Université Kasdi Merbah – Ouargla

FACULTÉ DES SCIENCES ET TECHNOLOGIES ET DES SCIENCES DE LA MATIERE

DEPARTEMENT DE MATHEMATIQUE ET D'INFORMATIQUE

Mémoire

Master en Informatique

Option : Informatique Industriel

Présenté par : Yahia KORICHI

Otmane BOUHAMIDA

Thème

Modélisation et simulation du problème du trou noir dans les réseaux mobiles P2P

Soutenu publiquement

Le: 30/06/2013

Devant le jury :

Dr. Mohamed Said Said	**MC (A)**	**President**	**UKM Ouargla**
Dr. Ahmed Korichi	**MC (A)**	**Encadreur/rapporteur**	**UKM Ouargla**
M. Saleh Euschi	**MA**	**Examinateur**	**UKM Ouargla**

L'année universitaire : 2012/2013

Université Kasdi Merbah – Ouargla

FACULTÉ DES SCIENCES ET TECHNOLOGIES ET DES SCIENCES DE LA MATIERE

DEPARTEMENT DE MATHEMATIQUE ET D'INFORMATIQUE

Mémoire

Master en Informatique

Option : Informatique Industriel

Présenté par : Yahia KORICHI

Otmane BOUHAMIDA

Thème

Modélisation et simulation du problème du trou noir dans les réseaux mobiles P2P

Soutenu publiquement

Le: 30/06/2013

Devant le jury:

Dr. Mohamed Said Said	**MC (A)**	**President**	**UKM Ouargla**
Dr. Ahmed Korichi	**MC (A)**	**Encadreur/rapporteur**	**UKM Ouargla**
M. Saleh EuschiMA	**Examinateur**		**UKM Ouargla**

L'année universitaire : 2012/2013

Dédicace

Ce modeste travail est dédié à:

*A celle qui a été toujours la source de grande affection et le goût de la vie .....ma **MERE***

*A celui quia été toujours la source d'inscription, de courage a tout le long de mes études.....mon **PERE***

A tous mes frères et sœurs

*A toutes ma famille (**Bouhamida**) et mes proches.*

A tous mes amis sons exception.

*A mon collègue **Yahia***

A toute la promotion informatique industrielle 2012/2013que je leurs souhaite un bon avenir.

A tous ceux qui m'ont aidé de près ou de loin à la réalisation de ce modeste travail.

Otmane

Dédicace

Ce modeste travail est dédié à:

A celle qui a été toujours la source de grande affection
*et le goût de la vie .....ma **MERE***

A celui quia été toujours la source d'inscription, de courage
*a tout le long de mes études ..... mon **PERE***

A tous mes frères et sœurs

*A toutes ma famille (**Korichi**) et mes proches.*

A tous mes amis sons exception.

*A mon collègue **Otmane***

A toute la promotion informatique industrielle 2012/2013
que je leurs souhaite un bon avenir.

A tous ceux qui m'ont aidé de près ou de loin à la réalisation
de ce modeste travail.

Yahia

Remerciement

Tout d'abord, nous tenons à remercier Allah, le clément et le miséricordieux de nous avoir donné la force et le courage de mener à bien ce travail.

*Nous voudrions exprimer nos vifs remerciements à notre encadreur « **Dr.Ahmed Korichi**», pour les orientations et les conseils qu'il a su nous prodiguer durant l'évolution de notre projet.*

Nous voudrions aussi remercier tous les professeurs qui ont contribué à notre formation.

Nos remerciements vont également à tous ceux et celles qui de près ou de loin nous ont apporté l'aide et l'encouragement,

Résume

Résumé: Les réseaux Mobile Peer-To-Peer (P2P) sont devenus de plus en plus populaires ces derniers années, cette popularité est dû aux caractéristiques avantageuses offertes par ces systèmes telles que: le passage à l'échelle, tolérance aux panne et le contrôle décentralisé. Chaque dispositif peut jouer le rôle de serveur en offrant ces ressources aux autres nœuds, et à la fois le rôle d'un client en consommant les ressources des autres nœuds. Toutefois, le milieu ouvert, la topologie dynamique, l'absence d'administration centrale sont des caractéristiques qui rendent ces réseaux vulnérables aux différentes attaques, telles que le l'attaque du trou noir, Eclipse, Sybil…etc. Dans ce mémoire, nous allons essayer d'étudier le problème du trou noir par approche de simulation. Nous analysons dans ce travail l'effet de cette attaque sur le fonctionnement général des réseaux mobiles P2P avec une évaluation des performances des solutions existantes.

Mots clés: réseaux mobile P2P, trou noir, simulation, évaluation des performances

Abstract: During this last years, mobile Peer-To-Peer networks are more and more popular, this popularity is due to its advantageous features given by this system such as: scalability, fault tolerance and decentralized control. Each device may play the role of a server when it gives its resources to other nodes, and at the same time the role of client when it consumes the resources of other nodes. However, the open environment, the dynamic topology and the absence of central administration are characteristics which make these networks vulnerable for different attacks like blackhole attack, Eclipse attack, Sybil attack…etc. In this thesis, we've tried to study the blackhole problem with simulation approach. We've analyzed the effect of this attack on the general functions of mobile P2P networks with an evaluation of the existent solutions performances.

Keywords: mobile Peer-To-Peer networks, blackhole, simulation, performance evaluation.

Tables des matières

Résume V

Tables des matières V

Liste des tableaux IX

Liste des figures X

Liste d'abréviation XI

Introduction générale

Introduction générale ..... a

1. Sujet ..... a

2. L'objectif ..... b

3. Structure de la thèse ..... b

Chapitre 01: Les réseaux Peer-To-Peer

1. Introduction 2

2. Définition 2

3. Exemple d'application des réseaux P2P 3

4. Caractéristique de réseau P2P 3

5. Classification de réseau P2P 4

5.1. Réseaux P2P centralisés 5

5.2. Réseaux P2P Décentralisés (pur) 7

5.2.1. Réseaux P2P décentralisés non structurés 7

5.2.2. Réseaux P2P décentralisés structurés 9

5.3. Les réseaux P2P hybride 11

6. Les avantages et les inconvénients des réseaux P2P 12

7. Comparaison entre les réseaux P2P et l'architecteur Client/serveur 15

8. Conclusion 15

Chapitre 02:La sécurité des réseauxPeer-To-Peer

1. Introduction 17

2. La sécurité des réseaux P2P 17

2.1. Les critères de la sécurité des réseaux 17

2.2. Mécanismes de bases de sécurité 18

3. Les attaques possibles dans les réseaux P2P 23

3.1. Pollution de DHT 23

3.2. L'attaque Sybil 24

3.3. L'attaque Eclipse 24

4. Le problème du trou noir (BLACKHOLE) 24

4.1. Le fonctionnement général du protocole AODV 25

4.2. L'attaque du trou noir 26

5. Etat de l'art 28

6. Conclusion 33

Chapitre 03: Implémentation

1. Introduction 35

2. La simulation comme un outil de dimensionnement 35

3. Choix de simulateur 35

3.1. Grille d'analyse d'un simulateur 36

3.2. Le simulateur retenu 38

4. L'implémentation 38

4.1. Présentation du Simulateur OPNET 38

4.2. Préparation de l'Environnement d'Implémentation 40

5. La simulation 41

6. Lesrésultats 45

7. Analyse de résultats 47

8. Conclusion 48

Conclusion générale 50

Références bibliographiques 51

Liste des tableaux

Tableau 1.1	Comparaison entre P2P est Client/serveur…….....	15
Tableau 3.1	Comparaison entre différents simulateurs réseaux …….....	36
Tableau 3.2	Grille d'analyse d'un simulateur ……...	38
Tableau 3.3	Variables d'environnement d'OPNET……..…. ……..	41
Tableau 3.4	Les paramètres de simulation…….	42
Tableau 3.5	AODV paramètres pour un nœud corrompu et un nœud normal ……..	44

Liste des figures

Figure 1.1 Classification de réseau P2P…….…... 5

Figure 1.2 Réseau P2P centralisé …….…….... 6

Figure 1.3 Réseau P2P décentralisé…….……. 7

Figure 1.4 Réseau P2P Hybride..……..…… 12

Figure 2.1 Cryptographiesymétrique……..... 19

Figure 2.2 Cryptographieasymétrique……..…… 20

Figure 2.3 Génération du MAC ……..... 21

Figure 2.4 Créationd'une signature numérique……..……... 22

Figure 2.5 La sécurité du réseau P2P ……..…….…… 22

Figure 2.6 L'attaque BLACKHOLE …….……..... 27

Figure 3.1 Fonctionnementd'OPNET ……... 39

Figure 3.2 L'environnement de simulation …….. 42

Figure 3.3 L'environnement de simulation avec trou noire …….. 45

Figure 3.4 End-to-end delay sans attaque ……...…. 45

Figure 3.5 End-to-end delay avec attaque……. 45

Figure 3.6 Network Load sans attaque ……...…. 46

Figure 3.7 Network Load avec attaque…… 46

Figure 3.8 Throughput sans attaque……. 46

Figure 3.9 Throughput avec attaque…….. 46

Figure 3.10 Trafic reçu par la destination.....…….. 46

Figure 3.11 Trafic reçu par le trou noir…….. 46

Figure 3.12 Trafic envoyé par le trou noir…….. 47

Figure 3.13 Trafic envoyé par la source ……. 47

Liste d'abréviation

AODV	Ad-Hoc On Demand Routing Vector
BT	BitTorrent
DOS	Denial of Service
MAC	Message Authentication Code
MANET	Mobile Ad-Hoc Network
OPNET	Optimized Network Engineering Tools
RERR	Route Error
RREQ	Route Request
RREP	Route Reply
P2P	Peer-To-Peer
IP	Internet Protocol
TCP	Transmission Control Protocol
TTL	Time-To-Live
DHT	Distributed Hachage Table
DES	Data Encryption Standard
AES	Advanced Encryption Standard
MIT	Massachusetts Institute of Technology
HMAC	Hashed Message Authentication Code
WPAN	Wireless Personal Area Network
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WWAN	Wireless Wide Area Network

Introduction générale

Introduction générale

Un réseau informatique est un ensemble de machines interconnectées qui permet l'échange d'informations et le partage des ressources, ce réseau est divisé en deux grandes catégories selon le moyen de connexion entre les machines: les réseaux filières et les réseaux sans fil, dans ces derniers réseaux, les terminaux sont interconnectes sans aucun moyen physique mais par les ondes radio.

