الجمهورية الجزائرية الديمقراطية الشعبية

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR
ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE DR. YAHIA FARES DE MEDEA

FACULTE DE TECHNOLOGIE

Département du Génie Électrique



Mémoire de Fin d'Études

Présenté pour l'obtention du Diplôme
de Master en Système Intelligent et Communicant

THEME

Mise en œuvre d'un canal de communication caché basé sur le champ d'identification IPv4 sur NS-3

Proposé et dirigé par ;

Dr. KHEDDAR HAMZA

Préparé et présenté par :

- Mr.MEKHANEG ABDELGHANI
- Mr.BENAHMADI ABDELMOUMEN

Promotion 2016-2017



REMERCIEMENT

En préambule à ce mémoire nous remerciant ALLAH qui nous aide et nous donne la patience et le courage durant ces langues années d'étude. Nous souhaitant adresser nos remerciements les plus sincères aux personnes qui nous ont apporté leur aide et qui ont contribué à l'élaboration de ce mémoire ainsi qu'à la réussite de cette formidable année universitaire. Ces remerciements vont tout d'abord au corps professoral et administratif de la Faculté de YAHIA FARES des Sciences et technologie, Juridiques et sociales, pour la richesse et la qualité de leur enseignement et qui déploient de grands efforts pour assurer à leurs étudiants une formation actualisée. Nous tenant à remercier sincèrement Monsieur, KHEDDAR HAMZA, qui, en tant que Directeurs de mémoire, se sont toujours montrés à l'écoute et très disponible tout au long de la réalisation de ce mémoire, ainsi pour l'inspiration, l'aide et le temps qu'ils ont bien voulu nous consacrer et sans qui ce mémoire n'aurait jamais vu le jour. On n'oublie pas nos parents pour leur contribution, leur soutien et leur patience. Enfin, nous adressons nos plus sincères remerciements à tous nos proches et amis, qui nous ont toujours encouragées au cours de la réalisation de ce mémoire. Merci à tous et à toutes.

DEDICACE

Je dédie ce travail

A

Ma très chère mère et mon très cher père

Pour leur soutien, leur présences,

Leur amour qui m'a encouragé dans mes études

Ainsi que

Mes chers frères

ET

Ma future femme nchl « KAWTHER »

Aussi

A Mes chers amis

Et spécialement redouane et amine (hsen).

Pour leur encouragement, leur soutien et l'ambiance

Que nous avons vécu Pendant toute notre carrière d'étudiant

A cet effet, je tiens à remercier tous mes collègues

Tous mes amis et aussi A tous ceux qui ont une relation

De proche ou de loin avec la réalisation du présent rapport.

A toute la promo (2016-2017) Et à toute la section SIC.

ABDELGHANI

DEDICACE

Je tiens à remercier en premier lieu dieu le tout puissant qui nous a donné le courage et la patience.

Je tiens à dédier ce modeste travail à mes très chers

parents qui n'ont pas arrêté de

me soutenir et m'aider à tracer

mon chemin vers la réussite à travers mes études.

Ainsi je dédié ce projet à

toute la famille BEN AHMADI ,ALOUAOUI

et MIAD

A mes chers amies Ahmed, Anter , Chikha,RFK

Hichem , mohamed , Razki , Kder , Ishak

A mon binôme Lyes

et tous mes collègues.

Moumene.

Résumé :

la stéganographie du réseau décrit les méthodes utilisées pour transmettre de l'information sur le réseau sans être détectées. La longueur du paquet est utilisée pour l'envoi de données secrètes. Dans cet memoire, une technique de steganographie a été proposé qui peut cacher un contenu de par une modification dans les identificateur des d'en-têtes de IPv4

Sécurité pour les données pratiques se cachant dans les réseaux de communication En utilisantTCP/ IP.

Mots clés : Stéganographie, VoIP, transmission numérique sécurisé.

ABSTRACT :

The steganography of the network describes the methods used to transmit information on the network without being detected. The length of the packet is used for sending secret data. In this paper, a steganography technique has been proposed that can hide a file data content by a change in the IPv4 header identifier

This work reports the areas of steganography, network protocols and security for practical data hiding in communication networks using TCP / IP.

Keywords: Steganography, VoIP, secure digital transmission.

الملخص:

إخفاء المعلومات في الشبكة يصف الطرق المستخدمة لنقل المعلومات عبر الشبكة دون أن يتم اكتشافها . يستخدم طول الحزمة لإرسال البيانات السرية. في هذه المقالة نقترح تقنية لاخفاء محتوى ملف و ذلك بالتعديل المُعَرف لرأس عناوين ipv4.

هذا العمل يتكلم عن مجالات اخفاء المعلومات ،و بروتوكولات الشبكة و أمن المعلومات المخفية في الشبكة، و ذلك باستعمال البروتوكولTCP/IP.

الكلمات المفتاحية : طريقة إخفاء، بروتوكول الإنترنت ، الارسال الرقمي الآمن.

TABLE DES MATIERES

LISTE DES FIGURES I

LISTE DES ACRONYMES II

INTRODUCTION GENERAL ..... 1+2

Chapitre I : Système de transmission sécurisé

1. Introduction 3
2. Système de communication numérique 3
   2.1. La chaine de transmission numérique 3
      2.1.1. L'émetteur 4
         2.1.1.1. Codeur en ligne (modulation en band de base) 4
         2.1.1.2. Filtre d'émission 5
         2.1.1.3. Modulation à l'émission 5
      2.1.2. Canal de transmission 5
      2.1.3. Le Récepteur 5
         2.1.3.1. Démodulation 6
         2.1.3.2. Filtre de réception 6
3. Transmission sécurisée de l'information 6
   3.1. Système de transmission cryptographique 7
   3.2. Système de tatouage 8
   3.3. Système de transmission stéganographique 10
      3.3.1. La Stéganographie dans l'Histoire 11
4. Comparraison entre Cryptographie et la Stéganographie 12
5. Comparaison entre Tatouage et la Stéganographie 13
6. Système de transmission stéganographique de la parole 13
7. Classification des systèmes stéganographiques de la parole 15
   7.1. Classification selon la clé 15
      7.1.1. Les principaux concepts cryptographiques 15
         7.1.1.1. Cryptosystème à clé symétrique 15
         7.1.1.2. Cryptosystème à clé publique 16

7.2. Classification selon le domaine d'insertion 16
7.3. Classification selon le protocole de transmission 17
7.3.1. Réseautage et TCP / IP : les bases 17
7.3.2. En-têtes UDP et ICMP 17
7.3.3. Cacher dans un Protocole Ouvert (http) 18
8. Steganalyse 19
9. Conclusion 21

chapitre II: les Technique De Stéganographie

1. Introduction 22
2. Les techniques de steganographie appliquées au réseau informatique 22
2.1. Les techniques de steganographie qui peuvent être appliquées au protocole IP 23
2.2. Les techniques de steganographie qui peuvent être appliquées au protocole TCP 24
2.3. Les techniques de steganographie appliquées au protocole RTP 26
2.4. Les techniques de steganographie appliquées au protocole RTCP 27
3. La VOIP et la stéganographie 30
4. Classification des techniques steganographie appliquées à la VOIP 31
4.1. La stéganographie par modifications de paquets 32
4.2. La stéganographie par modification de la relation temporelle 32
4.3. La stéganographie hybride 33
5. conclusion 34

Chapitre III: Réalisation de la technique avec NS-3

1. Introduction 35
2. Choix du simulateur 35
2.2. OPNET 35
2.3. NS-2 36
2.4. NS-3 36
3. Présentation du simulateur NS-3 37
4. Terminologie et abstractions 37
4.1. Les nœuds "Node" 37
4.2. Les application "Application" 38

4.3. Le canal de communication "Channel" 38
4.4. Les interfaces de la communication "NetDevice" 38
4.5. Les "Topology Helpers" 38
5. Architecture de base de Network Simulator 3 38
6. Installation du simulateur NS-3 39
7. Déroulement de la simulation 42
8. scénario de simulation.....44
8.1. Les étapes de création de programme de simulation 44
Résultats et Interprétations
8.2. Résultats 48
9. Conclusion 57

CONCLUSION GENERALE 58
ANNEX
BIBLIOGRAPHIE

Liste des figures

Chapitre I : Système de transmission sécurisé

Figure I. 1 La chaine de transmission numérique……...04

Figure I. 2 Techniques de la sécurité de l'information……...07

Figure I. 3 Protocole de chiffrement…….....07

Figure I. 4 Protocole de chiffrement…….....09

Figure I. 5 La stéganographie technique…….....10

Figure I. 6 diagramme des blocs pour la stéganographie audio……...14

Figure I. 7 chiffrement avec la clé symétrique……...15

Figure I. 8 chiffrement avec la clé public……...16

Chapitre II : Les technique de stéganographie

Figure II.1 : format d'entête IP……..23

Figure II.2 : format d'entête TCP……..25

Figure.II.3 : format d'entête RTP……..27

Figure.II.4.a :RTCP Rapport du récepteur (RR)…….....…28

Figure.II.4.b : RTCP Rapport de l'émetteur (SR)…….28

Figure.II.5 : VOIP et la Stéganographie…….....30

Figure.II.6 : Classification des techniques steganographie appliquées à la VOIP…….....32

Tableau. II.1 : comparaison entre différents techniques de Stéganographie……..34.

Chapitre III : Réalisation de la technique avec NS-3

Figuer.III.1 : Interface du simulateur…….....36

Figuer.III.2 : Architecture du nœud NS-3.....39

Figure III.3 : Etapes pour la réalisation d'une simulation……42

Figure.III.4 : Les étapes de nos simulations sous NS-3……...43

Figure.III.5 : Topologie du scénario……44

Figure.III.6 : En-tête NetAnim inclus dans le réseau……..48

Figure.III.7 : Les instructions d'animation XML NetAnim……49

Figure.III.8 : Les commandes d'exécutions NetAnim avec NS-3…….49

Figure.III.9 : le flux de Trafic réseau……..50

Figure.III.10 : configuration le traçage .pcap et tr…….…..51

Figure.III.11 : résultat d'exécution de programme avec NS-3……....52

Figure.III.12 : capture d'un paquet contient un message secret ''H''……..53

Figure.III.13 : capture d'un paquet contient un message secret ''E''……..54

Figure.III.14 : capture d'un paquet contient un message secret ''l''……....54

Figure.III.15 : capture d'un paquet contient un message secret ''l''……....55

Figure.III.16 : capture d'un paquet contient un message secret ''O''……..55

Liste des acronymes

AES : Advanced **E**ncryption **S**tandard

HAS : Humann **A**uditory **S**ystem

DES : Data **E**ncryption **S**tandard

HTTP: **H**yperactive **T**ext **T**ransport **P**rotocol

HTML : **H**yper **T**ext **M**arkup **L**anguage

IHL :International **H**umanitarian **L**aw

LSB : Least **S**ignificant **B**it

NS3 :Network **S**imulator **3**

PRBR : Packet **R**aw **B**it **R**ate

RSA : Rivest **S**hamir **A**dleman

RTP: Real-Time **T**ransport **P**rotocol

RTCP: Real-**T**ime **C**ontrol **P**rotocol

RTP: Real-time **T**ransfer **P**rotocol

ISN: Numéro de **S**équence **I**nitiale.

SVM :Machines à **V**ecteurs de **S**upport

SCTP : Stream **C**ontrol **T**ransmission **P**rotocol

SDP: Session **D**escription **P**rotocol

SIP: **S**ession **I**nitiation **P**rotocol

TTL : Time **T**o **L**ive

TOS : **T**ransport & **O**ffshore **S**ervices

TCP: Transmission **C**ontrol **P**rotocol

UDP: User **D**atagram **P**rotocol

URL: Uniform **R**esource **L**ocator

IPv4: Internet **P**rotocol **V**ersion 4

VoIP: Voice **o**ver **I**nternet **P**rotocol

INTRODUCTION GENRALE

Le problème d'échange de données secrètes a toujours existé, et ce depuis la naissance des grandes civilisations. La cryptographie offre un moyen pour protéger les données secrètes en les rendant inintelligibles aux personnes non autorisées, cependant, le simple fait de communiquer avec des messages chiffrés attire l'attention. Cela peut être problématique lorsqu'il s'agit d'un canal de communication surveillé par une tierce personne, qui peut, au moindre soupçon, détruire la communication entre les deux parties. Dans un tel cas de figure, une communication, contenant un message secret, entre deux personnes doit sembler normale aux yeux de la personne qui contrôle le canal. Pour ce genre de scénario, la stéganographie représente la solution alternative à la cryptographie.

La stéganographie, ou la science de communication secrète, est un procédé permettant de cacher un message secret au sein d'un médium hôte (original, cover) anodin, de telle sorte que le médium résultant (stégo) semble inaffecté (dissimulation indétectable) par l'insertion du message secret. Autrement dit, l'objectif est de rendre difficile, ou impossible, la distinction entre un médium original et un médium modifié par l'insertion d'un message secret.

De nos jours, avec le développement de l'Internet et l'explosion des médiums numériques (sons, images, et vidéos) partagés sur les différents réseaux de communication, la stéganographie devient une pratique populaire et accessible à toute personne souhaitant communiquer de façon discrète avec d'autres personnes. La communauté scientifique s'est alors particulièrement intéressée à cette discipline. Les chercheurs ont mis en évidence que la stéganographie appliquée aux médias numériques actuels représente un véritable challenge faisant appel à de nombreuses disciplines : mathématiques, statistiques, traitement du signal, théorie de l'information, et théorie des jeux.

Notre travail dans cette mémoire consiste à proposer d'une techniques stéganographiques, dont la sécurité du message secret est basée sur un système de transmission où on modifier le champ réservé aux données. Il s'agit ensuite d'étudier la performance de ces méthodes.

Le travail se compose de trois chapitre chaque un à un contenu diffèrent a l'autre mais tous sont définie et illustrer la stéganographie et la technique proposé.

Dans le premier chapitre on va définir des généralités sur tous ce concerne la communication numérique sécurisé, et donner des définitions et des comparaisons de la cryptographie, tatouage et la stéganographie.

Le deuxième chapitre spécifier les technique de stéganographie qui on peut appliquer dans un réseau informatique, et qu'ils peuvent être appliquées aussi dans des défirent protocoles définies comme (IP, TCP, RTP, RTCP).

On parle aussi de la VoIP et les classifications des technique stéganographique dans cette dernière.

Enfin, on parle sur la réalisation de l'application avec le logiciel KALI_LINUX à l'aide de NS-3 et on va arriver à des résultats qui on le interpréter.

Chapitre I

Système de Transmission Sécurisé

1. Introduction

Le contrôle des flux d'information est un problème central pour la sécurité d'un système quel qu'il soit : une entreprise, un État, un particulier ; tous ont des documents à préserver du regard d'autrui. Cela entraîne, par exemple, la volonté de s'assurer de la confidentialité du transfert d'informations, de nos jours pris en charge via des mécanismes cryptographiques. À défaut de savoir exactement ce qui peut arriver à la communication, on peut se prémunir des indiscrétions en chiffrant les données[1].

2. Système de communication numérique

une chaîne de transmission numérique a pour mission de transporter des données en minimisant le nombre d'erreurs et de pertes. D'autres paramètres sont tout aussi importants comme par exemple la puissance d'émission nécessaire ou la bande-passante.

C'est pourquoi l'étude des performances d'une chaîne de transmission est une étape essentielle de développement d'un système de télécommunications car l'écart parrapport aux performances théoriques peut être grand.

Cependant, la réalisation de prototype étant coûteuse et longue, il est apparu évident qu'une simulation sur ordinateur d'une chaîne complète de transmission permettrait de réduire les coûts et de donner une bonne estimation des résultats réels[1].

2.1 La chaine de transmission numérique

La chaine de transmission cité dans la figure1 est formée principalement de :

- L'émetteur
- Canal de transmission
- Récepteur

Le terme « chaine de transmission » cache en fait un ensemble de bloc, parmi lesquels nous pouvons retrouver ceux ci-dessous :

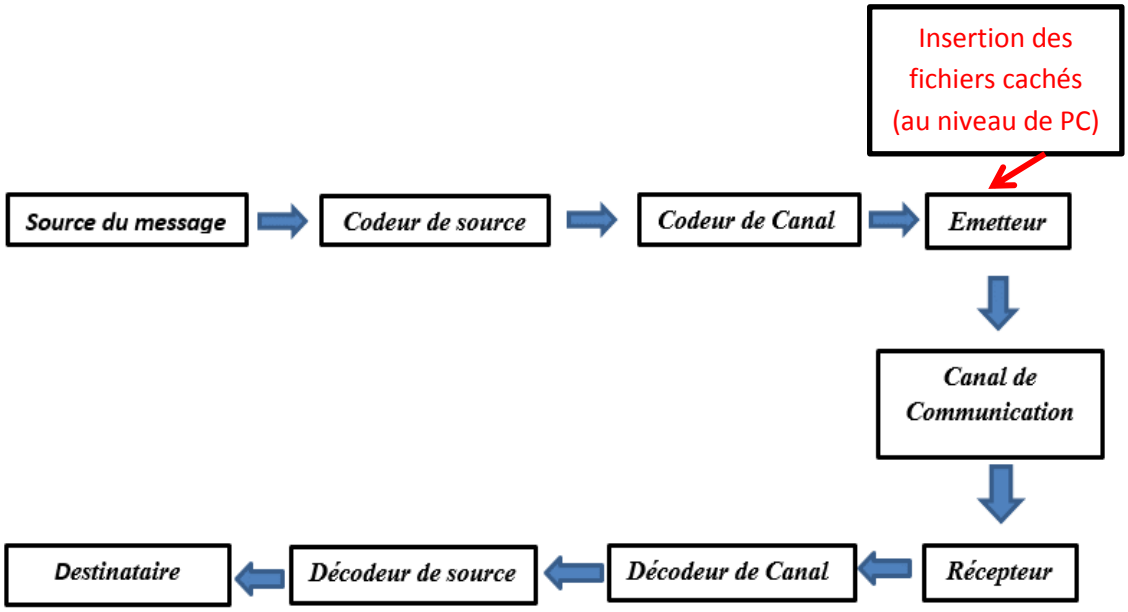


Figure I.1 : La chaine de transmission numérique [2].

