe utilisés pour se connecter au système. C’est seulement lorsque cette paire de valeurs arrive au serveur
que le calcul d’une fonction de hachage du mot de passe est réalisé ! Il serait bien plus intéressant de calculer cette valeur avant la transmission.

Une deuxième capture est effectuée lors de l’accès au serveur avec le protocole HTTPS ; cette fois-ci un mécanisme de chiffrement est décidé automatiquement entre les deux systèmes et le résultat est incompréhensible. On peut cependant remarquer au début du dialogue que le certificat de clé publique du serveur est envoyé grâce aux champs en texte clair SomeState1, SomeCity1...

```
...g...N.............0...........9.8.5.3.2.........../....
                      ..............d..b..................Q...&W...........J...F...B.....
                      .................i...C...Zv...k...j...ZQ...G...G...}+...c...\...\Mt)$....
                      .................0...0...u........0...{*...H........0...1...0...U
                      .................--1...0...U......SomeState1.0...U......SomeCity1.0...U.
                      .SomeOrganization1.0...U......SomeOrganizationalUnit1.0...U
                      ...localhost.localdomain1)O’...{*...H......root@localhost.loc
                      aldomain0...0...{*...H........0...0...0...0...0...0...0...0...0...0
                      ......a.LvW...f...mH...4...6...L<7J......0...aU...B....
                      ....?R...Inw......k#...G...a.0m.z.w0......q..4Q.1>YbU...!...#B......0...U...#
                      ...0...4Q.1>YbU...!...#B....0...0...1...0...U......1...0...U....
                      SomeState1.0...U......SomeCity1.0...U.
                      .SomeOrganization1.0...U......SomeOrganizationalUnit1.0...U.
                      ...localhost.localdomain1)O’...{*...H......root@localhost.loc
                      aldomain0...0...{*...H........0...0...0...0...0...0...0...0...0...0
                      ......a.LvW...f...mH...4...6...L<7J......0...aU...B....
                      ....?R...Inw......k#...G...a.0m.z.w0......q..4Q.1>YbU...!...#B......0...U...#
                      ...0...4Q.1>YbU...!...#B....0...0...1...0...U......1...0...U....
                      SomeState1.0...U......SomeCity1.0...U.
                      .SomeOrganization1.0...U......SomeOrganizationalUnit1.0...U.
                      ...localhost.localdomain1)O’...{*...H......root@localhost.loc
                      aldomain0...0...{*...H........0...0...0...0...0...0...0...0...0...0
                      ......a.LvW...f...mH...4...6...L<7J......0...aU...B....
                      ....?R...Inw......k#...G...a.0m.z.w0......q..4Q.1>YbU...!...#B......0...U...#
                      ...0...4Q.1>YbU...!...#B....0...0...1...0...U......1...0...U....
```
ANNEXE D. RECONSTRUCTION DES FLUX TCP CAPTURÉS

4. | q.i.g .......%....+V.#.m..E6...z.B.rN&7...[c...n.D\$..kc).m...4'.D.Y......,*..?N+.>>>>8...>am..'X]U...i~w...&.~.6J...].d...Ni.*t...#.x.b..Z=xWbz.x...Q.r8.C..cL'(..D....-S....
.8.....tLMEqI.Hq...k!..jx..$..=""'.4n......>.....H....?..v....
...T
!....w......!....r.o......m.{}. ...B&.\.....v..f......
......................^,5.........y;..M.V..918...U.#......B...Ze....v..Eb
..$..R....Q....0v...I/..ff.7....I8.a.j..n"....
.x6.}.8...A...R...g;"m.q.%.t.....1...g.,..=""""3. !.A1.....
q...y.a......5...^,.m.T=zp.kVjQ3..."....#~9..i..pf.n..bEDn.
'G..., :D..1CR.m...u...r...A.e....Y\...Z7J.)N....RQ.R.
W...2.M....3Gs.x.8....-...n.R.r...%] :..*Qd..t......K5....ur
....."*"..**m
E. Réalisation d’un câblage Ethernet