Les réseaux sans fil sont divisent en deux catégories: les réseaux sans fil avec infrastructure et sans infrastructure. Dans le premier on trouve les réseaux WPAN, WLAN, WMAN, WWAN selon l'espace de couverture à partir de la zone géographique moins au plus grand espace, et dans le deuxième on a les réseaux mobiles Ad hoc (MANET), et les réseaux mobiles Peer-To-Peer. Ce dernier type permet d'établir des communications directes, d'égal à égal, entre les différents nœuds du réseau, qui peuvent alors échanger différents types d'informations sans passer par un serveur central.

Ces dernières années, les réseaux peer-to-peer (P2P) sont devenus très populaires. Cette popularité vient des bonnes caractéristiques offertes par ces systèmes comme : la grande échelle, l'autonomie des nœuds et le contrôle décentralisé. Ce type de réseaux offre une bonne opportunité pour répondre aux limites des systèmes basés sur le paradigme Client/serveur. Les réseaux P2P sont utilisés avec succès dans plusieurs domaines comme : le partage de fichiers, le partage de capacité de calcul et l'échange de messages instantanés. Grâce à leurs caractéristiques avantageuses, de nouveaux domaines se dirigent vers l'utilisation de ces réseaux dans de nouvelles applications.

1. Sujet

Le grand défi relevé par les réseaux mobile P2P est la sécurité. Les réseaux mobiles P2P sont vulnérables à des attaques en raison de leurs caractéristiques telles que le milieu ouvert, la topologie dynamique, l'absence d'administration centrale, la

coopération distribuée. L'utilisation de liaisons sans fil rend ces réseaux sujets à des menaces de sécurité physique. Sans aucune sécurité adéquate, les nœuds mobiles sont facilement capturés, compromis et détournés par des nœuds malveillants. L'adversaire peut écouter et modifier les messages dans le canal de communication (attaque Men In the Middle), injecter des messages erronés, supprimer des messages (attaque DOS).

Parmi les attaques qui peut pénètre la sécurité des réseaux P2P est l'attaque de trou noire qu'est une type de l'attaque DOS. Cette attaque a un grand effet sur le fonctionnement de réseau P2P.

2. L'objectif

Dans le cadre de ce mémoire, nous nous intéresserons au problème de sécurité dans les réseaux P2P et en particulier le problème de trou noir. Dans cette vision nous allons essayons d'analyser ce problème par approche de simulation.

3. Structure de la thèse

Ce mémoire est organisé en trois chapitres. Chaque chapitre aborde des points spécifiques. Il est et structuré comme suit:

Le premier chapitre présente une introduction aux réseaux peer to peer, et les différents concepts liés à ces réseaux. Le deuxième chapitre explique les mécanismes de sécurité fondamentaux utilisés dans la sécurisation des réseaux P2P, et donne une bref sur les attaque possible dans les réseaux P2P et en particulier l'attaque de trou noir et les solutions existons pour empêche cette attaque.

Le dernier chapitre est réservé à l'implémentation du modèle de simulation du l'attaque de trou noire et l'analyse de performances. Enfin, nous terminons la thèse par une conclusion générale dans laquelle nous résumons l'essentiel de notre travail et nous donnons quelques orientations des travaux futurs.

Chapitre : 01

Les réseaux Peer-To-Peer

1. Introduction

Ces dernières années, l'utilisation des réseaux est en croissant, à cause de ces avantages comme l'échange de l'information et le partage des ressources. Ces réseaux ont été initialement fondés sur des architectures client-serveur.

Une telle architecture présente beaucoup d'inconvénients, l'existence d'un point central étant le plus évident. L'architecture P2P se pose comme une solution de rechange à l'architecture client-serveur en offrant une répartition du trafic et de la charge, une résistance aux fautes et l'anonymat.

Dans ce chapitre on propose une vision globale sur les réseaux P2P, tel que sa définition, son domaine d'application, ses caractéristiques, sa classification, ses avantages et ses inconvénient, une comparaison avec l'architecture client-serveur et on termine par une conclusion.

2. Définition

En cours de la recherche bibliographique de ce mémoire, nous avons trouvées plusieurs définitions au réseau P2P, nous citons les deux définitions suivantes parmi celles que nous avons trouvées dans [Patrick Marlier, 2007] et [Androutsellis. S et al, 2004] respectivement:

" Le terme "Peer-to-Peer", "poste à poste" ou "pair à pair" en français (ou plus couramment P2P), désigne un modèle de réseau informatique dont les éléments (les nœuds ou "peer") sont à la fois clients et serveurs lors des échanges. Ce modèle a permis une décentralisation des réseaux, en offrant une alternative aux traditionnelles architectures client/serveur ou des architectures N-tiers.

Comme leur nom l'indique, les Peer-to-Peer permettent d'établir des communications directes, d'égal à égal, entre les différents nœuds du réseau, qui peuvent alors échanger différents types d'informations sans passer par un serveur central."

"Peer-to-peer systems are distributed systems consisting of interconnected nodes able to self-organize into network topologies with the purpose of sharing resources such as content, CPU cycles, storage and bandwidth, capable of adapting to failures and accommodating transient populations of nodes while maintaining acceptable connectivity and performance, without requiring the intermediation or support of a global centralized server or authority".

L'utilisation des réseaux Peer-to-Peer est aujourd'hui en pleine croissance à cause de leurs avantages et caractéristiques et leur propagation dans tous les domaines. Pour cela plusieurs logiciels ont été développés.

3. Exemple d'application des réseaux P2P

Plusieurs domaines d'applications utilisent le principe de réseaux P2P, nous avons trouvé dans [Patrick Marlier, 2007] les exemples suivants:

- Le partage de fichiers avec des logiciels comme KaZaA ou eMule
- Les logiciels de téléphonie sur Internet dont le plus populaire Skype.
- Des programmes de messageries instantanées (ICQ, AIM)
- La Télévision par P2P: Les fondateurs de Kazaa et de Skype préparent la télévision via le peer-to-peer ("Vénice Project")
- Des moteurs de recherche tels qu'Amoweba (moteur de recherche distribué en P2P basé sur l'utilisation intelligente des liens favoris des internautes).
- Des projets permettant le partage de la puissance de calcul d'ordinateur du monde entier, tels que le "projet SETI" dont le but est de recherche des traces d'Intelligence Extra-terrestre.
- Des Plate-forme de développement tel que "JXTA3", technologie développée par Sun Microsystems, qui a pour but de pouvoir interconnecter n'importe quel système sur n'importe quel réseau. Elle utilise des protocoles basés sur XML et doit permettre de mettre en relation des ordinateurs, des téléphones portables, des PDA, etc. pour les faire communiquer de manière décentralisée. "Java Binding" est actuellement la version la plus aboutie.
- Le partage d'informations : informations collaboratives pour la détection de spam (cf. Bibliographie : Spam Attacks: P2P to the Rescue).

4. Caractéristique de réseau P2P

Les systèmes pair à pair (P2P) sont devenus de plus en plus populaires, cette popularité est dû aux caractéristiques avantageuses offertes par ces systèmes. Dans [Radad Al king, 2010] on trouve les caractéristiques suivantes:

- Grande échelle : il s'agit de faire coopérer un grand nombre de nœuds (jusqu'à des milliers ou des millions) pour partager leurs ressources tout en maintenant une bonne performance des systèmes. Cela signifie qu'un système P2P doit offrir des méthodes bien adaptées avec un environnement dans lequel il y a un grand volume de données à partager, un nombre important de messages à échanger entre un grand nombre de nœuds partageant leurs ressources via un réseau largement distribue.

- Autonomie de nœuds : chaque nœud gère ses ressources d'une façon autonome. Il décide quelle partie de ses données à partager. Il peut se connecter ou/et se déconnecter à n'importe quel moment. Il possède également l'autonomie de gérer sa puissance de calcul et sa capacité de stockage. Il est capable de décider la méthode de conception de bases de données et le SGBD le plus adéquat a ses besoins.

- Environnement dynamique : à cause de l'autonomie de nœuds, chaque nœud peut quitter le système à n'importe quel moment ce qui fait disparaitre ses ressources du système. De nouvelles ressources peuvent être ajoutées au système lors de la connexion de nouveaux nœuds. Alors, a cause de l'instabilité des nœuds, les systèmes P2P doivent être capables de gérer un grand nombre de ressources fortement variables. La sortie d'un nœud du système (ou la panne d'un nœud) ne doit pas mettre le système en échec. Elle doit être tolérée et avoir un "petit" impact sur la performance de tout le système.

- Hétérogénéité : à cause de l'autonomie des nœuds possédant des architectures matérielles et/ou logicielles hétérogènes, les systèmes P2P doivent posséder des techniques convenables pour résoudre les problèmes lies a l'hétérogénéité de ressources.

- Décentralisation : le fait que chaque nœud gère ses propres ressources permet d'éviter la centralisation de contrôle. Un système P2P peut fonctionner sans avoir aucun besoin d'une administration centralisée ce qui permet d'éviter les goulots d'étranglements et d'augmenter la résistance du système face aux pannes et aux défaillances.