- La source émet un message numérique sous la forme d'une suite d'éléments binaires
- Le codeur de source supprime les éléments binaires non significatifs (Compression de données ou codage de source).
- Le codeur canal introduit de la redondance dans l'information en vue de la protéger contre le bruit présent sur le canal de transmission. Le codage de canal n'est possible que si le débit de la source est inférieur à la capacité du canal de transmission (La probabilité d'erreur Pe tend dans ce cas vers 0 d'après les travaux de Shannon).
- La modulation a pour rôle d'adapter le spectre du signal au canal (milieu physique)sur lequel il sera émis.
- Enfin, du côté récepteur, les fonctions de démodulation et de décodage sont les inverses respectifs des fonctions de modulation et de codage situés du cote émetteur

2.1.1 L'émetteur

L'émetteur a pour fonction d'adapter le signal issu du transducteur en vue de le transmettre au canal de transmission. L'émetteur se compose de plusieurs bloc indépendants comme on peut le voir sur la Figure1. Le rôle et le fonctionnement de chaque bloc est détaillé dans les paragraphes suivants[2].

2.1.1.1Codeur en ligne (modulation en band de base)

Il est difficilement envisageable d'envoyer, à longue distance, un signal numérique sous la forme d'une simple suite d'impulsions rectangulaires. D'où l'intérêt d'utiliser un filtre de mise en forme adapté aux données du problème pour rendre la transmission plus robuste. Alors ce filtre de mise en forme doit satisfaire des critères liés aux spectres, transition et TEB (taux d'erreur par bit).

Dans cette partie on va traiter l'aspect spectrale de signal émis et pour cela on va étudier trois types de codeur en ligne qui se différent en fonction de ces critères [2].

2.1.1.2Filtre d'émission

A la sortie de codeur en ligne on obtient un spectre infini, en pratique il est impossible d'utiliser tout le spectre dans un canal réel, et il est alors nécessaire d'ajouter après cette forme d'onde un filtre de basse fréquence, qui servira à limiter la bande passante du signal émis. Ce filtre fait partie du filtre d'émission, ce dernier est composé aussi d'un filtre de blanchissant qui nous permet d'éliminer les interférences entre symboles (IES).

2.1.1.3Modulation à l'émission

Les modulations numériques consistent à utiliser une porteuse sinusoïdale haute fréquence modulée par un signal informatif numérique. Les techniques de modulation diffèrent mais les circuits modulateurs et démodulateurs sont identiques dans leur principe aux modulations analogiques.

2.1.2 Canal de transmission

Une ligne de transmission est une liaison entre les deux machines. On désigne généralement par le terme émetteur la machine qui envoie les données et par Récepteur celle qui les reçoit. La ligne de transmission, appelée aussi parfois canal de transmission ou voie de transmission.

2.1.3Le Récepteur

Le récepteur qui a pour fonction de reconstituer le message émis par la source à partir du signal reçu qui comprend des circuits de démodulation (pour les transmissions sur onde porteuse),de filtrage puis d'échantillonnage et de prise de décision. le démodulateur permet de ramener le signal modulé en bande de base. Le signal en bande de base est ensuit filtré puis échantillonné à des instants caractéristiques. Finalement un circuit de décision identifie la valeur des éléments binaires transmis à partir des échantillons reçus. Le choix effectué par le

circuit de décision est binaire, décision 0 ou décision 1, ce qui correspond à une opération dite de « détection ».

2.1.3.1 Démodulation

L'étape de la démodulation consiste à récupérer l'information utile en supprimant la porteuse. Ceci revient à passer du signal passe bande à un signal passe-bas. Nous avons considéré ici une démodulation fondée sur un filtre adapté à base de cosinus surélevé

2.1.3.2 Filtre de réception

L'étape du filtrage de réception du signal en sortie du canal est très essentielle, car il réduit la puissance de bruit (erreur binaire).

D'après les calculs qu'on a fait dans le cours on a trouvé que pour avoir un filtre de réception optimale il faut qu'on utilise un filtre adapté au signal d'entrée.

3. Transmission sécurisée de l'information

Dans le domaine de la transmission sécurisée de l'information, si l'on reconnaît la cryptographie comme l'art des codes secrets, la stéganographie est l'art de la dissimulation. Alors que la cryptographie consiste en une écriture indéchiffrable d'un message ou d'une information (ainsi rendue secrète), la stéganographie va plutôt s'attacher à cacher un message dans un contenu pour qu'il soit, non seulement indéchiffrable, mais imperceptible. Quant au tatouage, cet autre « principe de camouflage » offre des solutions techniques pour faire face aux problèmes de protection des droits et des copies. La figure 1.1, donné par résume les différentes techniques de la sécurité de l'information.

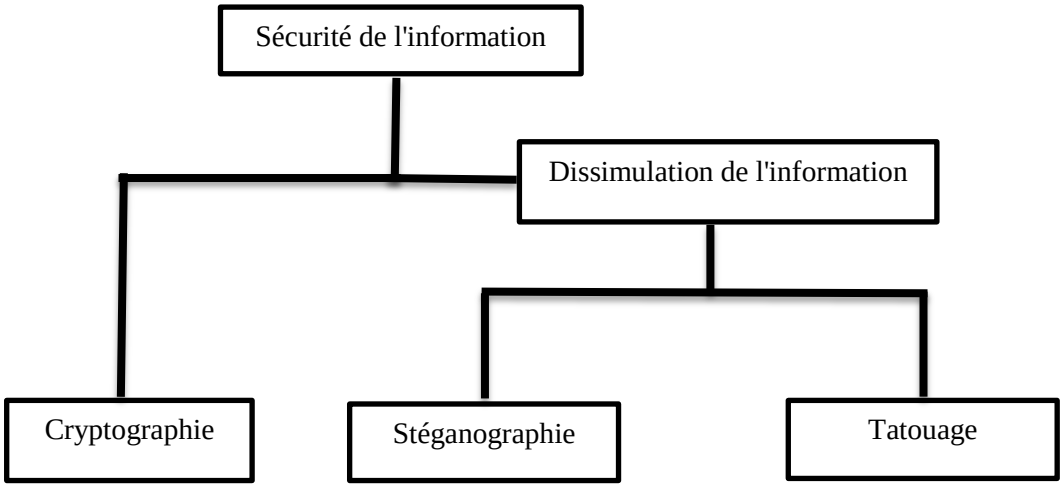


Figure I.2 : Techniques de la sécurité de l'information *[3]*.

3.1. Système de transmission cryptographique

La cryptographie utilise des concepts issus de nombreux domaines (Informatique, Mathématiques, Électronique). Toutefois, les techniques évoluent et trouvent aujourd'hui régulièrement racine dans d'autres domaines (Biologie, Physique, etc.)

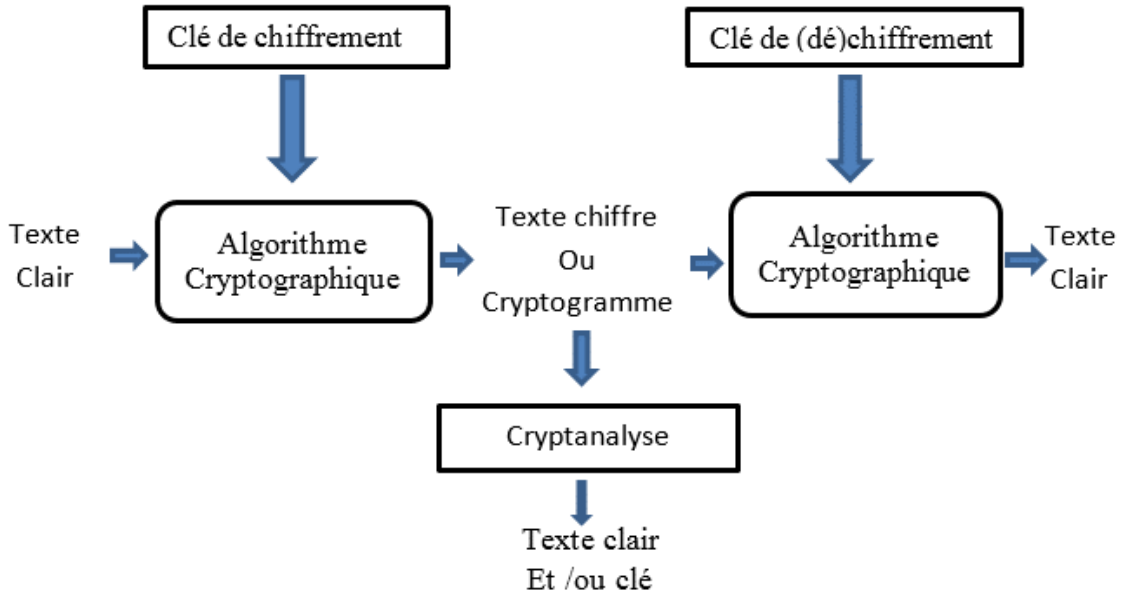


Figure I.3 : Protocole de chiffrement [4].

Cryptologie : Il s'agit d'une science mathématique comportant deux branches : la cryptographie et la cryptanalyse.

Cryptographie : La cryptographie est l'étude des méthodes donnant la possibilité d'envoyer des données de manière confidentielle sur un support donné.

Chiffrement : Le chiffrement consiste à transformer une donnée (texte, message, ...) afin de la rendre incompréhensible par une personne autre que celui qui a créé le message et celui qui en est le destinataire. La fonction permettant de retrouver le texte clair à partir du texte chiffré porte le nom de dé chiffrement.

Texte chiffré : Appelé également cryptogramme, le texte chiffré est le résultat de l'application d'un chiffrement à un texte clair.

Clef : Il s'agit du paramètre impliqué et autorisant des opérations de chiffrement et/ou déchiffrement. Dans le cas d'un algorithme symétrique, la clef est identique lors des deux opérations. Dans le cas d'algorithmes asymétriques, elle diffère pour les deux opérations.

Cryptanalyse : Opposée à la cryptographie, elle a pour but de retrouver le texte clair à partir des textes chiffré en déterminant les failles des algorithmes utilisés.

Crypto système : Il est défini comme l'ensemble des clés possibles (espace de clés), des textes clair set chiffré possibles associés à un algorithme donné.

3.2. Système de tatouage

Le terme de tatouage regroupe en fait un ensemble de techniques qui n'ont pas toutes les mêmes objectifs et ne visent pas le même type d'applications. Historiquement, le tatouage a été développé comme outil pour la protection des droits d'auteur, mais rapidement d'autres applications sont apparues, où le tatouage est par exemple utilisé pour la transmission de métadonnées robustes à des fins d'indexation, d'audimétrie ou pour fournir un contenu « amélioré » ou « étendu » (voir les *smart images* de la société américaine DigiMarc).

L'application protection du copyright elle-même regroupe plusieurs techniques (traçage, preuve de propriété, protection de copie, contrôle automatique de diffusion) dont les contraintes et les contextes d'utilisation sont très différents. C'est pourquoi il est plus judicieux de définir des profils regroupant les applications ayant les mêmes exigences mêmes si elles sont utilisées dans des domaines différents. On peut ainsi définir les profils suivants :

- super étiquetage ;
- fingerprint ou traçage de contenu ;
- preuve de propriété ;
- contrôle d'intégrité par tatouage fragile ou semi-fragile ;

- authentification .
- contrôle d'usage, notamment contrôle de copie.

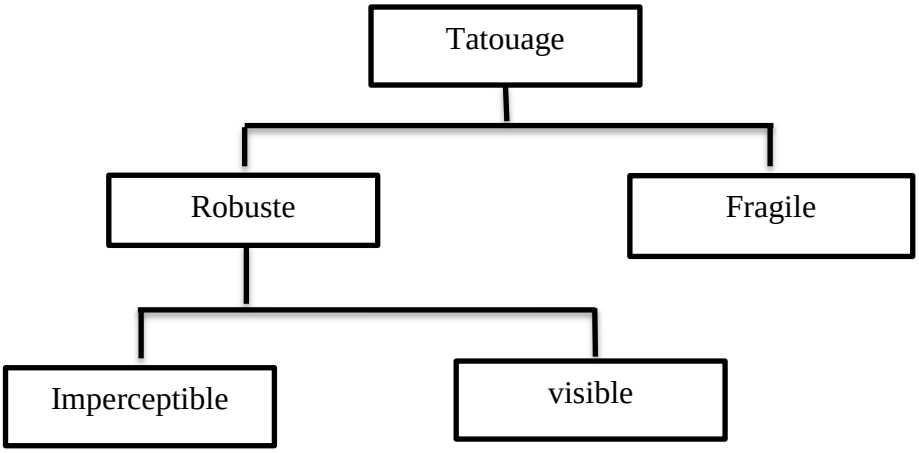


Figure I.4 : les types de tatouage [4].

Le tatouage comprend deux types : le tatouage fragile et le tatouage robuste.

Le tatouage numérique fragile : n'est utilisé que pour prouver l'authenticité des documents et l'intégrité des données. La protection de la marque "tatoue" étant très faible, le message qu'il transporte n'est pas vraiment important. La marque fait partie du document et ainsi, lorsque celui-ci est modifié, le marquage l'est également. Ce type de tatouage pose quand même un problème, car même s'il permet de prouver qu'un document a subi une transformation, il ne
prouve pas pour autant qui est l'auteur du document[3].

Le tatouage robuste : est plus dur à contourner et doit résisté à diverses attaques. Il doit Posséder les deux propriétés suivantes :

-la marque doit être très résistante vis à vis des différentes attaques connues telles que : ré échantillonnage, impression puis scanne, à la compression, à la coupure, aux bruits et aux changements de format.

- la marque doit être facilement reconnaissable après extraction et ceci malgré le dommage subi par les différentes attaques. Dans le cas contraire, la marque pourrait être incompréhensible ou avoir changée de sorte qu'elle n'ait plus rien à voir avec celle insérée à l'origine.

3.3. Système de transmission stéganographique

La stéganographie est l'art de "cacher" une information privée ou secrète dans un support. Le support peut être de plusieurs types tels qu'un fichier texte, image, audio, ou vidéo, mais peut également être un système de fichier, ou un code source. La caractéristique principale est que le fichier doit sembler ne contenir aucune information sensible, i.e. ne renfermer aucune information secrète. Le support associé à son message porte le nom de "stégo-médium». La stéganographie part du principe que la perception humaine n'est pas assez évoluée pour détecter les petites modification introduites dans les images et sont destinées à renfermer un message. De plus, personne ne sait, à priori, qu'un fichier renferme un message stéganographie (en dehors des personnes visées par le message)[5].

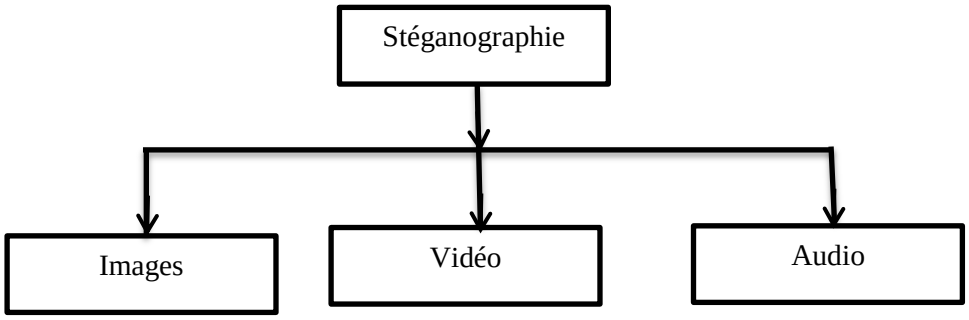


Figure I.5 : La stéganographie technique

La stéganographie technique regroupe toutes les techniques qui ne jouent pas sur les mots. La stéganographie technique est intéressante car elle permet de dissimuler des données dans plusieurs types de médias.

- *Audio*

Afin de transmettre de l'information de manière cachée dans du son, différentes techniques existent et se basent sur le fait qu'un son affecte la perception d'un autre :

- un son plus fort peut en cacher un autre.
- un son peut être caché temporairement lorsqu'il est moins fort et qu'il est placé avant ou après un son plus fort.

Il est également possible de cacher des données en utilisant la représentation des notes.

Prenons comme exemple un livre de Gaspar Schott, Schola Steganographique, où l'auteur explique que des messages ont été cachés dans de la musique, de sorte qu'une note correspondance à une lettre.

-Images, vidéo

Enfin, une image ou une vidéo peuvent également contenir un message. Une image est constituée de pixels. Il est possible d'insérer des bits du message secret à l'intérieur sans que ces modifications soient perceptibles à l'œil humain.

Aujourd'hui la stéganographie a énormément évolué et présente un intérêt grandissant. En effet, depuis 1996, cet art est de plus en plus employé, et on lui a porté une attention particulière depuis 2011 puisque différents groupes terroristes sont suspectés d'y avoir eu recours.

3.3.1. La Stéganographie dans l'Histoire

La première utilisation de la stéganographie remonte à la Grèce Antique où on utilisait certains esclaves pour transmettre les messages. Ceux-ci étaient écrits sur les crânes des messagers, et passaient donc inaperçu lorsque les cheveux repoussaient. Une fois suffisamment longs, le messager pouvait être envoyé, avec l'ordre de se faire raser le crâne une fois arrivé à destination. Le principal désavantage de cette méthode était l'attente pour l'envoi d'un message. Une autre technique était d'utiliser des tablettes de cire. Une fois la cire raclée, on gravait le message dans le bois de la tablette. Il suffisait ensuite d'y remettre de la cire, et le message était parfaitement caché[5].

En Chine ancienne, les messages étaient écrits sur de la soie, qui était ensuite roulée en boule, elle-même recouverte de cire. Un messager devait enfin avaler cette boule.

Au XVIIe siècle, Giovanni Porta, un scientifique italien, découvrit le moyen de cacher un message dans un œuf dur : en écrivant sur la coquille avec une encre contenant une once d'alun par pinte de vinaigre. L'encre pénètre alors la coquille et le message se voit écrit sur le blanc de l'œuf .sans apparaitre sur la coquille. Pour lire le message, il suffit d'éplucher l'œuf.

Enée le Tacticien, un historien de la Grèce Antique, imagina de percer de minuscules trous sous certaines lettres d'un texte anodin. Une fois toutes les lettres ainsi marquées relevées, on pouvait lire le message caché. Ces trous étaient invisibles pour une personne n'étant pas au courant de la méthode employée.

Durant la seconde guerre mondiale, on utilisa l'encre invisible. Cette encre, pouvant être créée notamment à partir de lait, de vinaigre, d'urine, de jus de citron ou encore de chlorure d'ammoniac, permettait d'écrire sur du papier sans pour autant afficher les caractères ainsi notés.

Déférentes méthodes linguistiques existent également. Pour cacher un message dans un texte, on peut jouer sur l'espace entre les mots, la ponctuation, ou encore l'orthographe. A l'origine, c'est l'acrostiche qui permettait de cacher ces messages. L'acrostiche est un poème dont la première lettre de chaque vers compose un mot ou une phrase. Dès qu'un enfant commence à écrire, il pratique donc souvent l'acrostiche pour son premier cadeau de fête des mère! Un des exemples les plus imposant fut sans doute le livre Hypnorotomachia Poliphili publié en 1499 par un anonyme. On découvre dans cet ouvrage que si on regroupe la première lettre de chacun des chapitres, au nombre de 38, on peut recomposer la phrase Poliam frater Franciscus Columna peramavit ce qui signifie Frère Francesco Colonna aime Polia passionnément.