La première chose à faire est de dérouler un câble Ethernet entre les deux points à relier, et de le placer si possible en hauteur et le long des murs. Il faut alors couper le câble.
Reste alors à placer des connecteurs sur les câbles. Il existe deux types de connecteurs Ethernet : série A et série B.
Lorsqu’on connecte une interface Ethernet (carte réseau, bridge) à un hub ou à un switch il faut réaliser deux connecteurs série A. Lorsqu’on veut connecter ensemble directement deux interfaces Ethernet (liaison d’ordinateur à ordinateur) il faut réaliser d’un côté une série A et de l’autre une série B.
La première étape dans les deux cas est le dénudage du câble sur une petite dizaine de centimètres. Il faut enlever la gaine protectrice sans abimer les câbles intérieurs.
On observe alors quatre paires de fils et du rembourrage. On enlève le rembourrage.
Chaque paire est composée d’un fil de couleur (vert, orange, bleu, marron) et d’un fil blanc. On nommera blanc-vert le fil blanc entouré autour du fil vert, et ainsi de suite pour les autres fils blanc.
Il s’agit alors d’aligner dans le bon ordre les différents fils. On procède de gauche à droite en respectant l’ordre suivant pour une série A :
blanc-vert, vert, blanc-orange, bleu, blanc-bleu, orange, blanc-marron, marron.
Et l’ordre pour une série B :
blanc-orange, orange, blanc-vert, bleu, blanc-bleu, vert, blanc-marron, marron.
F. Logiciels employés

F.1. Ethereal Network Protocol Analyzer

Logiciel libre permettant l’analyse des paquets d’un réseau soit directement soit après capture.

Trois vues différentes sont possibles pour chaque paquet : une description concise en une ligne, une vue arborescente des détails du paquet permettant facilement d’accéder à un protocole ou à un champ particulier, et enfin la version brute du paquet telle qu’il a été reçu par la carte réseau.

Ethereal permet aussi de reconstruire un flux TCP : à partir d’un paquet sélectionné il peut retrouver les paquets correspondants et en extraire toutes les parties données. Ensuite l’ensemble est présentée sous forme textuelle à l’utilisateur. Cela permet par exemple de retrouver facilement le dialogue entre un navigateur web et un serveur HTTP.

F.2. Nmap Network exploration tool and security scanner

Logiciel libre permettant notamment la découverte sur un sous-réseau IP des machines y appartenant, et la découverte des différents services disponibles sur chaque machine : serveurs de fichier (FTP), serveurs web (HTTP), email (smtp/pop3), serveurs sécurisés (SSH)...

F.3. ping

Utilitaire standard de tous les systèmes d’exploitation permettant de tester la liaison avec des ordinateurs distants. Les différentes variantes de ping envoient toutes un ou plusieurs paquets IP suivant le protocole ICMP (Internet Control Message Protocol), demandant le service ECHO_REQUEST. La machine réceptrice retourne les paquets de ce type à l’émetteur ce qui permet de vérifier que le chemin aller-retour est bien opérationnel et d’en déduire des statistiques de qualité comme le temps moyen d’aller-retour (Round Trip Time), le taux de perte de paquets ...

F.4. OpenSSH (serveurs et clients SSH)

Le client SSH est un programme permettant de se connecter à une machine distante afin de lui faire exécuter des commandes. C’est le successeur des programmes rsh et rlogin, fournissant une connexion chiffrée sécurisée entre deux machines sans relation préalable de confiance sur un réseau non sécurisé.
L'utilisateur prouve son identité à la machine distante selon différentes méthodes dépendant de la version utilisée du logiciel.
Le serveur sshd est le programme qui tourne en tâche de fond en attendant une demande de connexion ssh, et gère l'échange de clés, le chiffrement, l'identification, l'exécution de commandes et le transfert de données.
Le logiciel sftp permet de transférer des fichiers dans les deux sens à partir d'une connexion sécurisée SSH.

F.5. Kismet

Kismet est un détecteur, enregistreur et analyseur de trafic radio, et un système de détection d'intrusion. Il fonctionne avec toute carte Wi-Fi permettant le fonctionnement en mode monitoring et peut enregistrer les trafics de type a, b et g.
Kismet permet l'identification de réseaux sans fil en écoutant passivement les paquets qui sont à portée radio. Il détecte les noms des réseaux standard, détecte les réseaux cachés et peut déduire la présence de réseaux non diffuseurs à partir du trafic capté.
Kismet utilise un format de fichier reconnu par Ethereal.