- Auto configuration : puisque les systèmes P2P sont souvent déployés sur l'Internet, la participation d'un nouveau nœud à un système P2P ne nécessite pas une infrastructure couteuse. Il suffit d'avoir un point d'accès à l'Internet et de connaitre un autre nœud déjà connecte pour se connecter au système. Un système P2P doit être un environnement ouvert ; c'est-à-dire, un utilisateur sur un nœud doit être capable de connecter son nœud au système sans avoir besoin de contacter une personne et sans avoir besoin de passer par une administration centralisée.

5. Classification de réseau P2P

Trois grandes catégories de systèmes P2P -comme il est ampliatif dans la figure suivant- peuvent être identifiées : centralisé, décentralisé et hybride. La catégorie décentralisé peut encore être divisée en décentralisé mais structuré et décentralisé non structuré. La différence principale entre ces systèmes est le mécanisme utilisé pour rechercher des ressources dans le réseau P2P [Guy Pujolle, 2008]

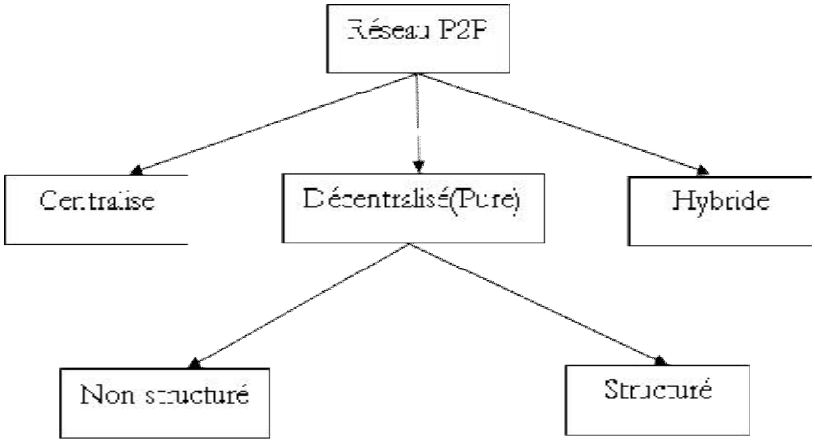

Figure 1.1: Classification des réseaux P2P

5.1. Réseaux P2P centralisés

Dans les systèmes P2P centralisés, la description et l'adresse des ressources sont stockées dans un annuaire d'un serveur central. Quand un nœud souhaite partager une ressource, il la déclare au serveur central, celui-ci stocke son adresse IP ainsi un numéro de port donné par le nœud où il pourra être contacté pour un téléchargement. Lorsqu'un utilisateur recherche une ressource, il envoie une requête au serveur central qui lui répond et transmet la liste des nœuds possédant le fichier demandé.

Après avoir reçu une requête d'un pair, l'index central recherche le meilleur pair dans son annuaire pour répondre à la requête. Le meilleur pair est celui qui est le plus économique, le plus rapide ou le plus disponible selon les besoins de l'utilisateur. Le serveur ne fournit que la capacité de recherche et négocie les téléchargements entre clients. Le contenu reste toujours du côté client.

Lorsque le nombre de participants devient trop grand, ce modèle comporte quelques inconvénients dus à son infrastructure centralisée, notamment la surcharge de l'annuaire chargé de recueillir des informations sur tous les participants. Cette catégorie de réseaux P2P ne passe malheureusement que mal à l'échelle et peut tomber en panne à cause d'un seul nœud. Napster a été l'exemple le plus connu reposant sur ce modèle.

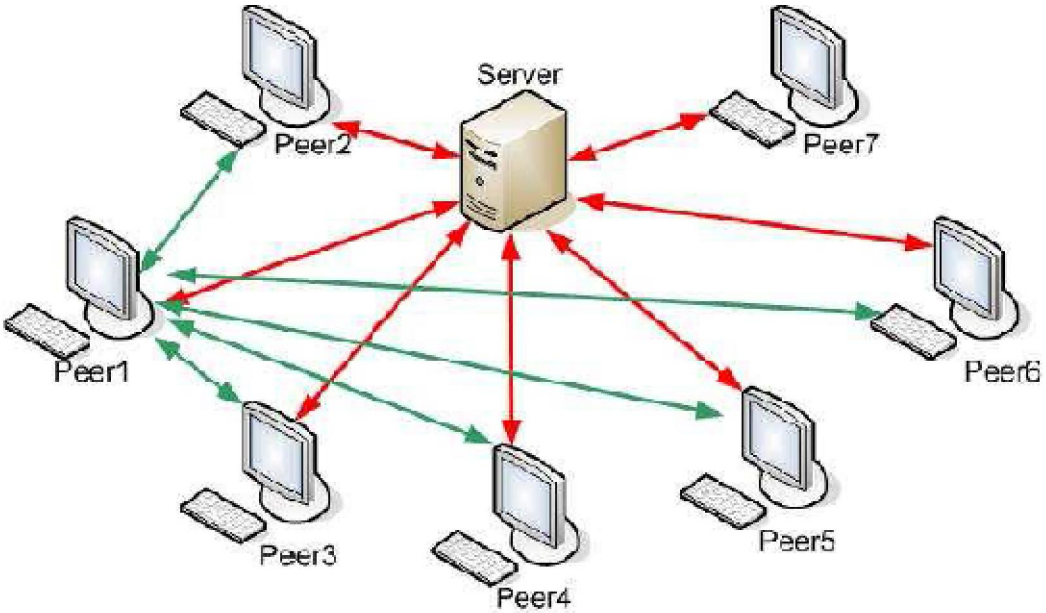

Figure 1.2: Réseau P2P centralisé

Nous expliquons ici un exemple de réseau P2P centralisé qu'est Napster qu'on a trouvé dans [Guy Pujolle, 2008].

Napster

Napster peut être considéré comme le premier réseau P2P. Son architecture est centralisée. Cela signifie que les éléments du réseau informent un serveur central des fichiers dont ils disposent et qu'ils le contactent pour obtenir les coordonnées (adresse IP et numéro de port) d'un élément possédant les fichiers recherchés. Chaque utilisateur doit exécuter le logiciel Napster sur l'ordinateur (client) afin de participer au partage des fichiers. Étant connecté à Internet, le client établit une connexion TCP avec le serveur central Napster et lui déclare les fichiers partagés. Ce serveur détient un annuaire avec toutes les adresses IP des clients participants, ainsi qu'une liste des ressources partagées. Le fichier en lui-même ne transite pas par le serveur central, qui fonctionne simplement comme un moteur de recherche. Une fois l'adresse IP trouvée, les ordinateurs clients peuvent se connecter directement entre eux. Il ne s'agit donc pas d'un réseau totalement pair à pair. Sans le serveur central, le réseau ne peut pas fonctionner.

On trouve dans [Guillaume D et al, 2010] quelque avantages et inconvénient de cette class:

Les avantages:

- Recherches non-exactes
- Charge minimale des pairs
- Contrôle des pairs/données possibles

Les inconvénients :

- Pérennité des serveurs
- Cout des serveurs
- Confiance envers des serveurs

5.2. Réseaux P2P Décentralisés (pur)

Dans ce type d'architecture, il n'y a plus de serveurs centraux -comme illustré dans la figure suivant- tous les nœuds sont égaux et jouent le même rôle, ainsi la suppression d'un pair du réseau, n'affecte pas les services offerts. Par contre, l'absence d'un serveur central ayant une vue globale sur la localisation des ressources hébergées par les pairs dans le réseau P2P. Ce cas la pose le problème suivant: Comment un pair peut découvrir et accéder à une ressource dans ce contexte ?

Pour cela, il existe deux méthodes pour la recherche de la ressource: la recherche par l'inondation et la recherche par algorithme connues respectivement sous le nom de réseaux P2P décentralisés non structurés et réseaux P2P décentralisés structurés.

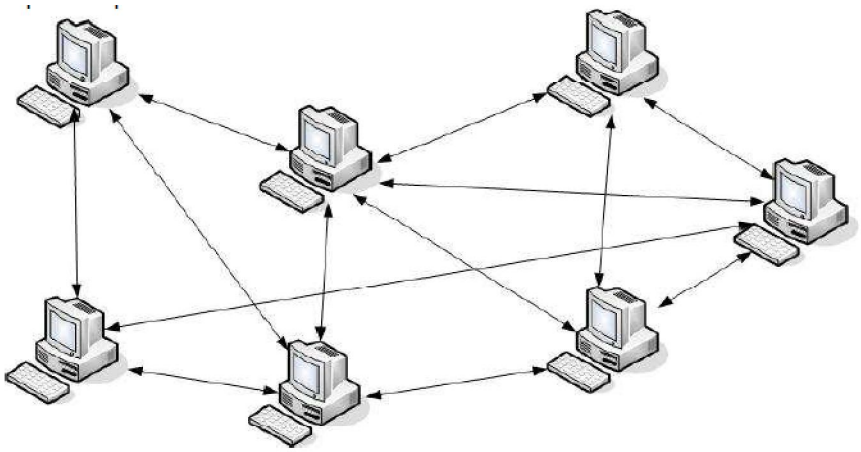

Figure 1.3: Réseau P2P décentralisé

5.2.1. Réseaux P2P décentralisés non structurés

Cette classification est base sur la notion de l'inondation qu'on lorsqu' un utilisateur peut découvrir une ressource, il transmettre une requête qui contiens le nom de la ressource vers les autre voisins jusqu'à atteindre le client qui dispose l'objet désiré, afin d'éviter l'inondation du réseau durant un temps trop long, le système associe à chaque requête un temporisateur TTL "Time To Live", la valeur attribuée au TTL est généralement 7. Lorsqu'il arrive à zéro, la requête n'est plus renvoyée.

L'inconvénient majeur de ce mécanisme, est que TTL = 0 avant le parcours de l'intégralité du réseau, ce qui peut aboutir à l'échec d'une recherche bien que l'objet désiré soit disponible sur le réseau P2P.