4. Comparaison entre Cryptographie et la Stéganographie

Tout comme la cryptographie, le but principal de la stéganographie est de protéger une information. La déférence intervient dans la manière avec laquelle chaque technique procède. La cryptographie va chiffré l'information pour qu'elle ne soit pas compréhensible par un tiers, alors que la stéganographie va la rendre invisible.

On utilisera dès lors cette dernière notamment lorsque les techniques cryptographiques sont inapplicables, ou lorsqu'on souhaite gardé secret le fait même de communiquer. C'est en effet là le principal avantage de la stéganographie par rapport à la cryptographie : le fichier renfermant le message caché reste anodin. Personne ne peut se douter qu'il cache un message. Au contraire, un message chiffré annonce clairement qu'il renferme une information, puisque, par définition, il est chiffré[4].

5. comparaison entre tatouage et la Stéganographie

Le tatouage consiste à cacher une information dans le but de protéger le support contre la copie, contre toute modification de ce support ou dans un but d'identification. On considère souvent le tatouage comme la forme moderne de la stéganographie, ou en tout cas comme la principale application de sécurité reposant sur la stéganographie.

6. Système de transmission stéganographique de la parole

La prolifération des données numériques dans leurs différents formats a suscité un intérêt particulier pour les chercheurs afin d'assurer leur sécurité. Des techniques telles que le cryptage et le tatouage sont déjà utilisées à cet égard. Cependant, la nécessité de nouvelles techniques et de nouveaux algorithmes pour contrer les tentatives malveillantes en constante évolution de l'intégrité des données numériques est devenue une nécessité dans l'ère numérique d'aujourd'hui. La stéganographie, qui signifie littéraire «écriture couverte» a attiré plus d'attention au cours des dernières années. Son objectif principal est de cacher le fait qu'une communication se déroule entre deux parties. L'expéditeur incorpore des données secrètes de n'importe quel type en utilisant une clé dans un fichier de couverture numérique pour produire un fichier stego, de telle sorte qu'un observateur ne peut pas détecter l'existence du message caché. À l'autre extrémité, le récepteur traite les reçus

Stego-file pour extraire le message caché. Un exemple de stéganographie audio est illustré à la Fig. 1 où le fichier de couverture utilisé est un signal audio numérique. Une application évidente est une communication cachée utilisant un signal audio de couverture inoffensif, comme des conversations par téléphone ou par vidéoconférence.

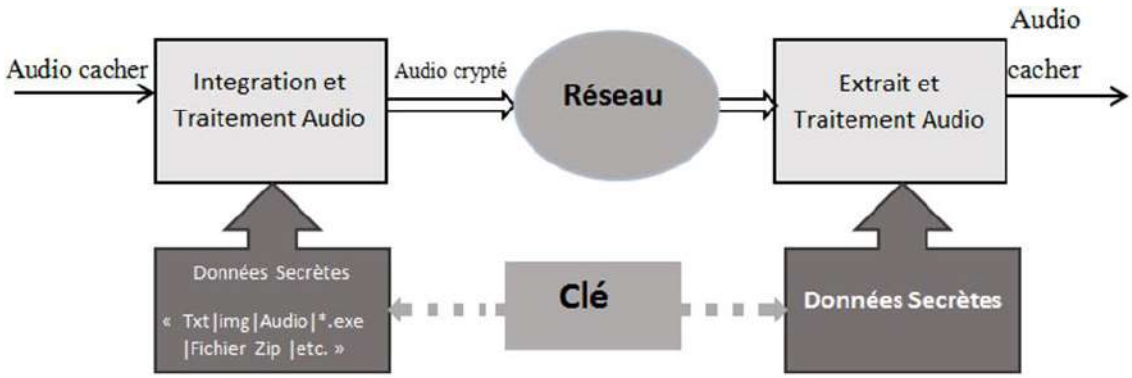


Figure I.6 : diagramme des blocs pour la stéganographie audio.

Afin de minimiser la différence entre le support original et celui obtenu après l'intégration des données cachées, les techniques récentes de stéganographie bénéficient des limitations naturelles des perceptions auditives et visuelles humaines d'une part et, d'autre part, des propriétés des médias numériques à travers En les utilisant comme une couverture pour véhiculer des communications secrètes. La stéganographie basée sur l'image et la vidéo repose sur le système visuel humain limité dans la variation de luminance remarquable à des niveaux supérieurs à 1 sur 240 en niveaux de gris uniforme ou 1 sur 30 de motifs aléatoires. Cependant, la stéganographie audio exploite la propriété de l'effet de masquage de « Humann Auditory System (HAS) ».

Diverses caractéristiques influencent la qualité des méthodes stéréo-graphiques audio. L'importance et l'impact de chaque fonction dépend de l'application et du milieu de transmission.

Les propriétés les plus importantes incluent la robustesse du bruit et la manipulation du signal, la sécurité et la capacité de dissimulation des données intégrées. L'exigence de robustesse est étroitement liée à l'application et est la plus difficile à satisfaire dans un système stéganographique. En outre, il existe un compromis entre la robustesse et la capacité de dissimulation. Généralement, ils ne coexistent pas dans le même système stéganographique.

7. Classification des systèmes stéganographiques de la parole

7.1.Classification selon la clé

Il existe deux types des clés de Stéganographie (cryptographie) :

7.1.1. Les principaux concepts cryptographiques

7.1.1.1. Crypto-système à clé symétrique

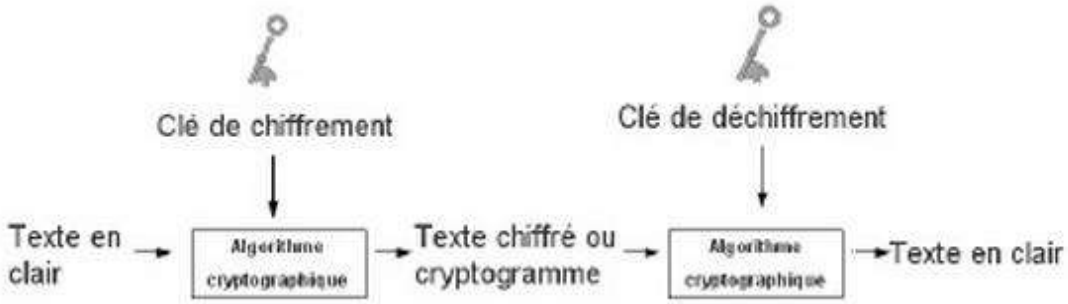


Figure I.7 : chiffrement avec la clé symétrique

Caractéristiques :

- Les clés sont identiques :K_E=K_D=K.
- La clé doit rester secrète.
- Les algorithmes les plus répandus sont le DES, AES, 3DES, ..
- Au niveau de la génération des clés, elle est choisie aléatoirement dans Ces algorithmes sont basés sur des opérations de transposition et de substitution des bits du texte clair en fonction de la clé, l'espace des clés.
- La taille des clés est souvent de l'ordre de 128 bits. Le DES en utilise 56, mais l'AES peut aller jusque 256.
- L'avantage principal de ce mode de chiffrement est sa rapidité.
- Le principal désavantage réside dans la distribution des clés : pour une meilleure sécurité, on pratiquera à l'échange de manière manuelle. Malheureusement, pour de grands systèmes, le nombre de clés peut devenir conséquent.

7.1.1.2. Cryptosystème à clé publique



Figure I.8 : chiffrement avec la clé public

- Une clé publique $\boldsymbol{P_K}$(symbolisée par la clé verticale),
- Une clé privée secrète $\boldsymbol{S_K}$(symbolisée par la clé horizontale),
- Propriété : La connaissance de$\boldsymbol{P_K}$ne permet pas de déduire$\boldsymbol{S_K}$.
- $\boldsymbol{D_{SK}(E_{PK}(M)) = M}$.
- L'algorithme de cryptographie asymétrique le plus connu est le RSA.

7.2. Classification selon le domaine d'insertion

Les techniques de stéganographie basées sur l'insertion fonctionnent en insérant des blocs de données Dans un fichier hôte. En utilisant une technique basée sur l'insertion, les données sont Point dans chaque fichier. Ce type de technique fonctionne en trouvant des endroits dans un fichier qui Peut être modifié, sans avoir d'effet significatif sur le fichier hôte.

Une fois ces zones redondantes identifiées, les données à masquer peuvent être rompues Up et inséré dans eux et sera assez difficile à détecter. Cela dépend de Le format de fichier, ces données peuvent être cachées entre les en-têtes, dans les tables Des données d'image ou dans plusieurs autres domaines.

Un moyen très courant de masquer des données est de l'insérer dans les bits les moins significatifs (LSB) d'un fichier 8 bits ou 16 bits, par exemple un fichier son 16 bits. Avec son Fichiers, on peut changer le premier et le second LSB de chaque groupe 16 bits sans Ayant un impact important sur la qualité du son. Parce que les données sont toujours .Étant inséré au même endroit pour chaque fichier, il peut être classé Technique d'insertion steganographique.

7.3. Classification selon le protocole de transmission

Pour comprendre cette technique, il est important que vous compreniez bien De réseautage et la suite de protocoles TCP / IP. Nous décrivons brièvement la terminologie du réseau de base dont vous aurez besoin pour comprendre cette section.

7.3.1. Réseautage et TCP / IP : les bases

Si vous souhaitez envoyer une lettre à quelqu'un, vous ne pouvez pas simplement écrire une lettre et la déposer dans La boîte aux lettres parce que le bureau de poste ne sait pas où le transmettre.

Afin de s'assurer que le courrier arrive à sa destination, il faut mettre la lettre Dans une enveloppe et adressez-vous. Ce même concept est utilisé dans les réseaux, Sauf que, au lieu de mettre des lettres dans des enveloppes, les données reçoivent un protocole En-têtes. Les en-têtes de protocole agissent comme une enveloppe pour identifier les données destination.

Le protocole que chaque ordinateur sur Internet utilise pour communiquer avec Quiconque dans le monde est la suite de protocole TCP / IP, qui a été développée dans Les années 1970 dans le cadre de la recherche originale qui a mené à Internet. Le protocole TCP / IP Suite contient en fait quatre protocoles de communication principaux : IP, TCP, UDP,et ICMP. Ces protocoles s'exécutent à la fois sur l'ordinateur émetteur et sur la réception Ordinateur pour normaliser les communications. Le protocole TCP sur L'ordinateur de l'expéditeur communique avec le protocole TCP sur le récepteur Ordinateur, et le protocole IP sur l'ordinateur de l'expéditeur communique avec le protocole IP sur l'ordinateur du récepteur.

Les en-têtes de protocole ont été créés afin que l'expéditeur puisse fournir des informations clés À propos de la communication au destinataire. Parce que ces en-têtes ont été créés il y a 30 ans, certaines informations ne sont pas nécessaires aujourd'hui ou peuvent être Modifié sans affecter le trafic. Cela rend le protocole basé sur l'en-tête Stego possible. Chaque paquet sur Internet doit contenir ces en-têtes, et vous pouvez facilement intégrer des données dans la partie inutile d'entre eux.

7.3.2. En-têtes UDP et ICMP

Il existe deux autres protocoles dans la suite de protocoles TCP / IP. UDP ou Datagramme utilisateur Protocole, est un protocole de transmission peu fiable. Avec UDP, le paquet est également très petit et ne donne pas beaucoup de place pour cacher les données.

Le dernier protocole est ICMP, ou Internet Control Message Protocol. Ceci est utilisé pour résoudre les réseaux et envoyer des messages d'erreur réseau. Par exemple, lorsque vous

effectuez un Ping sur un hôte pour voir s'il est en vie, vous utilisez ICMP. Ou si vous envoyez un message à un hôte invalide, vous recevrez très probablement un message ICMP "hôte inaccessible".

Étant donné que ICMP a une petite taille d'en-tête, il ne constitue pas un bon candidat pour l'en-tête Stego ; cependant, car il y a généralement beaucoup de trafic ICMP survenant sur un réseau, il constitue un bon candidat pour se cacher dans un protocole explicite.

7.3.3. Cacher dans un Protocole Ouvert (http)

La dernière catégorie de réseau Stego consiste à cacher des données dans un protocole évident. Essentiellement, c'est ce qu'on appelle le camouflage des données, où vous faites ressortir les données comme autre chose. Avec cette technique, vous prenez des données, mettez-la en réseau normal trafic, et modifier les données de telle sorte qu'il ressemble à un protocole évident.

Par exemple, la plupart des réseaux transportent de grandes quantités de trafic HTTP ou web. Vous pouvez envoyer des données sur le port 80, et cela ressemblerait au trafic Web. Le problème est-ce que si quelqu'un a examiné la charge utile, il ne semblerait pas normalLe trafic web, qui contient généralement du code HTML. Et si vous avez ajouté des symboles tels que comme <></ pour les données ? Parce qu'il s'agit des types de caractères HTML contient, le trafic ressemblerait au trafic Web et devrait probablement observateur occasionnel.

C'est exactement le processus utilisé par le programme Reverse WWW Shell. Inverser. WWW Shell non seulement masque les données pour se ressembler au trafic Web, il le fait dans Une façon qui peut contourner la plupart des pare-feu. Au lieu de l'attaquant essayant de se connecter un client qui, dans la plupart des cas, est protégé par un pare-feu, Reverse WWW Shell est installé sur un système client derrière un pare-feu. Puis, à intervalles réguliers, se connecte sur le port 80. Maintenant, le pare-feu pense que c'est un ordinateur client surfer le web et permet la circulation. En réalité, le client lance une connexion Sortant vers un attaquant et lui envoie une invite de commande.

Maintenant, l'attaquant peut taper les commandes qu'il veut sur le client. Pendant ce temps, toutes les commandes et les données sont cachées en HTML circulation.

8. Steganalyse

Contrairement à la stéganographie, la stéganalyse est l'art et la science de détecter si un medium donné cache un message secret, et si possible, de récupérer ce message caché. Ceci est analogue à la cryptanalyse appliquée à la cryptographie[3].

La Stéganalyse est en effet une tâche très difficile, en raison de la grande diversité des mediums, la grande variation des données, les différents algorithmes d'insertion et généralement la faible distorsion due à l'intégration du message. Malgré cela, la stéganalyse est encore possible, car l'insertion du message perturbe les statistiques du medium original.

En d'autres termes, la présence d'un message intégré rend un medium original et sa version stégo correspondante différents à certains aspects, bien que cette présence est souvent imperceptible à l'œil humain.

Selon la littérature, les méthodes de stéganalyse peuvent généralement être classées en deux catégories : spécifiques et universelles. Alors que la première vise à casser un algorithme stéganographique spécifique, la deuxième tente à briser tous les algorithmes de stéganographie. En général, les approches spécifiques ont une précision de détection plus élevée par rapport à celles universelles, car elles ont une connaissance préalable de la méthode d'insertion. Néanmoins, la stéganalyse universelle est plus attrayante dans l'utilisation pratique, car elle fonctionne indépendamment de la technique d'insertion et donc elle s'applique à des algorithmes d'insertion inconnus.

La stéganalyse universelle peut être considérée comme un processus de reconnaissance de formes. Elle doit au final déterminer à quelle classe : médium original, ou médium stégo, appartient un médium sous test. Un principe général d'un algorithme de stéganalyse universel est d'identifier et d'extraire des caractéristiques qui sont particulièrement sensibles à l'intégration de message. Ces caractéristiques doivent être en mesure de capter les variations résultantes de cette intégration. Cela signifie que les caractéristiques extraites d'un médium original devraient être différentes de celles médium stégo correspondant.

En général, plus la différence est grande, meilleur est le choix des caractéristiques extraites. Après l'extraction de caractéristiques, un classificateur est généralement utilisé pour distinguer le deux médiums propre et stégo à partir de leurs vecteurs caractéristiques.

Globalement, la performance d'un système de stéganalyse dépend notamment de choix du vecteur de caractéristiques à N dimensions, extrait à partir du médium, et de l'efficacité du classificateur utilisé. Naïvement, on pourrait s'attendre à ce que N doit être aussi grand que

possible pour que le vecteur de caractéristiques soit plus efficace. Or, des études récentes montrent que d'une part, N ne doit pas être nécessairement très grande et d'autre part, un N très grand, généralement entraîne des coûts informatiques élevés et un impact négatif sur la précision de la détection Les transformées en ondelettes sont très utilisées pour extraire les

vecteurs des caractéristiques des mediums originaux et stégos .

Pour la classification (ou stéganalyse), les vecteurs de caractéristiques extraites à partir d'un ensemble de médiums avec ou sans une information cachée dans chacun d'eux, sont introduits dans un algorithme d'apprentissage pour apprendre le classifieur avant de l'utiliser pour séparer les deux types de médiums : original et stégo. A ce titre, l'analyse discriminante linéaire de Fisher (FLD) [Farid, 2002], et l'analyse discriminante non linéaire, tels que les 19 Machines à vecteurs de support (SVM), sont largement utilisées avec succès dans des techniques de stéganalyse antérieures. Nous rappelons ci-dessous l'analyse discriminante linéaire de Fisher utilisée dans notre étude, mais aussi les Machines à vecteurs de support (SVM) (que nous n'avons pas pu utiliser, faute de temps)

La stéganalyse consiste à identifier la présence d'un message. Seule cette présence doit être déterminée. Dans un second temps, le message lui-même pourra être retrouvé, mais ce n'est pas l'objectif principal de la stéganalyse.

Il existe deux catégories d'attaques :

***Les attaques passives* :** elles visent à identifier la présence d'un message, dans le but secondaire de pouvoir le reconstituer par la suite. Ces attaques peuvent prendre plusieurs formes :

- la lecture ou l'écoute du fichier,
- la comparaison avec le fichier original (si il est disponible),
- certaines attaques statistiques (attaques sur le LSB)
- la détection des signatures des logiciels utilisés (étude du code hexadécimal)

Les attaques actives : elles consistent à détruire le message caché, sans prêter attention à ce qu'il signifie. L'objectif est de supprimer le message, ou en tout cas, à le rendre inutilisable. Cette destruction aura souvent lieu par l'intermédiaire de modification du support (redimensionnement (image, vidéo), filtrage (sons), compression, ...)[4].