F.6. Airsnort

Airsnort est un outil conçu pour récupérer la clé WEP d'un réseau Wi-Fi en exploitant la faille de chronométrage RC4.
Il place la carte réseau en mode moniteur et enregistre tous les paquets chiffrés utilisant un vecteur d'initialisation (IV) faible. Plus la clé est longue plus le nombre de paquets nécessaire est grand. Cependant l'attaque est probabiliste et il est possible de trouver la clé avec un très petit nombre de paquets (en modifiant les paramètres d'une heuristic de recherche).

F.7. AdBanking

Logiciel développé initialement au Burkina Faso par Adfinance, la division microcrédit de l'ONG internationale Aquadev, il est écrit en langage PHP et destiné à être exécuté sur le serveur web Apache.
Ce logiciel permet de gérer tous les aspects d'un institut de microfinance et est utilisé avec succès dans de nombreux pays d'Afrique.

F.8. Apache

La référence des serveurs HTTP et HTTPS, employé par 60% des serveurs web.
F.9. OpenSSL

Boîte à outils implémentant les protocoles Secure Socket Layers SSL (v2/v3) et Transport Layer Security TLS v1, ainsi qu’une librairie de fonctions cryptographiques d’intérêt général.

OpenSSL permet de générer des certificats X509 et des listes de révocation de certificats (CRL), des paires de clés RSA, DSA et Diffie-Hellman.

OpenSSL permet donc de mettre en place un système de cryptographie à clé publique (Public Key Infrastructure, PKI).

Il est important de savoir que RSA peut être utilisé à la fois pour signer et pour chiffrer tandis que DSA ne peut servir qu’à signer. On utilisera donc des clés RSA pour répondre aux besoins de confidentialité.

La première est chose à faire est de générer une paire de clés privée/publique. Avec OpenSSL cela s’obtient grâce à la commande :

\`openssl genrsa -out privkey.pem 2048\`

où privkey.pem est le fichier contenant le résultat et 2048 la longueur en bits de la clé. 2048 est la clé minimale recommandée pour RSA.

La deuxième étape est la génération d’un certificat de clé publique. Deux cas sont possibles, les certificats authentifiés par une autorité de certification ou les certificats autosignés.

Pour créer un certificat de clé publique authentifié, on commence par une demande de certificat, ou plus précisément une demande de signature de certificat :

\`openssl req -new -key privkey.pem -out cert.csr\`

Cette commande place dans cert.csr la demande de signature d’un certificat basé sur la clé publique trouvée dans privkey.pem. Le nouveau fichier doit être envoyé à l’autorité de certification, qui après vérification de l’identité du requérant, renvoie le certificat signé par l’autorité.

Pour un certificat autosigné valable pour trois ans (1095 jours) il suffit d’utiliser la commande suivante :

\`openssl req -new -x509 -key privkey.pem -out cacert.pem -days 1095\`

Il reste alors à configurer Apache pour employer ce certificat.

Rajouter dans le fichier httpd.conf les lignes suivantes pour confidentialiser le trafic :

\`
SSLProtocol all
SSLCipherSuite HIGH :MEDIUM
\`
est accessible en permanence par Internet (Un niveau de sécurité supplémentaire sera de restreindre les heures d'accès au serveur).

Pour signer des certificats avec OpenSSL, il faut d’abord générer une nouvelle paire de clés et une demande de signature, comme précédemment. Ensuite le certificat est signé par l’autorité :

    openssl x509 -req -in client.cert.csr -out client.cert.cert -signkey my.CA.key -CA my.CA.cert -CAkey my.CA.key -CAcreateserial -days 365

Le certificat du client est le fichier client.cert.cert. On créera un certificat client par poste utilisateur.