Ces architectures non structurées sont extrêmement résistantes aux nœuds entrant et sortant du système. Par contre, l'actuel mécanisme de recherche passe mal à l'échelle et génère une charge importante pour les participants au réseau. Cette méthode est utilisée dans le système : Gnutella et FreeNet.

Nous expliquons ici un exemple de réseau P2P décentralisé non structurés qu'est Gnutella qu'on a trouvé dans [Guy Pujolle, 2008].

Gnutella

Gnutella a été le premier réseau P2P totalement décentralisé. Crée en mars 2000 par Justin Frankelet Tom Pepper, succédant à Napster, dont la centralisation présentait une forte faiblesse, Gnutella a tiré profit de cette expérience. Gnutella est un protocole ouvert, décentralisé pour des recherches distribuées sur une topologie plate de pairs.

Selon Gnutella, tous les pairs sont à la fois serveur et client. Ce protocole n'a pas de répertoire centralisé et n'a aucun contrôle sur la topologie ou l'emplacement des fichiers. Le réseau est formé avec des pairs joignant le réseau d'après certaines règles simples. L'emplacement des données n'est fondé sur aucune connaissance de la topologie. Pour localiser un objet, un client demande à ses voisins qui, eux-mêmes, demandent à leurs voisins. Ce système permet simplement l'entrée et la sortie des clients, mais le mécanisme utilisé passe mal à l'échelle et génère de fortes charges dans le réseau.

On trouve dans [Guillaume D et al, 2010] quelque avantages et inconvénients de cette class

Les avantages :

- Distribution Complete
- Recherches non-exactes

Les inconvénients :

- Passage à l'échelle limité (inondation)
- Charge non-homogène des pairs (super pairs)
- Localisation de données rares (chemin aléatoire)

5.2.2. Réseaux P2P décentralisés structurés

Les systèmes P2P décentralisés structurés mettent en œuvre un algorithme de recherche. Cet algorithme est complètement déterministe, et les liens entre les pairs sont établis suivant des règles bien définies.

L'infrastructure de recherche fonctionne comme une table de hachage distribuée, ou DHT (Distributed Hash Table), implémentée à travers les pairs. Cette structure permet la découverte efficace des données par le biais de clés. Elle est particulièrement appropriée au développement de réseaux à grande échelle. Dans cette catégorie, on peut placer Chord, CAN (Content Adressable Network), Tapestry, Pastry, Kademlia et Viceroy.

Une table de hachage distribué (DHT) hache premièrement le nom du fichier recherché. Pour cela, la DHT utilise une fonction de hachage standard -telles que SHA-1 ou MD5- sécurisée pour faire correspondre à chaque nom de fichier son « empreinte » sous forme d'une chaîne de bits de longueur fixe. Cette fonction de hachage garantit que pour deux ressources différentes les clés générées sont uniques. Ainsi, la **clé** permet d'identifier et de retrouver la ressource de manière fiable. Deuxièmement hache l'adresse IP donne l'**identifiant** d'un utilisateur .Il s'agit ensuite de stocker de manière distribuée les couples (clé, identifiant) sur les nœuds du réseau pour qu'à chaque ressource du réseau soit associée l'adresse de l'utilisateur possédant la ressource. De la redondance dans le stockage est également introduite afin que le départ d'un nœud du système n'engendre pas la perte des métadonnées qu'il stocke et ne rende impossible l'accès à ces données.

Les DHT présentent de bonnes propriétés du fait de l'utilisation d'un modèle P2P pur : aucun pair ne joue de rôle particulier ou central, et chacun agit de manière strictement équivalente. Parmi les propriétés de DHT on trouve dans (Guy Pujolle, 2008) les suivants:

Performance : Dans des conditions normales de fonctionnement, le nombre de sauts nécessaires est limité. Par exemple, dans une communauté de 106 pairs utilisant une base d'identifiants hexadécimale, la longueur moyenne d'une requête avoisine cinq sauts.

Passage à l'échelle (évolutivité): Deux caractéristiques confèrent aux DHT de bonnes performances de passage à l'échelle. La première est liée au nombre moyen de sauts nécessaires au routage des requêtes, qui reste petit, même dans le cas de communautés comptant un grand nombre de participants. La seconde est relative aux tables de routage, qui restent elles aussi d'une taille raisonnable en regard du nombre de participants.

Fiabilité : L'utilisation d'un algorithme de découverte et de routage permet, pour une clé donnée, de déterminer le pair d'identifiant le plus proche. Dans des conditions statiques, une réponse négative à une requête signifie que la ressource requise n'est pas disponible dans la communauté.

Tolérance aux fautes : Du fait de l'absence de centralisation, qui exclut tout point central, les DHT présentent une bonne tolérance aux suppressions aléatoires de nœuds. Les requêtes peuvent être acheminées même si une partie des nœuds disparaît. Par contre, chaque nœud racine d'une ressource particulière s'apparente à un point central. Des mécanismes de redondance sont souvent mis en place pour éviter l'inaccessibilité d'une ressource présente dans une DHT.

Un exemple de réseau P2P décentralisé structurés qu'est Chord qu'on a trouvé dans [Guillaume D et al, 2010]

Chord

Chord organise son espace d'adressage suivant un anneau dont les 2m adresses (ou identifiants, id) possibles sont ordonnées le long de sa circonférence. Chaque pair ainsi que chaque ressource possède un identifiant obtenu par une fonction de hachage SHA-1 (dans ce cas m = 160 bit) qui garantit une distribution homogène des ressources sur l'anneau Chord.

Chord se limite une fonction de routage, c'est dire qu'étant donne un identifiant, Chord localise le pair responsable qui est celui possédant le plus petit identifiant supérieur ou égal à celui de la ressource. Quand un pair rejoint le réseau, il prend en charge une partie des identifiants attribués à son successeur direct, et quand il quitte le réseau, tous ses identifiants sont attribués à son successeur. Chord ne propose donc pas toutes les primitives de stockage / recherche / réplication pour opérer une DHT, et encore moins une application de partage de fichier fonctionnelle.

L'intérêt de Chord est de proposer une structure simple et efficace permettant de router les messages. Pour cela, chaque pair du réseau maintient une table de pointeurs contenant les informations «id, ip, port» pour un certain nombre de pairs. Plus cette liste est grande, plus elle est couteuse à maintenir, mais plus le routage est rapide (le cas extrême étant de connaitre tous les pairs du réseau, le routage ne nécessite alors qu'un message). Chord parvient à trouver un compromis entre la taille de la table de routage comportant O(log(N)) entrées et le routage nécessitant O(log(N)) messages. Pour cela, un pair, d'id currentID, choisit chaque pointeur de stable de telle sorte que le pair s´sélectionne soit le seul représentant de l'intervalle [(currentID+2i) − (currentID+2i+1)] avec i+1 < m. Un pair connait donc un successeur représentant une portion de l'anneau qui est deux fois plus grande pour chaque nouvelle entrée.

Le routage est ensuite itératif, de proche en proche, chaque pair envoyant la requête au successeur connu le plus proche de l'identifiant recherché.

Les principales limites de Chord sont, d'une part sa topologie en anneau obligeant de parcourir l'ensemble de l'espace d'adressage dans le pire cas, et d'autre part, l'absence de primitives pour opérer une DHT. Ces faiblesses sont résolues par l'architecture Kademlia.

On trouve dans [Guillaume D et al, 2010] quelque avantages et inconvénient de cette classe

Les avantages :

- Distribution complète
- Passage l´échelle / Charge homogène
- Localisation de données rares
- Stockage des données

Les inconvénients :

- Recherches exactes uniquement

5.3. Les réseaux P2P hybride

Les réseaux P2P hybrides permettent de résoudre certains des problèmes de l'approche purement distribuée, tout en gardant l'efficacité de la solution centralisée. Les réseaux fondés sur un tel mécanisme de localisation et de routage de données peuvent supporter un nombre de pairs de l'ordre du million.

Cette solution combine les caractéristiques des modèles centralisé et décentralisé. La décentralisation garantit notamment l'extensibilité, la tolérance aux fautes et le passage à l'échelle.

La centralisation partielle implique quelques centres serveurs qui contiennent des données importantes pour le système. Chaque utilisateur élit son « super-pair », qui fait office de serveur central pour des nœuds locaux et qui peut communiquer avec d'autres « super-pairs ».FastTrack, KaZaA, BitTorrent, eDonkey/eMule sont quelques exemples de ce système.

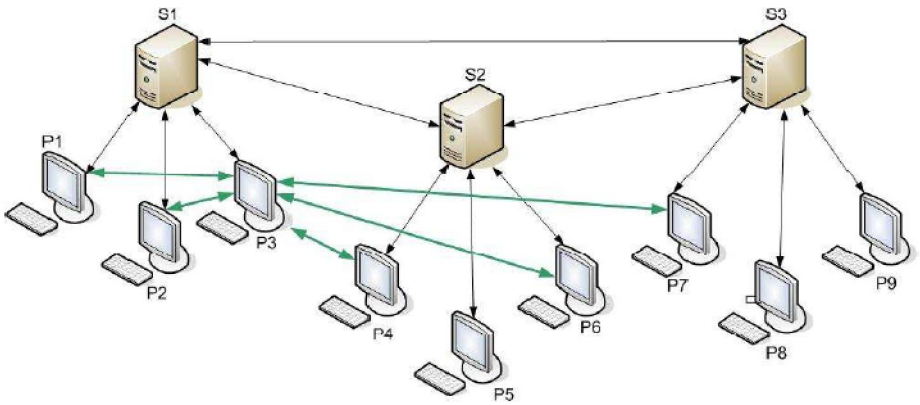

Figure 1.4: Réseau P2P Hybride

Voilà un exemple de réseau P2P Hybride qu'est BitTorrent qu'on a trouvé dans [Guy Pujolle, 2008].