9. Conclusion

La stéganographie reste un vaste champ de recherches de nos jours, même si les techniques les plus utilisées et les plus connues utilisent sans conteste les fichiers images et les fichiers audio pour les non informaticiens, tandis que les canaux cachés restent plus difficiles à mettre en place et ne sont pas à la portée des néophytes.

Chapitre II

Les Techniques de Stéganographie

1. Introduction

La téléphonie IP ou la voix sur IP (VoIP) est un service en temps réel qui permet aux utilisateurs d'effectuer des appels téléphoniques via des réseaux de données IP. C'est l'un des services les plus importants des réseaux basés sur IP et affecte l'ensemble du structures des télécommunications. Une connexion téléphonique sur IP (ToIP) se compose de deux phases dans lesquelles certains types de trafic sont échangés entre les parties appelantes: la phase de signalisation et la phase de conversation.

Pendant La première phase : certains messages de protocole de signalisation, tels que les messages de Session Initiation Protocol (SIP), comme : l'accusé de réception (ACK), 200, 180…etc, sont échangés entre l'appelant et appelé. Ces messages sont destinés à configurer et à négocier les paramètres de connexion, entre les parties appelantes.

Pendant la deuxième phase : deux flux audio sont envoyés Bi-directionnellement (en mode full-duplex) via le Protocole de transport en temps réel (RTP). Ce dernier est le plus souvent utilisé pour le transport de données vocales [5].

2. Les techniques de steganographie appliquées au réseau informatique

La stéganographie dans la pile protocolaire TCP/IP utilise quelques champs d'entêtes IP ou TCP pour établir des canaux de communication cachée. Les données secrètes sont généralement insérées (transmettre) dans des champs qui sont optionnel ou souvent inutiles.
Dans la pile TCP / IP, il existe un certain nombre de méthodes disponibles, permettant échangées secrètement les données entre les parties de communication par la création des canaux cachées. Une analyse des en-têtes de protocoles TCP / IP, donne des champs qui sont soit inutilisé ou facultatif. Cela révèle de nombreuses possibilités où les données peuvent être cachées et transmis. L'en-tête IP possède des champs disponibles pour être utilisé comme canaux cachés (figure. II.1).
Notez que ces méthodes steganographique jouent un rôle important de la communication VoIP car les protocoles mentionnés ci-dessus sont présents dans chaque paquet (peu importe, s'il s'agit d'un message de signalisation ou d'un paquet de donnée) [6].

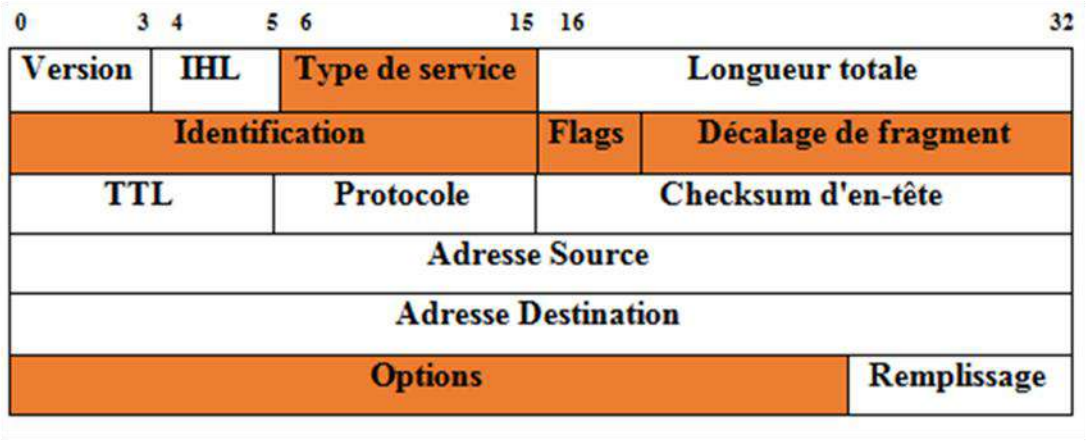


Figure.II.1 : format d'entête IP**.**

Pour ce type de méthode steganographique ainsi la bande passante des messages cachées peut être s'exprime comme suit :

$$PRBR = \frac{SB_0 + \sum_{j=1}^{l} SB_j}{l+1} [bits/packet] \qquad (II.1)$$

Où **:**

- *PRBR (PacketRaw Bit Rate) :* désigne la bande passante du canal caché créé par TCP IP en [bits / paquet].
- SB_0**:** est la quantité totale de bits qui peuvent être envoyés secrètement sur les champs du premier paquet.
- *L :* est le nombre de paquets envoyés en plus du premier paquet.
- SB_j: désigne la quantité totale de bits qui peuvent être dissimulés et envoyés dans les champs des paquets.

2.1. Les techniques de steganographie qui peuvent être appliquées au protocole IP

Le champ type de service : les huit bits du type de service (ToS) dans l'entête IP (figure. II.1) sont utilisés pour indiquer les paramètres de qualité de service aux routeurs sur le chemin d'un paquet.

Ils sont maintenant rarement utilisés avec leur sémantique originale, ce champ a été réutilisé dans par exemple, la mise en œuvre de DiffServ. Il est possible d'utiliser les bits dans ce champ en tant que transporteur stéganographique. Cependant, cette technique est facilement détectée par le processus de steganalyse, car le champ est mis à zéro dans presque toutes les configurations par défaut du système d'exploitation[6]..

Le champ d'identification : Une valeur d'identification (ID) (figure.II.1) attribuée par l'expéditeur pour faciliter l'assemblage des fragments d'un datagramme, et reçoit 16 bits de l'en-tête IP. Étant donné que l'ID de l'entête IP est utilisé pour distinguer les fragments constituant un seul paquet. Les identifiants IP qui sont uniques dans une fenêtre de temps donnée sont nécessaires pour assurer que les fragments de paquets ne sont pas réassemblés en un seul paquet sur l'hôte récepteur.

Le champ Flags: les paquets IP incluent deux drapeaux :

Do not fragment (DF) : égal à 1, si le paquet contient le dernier fragment, ou si le paquet n'a pas été fragmenté.

Fragments (MF) : égal à 0 indiquant que le paquet sera perdu s'il ne peut pas être envoyé sans fragmentation.

Lorsque la taille des paquets est inférieure au maximum taille du segment, le drapeau DF n'a aucun effet sur le comportement des paquets. Alors on peut exploite le DF pour créer un système steganographique (un canal cachées) et envoyer les données secrètes.

Le champ fragmentation : lorsque les paquets IP sont fragmentés, les fragments individuels contiennent un champ décalé, cela permet à l'hôte récepteur de reconstruire les fragments dans les positions correctes dans ses tampons de réception. L'information peut être transmise de façon dissimulée en modulant la taille des fragments créés par un hôte et donc le fragment se décompose. Comme pour les champs d'identification IP et de ToS, ceci la méthode d'encodage stéganographique est facilement détectée**.**

Le champ Options : les paquets IP contiennent très rarement des «options», de sorte que leur potentiel stéganographique est limité. L'utilisation de l'option IP est décrite, mais en plus d'être facilement détectable, les paquets avec cette option présente peuvent voyager au plus 20 sauts, donc il est peu utile dans l'Internet ouvert [6].

2.2. Les techniques de Steganographie qui peuvent être appliquées au protocole TCP

Au niveau de la couche de transport, TCP est destiné à fournir un service de communication de processus à processus fiable dans un environnement multi-réseau. TCP est donc un protocole de transport sécurisé et axé sur la connexion. L'en-tête du protocole TCP est illustré à la figure II.2 [6].

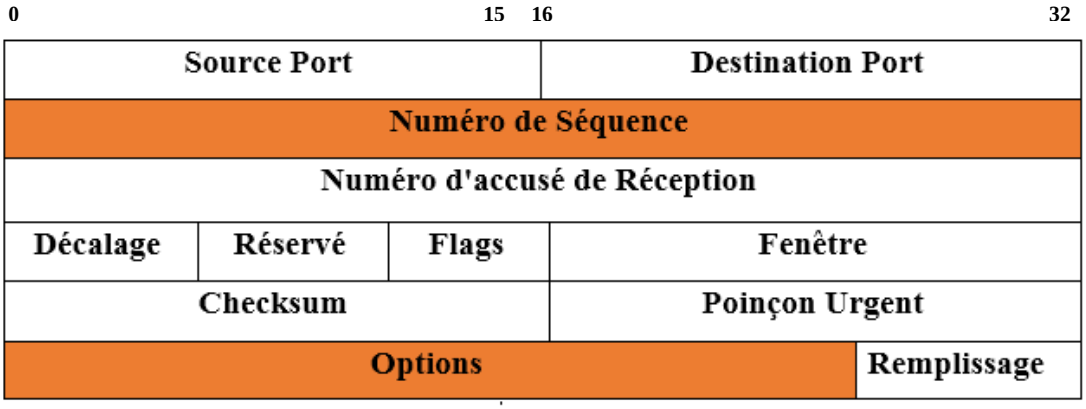


Figure II.2 : format d'entête TCP.

Numéro de séquence : les numéros de séquence TCP prennent en charge les fonctions de fiabilité fourni par TCP (et dans une certaine mesure, les fonctions de contrôle de flux). Chaque octet de données transmises sur un flux TCP reçoit un numéro de séquence.

Dans TCP, une connexion (définie par une paire de sockets) peut être réutilisée, et donc l'hôte doit pouvoir détecter si un segment provient d'une connexion courant ou d'un précédent.

Lorsqu'une connexion est établie, les deux hôtes doivent choisir un numéro de séquence initiale (ISN). L'algorithme qui génère ces numéro séquence initiaux doit garantit que les chevauchements dans l'espace de ce dernier (numéro de séquence) entre différents connexions sont empêchées.

Une mise en œuvre du prototype de stéganographie en utilisant TCP ISN (et l'ID IP), Couvert TCP, est décrit dans. Il remplace simplement le champ choisi avec les données à envoyer, peut-être être détecté soit en observant que le champ ne satisfait pas le chevauchement nécessaire et les contraintes d'unicité, ou en comparant les données observées avec les motifs statistiques de suspect texte clair [6].

TimestampTCP: l'option d'horodatage TCP permet à un hôte de mesurer avec précision le temps de parcours d'un chemin, et atténue également les problèmes liés à numéro de séquence aller-retour dans les réseaux avec une large bande passante x produits de retard .Pour nos besoins, il suffit de comprendre les contraintes sur les valeurs des timestampTCP, vous trouverez en plus de détails sur les en fonction de fonctionnalités.

L'option timestamps se compose de deux 32 champs de bits, TS value et TS écho répondre. Le champ de valeur TS est défini en fonction de l'horlogetimestampsde l'expéditeur, et il est dans ce domaine que les données cachées peuvent être intégrées.

Les seules contraintes qui pèsent sur l'horloge d'horodatage sont que sa fréquence de tique soit entre 1 Hz et 1 kHz, et que ce soit strictement monotone.

Un canal caché sur la base de la modulation de bit le moins des horodatages TCP transmis par un hôte, est décrite dans le schéma .Procédé fonctionne en incrémentant l'horodatage associé à un paquet (et de retarder en conséquence) afin de transmettre un ` 1' bit de texte chiffré. L'utilisation de TCP timestamp n'est pas universelle, mais il est déployé en standard sur les versions les plus récentes de Linux et d'autres systèmes d'exploitation Unix, donc l'observation de horodatages d'un système d'exploitation qui ne les supporte pas serait suspecte.

Ordre de paquet : en plus du contenu du paquet, la commande des paquets peut être utilisé pour transporter des informations. Cela repose sur d'être utilisé sur un réseau IPSec pour récupérer l'ordre d'origine, ce qui limite son applicabilité. Étant donné que les paquets sont rarement réorganisés par l'hôte de transmission, un gardien qui est proche de alice sera sans aucun doute remarqué le montant anormalement élevé de ré ordonnancement[6].

2.3. Les techniques de steganographie appliquées au protocole RTP

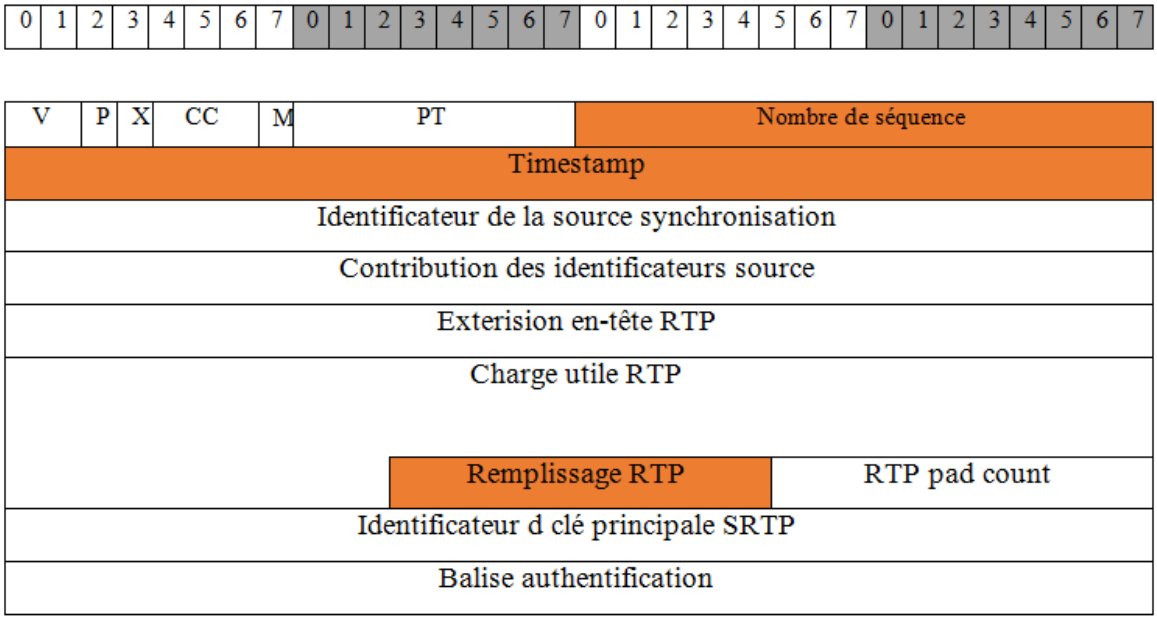
En phase de conversation de l'appel lorsque le flux de la voix est transmis, en plus de protocoles présentés à la section 2.1 et 2.2 les champs du protocole RTP mai également être utilisés comme un canal caché. Figure.II.3 présente l'en-tête RTP [7].

RTP offre les possibilités suivantes pour la communication cachée :

Champ de remplissage (padding) : peut être nécessaire dans certains algorithmes de cryptage. Si le bit de remplissage (P) est défini, le paquet contient un ou plusieurs remplissages supplémentaires (octets) à la fin de l'en-tête RTP qui ne font pas partie de la charge utile (payload).

En-tête d'extension (quand X bit est défini) : situation semblable comme avec le mécanisme de remplissage, une extension d'en-tête de longueur variable peut être utilisée.

Valeurs initiales des champs numéro de séquence et de timestamp : car les deux valeurs initiales de ces champs doivent être aléatoires, le premier paquet RTP du flux audio peut être utilisé pour une communication secrète.



FigureII.3 : format d'entête RTP.

Les bites les moins signifiants de timestamp (LSB) :

Peut être utilisé de la même manière que proposé dans la messagerie confidentielle via TCP Timestamps.

Il faut souligner cependant que la stéganographie dans les champs libres / inutilisés / facultatifs pour le protocole RTP peut être potentiellement éliminé ou fortement limitée par les *active warden*. La normalisation des valeurs des champs des en-têtes RTP (par exemple, appliquée aux Timestamps) ou de petites modifications appliquées peut suffire à limiter la bande passante cachée [7].

2.4. Les techniques de steganographie appliquées au protocole RTCP

L'échange RTCP est basé sur la transmission périodique des paquets de contrôle à tous les participants de la session. Généralement, il fonctionne sur deux types de paquets (rapports) appelés: Rapport du récepteur (RR) et Rapport de l'émetteur (SR). Certains paramètres qui sont inclus dans ces rapports peuvent être utilisés pour estimer l'état du réseau. Plus sur tous les messages RTCP doivent être envoyés dans un paquet composé qui comprend au moins deux types de rapports RTCP. Figue.II.4 présente les en-têtes des rapports SR et RR du protocole RTCP [7].

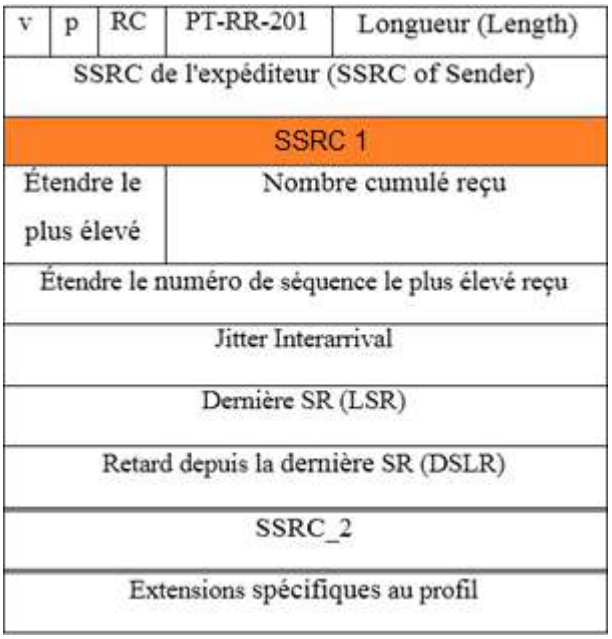


Figure II.4.a : RTCP Rapport du récepteur (RR)

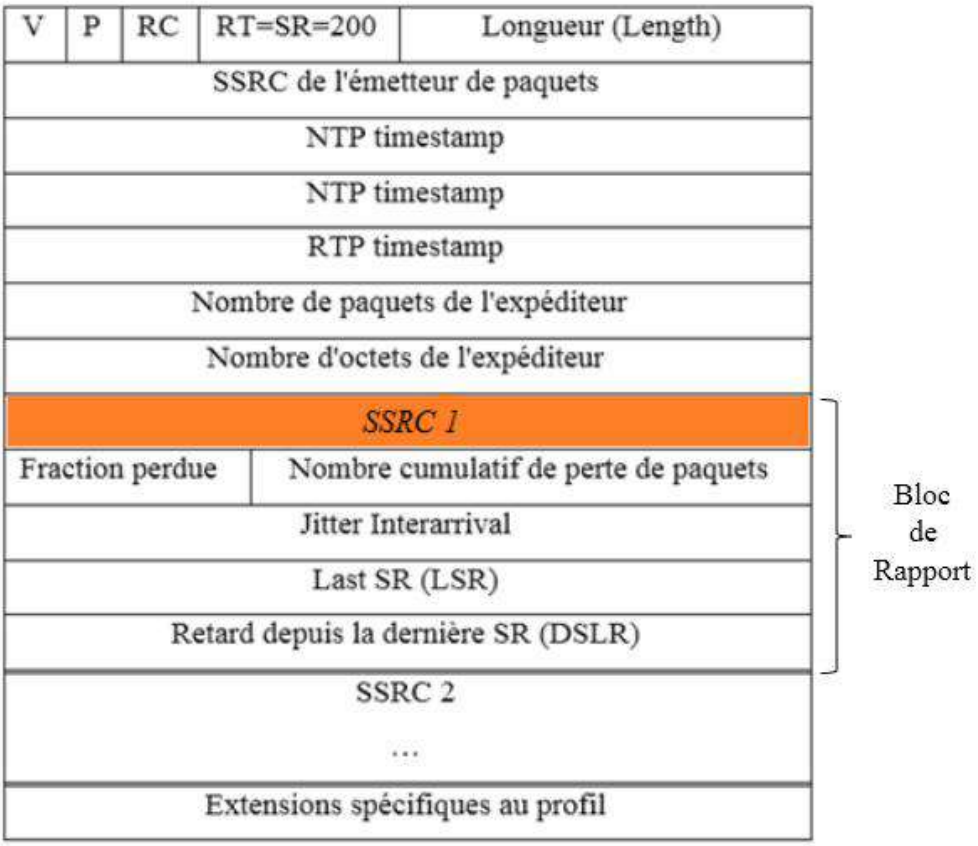


Figure II.4.b : RTCP Rapport de l'émetteur (SR).