Pour forcer la vérification des certificats utilisateurs Apache doit recevoir les instructions suivantes :

    # require a client certificate which has to be directly
    # signed by our CA certificate in ca.crt
    SSLVerifyClient require
    SSLVerifyDepth 1
    SSLCACertificateFile conf/ssl.crt/ca.crt
G. Rapports hebdomadaires

G.1. Première semaine

G.1.1. Rencontre des intervenants et formalités douanières

Jérôme est arrivé à Kigali samedi 5 février vers 20h comme prévu. Arthur et Adrien Kabale étaient sur place pour faciliter le passage en douane du matériel. L'électronique passa sans encombre mais les antennes restèrent bloquées. On se rendit compte que le formulaire EX-1 emporté par Jérôme était sans valeur car il aurait dû être complété par la douane belge. De plus l'importation à titre permanent des antennes est une procédure complexe. Elles retourneront donc avec Jérôme en Belgique. Il faudra dès lors se mettre en ordre avec la TVA.

L'équipe sort de l'aéroport vers 22 heures.

Le dimanche matin, Adrien accueille Jérôme à domicile pour faire plus ample connaissance. L'après-midi, Arthur fait découvrir le centre-ville à Jérôme et une première visite des sites de déploiement du matériel est effectuée.

G.1.2. Lundi


L'après-midi, dès que le formulaire est prêt Arthur et Jérôme partent le chercher, et reprennent contact avec les autorités douanières. Celles-ci veulent reporter au lendemain la sortie du matériel mais Arthur réussit à obtenir les antennes déjà en fin d'après-midi.

G.1.3. Mardi

L'un des bridges Cisco devra être placé à l'extérieur sur une tour de télécommunication supportant déjà plusieurs antennes. Il est donc nécessaire de fabriquer un boîtier pour abriter le bridge, celui-ci étant prévu pour un usage indoor.

Adrien demande alors à Bruxelles un accord de financement des frais afhérents au projet de connexion sans fil.

Le reste de la journée est consacré par Jérôme à la rédaction de divers documents (rapports de stage et mémoire).
G.1.4. Mercredi


En fin de journée tout le matériel nécessaire au déploiement sur site des antennes est prêt.

G.1.5. Jeudi

Nous (Arthur, Bonny, étudiant en informatique au KIST et stagiaire chez Aquadev Central Africa, et Jérôme) passons en début de matinée au KIST pour les procédures d’autorisation. On nous annonce que nous devons rencontrer le responsable du département Information and Communications Technologies qui est en charge de la tour de télécommunications. Cela n’est pas possible ce jour-là et nous prenons rendez-vous pour le lendemain matin.

On se dirige donc alors vers Nyamirambo, quartier de Kigali où est installé le siège de l’institut de microfinance Inkingi, partenaire de l’expérimentation.

Le bâtiment est idéalement situé, au-dessus d’une plaine en légère pente en direction du KIST qui se trouve lui au sommet d’une colline. De plus les autres constructions environnantes sont plus petites et ne devraient pas trop perturber la propagation du faisceau hertziens.

Nous mettons en place un mât attaché à la balustrade entourant l’étage administratif de Inkingi, et y fixons solidairement la première antenne. On réalise une boîte sommaire en carton pour abriter le bridge (qui sera placé à l’intérieur du bâtiment) et nous plaçons des câblages Ethernet et électrique jusqu’au bureau de la personne associée au projet chez Inkingi. En fin de journée, le matériel a été testé et tout semble opérationnel.

G.1.6. Vendredi

Arthur, Bonny et Jérôme partent le matin voir le responsable du département ICT du KIST. Celui-ci n’a pas d’objection à notre projet mais confirme ne pas avoir autorité pour nous garantir l’accès à la tour. Il nous redirige vers un professeur, qui n’est pas présent sur le site. Nous réussissons à rencontrer ce professeur vers 10h15, et il nous explique que lui non plus ne peut pas nous donner cette autorisation. Nous sommes alors envoyés au bureau du recteur, dont la secrétaire se rappelle nous avoir vu dans la semaine. Elle nous demande de représenter la lettre d’introduction signée par le directeur d’Inkingi, que Arthur leur avait remise le jour précédent. Nous devons alors rejoindre les bureaux d’Aquadev pour récupérer cette lettre, et vers 11h30 on nous introduit dans le bureau du directeur de l’administration du KIST.