BitTorrent

BitTorrent (ou simplement BT) est un réseau P2P hybride qui permet le partage des fichiers à travers Internet. L'efficacité de ce réseau augmente lorsqu'il y a beaucoup de clients connectés, car plus il y a de clients qui téléchargent, plus il y a de clients qui partagent, et il n'est pas nécessaire d'attendre dans une file virtuelle pour commencer à télécharger.

BT étant un protocole Open Source, diverses applications peuvent l'implémenter, notamment Azureus, ABC, BitComet, etc., certaines d'entre elles offrant diverses améliorations, notamment une interface graphique améliorée, de plug-in, etc.

Bien que fondé sur la centralisation des informations sur un serveur, BitTorrent soulage la bande passante en permettant aux clients (les pairs) de s'échanger des parties des fichiers qu'ils ont téléchargées. Le serveur fonctionne alors comme une graine (en anglais seed) qui démarre le processus et envoie au moins une copie entière du fichier originel. On peut supprimer la ressource du serveur au bout d'un certain temps et laisser les clients s'échanger entre eux, ceux qui ont un fichier complet devenant eux-mêmes des graines.

6. Les avantages et les inconvénients des réseaux P2P

Les réseaux P2P ont plusieurs avantages, nous avons trouvé dans [Patrick Marlier, 2007]:

- **La répartition de la charge :** les échanges sont gérés directement par les paires, ce qui élimine un des principaux problèmes des architectures clients/serveurs : la répartition de la charge. Les P2P ne posent pas le problème de congestion des réseaux qui peuvent se

produire autour d'un serveur central devant répondre à de très nombreuses demandes. Chaque pair gère ses propres données et répond aux requêtes des autres pairs.

- **La capacité de stockage :** chaque nœud ne possède qu'une infime partie des données du réseau, qu'il partage avec les autres ordinateurs. La capacité de stockage est ainsi infiniment supérieure à celle d'un serveur traditionnel, qui ne pourrait supporter une telle quantité d'information (que ce soit au niveau technique ou au niveau du coût de mise en place).
- **La puissance de calcul :** pour les utilisateurs moyens, chaque ordinateur utilise moins de 20% de sa puissance de calcul: "travailler sous Word ou Excel (voir les 2 en même temps) n'occupe le processeur que de manière très faible, le reste étant simplement inutilisé.1" Une application répartie, s'activant en général avec l'écran de veille des ordinateurs, basée sur la technologie Peer-to-Peer peut donc permettre de mutualiser cette puissance non utilisée pour des recherches demandant des capacités considérable, qu'un serveur isolé ne peut posséder.

Les Peer-to-Peer apparaissent également dans les entreprises qui souhaitent utiliser leurs nouvelles possibilités :

- **Outils de travail collaboratif (gestion d'agenda, etc.) Exemple :** le logiciel "groove2", utilisé dans les entreprises permet le partage des documents d'un projet, de conduire des réunions, assigner des tâches, etc.
- **Résistance aux pannes (sauvegardes croisées) :** les données étant présentes sur de nombreux postes différents, les P2P peuvent donc être utilisés pour effectuer facilement des sauvegardes réparties à travers le réseau, évitant toutes pertes d'informations, ou la mise en place de lourds systèmes de sauvegardes.
- **Extensibilité :** auto-configuration des pairs. Il est très facile de rajouter de nouveaux pairs. Ceux-ci sont gérés dynamiquement.

Les inconvénients :

Malgré les réseaux P2P sont très populaires et très utilisable aujourd'hui, mais ils ont des inconvénients, nous citons ici quelques une [Nathalie. B et al, 2003]

- **Les problèmes de comportement des utilisateurs**

Les systèmes d'échanges de fichiers peer-to-peer peuvent facilement souffrir de l'anarchie générale. L'anonymat aidant, les membres sont parfois tentés d'avoir des comportements malveillants.

Sans un minimum de contrôle, on peut voir apparaître des activités comme la diffusion de virus ou le freeloading.

- **Les problèmes de comportement des entreprises**

- Une atteinte à la vie privée

Notre vie privée n'est pas nécessairement protégée lorsque nous utilisons des outils peer-to-peer. En effet, les adresses IP des utilisateurs peuvent être récupérées lorsque le logiciel est centralisé.

- La pollution des réseaux

Sans même annoncer d'ultimatum, plusieurs entreprises proposent de polluer les réseaux d'échange de musique entre particuliers en y incorporant des fichiers de moindre qualité ou incorrects. L'objectif est de rendre ces réseaux gratuits et anarchiques moins attractifs.

Une poignée de sociétés indépendantes développent en effet de nouvelles technologies destinées à polluer les réseaux. Leurs clients potentiels sont les industries de la musique et du cinéma, qui cherchent par tous les moyens à détourner les adeptes des téléchargements gratuits au profit de systèmes sécurisés et payants.

- **La propagande**

Nul n'est sans savoir que les systèmes peer-to-peer sont pour la plupart envahis par les bannières publicitaires même si à présent, des versions allégées des logiciels sont proposées sans publicités.

- **Les réseaux pair à pair restent imparfait à cause de :**

- La confiance et le certificat
- L'anonymat
- La sécurité
- La performance

7. Comparaison entre les réseaux P2P et l'architecteur Client/serveur

Modèle P2P	Modèle Client/serveur
Architecture décentralisée	Architecture centralisée
Topologiedynamique	Topologiestatique
Auto-organisé	Supervisé
Indépendance des pairs	Dépendance du serveur
Pas de structure (pairs)	Structure hiérarchique
Les pairs partages et consomme des ressources	Les clients ne partage jamais des ressources
Le contenu est existé dans les pairs	Le contenu reste toujours chez le serveur
Attaquesdifficiles (mobilité, anonymat)	Attaques plus simples
Communication par Messages	Orienté RPC

Table 1.1: Comparaison entre P2P est Client/serveur

8. Conclusion

Les réseaux Peer-to-Peer sont aujourd'hui de plus en plus présents dans le monde informatique, que ce soit pour les simples utilisateurs à travers les réseaux d'échanges de fichiers, de messageries instantanés ou de voix sur IP, ou encore pour les entreprises, pour la mise en place d'applications réparties comme le partage d'agendas, etc. Ils sont classés en trois grandes familles: les réseaux centralisés, les réseaux purs et les réseaux hybrides.

Les réseaux P2P ont plusieurs avantages, Mais également ont des problèmes de sécurité à cause de ces environnement ouvert et l'absence d'un structure fixe, et autre causes. Donc ils sont vulnérables à plusieurs attaques comme l'attaque Sybil, Éclipse, DOS et l'attaque de trou noir. Le chapitre suivant donne une vue globale sur la sécurité dans les réseaux P2P.

Chapitre : 02

La sécurité des réseaux Peer-To-Peer

1. Introduction

Comme nous avons vus dans le chapitre président, les réseaux P2P sont plus en plus utilise, mais comme tous les réseaux dans le monde informatique, la sécurité reste toujours un critère espéré a réalisé pour augmenter l'efficacité, l'accessibilité des donnes. Pour cela la politique de sécurité de ces réseau doit être robuste, en particulier les réseaux de liaison radio qui sont par leur nature très vulnérable aux attaques.

Dans ce chapitre, nous présentons les critères de la sécurité à garantir, puis les mécanismes de bases de sécurité, puis nous étudions les attaques qui peuvent survenir dans les réseaux P2P et on précise à l'attaque du trou noire, un vus globales sur les recherches existent au problème du trou noire (état de l'art),et on termine par une conclusion.

2. La sécurité des réseaux P2P

. La sécurité des réseaux consiste à protéger ces réseaux et leurs services contre les menaces accidentelles ou délibérées touchant la confidentialité, l'intégrité de l'information et la disponibilité de ces réseaux et les services.

2.1. Les critères de la sécurité des réseaux

Afin d'éviter un certain nombre d'écueils classiques, une politique de sécurité réseau doit être respecté un ensemble de principes génériques:

a. La confidentialité de données

Ensemble des mécanismes permettant qu'une communication de données reste privée entre un émetteur et un destinataire. La cryptographie ou le chiffrement des données est la seule solution fiable pour assurer la confidentialité des données.[Liorens etal,2003]

b. L'intégrité des données

L'intégrité peut être vue comme un ensemble des mécanismes garantissant qu'une information n'est pas modifiée, c'est-à-dire les données reçues sont exactement celles qui ont été émises par l'émetteur autorisé. Une information n'est modifiée que dans des conditions prédéfinies (selon des contraintes précises).

c. La Disponibilité

La disponibilité est une terminologie du milieu de la sécurité pour caractériser le bon fonctionnement de réseau, est un service réseau qui donne une assurance aux entités autorisées d'accéder aux ressources réseaux avec une qualité de service adéquate.

d. L'authentification

L'authentification peut être définie comme un processus de prouver une identité revendiquée, seules les pairs autorisées ont le droit d'accès au réseau. L'authentification est le moyen clé de sécurité pour assurer:

- La confidentialité : c'est lui qui lit une donnée est bien celui qui est autorisé à le faire.
- L'intégrité : celui qui a émis un message est bien celui dont le nom figure dans le message.
- La signature numérique assure l'intégrité et elle est basée sur l'authentification.

e. Non-répudiation

Mécanisme permettant de garantir qu'un message a bien été envoyé par un émetteur et reçu par un destinataire, c'est-à-dire aucun des correspondants ne pourra nier l'envoi ou la réception du message.

2.2. Mécanismes de bases de sécurité

a. La cryptographie

La cryptographie est une science qui étudie les outils servant à sécuriser les informations. De tout temps, l'art du chiffrement-déchiffrement a été employé. Le chiffrement et le déchiffrement des données sont effectués par des algorithmes cryptographiques. Ces algorithmes reposent généralement sur des problèmes mathématiques complexes, difficiles à résoudre, tels que la factorisation des nombres premiers, les logarithmes discrets, etc. [Liorens et al, 2003]

Les algorithmes cryptographiques modernes nécessitent une clé pour le chiffrement et une clé pour le déchiffrement

Il existe deux grands types d'algorithmes cryptographiques: Chiffrement symétrique ou à clé secrète et Cryptographie asymétrique ou à clé publique

- ✓ **Algorithme symétrique**

Chiffrement : transforme un message clair M en un message chiffré C tel que $C = e_k(M)$ avec une clé k

Déchiffrement : transforme un message chiffré C en un message clair $M = d_k(C)$

Contraintes :

- difficile de déduire M de C sans k

Avantages:

- Rapidité du chiffrement/déchiffrement

Inconvénients :

- Echange de la clé k par un autre canal.
- Pour n participants on a besoin de n (n-1)/2 clés secrètes enregistrées.