Pour les sessions avec un petit nombre de participants, l'intervalle entre les messages RTCP est de 5 secondes et, en outre, la transmission de la communication RTCP ne devrait pas dépasser 5% de la bande passante disponible de la session. Pour créer des blocs de rapports de chaînes cachées, les rapports SR et RR (figure II.4.a et 4.b) peuvent être utilisés. Les valeurs des paramètres transférés dans ces rapports (en plus de SSRC_1qui est l'ID source) peuvent être modifiées, de sorte que la quantité d'informations qui peuvent être transférées dans chaque paquet est de 160 bits. Il est clair que si nous utilisons ce type de technique steganographique, nous perdons certaines (ou toutes) des fonctionnalités RTCP. D'autres champs optionnels/ inutilisés dans ces rapports peuvent également être utilisés de la même manière [7]..

Le PRBR total pour cette technique steganographique est le suivant :

$$PRBR_{RTCP} = S_{CP} * N_{RB} * S_{RB}[bits / packet] \qquad (II.2)$$

Ou :

- $\boldsymbol{PRBR_{RTCP}}$(Packet Raw Bit Rate) :c'est la bande passante du canal caché créé avec RTCP libre / inutilisé champs stéganographie (en bits / paquet),
- $\boldsymbol{S_{CP}}$: la taille du paquet RTCP composé (le nombre de types de paquets RTCP à l'intérieur du composé)
- $\boldsymbol{N_{RB}}$: est le nombre de blocs déclarés à l'intérieur de chaque type de paquet RTCP
- $\boldsymbol{S_{RB}}$: est le nombre de bits qui peuvent être envoyés en cache dans un bloc de rapport RTCP.

Il est également intéressant de noter que les messages RTCP sont basés sur des protocoles IP / UDP, de même que pour un paquet RTCP, les deux protocoles peuvent être utilisés pour une transmission cachée.

Pour améliorer la capacité de ce canal caché, on peut envoyer des paquets RTCP plus fréquemment que chaque 5 secondes (valeur par défaut proposée en standard) bien qu'il soit plus facile à découvrir. La stganalyse de cette méthode n'est pas aussi simple que dans le cas de mécanismes de sécurité de la stéganographie. *active warden* peut être utilisé pour éliminer ou limiter considérablement les champs dans lesquels une communication cachée peut avoir lieu bien qu'il s'agisse d'une limitation sérieuse de la fonctionnalité RTCP pour les utilisateurs ouverts[7].

3. La VOIP et la stéganographie

Actuellement, les méthodes de stéganographie qui peuvent être utilisés dans les réseaux de télécommunication sont conjointement décrits par le terme réseau ou stéganographie, en particulier lorsqu'il est appliqué à la téléphonie IP, par les termes «stéganographie VoIP» ou «stéganophonie».

Ces termes se rapportent à des techniques de dissimulation des informations dans une couche quelconque de la pile de protocole TCP / IP (Figure. II.5), compris les techniques appliquées aux codecs vocaux, ou ceux qui utilisent la parole elle-même[5].

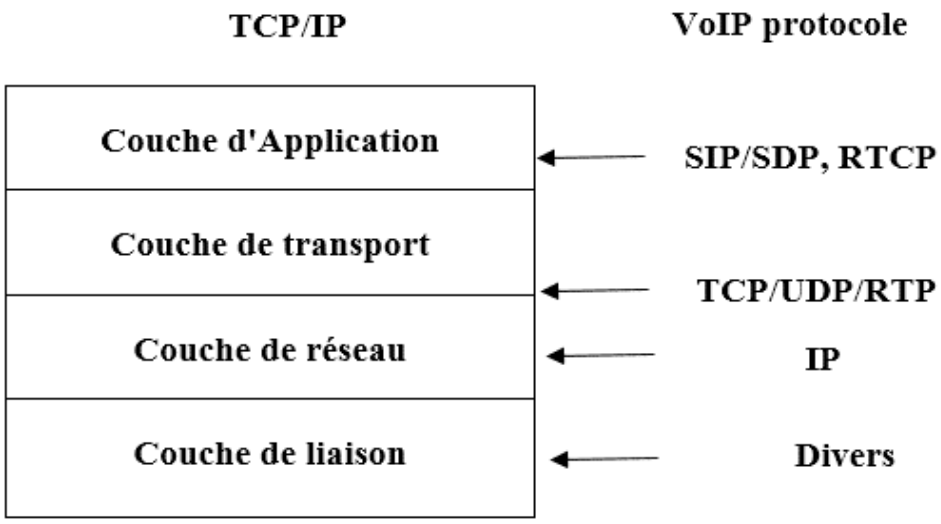


Figure II.5 : VOIP et la Stéganographie [5]**.**

C'est en raison des caractéristiques suivantes que la téléphonie IP est un porteur parfait pour des buts stéganographiques suivants :

- Il est très populaire, dans son utilisation ne sera pas considérer comme une anomalie.
- Le grand volume de données VoIP. Plus la présence et l'utilisation de ces transporteurs sont fréquentes dans les réseaux, plus leur capacité de masquage est grande, car les communications cachées peuvent passer invisibles parmi la masse des données échangées.
- Une bande passante steganographique potentiellement élevée qui peut être atteinte. Par exemple, pendant la phase de conversation d'un appel basé sur G.711, chaque paquet RTP comporte 20ms de voix, dans ce cas, le débit du flux RTP est de 50 paquets par seconde. Ainsi, même en supprimant simplement 1 bit dans chaque paquet RTP, nous gagnons un bandeau de bande stéganographique assez élevé 50 bit /s.

- Cela implique l'utilisation combinée d'une variété de protocoles. Ainsi, de nombreuses possibilités de cacher des informations proviennent des différentes couches de la pile TCP / IP. La communication cachée peut être activée en employant des méthodes stéganographiques appliquées à la voix des utilisateurs qui est véhiculée dans la charge utile des paquets RTP, en utilisant le schématique de la stéganographie des médias numériques connus ou en utilisant des protocoles VoIP comme support stéganographique. Cela fait de VoIP un opérateur multidimensionnel.
- C'est un service en temps réel qui induit des exigences strictes supplémentaires pour les méthodes de stéganographie et ses méthodes de détection (stéganalyse). Il crée également de nouvelles opportunités pour la stéganographie (par exemple, l'utilisation de paquets excessivement retardés rejetés par le récepteur sans traitement, car ils ne peuvent pas être considérés pour la reconstruction de la voix).
- Les appels VoIP sont dynamiques et de longueur variable, ce qui rend VoIP basée la stéganographie est encore plus difficile à détecter.

4. Classification des techniques steganographie appliquées à la VOIP

Dans cette section, nous classons les techniques stéganographiques de la VoIP principales basées sur le point d'application et l'approche utilisé pour la dissimulation des données.

Un nombre considérable de méthodes stéganographiques ont été développées, et ils couvrent toutes les couches de la pile TCP / IP. De plus, bon nombre des méthodes stéganographiques peuvent être adaptées avec succès au trafic VoIP, et de nombreuses nouvelles méthodes VoIP ont été introduites et sont abordées dans cette section. Cependant, si on analysela VoIP du point de vue de trafic, en général, toute technique de stéganographieVoIP peut être classée comme suit (Figure. II.6) [8].

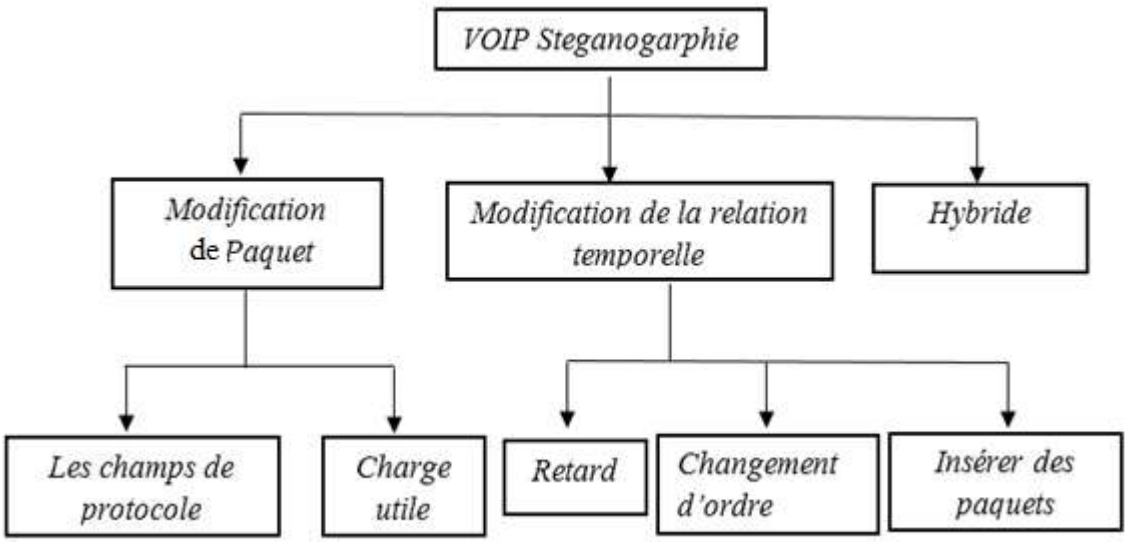


Figure II .6: Classification des techniques steganographie appliquées à la VOIP *[8]*.

4.1. La stéganographie par modifications de paquets

La modification peut se faire soit à des champs de protocole, ou la charge utile du message (payload).Les protocoles dans VoIP sont classés dans les protocoles de signalisation et de transmission. Les champs redondants et facultatifs dans ces protocoles, ainsi que les protocoles de réseau TCP / IP, peuvent être utilisés pour cacher les problèmes de sécurité. Certains exemples incluent l'utilisation de SIP et SDP, qui sont des protocoles de signalisation VoIP, ainsi que RTP et RTCP, qui sont des protocoles de transmission VoIP.

La modification de la charge utile des messages est similaire aux techniques steganographiques vocales traditionnelles. Il utilise les mêmes méthodes utilisées dans le tatouage audio numérique et les techniques steganographiques de codec vocal. Ces méthodes ont tendance à fournir une capacité stéganographique plus faible que les modifications au champ de protocole, il est plus difficile de mettre en œuvre et de détecter. Le principal inconvénient de cette technique est que la modification de la charge utile du message peut entraîner une diminution de la qualité de la voix[8].

4.2. La stéganographie par modification de la relation temporelle

Les techniques qui modifient l'ordre des messages envoyés ou reçus sont classées dans le rééchelonnement des messages. Le rééchelonnement peut se faire de différentes façons :

- En forçant le récepteur à jeter le paquet, (en retardant le message pendant une période), ou en retardant certains messages intentionnellement.

- En convainquant le récepteur que certains paquets ont été perdus (c'est-à-dire en ignorant certains nombres de séquence).

Le ré-ordonnancement des paquets nécessite une synchronisation entre l'émetteur et le récepteur. Il fournit une capacité stéganographique plus faible que les techniques de modification du champ de protocole et est aussi facile à mettre en œuvre[8].

4.3. La stéganographie hybride

Les méthodes steganographiques hybrides modifient à la fois le contenu des paquets et leur temps relation. Un exemple de cette solution est la méthode LACK (Lost Audio Packets Steganography) qui modifie les deux paquets et leurs dépendances temporelles. En ce qui concerne toute méthode de stéganographie en réseau, cache profond, Techniques peut être appliqué, améliorer l'indétectable et rendre plus difficile l'exécution du stéganogramme.

Ces techniques modifient à la fois le paquet ainsi que son calendrier. En conséquence, ils combinent les caractéristiques des deux systèmes.

Cette classification décrit précisément les possibilités actuelles de dissimulation d'informations dans VoIP. Cependant, il convient de noter que l'accent principal de la communauté de recherche au cours de la dernière décennie a été consacré aux méthodes du groupe S1 (Modifications de paquets Steganographie). Les solutions du groupe S2 (Modification de la relation temporelle) sont plus difficiles à déployer pratiquement, car elles offrent habituellement une faible bande passante steganographique et nécessitent une synchronisation. En outre, ils peuvent considérablement dégrader la qualité de l'appel. Les méthodes du groupe S3 (hybride) sont des découvertes assez récentes [8].

Tableau. II.1 : comparaison entre différents techniques de Stéganographie.

technique de steganographie VOIP	Sous-classification	Capacité de stéganographie	La mise en œuvre	Qualité vocale
Modifications de paquets Steganographie	Modification des champs de protocole	Haute	Facile	Pas affecté
	Modification de la charge utile du message	Modification inférieure aux champs	Plus difficile que les champs modification	Réduire la qualité de la voix
Modification de la relation temporelle	N/A	Capacité inférieure à la modification des champs de protocole	facile	Réduire la qualité de la voix
Hybride	N/A	Modérer	Modérer	Modérer

5. Conclusion

Les chercheurs ont également ciblé divers protocoles spécifiques à la VoIP comme SIP avec SDP, RTP et RTCP en tant que transporteurs stéganographiques. Un petit effort a été consacré au déploiement des méthodes qui modifient les relations temporelles entre les paquets dans le flux RTP, qui est une branche importante du domaine du stéganogramme du réseau. C'est principalement parce que ces solutions sont assez difficiles à déployer pratiquement, car elles offrent habituellement une faible bande passante stéganographique et nécessitent une synchronisation. Une direction de recherche intéressante pourrait être le développement de méthodes hybrides qui modifient les paquets VoIP et leurs relations temporelles, car il a été prouvé que ces méthodes offrent une bande passante steganographique décente tout en étant indétectable.

Chapitre III

Réalisation de la technique avec NS-3

1. Introduction

Le but de notre application est réalisation une méthode pour cacher des données envoyées dans un réseau public multi client.

Ces données envoyer pour tous les clients qui sont connecté dans ce réseau mais un seul client qui sera eux ces donnée par le décryptage avec le même programme qui utilisé dans l'envoi par le client source.

Pour cela nous avons travaillé avec le logiciel NS-3 qui est un simulateur possède des scripts dont nous pouvons les utilisés n'importe quand contrairement aux autres simulateurs.

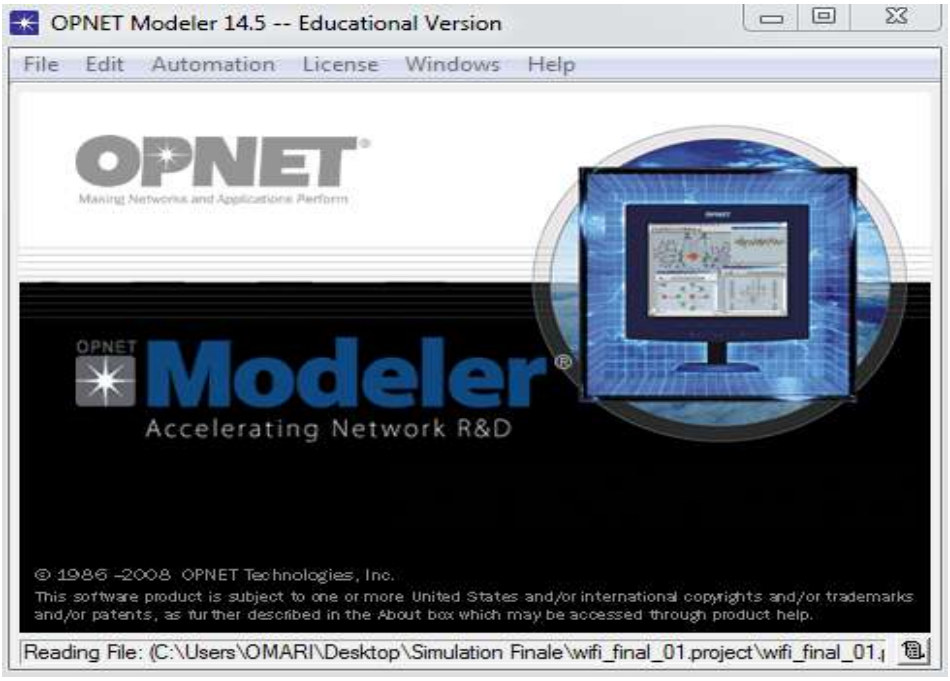
2. Choix du simulateur

En général, un simulateur de réseau est composé d'un large éventail de technologies et de protocoles réseaux et aide les utilisateurs à construire des réseaux complexes à partir de blocs de construction de base comme des grappes de nœuds et de liens.

Il existe plusieurs simulateurs réseaux, nous allons présenter par la suite quelques un que nous avons travaillé et essayé de travailler avec, tel que :

2.2. OPNET

OPNET est très réputé dans l'industrie pour la modélisation et aussi la simulation des réseaux. Parmi ses avantages, il permet de concevoir et d'étudier des réseaux de communications, des nouvelles technologies, des protocoles et des applications avec facilité et évolutivité. Il est utilisé spécialement par les entreprises des technologies les plus performantes pour accélérer et améliorer leurs procédés de recherches et de développements.



Figuer.III.1 : Interface du simulateur

2.3 NS-2

Bénéficie d'utilisation répandue dans le milieu de la recherche, le code de simulation a été contribué par plus de cent personnes et organisations, et l'utilisation du simulateur est toujours référencé dans de nombreux travaux de recherche en réseau.