Celui-ci se rappelle avoir déjà vu l’autorisation signée par le recteur. Mais cette autorisation a apparemment été égarée par le secrétariat. Il nous assure qu’il va s’occuper de ce problème rapidement, mais comme le recteur du KIST est actuellement occupé avec des visiteurs nous ne pourrons pas obtenir l’autorisation avant lundi matin. Nous convenons
Fig. G.1.: Vues du mât installé au siège de Inkingi à Nyamirambo.

Fig. G.2.: Vues de l’antenne installée à Nyamirambo.
Fig. G.3: Vues de la tour de télécommunications du KIST depuis le siège de Inkingi à Nyamirambo.

de reprendre contact par téléphone dans l’après-midi pour être au courant de l’évolution du dossier.

G.1.7. Conclusions

Cette première semaine de coopération entre Jérôme et Arthur s’avère fructueuse, étant tous les deux motivés pour faire avancer le projet. Malheureusement nous sommes ralentis par de nombreux détails et nous prenons un léger retard : nous avions envisagé de finir les installations matérielles ce vendredi.

Cependant il reste encore deux semaines et nous espérons pouvoir concrétiser d’autres projets techniques (confection sur place d’antennes, liaisons privées virtuelles par l’Internet…).

G.2. Deuxième semaine

G.2.1. Lundi

Jérôme consacre le début de la matinée à la rédaction de ses différents rapports et de son mémoire pendant qu’Arthur s’occupe de ses autres activités.

Nous nous rendons ensuite au KIST où nous rencontrons à nouveau le Director of Administration. Celui-ci a des objections concernant notre projet car les guichets de Inkingi au KIST pourraient être fermés par les autorités du KIST pour raisons administratives. Nous lui expliquons que notre installation est temporaire et est aussi destinée à être déployée sur d’autres sites à l’avenir. Il nous redonne alors rendez-vous dans l’après-midi pour rencontrer le responsable technique.

Lors de notre deuxième visite l’après-midi nous obtenons l’accord oral des deux parties.

### G.2.2. Mardi

L’antenne est assez grande et la hisser jusqu’au point d’attache est un problème. Bonny nous présente un de ses amis qui réussit à la monter à l’endroit voulu (avec l’aide de Bonny).

Nous avons quelques doutes quand au bon alignement de l’antenne. On utilise une paire de jumelles pour améliorer la précision.

Nous posons les câbles d’alimentation électrique et réseau (Ethernet).

Le matériel posé au KIST fonctionne sans problème lors des tests.

![Image](image_url)

**Fig. G.4:** Alignement de l’antenne du KIST par Bonny

L’après-midi nous nous rendons à Nyamirambo pour activer le matériel déjà posé là-bas. Dès le premier test la liaison fonctionne très bien. Des transferts de fichiers nous permettent d’évaluer la liaison à plus de 300 kB/s avec des pointes à 400 kB/s. Le coût d’une telle liaison chez RwandaTel (ligne louée) serait beaucoup plus élevé.

Arthur se connecte au serveur AdBanking du KIST depuis Nyamirambo, tout fonctionne exactement comme si nous nous trouvions dans les guichets du KIST.
Nous observons une coupure brève de la liaison. Après examen de l’antenne de Nya-
mirambo nous concluons que c’est dû au vent qui écarte temporairement l’antenne de sa
position optimale. Le mât utilisé pour l’attacher est en bois et donc sujet à flexion. Pour
une installation permanente il faudrait utiliser un mât en métal.
Nous procédons à diverses mesures pour évaluer la connexion puis rentrons au bureau.

\[\text{FIG. G.5.: Vues de l’antenne placée sur la tour au KIST}\]

**G.2.3. Mercredi**

Nous élaborons une solution de connexion sécurisée par l’Internet d’un serveur AdBan-
king. Arthur sélectionne l’IMF Coopedu, informatisée avec AdBanking depuis près d’un
an.
Plusieurs approches sont envisagées :
1. connexion directe du serveur web à l’Internet
2. connexion du serveur web indirecte par un routeur/NAT configuré de manière à
rendre accessible le service HTTP du serveur (mécanisme de redirection de port\(^1\)).
3. Établissement d’une liaison VPN (Virtual Private Networking).
La première solution sera d’abord testée. Mais elle pose le problème d’exposer largement
le serveur à d’éventuels attaquants sur l’Internet. Pour mettre en production un tel
système il serait nécessaire de réaliser au préalable une étude détaillée de la sécurité du
serveur et de s’assurer de l’installation régulière des dernières mise à jour.