Parmi les algorithmes symétriques les plus connus, on trouve: le DES (Data Encryption Standard), et son successeur l'AES (Advanced Encryption Standard).

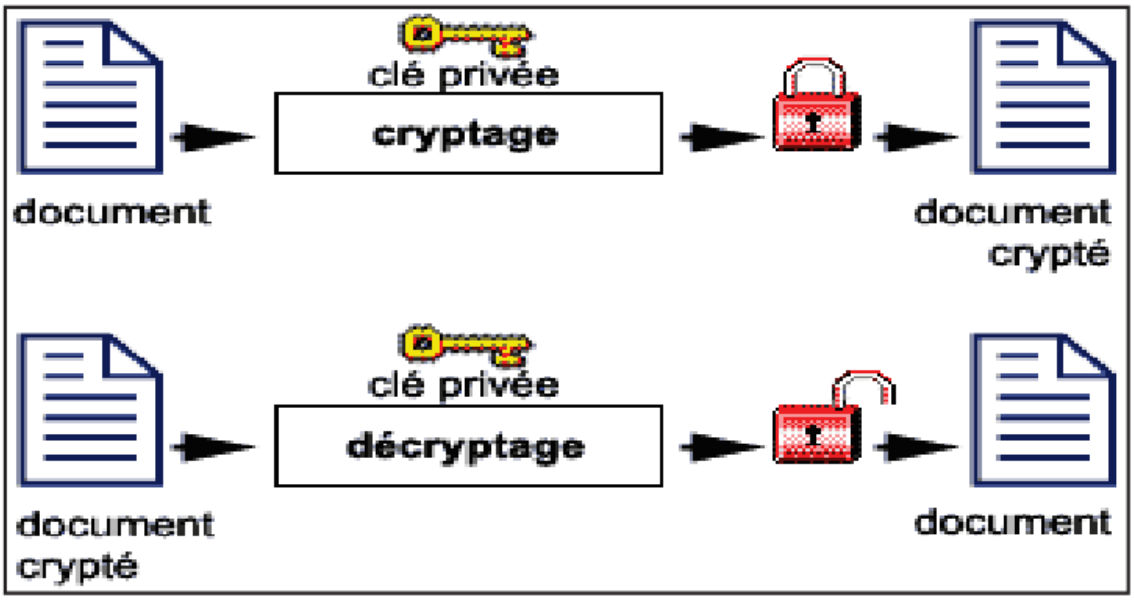

Figure 2.1: Cryptographie symétrique

✓ **Algorithmes asymétriques**

Chiffrement de données avec une paire de clés: clé publique K_{pub}, clé privée K_{priv}, la clé publique K_{pub} connue de tous, sert à chiffrer

Le message $C= e_{Kpub}(M)$ peut être véhiculé au vu et au su de tout le monde

La clé privée K_{priv} tenue secrète, sert à déchiffrer $M= d_{K\ prive}(C)$

Contraintes :

- difficile de déduire K_{priv} de K_{pub}

Avantages :

- Une seule clé secrète à enregistrer
- Très utile pour échanger les clés pour ouvrir un tunnel de communication chiffré (VPN : IKE pour IPsec, TLS/SSL). Utilisés aussi dans PGP.

Inconvénients :

- Lenteur
- Pas d'authentification de la source
- Attaque Man-In-The-Middle

Le nombre des algorithmes de chiffrement asymétrique est important, les plus connus sont RSA (Rivest Shamir Adleman), Merkle-Hellman, ECC-EllipticCurveCryptography, Rabin et ElGamal.

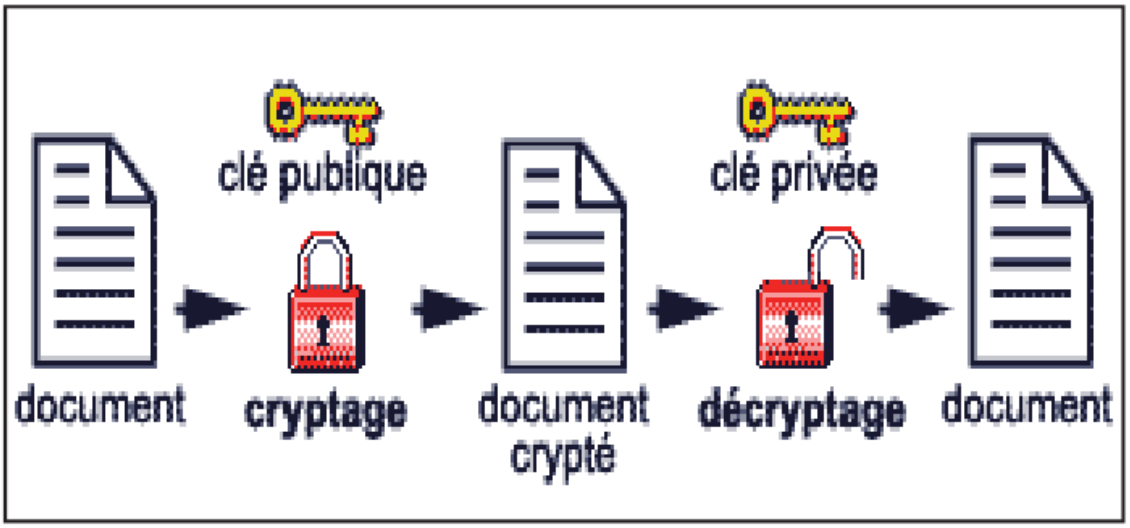

Figure 2.2: Cryptographie asymétrique

b. Fonction de hachage

Une fonction de hachage prend en entrée un texte de longueur arbitraire et renvoie en sortie un texte de taille fixe appelé le condensât ou bien l'empreinte.

Une fonction de hachage H doit avoir les propriétés suivantes :

– H appliqué sur un message produit une empreinte d (digest) de taille fixe.

– Pour toute empreinte d, il n'est pas possible de trouver x t.q : H(x)=d (propriété appelée one-way ou fonction à sens unique).

– Pour tout message x, il n'est pas possible de trouver y # x et H(y)=H(x).

– Il n'est pas possible de trouver une paire de messages (x, y) t.q: H(x)=H(y).

Les fonctions de hachage : Garantir l'intégrité d'un message M.
Exemples des fonctions de hachage: SHA, MD5

c. Code d'authentification de message (MAC)

Un code d'authentification de message, ou MAC (Message Authentication Code), est le résultat d'une fonction de hachage à sens unique dépendant d'une clé secrète. En d'autres termes, on peut construire un MAC à partir d'une fonction de hachage ou d'un algorithme de chiffrement par blocs.[Liorens et al, 2003]

Un moyen simple de transformer une fonction de hachage à sens unique en un MAC consiste à chiffrer l'empreinte d'un message avec un algorithme à clé secrète.

Une méthode de calcul de MAC à partir de fonctions de hachage plus élaborées et plus sûres est HMAC (RFC 2104). La méthode HMAC peut être utilisée avec n'importe quelle fonction de hachage itérative telle que MD5 ou SHA-x(x = 1, 256, 384, 512).

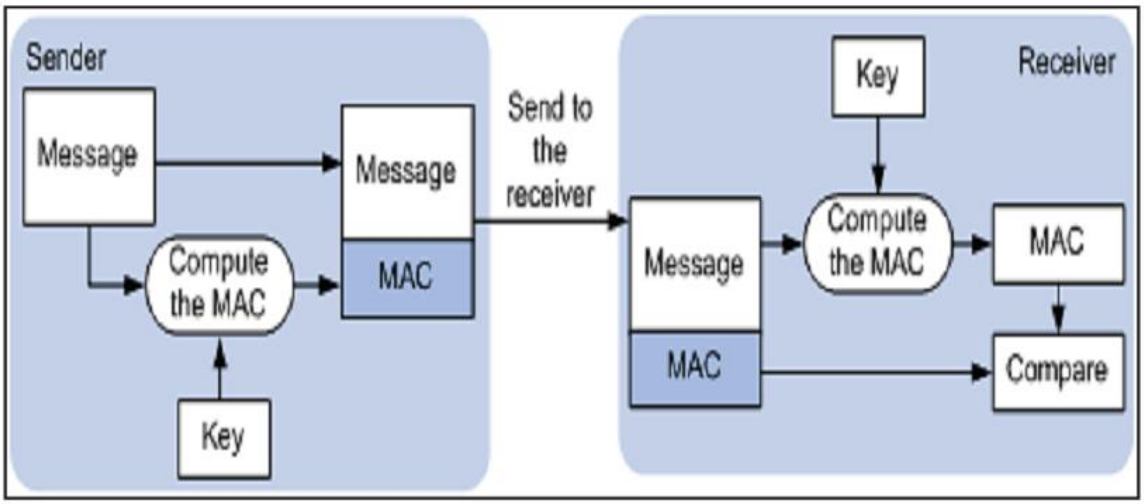

Figure 2.3: Génération du MAC

d. La signature numérique :

La signature numérique est un système assurant l'intégrité, l'authentification et la non-répudiation des données, il repose sur la cryptographie asymétrique. L'émetteur crée une empreinte de son message, chiffre l'empreinte avec sa clé privé puis il envoie le message et la

signature, le récepteur utilise la clé publique de l'émetteur pour déchiffrer la signature, il recalcule l'empreinte du message et la compare avec celle reçue. Si le condensât nouvellement calculé égale au condensât accompagnant le message alors le message n'a pas été modifié et il est prouvé authentique.