Cependant, une lacune majeure de NS-2 est son évolutivité en termes d'utilisation de la mémoire et du temps d'exécution de la simulation. Ceci est particulièrement un problème en ce qui concerne les nouveaux domaines de recherche dans les réseaux informatiques, ou des architectures maillés qui exigent une simulation de réseaux très larges.

Outre NS-2, plus d'une douzaine de simulateurs des réseaux sont actuellement utilisés dans les universités et l'industrie. Parmi les simulateurs les plus connus nous choisissons le simulateur NS-3 pour réaliser notre travail.

2.4 NS-3

Le simulateur NS-3 est un simulateur réseau, utilisant des scripts écrit en C++ ou en Python. Nous avons choisis de travaillé avec ce simulateur pour la simple raison que ce simulateur possède des scripts dont nous pouvons les utilisés n'importe quand contrairement

aux autres simulateurs, par exemple le simulateur OPNET est un simulateur qui n'est pas gratuit donc c'est impossible de l'utiliser ou de travailler avec ce type de simulateur.

3. Présentation du simulateur NS-3

Le simulateur NS-3 vise à remplacer NS-2, écrit en C++, python et OTel (version orientée objet de Tel), pour tenter de remédier à ses limites (l'utilisation de multiples interfaces sur un nœud…).

Il peut être utilisé sur les plateformes Linux/Unix, OS X (Mac) et Windows.

Son développement a d'abord commencé en juillet 2006, et devait durer quatre ans, il est financé par les instituts comme l'université de Washington, Georgia Institue of Technologie et le Centre de l'ICSI pour la recherche sur Internet, la première version majeure publique et stable a été publié en juin 2008. Les développeurs de NS-3 ont décidé que l'architecture de simulation devait être remaniée complètement en partant du Zéro.

Dans cette optique, l'expérience tirée de NS-2 doit être associé avec les progrès des langages de programmation et du génie logiciel. L'idée de la rétrocompatibilité avec NS-2 a été abandonnée dès le départ. Cela libère NS-3 de contraintes héritées de NS-2 et permet la construction d'un simulateur qui est bien conçu depuis de début [14].

4. Terminologie et abstractions

Dans cette section, nous allons examiner certains termes qui sont couramment utilisés dans les réseaux, mais ont une signification particulière dans le NS-3.

4.1. Les nœuds "Node"

Dans le NS-3 l'abstraction de base de dispositif informatique est appelé le noeud. Cette abstraction est représentée en C ++ par la classe "Node". La classe Node fournit des méthodes pour gérer les représentations des dispositifs informatiques dans les simulations.

Vous devriez penser à un nœud comme un ordinateur sur lequel vous allez ajouter des fonctionnalités. On ajoute des choses comme des applications, des piles de protocoles et les cartes périphériques avec leurs pilotes associés pour permettre à l'ordinateur de faire un travail utile, dans notre travail les nœud sont les deux eNode-B, le romote host et le UE.

4.2. Les application "Application"

Représente un code exécuté par un utilisateur. Ce code peut être nécessaire au déroulement d'une simulation. L'échange de paquets durant une simulation nécessite par exemple la description d'une application au sein des nœuds participants. Les applications peuvent être attachées à un Node.

4.3. Le canal de communication "Channel"

Dans le monde réel, qui peut connecter un ordinateur à un réseau. Le canal "Channel" c'est le lien qui relie les « NetDevices » installés dans les nœuds. Des spécialisations de cette classe sont définies.

4.4. Les interfaces de la communication "NetDevice"

Appelée NetDevice, qui modélise à la fois les équipements et les pilotes de la communication. Des spécialisations sont fournies. Et le protocole stack représente le protocole utilisé durant la simulation par exemple le IPV4 (Internet Protocol Version 4).

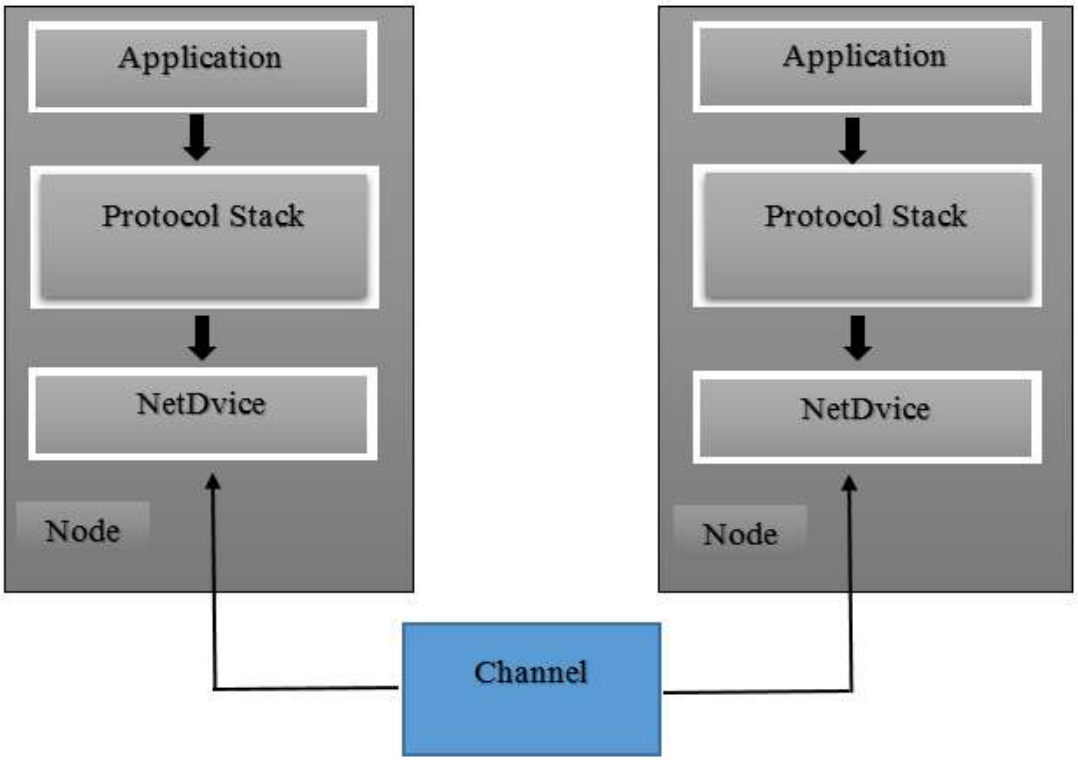
4.5. Les "Topology Helpers"

Dans NS-3 nous dire que vous voulez trouver des nœuds avec NetDevices attachés. Dans un grand réseau simulé, vous aurez besoin d'organiser de nombreuses connexions entre les nœuds, NetDevices et canaux. depuis la connexion NetDevices aux nœuds, NetDevices aux canaux, l'attribution des adresses IP, etc., sont telles tâches commune (qui sont répéter à chaque nœud en NS-3) , le NS-3 fournis ce que nous appelons les Topology Helpers pour faire la simulation facile que possible .

5. Architecture de base de Network Simulator 3

NS3 est totalement sans rapport avec son prédécesseur NS2. NS3 a été écrit à partir de zéro et utilise un noyau C ++. L'interface de script peut être python ou C ++. NS3 a une implémentation modulaire et contient une bibliothèque centrale qui Prend en charge les aspects génériques du simulateur et une bibliothèque de simulateurs qui traite de la spécification d'objets de temps de simulation, d'agendas et d'événements. Une bibliothèque commune définit des objets indépendants des architectures de réseau spécifiques, comme les objets de traçage. Les bibliothèques de nœuds et de périphériques sont responsables de la

définition des classes à utiliser pour construire le réseau et les périphériques dans le simulateur. Les entités de protocole sont écrites pour être plus proches de la mise en œuvre du monde réel. Les implémentations de paquets sont basées sur des paquets du monde réel afin de permettre la communication entre les agents simulés et le monde extérieur. L'une des principales fonctionnalités de NS3 est la possibilité d'exécuter une simulation distribuée. La simulation distribuée ici est définie comme la capacité du processus à utiliser plusieurs processeurs ou machines. La figure III.2 montre l'architecture de base d'une simulation NS3



Figuer.III.2 : Architecture du nœud NS-3.

6. Installation du simulateur NS-3

Pour installer NS-3 nous devons avoir une interface Linux, et cela ce fait soit en installant Linus directement sur la machine ou bien utiliser une machine virtuel (VirtualBox ou VMware), alors on peut utiliser Kali Linux comme interface de Linux, et les étapes suivantes sont des commandes pour télécharger et installer les différents paquets utiliser dans Kali Linux.

- Kali Linux

La liste suivante de paquage doit être téléchargée pour la version Kali Linux

- Package pour C++, c'est le package minimal pour le besoin de l'installation de ns-3.

sudo apt-get install gcc g++ python

- Package pour Python.

sudo apt-get install gcc g++ python python-dev

- Package pour Mercurial.

sudo apt-get install mercurial

- Package pour Bazar utilisé pour l'exécution des scripts Python sur ns-3

sudo apt-get install bzr

- Debugging:

sudo apt-get install gdb valgrind

- GNU Scientific Library (GSL) pour éviter les erreurs dans les modèles du réseau WiFI .

sudo apt-get install gsl-bin libgsl0-dev libgsl0ldbl

- The Network Simulation Cradle (nsc) requires the flex lexical analyzer and bison parser generator:

sudo apt-get install flex bison libfl-dev

- Installation des paquets gcc et g++ de la leur dernière version.

sudo apt-get install g++-4.6 gcc-4.6

- To read pcap packet traces

sudo apt-get install tcpdump

- Database support for statistics framework

sudo apt-get install sqlite sqlite3 libsqlite3-dev

- Xml-based version of the config store (requires libxml2 >= version 2.7)

sudo apt-get install libxml2 libxml2-dev

- A GTK-based configuration system

sudo apt-get install libgtk2.0-0 libgtk2.0-dev

- To experiment with virtual machines and ns-3

sudo apt-get install vtun lxc

- Support for utils/check-style.py code style check program

sudo apt-get install uncrustify

- Doxygen and related inline documentation:

sudo apt-get install doxygen graphviz imagemagick sudo apt-get install texlive texlive-extra-utils texlive-latex-extra

- The ns-3 manual and tutorial are written in reStructuredText for Sphinx (doc/tutorial, doc/manual, doc/models), and figures typically in dia:

sudo apt-get install python-sphinx dia

- Support for Gustavo Carneiro's ns-3-pyviz visualizer

sudo apt-get install python-pygraphviz python-kiwi python-pygoocanvas libgoocanvas-dev

- Support for openflow module (requires some boost libraries)

sudo apt-get install libboost-signals-dev libboost-filesystem-dev

- Support for MPI-based distributed emulation

sudo apt-get install openmpi*

Après toutes ces étapes nous allons maintenant passer à l'installation de ns-3, en commençant par le téléchargement du dossier NS-3.

- cd
- mkdir tarballs
- cd tarballs
- wget http://www.nsnam.org/release/ns-allinone-3.13.tar.bz2
- tar xjf ns-allinone-3.13.tar .bz2

Après toutes ces étapes nous allons maintenant passer à l'installation de NS-3 , nous allonsutiliser le fichier exécutable « Build.py » qui se trouve dans le répertoire NS-3 :

build.py --enable-examples --enable-tests [15] [16].

7. Déroulement de la simulation

Voici les démarches de déroulement d'une simulation, telles qu'illustrées à la figure III.3. Premièrement, il faut définir le problème : comprendre et avoir une vue d'ensemble du problème (conception).

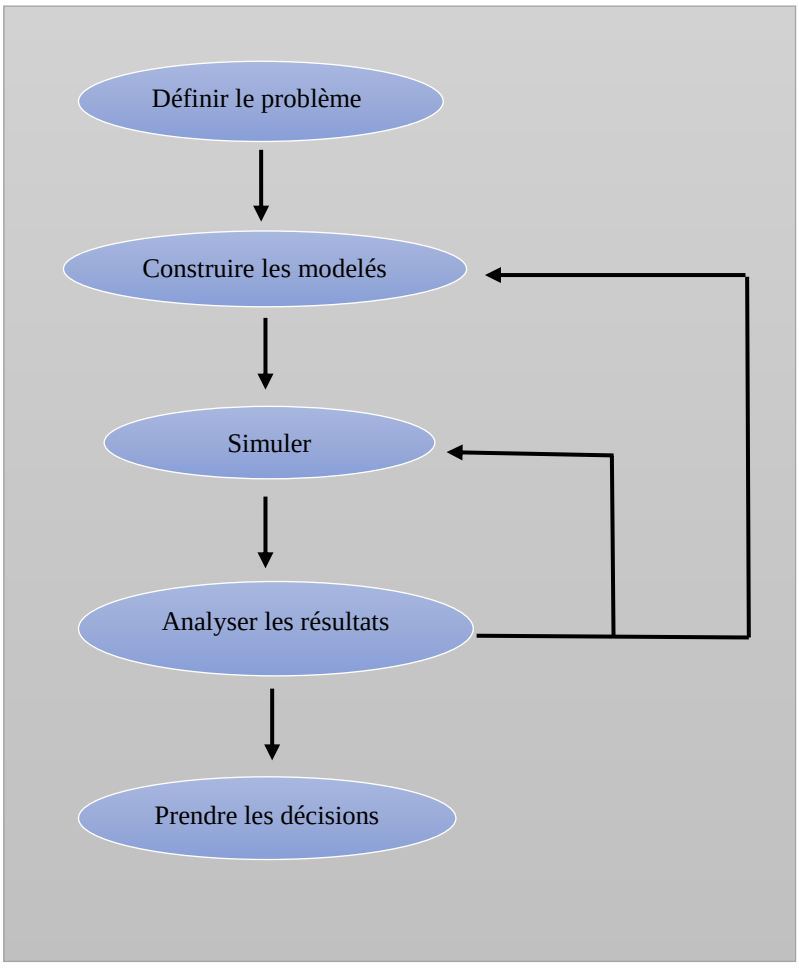


Figure III.3 : Etapes pour la réalisation d'une simulation**.**

Premièrement, nous avons utilisé une machine virtuelle (VMware Player), sur laquelle nous avons installé le système linux (kali linux) (voir Figure.III.4 qui nous montre les différentes étapes de démarrage du VMware, kali linux et NS-3)

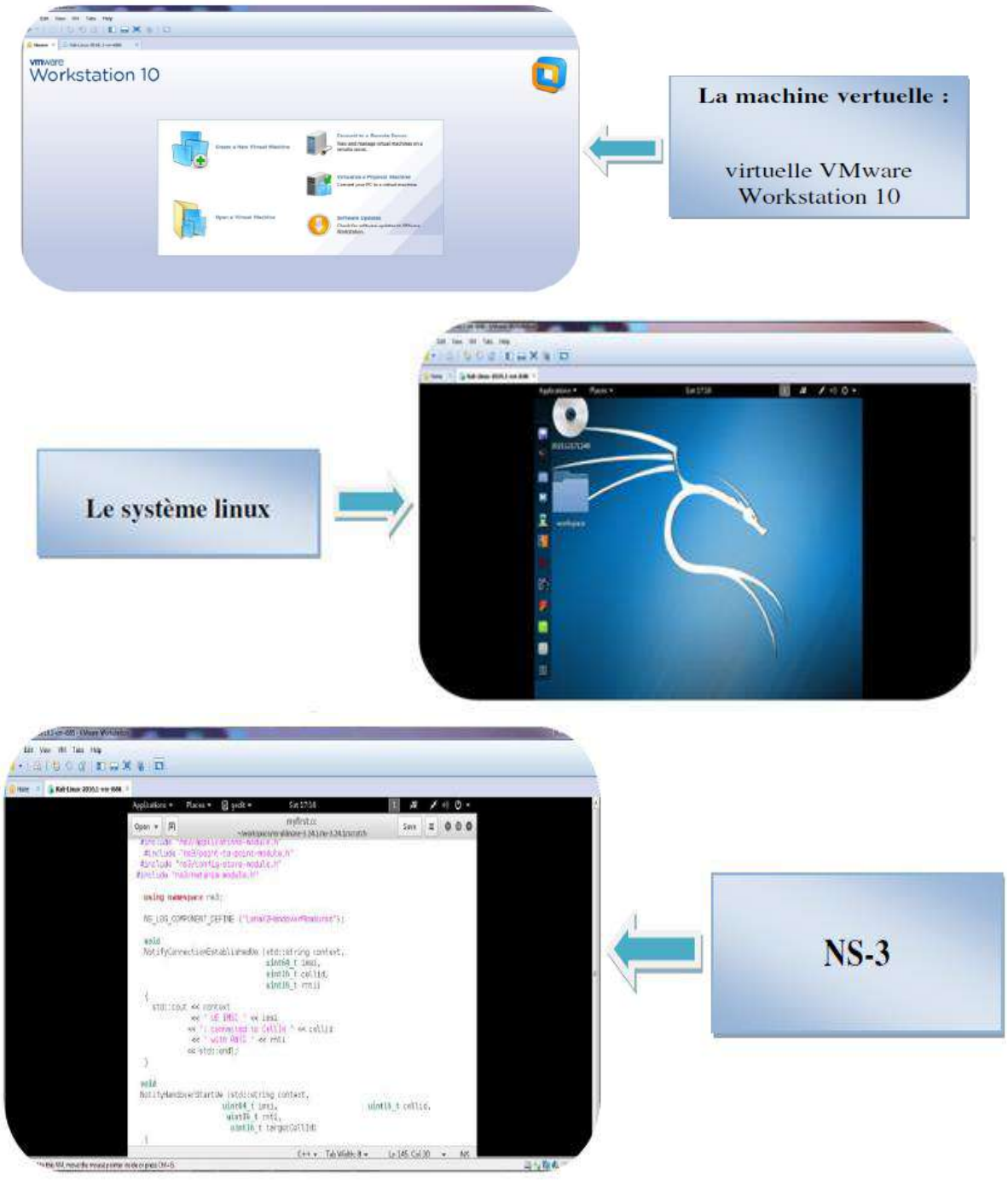


Figure.III.4 : Les étapes de nos simulations sous

8. scénario de simulation

Ce scénario comprend deux nœuds connectés sur un réseau local avec une adresse réseau de 10.1.1.0. La connexion entre les deux nœuds est point à point avec un débit de données de 5 Mbps et un délai de 2 ms. Node0 est un client UDP et node1 est un serveur UDP avec les adresses IP 10.1.1.1 et 10.1.1.2 respectivement. Toute la longueur de la simulation est de 10 secondes, mais l'application du nœud du serveur démarre après une seconde et l'application du nœud client démarre après deux secondes.