\(^{1}\text{port forwarding}\)
G.2. DEUXIÈME SEMAINE

La deuxième solution est probablement le meilleur compromis entre complexité et sécurité : le routeur est un système dédié à cette fonction et donc par nature plus simple à protéger, et la redirection de port est une fonctionnalité largement répandue et facile à mettre en œuvre (lorsque les logiciels de routage le permettent).

La troisième solution est lourde à mettre en œuvre et fournit des services inutiles. Mais d’un point de vue technique elle est très proche de notre solution sans fil : un VPN correctement configuré crée l’illusion pour les systèmes informatiques l’utilisant qu’ils sont reliés ensemble par une liaison câblée privée.

G.2.4. Jeudi

Jérôme continue la rédaction de ses rapports et mémoire. Arthur s’occupe des affaires courantes de Aquadev.

Jérôme détermine les besoins pour la fabrication locale d’un type d’antenne particulier appelé guide d’onde. L’objet doit avoir la forme d’un cylindre de 51 cm de long, 9 cm de diamètre et un des deux fonds doit être fermé, l’autre ouvert.

De plus un trou doit être percé à 5,1 cm du fond fermé pour y placer un connecteur d’antenne de type N femelle, auquel doit être soudé une tige de 3,1 cm de long qui servira d’antenne. Arthur va se renseigner sur la possibilité de se fournir en connecteurs de ce type. Jérôme sait qu’à Bruxelles il est difficile d’en trouver.

G.2.5. Vendredi

Nous nous préparons à effectuer un test de connexion par Internet au serveur AdBanking de Aquadev avant de procéder au même test chez Coopedu. Nous nous renseignons sur les détails informatiques : les ordinateurs connectés à Internet sont identifiés par une adresse IP publique\(^2\). Lorsqu’on utilise une connexion classique par fournisseur d’accès, l’adresse est dite dynamique : elle peut changer à chaque connexion. Nous allons utiliser une technique pour ne pas devoir communiquer la nouvelle adresse IP aux clients à chaque connexion, appelée le DNS\(^3\) dynamique. Un compte est créé chez DynDNS, fournisseur gratuit d’un service de DNS dynamique. Le logiciel permettant de mettre à jour automatiquement notre nom de domaine nouvellement créé (aquadevligi1 ath.cx) est téléchargé. La machine qui sera utilisée pour partager la connexion Internet fonctionne sous Windows XP Service Pack 1. Il va donc falloir trouver des programmes permettant de partager la connexion Internet et de fournir le service de redirection de port. Sous Windows XP Service Pack 2 un service de Pare-Feu (Firewall) a été introduit dans le panneau de contrôle rendant cette étape inutile.

Nous espérons faire le premier test lundi.

\(^1\)Une adresse IP (Internet Protocol) est une adresse numérique (codée sur 32 bits, soit théoriquement 2\(^32\) possibilités) identifiant de façon unique un système informatique connecté à l’Internet. Il existe aussi des adresses IP dites privées, réservées à usage interne. Elles commencent par 192.168 ou par 10.

\(^2\)Domain Name System, hiérarchie arborescente de serveurs établissant une correspondance entre des noms alphabétiques (tels google.com, www.aquadev.org, cs.uleb.ac.be...) et l’adresse numérique des serveurs.)
G.3. TROISIÈME SEMAINE

G.2.6. Conclusions

L’objectif principal du stage a été accompli avec succès et nous espérons pouvoir mener à bien d’autres petits projets : connexion par Internet et fabrication locale d’antenne.
Le projet de connexion par Internet est déjà bien avancé et devrait être terminé en début de semaine prochaine.
La fabrication locale d’antenne est très intéressante car si elle est suffisamment efficace le coût de la solution diminuerait significativement (une antenne coûte près de 100 euro).
Deux problèmes se posent : d’une part la précision de la réalisation devrait jouer une part importante dans la qualité du guide d’onde, et d’autre part la fourniture d’un connecteur de type N sans lequel il ne peut y avoir d’antenne.