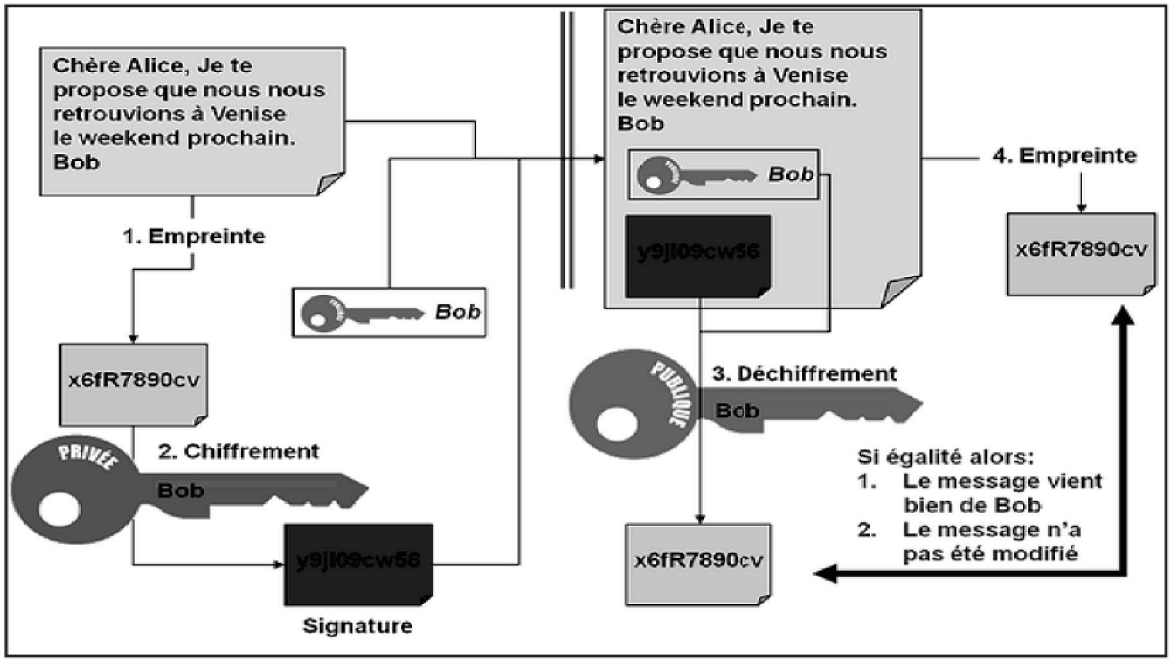

Figure 2.4: Création d'une signature numérique

On peut résumer les critères de la sécurité et leurs mécanismes dans le diagramme suivant :

Les critères Les mécanismes Les algorithmes

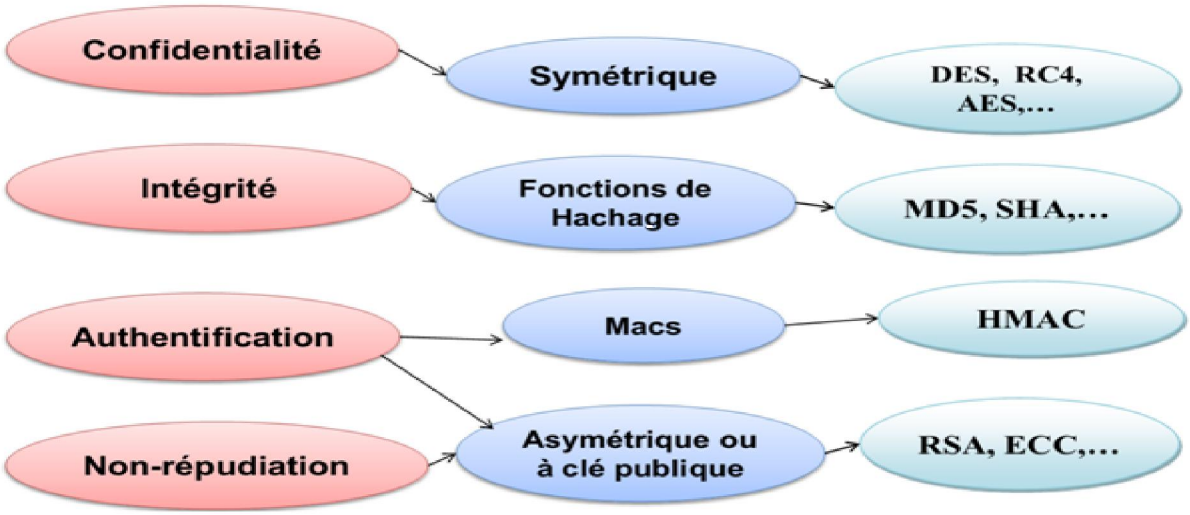

Figure 2.5: La sécurité des réseaux P2P

3. Les attaques possibles dans les réseaux P2P

Comme nous avons dit à la fin de chapitre présidant, que les réseaux P2P ont des problèmes de sécurité, ils sont vulnérables au plusieurs menaces et attaques. Nous citons ici quelques attaques et on précise a notre problème (trou noir).

3.1. Pollution de DHT

Les tables DHT (Distributed Hash Table) sont utilisées dans les réseaux structurés pour permettre l'acheminement des informations entre les différents pairs du réseau. Ces tables sont cependant basées sur la présomption que tous les nœuds sont des pairs de confiances.

Le principe de la pollution de DHT est de renvoyer des résultats erronés au demandeur. Cela peut concerner aussi bien des identifiants des fichiers, des IP et ports, qui seront falsifiés. Ainsi de propagation de pairs en pairs, l'ensemble du réseau va enregistrer et diffuser de mauvaises informations, le rendant complètement inopérant.

Un premier type d'attaque consiste à falsifier les tables de routage. Chaque pair participe au système de routage du réseau. Un nœud malicieux peut donc essayer d'introduire de fausses destinations, qui ne mèneront nulle part. Les nœuds construisent leur table de routage avec les informations données par les autres nœuds. Si ces informations sont fausses, des nœuds sains risquent eux-mêmes d'effectuer un mauvais routage, ou encore de propager l'information erronés.

Ces attaques sont assez proches de l'attaque « Eclipse », sauf qu'ici, les nœuds ne sont pas forcément « éclipser », mais peuvent posséder de mauvaises informations et conduire à un mauvais fonctionnement de l'ensemble du réseau.

Ces attaques peuvent être contrées assez facilement par les pairs sains entêtant si les destinations sont réellement accessibles avant de les ajouter dans leur table de routage. Les informations erronées données par des nœuds malicieux peuvent ainsi être détectées.

Lors de leur connexion dans le réseau, les nœuds sont aussi extrêmement vulnérables. Ils doivent en effet se connecter à d'autres pairs pour obtenir les informations nécessaires pour participer au réseau. Si un nœud malicieux parvient à être le contact des nouveaux arrivants, il va pouvoir leur fournir des informations erronées pour les faire entrer dans un réseau parallèle, contrôlé par le pirate.

Un autre type d'attaque consiste à fournir des informations lorsqu'on l'interroge sur les données dont il est responsable. Il peut par exemple dire qu'il possède certains fichiers, et refuser les connexions quand d'autres pairs souhaitent les obtenir, etc. [Patrick Marlier, 2007]

3.2. L'attaque Sybil

L'attaque Sybil est une attaque visant à éviter les systèmes de partages basés sur la réputation. Elle consiste à voler une identité (possédant beaucoup décrédite) ou à se forger de nombreuses identités pour casser le système de réputation. Il est alors possible de se bâtir une très large influence sur le réseau, grâce à l'utilisation des différentes identités (chaque identité peut certifier que les autres sont des identités de confiance partageant beaucoup).Ainsi, le pair va pouvoir utiliser largement le réseau sans y apporter sa contribution. (Ex: download massif de données sans en partager.)

La résistance d'un système à une attaque de type Sybil dépend de la facilité avec laquelle il est possible de se créer des identités. [Patrick Marlier, 2007]

3.3. L'attaque Eclipse

L'attaque Eclipse est plus générale que l'attaque Sybil décrite précédemment et vise principalement les réseaux P2P structurés. Dans ces réseaux, chaque nœud maintien des pointeurs vers ses voisins. L'attaque consiste alors à contrôler plusieurs pairs influant sur le réseau (une grande partie des voisins), pour ne pas rediriger le trafic vers les bons pairs (les pairs «sains»), et donc modifier l'utilisation normal du routage. L'attaquant cache alors les bons pairs sur le réseau, d'où le nom d'« attaque Eclipse ».

Cette attaque peut être lancé en utilisant l'attaque Sybil, c'est à dire en se forgeant de nombreuses identités sur le réseau, afin d'être présent comme voisin sur un maximum de nœud dans le réseau.[Patrick Marlier, 2007]

4. Le problème du trou noir (BLACKHOLE)

Afin de comprendre cette attaque sur les réseaux P2P et les solutions proposées contre cette attaque, il est nécessaire de comprendre le fonctionnement général de protocole de routage. Plusieurs protocoles de routages sont concernés par la notion de sécurité (AODV, DSR, OLSR, TORA..), dans cette section nous donne une définition globale sure le protocole de routage AODV qu'on va utiliser dans noter implémentation.

4.1. Le fonctionnement général du protocole AODV

Ad hoc On demand Distance Vector (AODV) est un protocole de routage réactif ce qui signifie que les routes sont construites à la demande, Si un nœud source veut envoyer des paquets de données vers un nœud destination, il doit établir et maintenir une route vers ce nœud destination durant le temps qu'il en fait usage.