Figure.III.5 : Topologie du scénario

8.1. Les étapes de création de programme de simulation

Étape 0 : déclaration d'en-tête du programme

Le code approprié commence par un certain nombre d'instructions d'inclusion

```
#include "ns3/core-module.h"
#include "ns3/network-module.h"
#include "ns3/internet-module.h"
#include "ns3/point-to-point-module.h"
#include "ns3/applications-module.h"
using namespace ns3;
NS_LOG_COMPONENT_DEFINE ("FirstScriptExample");
Int main (int argc, char *argv[])
{
 bool tracing = true;
  LogComponentEnable ("UdpEchoClientApplication", LOG_LEVEL_INFO);
  LogComponentEnable ("UdpEchoServerApplication", LOG_LEVEL_INFO);
```

Le projet ns-3 est implémenté dans un namespace C ++ appelé ns3. Ceci regroupe toutes les déclarations liées à ns-3 dans une portée en dehors de l'espace de noms global, ce qui, nous l'espérons, aidera à l'intégration avec un autre code. L'instruction C++ en utilisant introduit namespace ns-3 dans la région déclarative actuelle (globale).

Étape1 : création des nœuds

Les trois lignes de code dans notre script créeront réellement les nœuds objets qui représenteront les ordinateurs dans la simulation.

```
NS_LOG_INFO (" Create nodes .");
NodeContainer nodes;
nodes.Create (2) ;
```

Étape 2 : création de lien ppp

Nous construisons un lien point à point et, dans un schéma qui vous connaîtra bien, nous utilisons un objet topologie assistant pour effectuer le travail de bas niveau requis pour mettre le lien ensemble.

```
PointToPointHelper pointToPoint;
pointToPoint.SetDeviceAttribute ("DataRate", StringValue("5Mbps"));
pointToPoint.SetChannelAttribute ("Delay", StringValue ("2ms"));
```

Rappelons que deux de nos abstractions clés sont NetDevice et the Channel. Dans le monde réel, ces termes correspondent approximativement aux cartes périphériques et aux câbles réseau.

Étape 3 : connecter des nœuds et des liens

Nous avons maintenant des nœuds et des périphériques configurés, mais nous n'avons pas de piles de protocole installées sur nos nœuds. Les deux lignes suivantes de code prendront soin de cela.

```
NetDeviceContainer devices;
 devices = pointToPoint.Install (nodes);
InternetStackHelper stack;
 stack.Install (nodes);
```

Étape 4 : configurez le réseau

Ensuite, nous devons associer les périphériques sur nos nœuds aux adresses IP. Nous fournissons un assistant de topologie pour gérer l'allocation des adresses IP

```
Ipv4AddressHelper address;
address.SetBase ("10.1.1.0", "255.255.255.0");
Ipv4InterfaceContainer interfaces = address.Assign (devices);
```

Déclarer un objet d'adresse helper et lui dire qu'il devrait commencer à attribuer des adresses IP du réseau 10.1.1.0 en utilisant le masque 255.255.255.0 pour définir les bits attribuables. Par défaut, les adresses attribuées commencent à l'une et augmentent de manière monotone, de sorte que la première adresse attribuée à partir de cette base sera 10.1.1.1 suivie de 10.1.1.2, etc.

Étape 5 : Création de l'application

Une autre des principales abstractions du système ns-3 est l'application.

```
UdpEchoServerHelper echoServer (9);
 ApplicationContainer serverApps = echoServer.Install (nodes.Get (1));
 serverApps.Start (Seconds (1.0));
 serverApps.Stop (Seconds (10.0));
UdpEchoClientHelper echoClient (interfaces.GetAddress (1), 9);
 echoClient.SetAttribute ("MaxPackets", UintegerValue (20));
 echoClient.SetAttribute ("Interval", TimeValue (Seconds (1.0)));
 echoClient.SetAttribute ("PacketSize", UintegerValue (1024));
```

Étape 6 : Création de la réception:

On va créer l'application Container et installez-la sur le nœud 1

```
ApplicationContainer clientApps = echoClient.Install (nodes.Get (0));

 clientApps.Start (Seconds (2.0));
 clientApps.Stop (Seconds (10.0));
```

Étape 7 : configure le traçage

On confugurer le tracage **Pcap** et **Tr** pour sera activé.

```
if (tracing)
{
AsciiTraceHelper ascii;
pointToPoint.EnableAsciiAll (ascii.CreateFileStream("udp-clien.tr"));
pointToPoint.EnablePcapAll ("udp-clien ", false );
}
```

Étape 8 : simulation réelle

```
 Simulator::Run ();
 Simulator::Destroy ();
 return 0;
}
```

Ce que nous devons la fonction globale Simulator faire à ce stade, c'est d'exécuter la simulation. Cela se fait en utilisant: **Run**

8.2. Résultat

Partie I : Résultat obtenu par NetAnim

NetAnim est un outil graphique utilisé pour visualiser les activités du réseau pendant la simulation.

La configuration de NetAnim présenté sur les figure III.6 et III.7 (voir la page suivante).

first.cc

Fichier Édition Rechercher Options Aide

```
 * This program is free software; you can redistribute it and/or modify
 * it under the terms of the GNU General Public License version 2 as
 * published by the Free Software Foundation;
 *
 * This program is distributed in the hope that it will be useful,
 * but WITHOUT ANY WARRANTY; without even the implied warranty of
 * MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
 * GNU General Public License for more details.
 *
 * You should have received a copy of the GNU General Public License
 * along with this program; if not, write to the Free Software
 * Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA  02111-1307  USA
 */

#include "ns3/core-module.h"
#include "ns3/network-module.h"
#include "ns3/netanim-module.h"
#include "ns3/internet-module.h"

#include "ns3/point-to-point-module.h"
#include "ns3/applications-module.h"

using namespace ns3;

NS_LOG_COMPONENT_DEFINE ("UDP-simulation");
```

Figure.III.6 : En-tête NetAnim inclus dans le réseau.

```
  UdpEchoClientHelper echoClient (interfaces.GetAddress (1), 9);
  echoClient.SetAttribute ("MaxPackets", UintegerValue (5));
  echoClient.SetAttribute ("Interval", TimeValue (Seconds (1.0)));
  echoClient.SetAttribute ("PacketSize", UintegerValue (1024));

  ApplicationContainer clientApps = echoClient.Install (nodes.Get (0));
  clientApps.Start (Seconds (2.0));
  clientApps.Stop (Seconds (10.0));
if (tracing)
    {
      AsciiTraceHelper ascii;
      pointToPoint.EnableAsciiAll (ascii.CreateFileStream ("udp-clien.tr"));
      pointToPoint.EnablePcapAll ("udp-clien", false);
    }

AnimationInterface anim ("animation.xml");
anim.SetConstantPosition (nodes.Get(0), 1.0, 2.0);
anim.SetConstantPosition (nodes.Get(1), 2.0, 3.0);

  Simulator::Run ();
  Simulator::Destroy ();
  return 0;
}
```

Figure.III.7 : Les instructions d'animation XML NetAnim.

La figure.III.7 et 8 montres la configuration de simulation doit capturer et enregistrer les activités dans un fichier XML à l'aide des instructions AnimationInterface anim ("animation.xml") et, par la suite le fichier XML peut être chargé sur NetAnim pour l'animation.

Pour exécuté le programme et pour obtenir ces résultats on ait utilisé les commandes suivant :

Nous allons au dossier ns-allinone3.xx après on ouvrir le dossier ‘’netanim’’ puis suit cet instructions :

- make clean
- qmake NetAnim.pro
- make

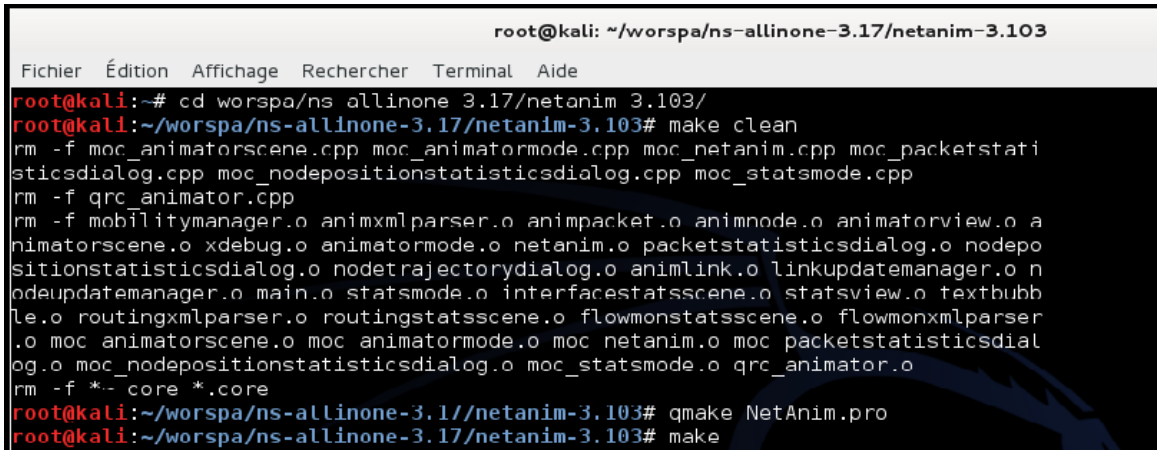


Figure.III.8 : Les commandes d’exécutions NetAnim avec NS-3

Pour atteint le flux de trafic réseau on doit utiliser la commande **./NetAnim.**

La ligne pointillée indique le flux de Trafic réseau entre les deux nœuds.



Figure.III.9 : le flux de Trafic réseau.

La figure III.9 montre les deux nœuds du réseau à partir de Le scénario UDP-simulation Le nœud 0 est le serveur UDP et Le nœud 1 est le client UDP.

Partie II : Résultat obtenu par WireShark

Wireshark est un logiciel d'analyse réseau (sniffer) qui permettant de visualiser l'ensemble des données transitant sur la machine qui l'exécute, et d'obtenir des informations sur les protocoles applicatifs utilisés. Les octets sont capturés en utilisant la librairie réseau PCAP, puis regroupés en blocs d'informations et analysés par le logiciel.

```
int main (int argc, char *argv[])
{ bool tracing = true;

  LogComponentEnable ("UdpEchoClientApplication", LOG_LEVEL_INFO);
  LogComponentEnable ("UdpEchoServerApplication", LOG_LEVEL_INFO);

NodeContainer nodes;
nodes.Create (2);

PointToPointHelper pointToPoint;
pointToPoint.SetDeviceAttribute ("DataRate", StringValue ("5Mbps"));
pointToPoint.SetChannelAttribute ("Delay", StringValue ("2ms"));

NetDeviceContainer devices;
devices = pointToPoint.Install (nodes);

InternetStackHelper stack;
stack.Install (nodes);
Ipv4AddressHelper address;
address.SetBase ("10.1.1.0", "255.255.255.0");
Ipv4InterfaceContainer interfaces = address.Assign (devices);

if (tracing)
    {
      AsciiTraceHelper ascii;
      pointToPoint.EnableAsciiAll (ascii.CreateFileStream ("udp-
clien.tr"));
      pointToPoint.EnablePcapAll ("udp-clien", false);
    }
UdpEchoServerHelper echoServer (9);
ApplicationContainer serverApps = echoServer.Install(nodes.Get(1));
 serverApps.Start (Seconds (1.0));
```

Figure.III.10 : configuration le traçage .pcap et tr.

La figure III.10 montre La configuration de traçage on est modifié l'état de traçage

Et on le met ‘’true’’ pour atteint les files nommé .Pcap et .Tr

Pour exécuté notre programme nommé « first » il suffit d'utilisé l'instruction des commandes suivante :

. /waf - -run scratch/first

Le message affiché est présenté au bas Figure.III.11 (page 53).

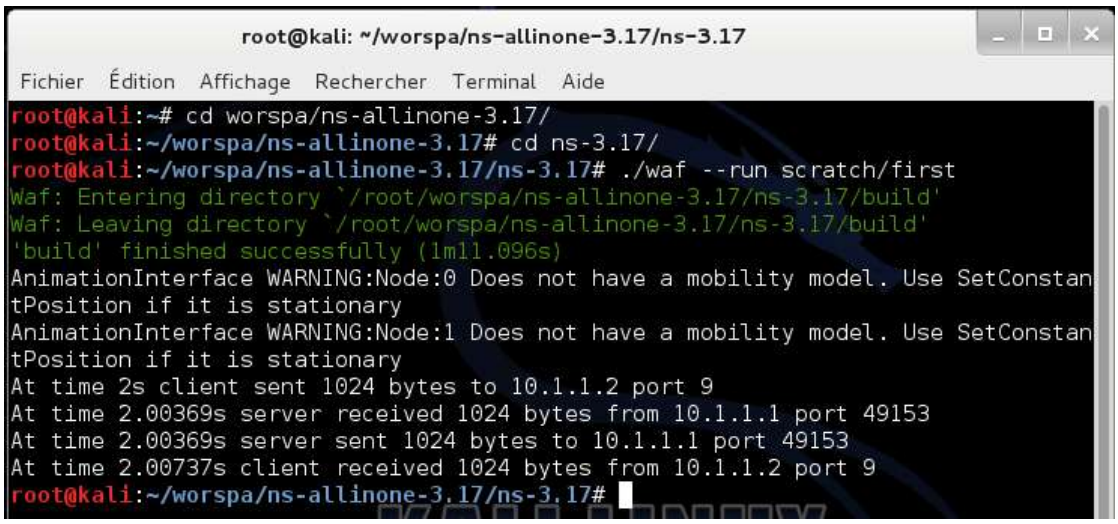


Figure.III.11 : résultat d'exécution de programme avec NS-3

Dans KALI LUNIX on doit utiliser des commandes prédéfini pour exécuté le programme qui permet d'envoie notre texte depuis le client numéro un (01) qui a l'adresse IP 10.1.1.1 vers le client numéro (02) qui a l'adresse IP 10.1.1.2.

Après l'exécution de programme un message sera afficher qui permet de nous voir le nombre de bites envoyé et recevez par les deux clients (les nœuds) avec un détail de temps,

Pour bien vu des resultats d'operation on utulisant le WareShark .

Premiérement on exécute les fichier «udp-clien-0 » et « udp-clien-1 » de l'extension .pcap qui se trouve dans le dossier ns-3.17 .

Cet type de ficier permet a nous de poursuivre les etape de l'envoi et donne touts les details : numero de paquet,source, distination, protocol,long de paquet et quelque information de plus.

Dans l'etat normal où nous envoions nos message (paquets) le compteur qui se trouve dans le programme incrementé apres chaque paquet envoyé normal .

Pour envoyer le message il a y un condition qui est :

$$\boldsymbol{nombre\ des\ paquets} \geq \boldsymbol{nombre\ des\ lettres\ envoyes} \qquad (III.1)$$

Pour on assure l'envoie total de message(texte) voulons envoyer et sa chifferemnt .

Dans notre cas on a envoyé le message « hello » comme just un texte de test , en etat normal on obtien :

En envoi :

paquet _1= h envoyé le compteur sera égale à 1 (cpt= 1) ,

paquet_2= e envoyé le compteur sera égale à 2 (cpt= 2),

paquet _3= l envoyé le compteur sera égale à 3 (cpt= 3),

paquet _4= l envoyé le compteur sera égale à 4 (cpt= 4) ,

paquet _5= o envoyé le cpt = 1 le compteur sera égale à 5 (cpt= 5),

En reception :

paquet_1 reçus = h ,

paquet_2 reçus = e

paquet_1 reçus = l

paquet_1 reçus = l

paquet_1 reçus = o

Nous avons fais un changement dans le principe de fonctionnement d'identificateur (ID_fragment) qui se touve au l'entet des protocole de transmission où l'incrémentation de compteur sera avec un chiffrement de paquet envoyé utilisant le code ASCII (en héxadécimale)de lettre (paquet) envoyer jusqu'à la fin de nombre de paquets a envoyer .

Juste après la fin de nos message qui nous voulons caché l'incrémentation revenue a la fonctionnement dans l'etat normale.

Dans cet cas nous recevrons le meme numero de paquet mais pas le contenu directemnt ,on obtien une séquence de numéro apparaite dans les autre destiantaire qui n'avez pas le programme de décryptage.

Au contraire dans les client qui eux le programme qui cet séquence de numero sera changer et le contenue sera afficher avec sons code_ASCII.

Les resultats obtenue présente sur les figures (Figure.III. 12 ,13,14,15,16)

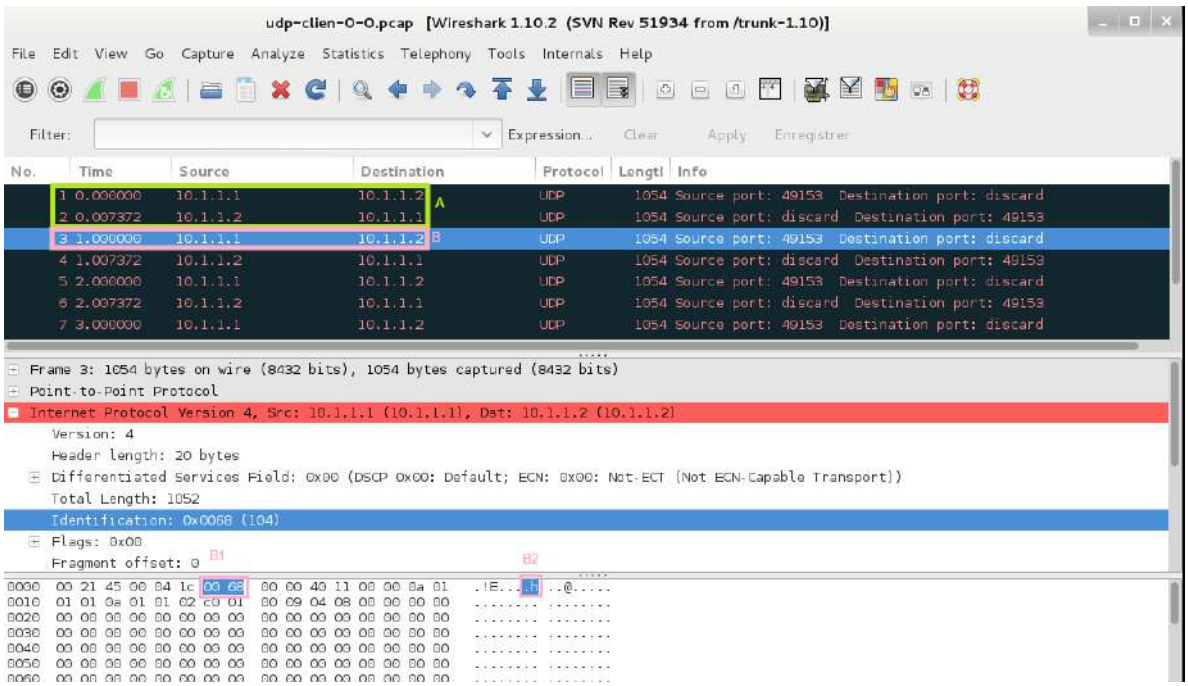


Figure.III.12 : capture d'un paquet contient un message secret ''H''

-Le champ A en vert représent les deux premier paquet (1 et 2) qui est toujours envoyer par l'emetteur/recepteur pour configurer et établir une connexion entre eux.