G.3. Troisième semaine

G.3.1. Lundi

Jérôme consacre la matinée à la rédaction de ses différents rapports et de son mémoire pendant qu’Arthur s’occupe de ses autres activités. Nous essayons de configurer le modem du serveur AdBanking sous Linux. Le matériel est prévu uniquement pour Windows (winmodem) et les modules capables de le contrôler sous Linux sont difficiles à trouver. Nous finissons par réussir l’installation mais la vitesse de connexion obtenue est trop réduite que pour être utilisable.
On discute de manière plus détaillée des possibilités de fabrication d’antenne.
Nous essayons d’obtenir un logiciel de redirection de port sous Windows. Comme c’est assez volumineux nous finissons par utiliser un cybercafé le soir pour télécharger le programme. Le portable de Freddy permettra de partager une connexion internet téléphonique avec le serveur AdBanking.

G.3.2. Mardi

Nous réalisons les tests de connexion au serveur AdBanking de Aquadev d’abord par l’intermédiaire d’un serveur en Belgique et ensuite depuis un cybercafé. Tout fonctionne bien.

G.3.3. Mercredi

Les recherches de châssis de connecteur d’antenne type N restent infructueuses ; je suis donc contraint d’abandonner mon projet de fabrication d’antenne.
Démontage des installations du KIST ; démontage des installations de Nyamirambo.
G.3. TROISIÈME SEMAINE

G.3.4. Jeudi

Emballage du matériel pour le voyage de retour en Belgique.

G.3.5. Vendredi

Rédaction de rapports et procédures administratives douanières pour le retour en Belgique des matériels utilisés (antennes et bridges).

G.3.6. Conclusions

G.3.6.1. Liaison sans fil

La connexion sans fil, premier objectif de mon stage au Rwanda, a très bien fonctionné. Mais les bons résultats quantitatifs obtenus ne doivent pas masquer la réalité du terrain : cette technologie est inadaptée à ce pays à cause de la nécessité⁴ de liaisons en ligne de vue. D’autre part les IMFs sont à la recherche d’une solution globale de connectivité ; la solution testée impliquait deux antennes directionnelles et dans une telle configuration il faudrait installer un bridge au siège pour chaque liaison mise en place. De plus le matériel exploité n’était pas destiné à un fonctionnement en extérieur. Deux possibilités se présentent pour un fonctionnement opérationnel :

1. l’emploi de bridges outdoor, conçus pour résister notamment à la saison des pluies, et ce conjointement avec une alimentation des bridges en PowerOverEthernet, ce qui évitera de placer des rallonges 230 volts sous la pluie ;
2. Le placement de bridges indoor à l’intérieur d’un bâtiment, conjointement à l’emploi d’un plus grand câble d’antenne. Ce câble devra cependant être correctement choisi afin de ne pas causer de trop grandes pertes de puissance (j’ai utilisé du câble LMR-400 qui convient très bien et dont le prix est abordable).

Si la topologie des lieux l’avait permise (liaison visuelle avec plusieurs agences) j’aurais installé une antenne active omnidirectionnelle au siège de l’IMF et placé une antenne directionnelle dans chaque agence à rélier, chacune visant cette antenne omnidirectionnelle. Ce scénario réduit alors les coûts d’installation (liaison point-to-multipoint) par rapport au premier cas (liaisons point-to-point) mais les antennes omnidirectionnelles présentent des gains moins élevés et sont plus onéreuses. Ceci s’explique par le fait que le gain ne se fait pas ici au détriment de la zone spatiale couverte : il est régulier sur un plan perpendiculaire à l’antenne. Un facteur de diminution de coût est l’emploi d’antennes directionnelles fabriquées localement. Malheureusement cela n’a pu être testé faute du connecteur nécessaire (et de temps pour fabriquer une alternative à ce connecteur). Le modèle proposé⁵ devrait probablement offrir des performances suffisantes pour la distance qui a été couverte (si les critères de dimensionnement sont relativement bien respectés).