-Le champ B en rose represnt le premier lettre envoyer(paquet N°3) .

-La case B1 est le code ASCII de la lettre envoyer qui est le premier lettre dans notre texte , la lettre « h » (la case B2)

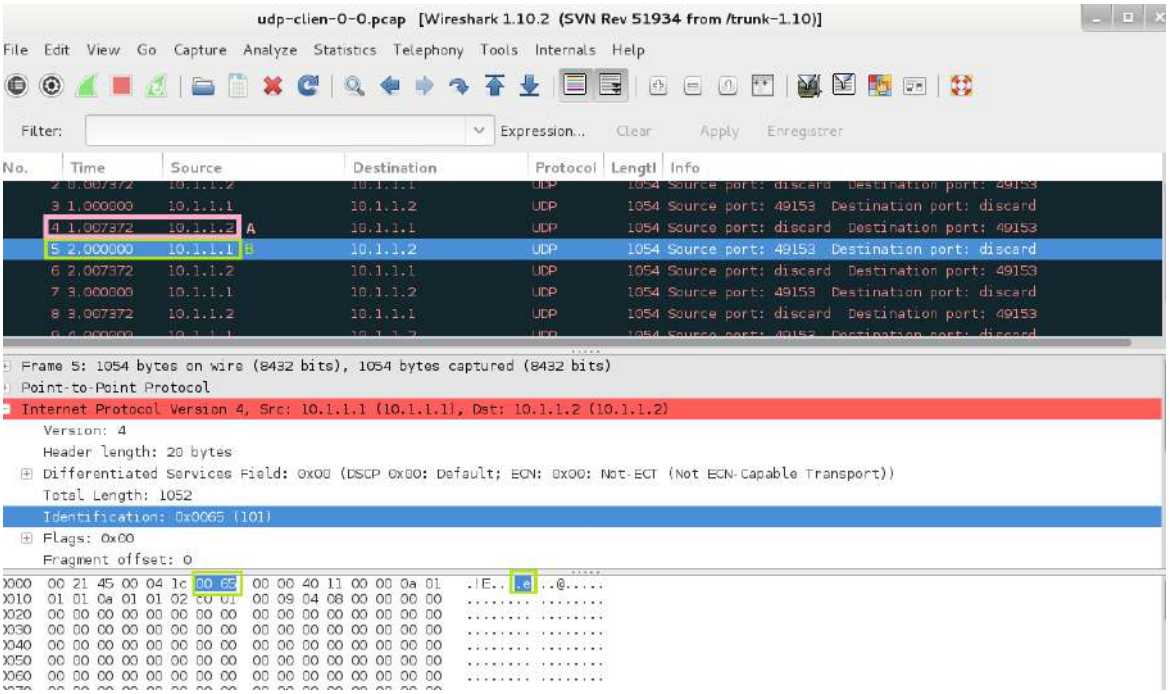


Figure.III.13 : capture d'un paquet contient un message secret ''H''

-Le champ A en rose represnt (paquet N°4) la répense sur le message qui est déjà envoyer (répense sur le trame N°3) c a d il a été bien reçus .

-Le champ B en vert (paquet N°5) represnt le deuxieme lettre dans notre texte envoyer qui est le « e » .

- les deux petits champs en vert indiqué la lettre reçu avec sa code ASCI .

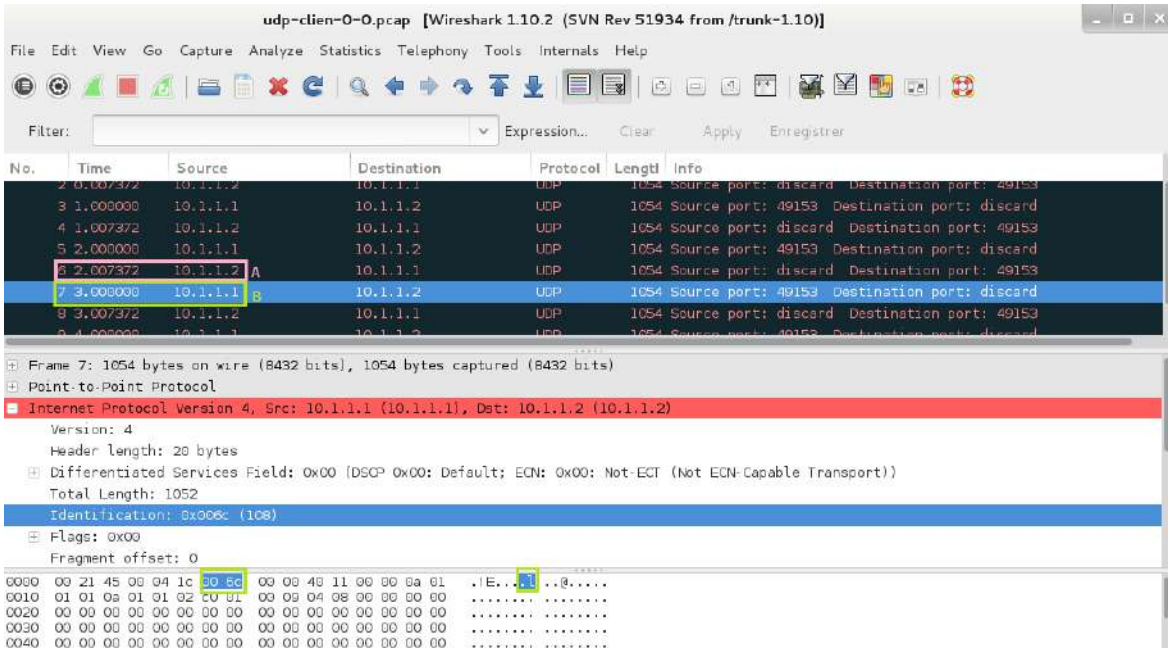


Figure.III.14 : capture d'un paquet contient un message secret ''l''

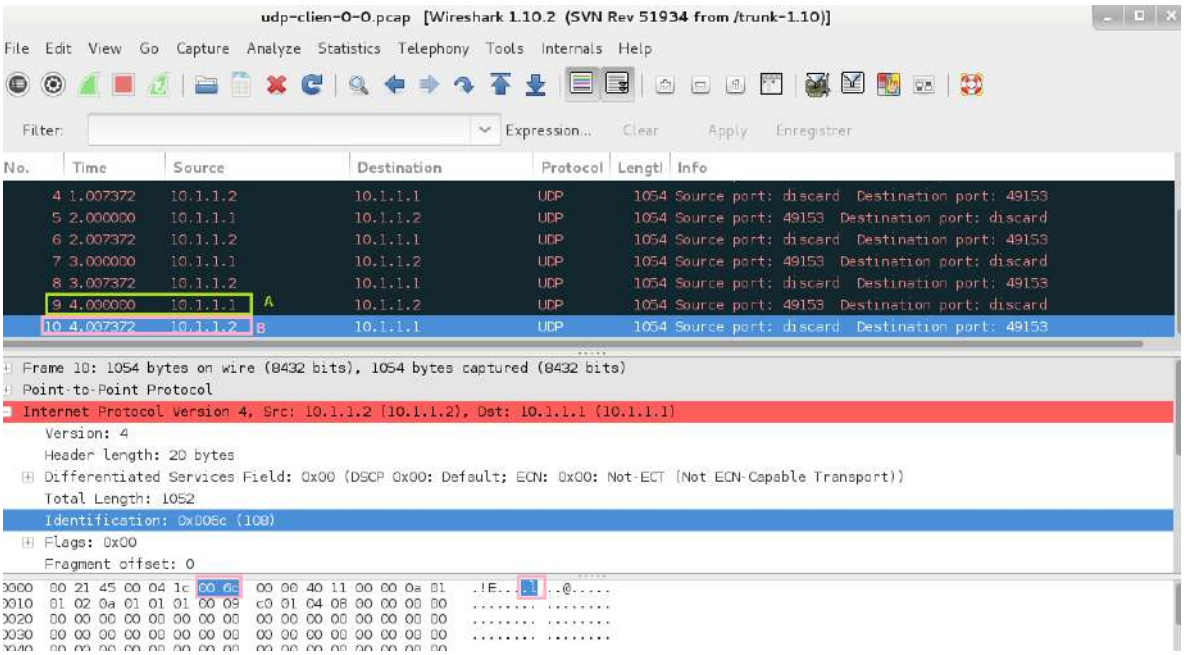


Figure.III.15 : capture d'un paquet contient un message secret ''l''

-Dans les deux figures (Figure.III.14 et 15) on a envoyer la meme lettre deux fois c'est la lettre « l » (paquet N°7 et 9) comme on vu au les champ A.

- La répense de l'accusission vu dans les paquets N°8 et 10 (les champ B).

- Dans la reception on obtien une lettre « l » avec sa code ASCII = 00 6c

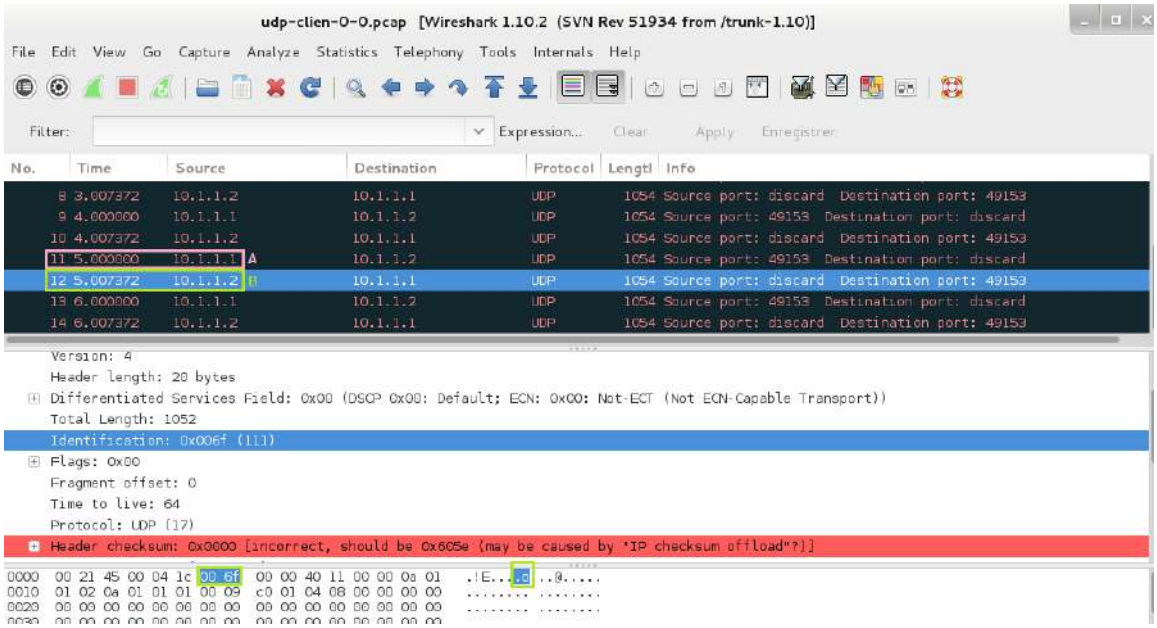


Figure.III.16 : capture d'un paquet contient un message secret ''O''

-la dernière figure représente l'envoie de dernier lettre dans notre texte la lettre « o » qui a été envoyé dans le paquet N°11 (champ en rose A) et on obtient aussi un message d'acquisition (paquet N°12, champ en vert B).

- le code qui afficher dans la réception 00 6f c'est le code ASCII de la lettre « e ».

9. Conclusion

Dans ce chapitre, comme on a vu, nous avons utilisé le simulateur NS-3 pour réalisation de projet.

Nous avons créé un scénario comprend deux nœuds connecté à un réseau local avec le protocole UDP, et nous avons intégré un fichier texte chiffré dans les champs ID entête IP, pour bien comprendre le fonctionnement de la steganographie des donnée sous forme de texte.

Après l'exécution de programme de ce scénario on arrive à les résultats présenté sur les figues.

Cette dernières implique que la steganographie est une technique utile pour protéger et cacher des données envoyer dans un réseau face aux attaque ou bien des intrusion.

CONCLUSION GENERALE

La technique qui aurait été employée, la stéganographie, consiste à cacher un message dans un support "innocent". Elle peut, de surcroît, se combiner à la cryptographie, qui se charge de dissimuler le sens de la missive et non plus son existence. Le résultat est alors particulièrement efficace. Le message secret s'abrite d'abord derrière son invisibilité. En cas de découverte, il restera à le décoder. Un défi pour les services secrets qui, dans le cas du terrorisme, doivent réaliser ces deux opérations au plus vite pour que l'information recueillie ne soit pas obsolète.

Il faut savoir que si la steganographie est très pratique, son utilisation informatique est détectable. Il ne faut pas oublier que cela est avant tout un code informatique. La sécurité de la stéganographie repose sur le fait que le message ne sera sans doute pas détecté.

Perspectives:

Ce travail pourrait être poursuivi sur plusieurs points pour améliorer les performances:
Par exemple lors de la transmission de l'information (audio) sur un canal, présenter les outils de communication et le lien avec le marquage audio.

ANNEX

first.cc

```
/* -*- Mode:C++; c-file-style:"gnu"; indent-tabs-mode:nil; -*- */
/*
 * This program is free software; you can redistribute it and/or
modify
 * it under the terms of the GNU General Public License version 2 as
 * published by the Free Software Foundation;
 *
 * This program is distributed in the hope that it will be useful,
 * but WITHOUT ANY WARRANTY; without even the implied warranty of
 * MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
 * GNU General Public License for more details.
 *
 * You should have received a copy of the GNU General Public License
 * along with this program; if not, write to the Free Software
 * Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA  02111-
1307  USA
 */

#include "ns3/core-module.h"
#include "ns3/network-module.h"
#include "ns3/internet-module.h"
#include "ns3/point-to-point-module.h"
#include "ns3/applications-module.h"

using namespace ns3;

NS_LOG_COMPONENT_DEFINE ("FirstScriptExample");

int
main (int argc, char *argv[])
{ bool tracing = true;
  LogComponentEnable ("UdpEchoClientApplication", LOG_LEVEL_INFO);
  LogComponentEnable ("UdpEchoServerApplication", LOG_LEVEL_INFO);

  NodeContainer nodes;
  nodes.Create (2);

  PointToPointHelper pointToPoint;
  pointToPoint.SetDeviceAttribute ("DataRate", StringValue
("5Mbps"));
  pointToPoint.SetChannelAttribute ("Delay", StringValue ("2ms"));

  NetDeviceContainer devices;
  devices = pointToPoint.Install (nodes);

  InternetStackHelper stack;
  stack.Install (nodes);

  Ipv4AddressHelper address;
```

```
  address.SetBase ("10.1.1.0", "255.255.255.0");

  Ipv4InterfaceContainer interfaces = address.Assign (devices);

  UdpEchoServerHelper echoServer (9);

  ApplicationContainer serverApps = echoServer.Install (nodes.Get
(1));
  serverApps.Start (Seconds (1.0));
  serverApps.Stop (Seconds (10.0));

  UdpEchoClientHelper echoClient (interfaces.GetAddress (1), 9);
  echoClient.SetAttribute ("MaxPackets", UintegerValue (20));
  echoClient.SetAttribute ("Interval", TimeValue (Seconds (1.0)));
  echoClient.SetAttribute ("PacketSize", UintegerValue (1024));

  ApplicationContainer clientApps = echoClient.Install (nodes.Get
(0));
  clientApps.Start (Seconds (2.0));
  clientApps.Stop (Seconds (10.0));
if (tracing)
    {
      AsciiTraceHelper ascii;
      pointToPoint.EnableAsciiAll (ascii.CreateFileStream ("udp-
clien.tr"));
      pointToPoint.EnablePcapAll ("udp-clien", false);
    }
  Simulator::Run ();
  Simulator::Destroy ();
  return 0;
}
```

Bibliographies

[1] Mini-projet-Transmission-marnaoui-mohamed-taher-idriss-ferid

[2] yassine Nasser University Mohamed V, Faculté Des Sciences Rabat Agdal, Physique - Informatique, Faculty Member | Globalization and Accounting +1 Address: Morocco Project de communication numérique Réalisation d'une chaîne de transmission numérique.

[3] Bergmair, R. (2007). A comprehensive bibliography of linguistic steganography.In Proceedings of the SPIE Conference on Security, Steganography, and Watermarking of Multimedia Contents, volume 6505.

[4] Computer Security Institute. Csi/fbi 2007 computer crime and security survey, 2007.

[5]Warsaw University of Technology, Poland, NowowiejskaACM Computing Surveys (CSUR) Surveys Homepage archive Volume 46 Issue 2, November 2013 Article No. 20 ACM New York, NY, USA table of contents doi>10.1145/2543581.2543587

[6] Embedding Covert Channels into TCP/IPSteven J. Murdoch and Stephen Lewis University of Cambridge, Computer Laboratory,15 JJ Thomson Avenue, Cambridge CB3 0FD, United Kingdom http://www.cl.cam.ac.uk/users/fsjm217, srl32g/

[7] Steganography of VoIP Streams Wojciech Mazurczyk, Krzysztof Szczypiorski Warsaw University of Technology, Faculty of Electronics and Information Technology, Institute of Telecommunications, 15/19 Nowowiejska Str., 00-665 Warsaw, Poland{W.Mazurczyk, K.Szczypiorski}@tele.pw.edu.pl

[8] ReLACK: A Reliable VoIP Steganography Approach Mohammad Hamdaqa, Ladan Tahvildari Software Technologies Applied Research (STAR) Group Department of Electrical and Computer Engineering University of Waterloo Waterloo, Canada {mhamdaqa, ltahvild}@uwaterloo.ca/.

[9] « http://www1.cse.wustl.edu/~jain/cse567-08/ftp/simtools/index.html », Date de consultation juin 2013.

[10] « www.nsnam.org », Date de consultation juin 2013.

[11]«http://www.nsnam.org/wiki/index.php/Installation#Operating_system_and_ compiler_support », Date de consultation juin 2013.