⁴Il est théoriquement possible d’obtenir des liaisons sans ligne de vue ; ceci est dû à la courbure de l’horizon radio (ce phénomène est expliqué dans le mémoire). Mais les difficultés d’installations sont beaucoup plus grandes (problème d’alignement des antennes) et les résultats sont difficilement prévisibles (qualité de la liaison, possibilité de la liaison).

⁵Voir rapport de stage final.
G.3.6.2. Liaison par Internet

L’autre technique envisagée exploite le réseau public de télécommunications existant. Elle est plus facile à mettre en œuvre car reposant uniquement sur des logiciels relativement simples à configurer. Le mécanisme principal de sécurité est le même que pour la liaison radio : sécurisation au niveau de l’application. Deux problèmes cependant : d’abord le faible débit obtenu, ensuite la facturation à la minute des communications. Ces deux facteurs pourraient s’améliorer avec le temps : le secteur des télécommunications est en cours de libéralisation au Rwanda avec l’installation de l’américain Terracom. Des accès ADSL sont envisagés dans la capitale. Ceci est une perspective réaliste dans la mesure où la technologie ADSL s’adapte très bien à des réseaux téléphoniques téléphoniques en mauvais état ; les modems ADSL testent l’état de la ligne de transmission jusqu’aux DSLAM (Digital Subscriber Line Access Modules, placés dans les locaux techniques existants) pour déterminer quelle sera la vitesse possible maximale. L’obstacle principal est le nombre de clients potentiels : il faut que la demande soit suffisante pour que les opérateurs investissent dans cette technologie.

Les logiciels de redirection de ports sont très faciles à mettre en place dans les modems-routeurs ADSL actuellement disponibles en Europe pour une centaine d’euro et ne nécessitent pas le fonctionnement en permanence d’un ordinateur (facilité de fonctionnement et faible consommation électrique).

On surveillera cependant l’apparition sur le marché du matériel à la norme WiMax (IEEE 802.16) permettant de créer des réseaux sans fil sur de grandes distances. Ce type de matériel est en phase de test et ne se trouve pas encore facilement dans le commerce. Cela sera peut-être moins cher à déployer pour les opérateurs qu’ADSL.

Avantage supplémentaire par rapport au sans fil, si des problèmes surviennent ce sera à l’opérateur télécom de les régler et non pas à AdFinance, dont ce n’est pas le cœur de métier.

G.3.6.3. Module multi-agences

Le module multi-agences pour AdBanking en cours de développement à Dakar devrait permettre à chaque agence de disposer de son serveur, et de transférer quotidiennement les mise à jour de leur base de données locale à un serveur principal situé au siège de l’IMF. Ce transfert pourrait se faire par une connexion Internet par téléphone.

Avec ce système chaque agence peut fonctionner de manière autonome : si le serveur central est en panne ou en maintenance les autres agences ne sont pas affectées. Par contre il y a un certain surcoût car il faut acheter un serveur par agence. Mais les coûts d’utilisation sont modiques.
<table>
<thead>
<tr>
<th>Solution</th>
<th>Capacité</th>
<th>Coût de mise en place</th>
<th>Coûts d'utilisation</th>
<th>Sécurité</th>
</tr>
</thead>
</table>

Tab. G.1.: Grille de comparaison des solutions

G.3.6.4. Tableau récapitulatif

La solution Wi-Fi sera donc intéressante lorsque les opérateurs de télécommunication ne fournissent pas de services suffisants et lorsque le relief le permet. J’insiste encore une fois sur le placement en hauteur des antennes, si possible sur une tour ou un mât. La haute capacité fournie par le Wi-Fi permet d’envisager l’utilisation de ce canal de communication pour d’autres fonctionnalités : Voice Over IP, transferts de fichiers... ce qui pourrait aussi permettre d’associer d’autres structures aux frais d’installation.

---

6Un contrôlé par adresse IP est aussi envisageable en complément, mais celles-ci pouvant varier il n’est pas trivial à mettre en place. Un mécanisme de certificats cryptographiques distribués aux clients apporteraient une grande fiabilité au système (si correctement employé). Voir pour plus d’informations à ce sujet le rapport final de stage.
Bibliographie