Le protocole AODV est basé sur l'utilisation des deux mécanismes "Découverte de route" et "Maintenance de route" (utilisés par le DSR), en plus du routage nœud-par-nœud, le principe des numéros de séquence. Il utilise trois types de paquets de routage à savoir : RREQ (Route REQuest), RREP (Route REPly), RERR (Route ERRor).

- ✓ **Découverte des routes**

Avec le protocole AODV, chaque nœud doit maintenir une liste de ses voisins actifs. Cette liste est obtenue par un échange périodique des messages HELLO de chaque nœud avec ses voisins immédiats. Quand un nœud source S veut envoyer des données à un destinataire D et qu'aucune route vers cette destination n'est stockée dans la table de routage de la source, le nœud S initialise une procédure de découverte de routes.

La source S envoie à ses voisins une demande de route RREQ qui contient l'adresse de S, l'identifiant de la requête, un compteur de séquence, l'adresse de D et le compteur de nombre de sauts avec une valeur initiale zéro. La source attendra une période RREP_WAIT_TIMEOUT, si une réponse est reçue alors l'opération de découverte de route est terminée, sinon elle rediffuse le RREQ et attend une période plus grande si aucune réponse n'est reçue, elle continuera la rediffusion du RREQ jusqu'à un nombre maximum de tentatives RREQ_RRTRIES (03 tentatives), si après RREQ_RETRIES tentatives d'établissement de route, il n'y a aucune réponse alors le processus est abandonné et un message d'erreur est signalé à l'application. Après une certaine période d'attente (10 s), l'application demande la route et par conséquent l'opération de découverte de route est initiée. Chaque nœud qui reçoit le message RREQ recherche dans sa table de routage locale s'il existe une route vers le nœud D sinon le nœud qui traite la requête RREQ incrémente le nombre de sauts et la diffuse à nouveau. Lorsque la requête atteint la destination D ou un nœud qui connaît une route vers la destination, une réponse RREP est diffusée sur la même route de réception du RREQ (chemin inverse). La réponse RREP contient l'adresse source, l'adresse de destination, le nombre de sauts, un numéro de séquence de destination et la durée de vie du paquet. La réponse RREP passe par la route inverse vers le nœud source S. Ainsi chaque nœud, sur cette route, enregistre une entrée dans sa table de routage local

vers le nœud destination avant de renvoyer le paquet. Une fois la source S reçoit le message, elle commence à envoyer les données vers D.

- ✓ **Maintenances des routes**

L'échange des messages HELLO entre les voisins immédiats permet de mettre à jour la liste des voisins de chaque nœud. Lorsqu'un nœud N détecte qu'un autre nœud Q n'est plus accessible (Q a quitté le réseau ou est hors porté radio), N procède à une mise à jour des liens dans sa table de routage. En effet, il recherche dans sa table de routage toutes les routes qui passent par le nœud Q et les détruit avant d'annoncer à ses voisins actifs que la route passant par le nœud Q n'est plus valide. Un message RERR est envoyé alors au nœud source. Ainsi, la mise à jour est diffusée à travers le réseau saut-par saut et le nœud source initie une nouvelle procédure de recherche de route vers la destination. [Houda Hafi,2010]

4.2. L'attaque du trou noir

Dans l'article de [K. Lakshmi et al, 2010] nous avons trouvées la description du problème du trou noir qui la suivante:

L'attaque de trou noire (BLACKHOLEen anglais) est une attaque de type DOS (Denial Of Service), dans laquelle un nœud corrompu utilise la vulnérabilité de route, pour découvre les paquets de protocole de routage a objective de annoncer qu'il a le plus courte chemin vers le nœud qui va intercepte les paquets.

Cette attaque vise à modifier le protocole de routage, donc ce trafic dérouler à travers un nœud spécifique qu'est contrôlé par l'attaquant. Pendant le processus du découverte du route, le nœud source envoyer un paquet de type RREQ(Route REQuest) vers les nœuds intermédiaires pour trouver un chemin fraîche vers la destination. Le nœud corrompu repend immédiatement la source que ces nœuds non pas réfère la table de routage.

Le nœud source suppose que le processus de la découverte de la route est complet, alors il ignore les autres RREP(Route REPly) message des autres nœuds et sélectionner la route à travers le nœud corrompu pour envoyer les paquets. Le nœud corrompu fait ça par assigne un numéro de séquence élevé du paquet de repense. L'attaquant effacer les messages reçus à la place de retransmettre le, comme les conditions du protocole dit.

La figure ci-dessous illustre cette attaque où la source S veut transmettre des données vers la destination D, elle diffuse une requête RREQ, le paquet RREQ va être reçu par les nœuds N1, N2, N3.

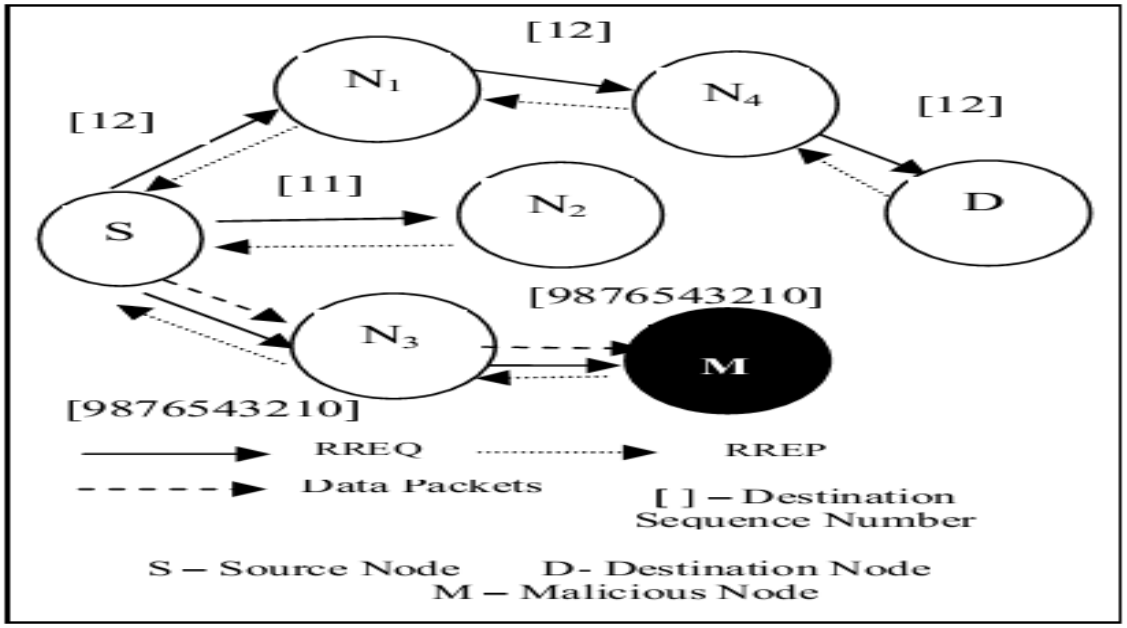

Figure2.6: L'attaque BLACKHOLE

Supposons le nœud N3 a une route vers la destination dans sa table de routage, le nœud N3génère un paquet de réponse RREP et mettre à jour sa table de routage par le nombre de sauts et le numéro de séquence de la destination.

Le numéro de séquence de la destination est un entier de 32 bits associé à chaque route et permet l'utilisation des routes les plus fraîches autrement dit les plus nouvelles. Une route est jugée fraîche que si la base du numéro de séquence de la destination est assez élevée. Le nœud N3 va envoyer le paquet vers le nœud M, tant que les nœudsN1 et N2 n'ont pas une route vers la destination D, ils seraient à nouveau diffusé le message de contrôle RREQ. Ainsi le paquet RREQ diffusé par le nœud N3devrait également être reçu par le nœud M (supposons M est un nœud malicieux). Donc le nœud M va générer un faux message de contrôle RREP et l'envoyer au nœud N3avec un numéro de séquence de destination très élevé, qui serait ensuite envoyé au nœud S.

Cependant, tant que le numéro de séquence de destination est élevé, la route à partir du nœud N3 sera considéré comme plus fraiche et donc la source serait commencée à envoyer des paquets de données au nœud N3. Le nœud N3 serait envoyer les même paquets au nœud malicieux. Le message de contrôle RREQ à partir du nœud N1, finirait par atteindre le nœud D (nœud de destination), ce qui générerait un message de contrôle RREP et la route du retour.

Toutefois, le nœud S a déjà reçu un paquet de réponse RREP avec numéro de séquence supérieur à celui de D, le nœud S ignore les deux véritables messages de contrôle RREP. Pour

chaque message de contrôle RREP reçu, la source devrait d'abord vérifier si elle possède une entrée pour la destination dans la table de routage ou non. S'il en trouve un, le nœud source serait de vérifier si le numéro de séquence de destination dans le message de contrôle reçu est plus élevé que celui qu'il a envoyé dans la dernière RREQ ou non. Si le numéro de séquence de destination est plus élevé, la source met à jour sa table de routage avec le nouveau message RREP, sinon le message de contrôle RREP sera rejeté.

5. Etat de l'art

On court de la recherche bibliographique de ce mémoire, nous avons trouvées plusieurs études sur ce problème et des solutions proposées pour empêcher cette attaque, nous résumons les dans les paragraphes suivants

En 2002 Deng [Deng et al, 2002] ont proposé une solution contre l'attaque trou noir en modifiant le protocole AODV. Dans cette méthode chaque nœud intermédiaire doit inclure l'information« next hop » quand il envoie un paquet RREP. Une fois la source a reçu le paquet RREP et avant d'envoyer les paquets de données, il extrait l'adresse du « next hop » et lui envoie une nouvelle demande de route (FurtherRequest) afin de vérifier qu'il possède une route vers le nœud intermédiaire qui a envoyé le message de réponse, et qu'il a aussi une route vers le nœud destination. Le « next hop » répond avec un paquet de réponse de route (FurtherReply) qui comprend le résultat de contrôle. La source vérifie les informations des paquets FRREP et agit selon les règles suivantes:

1) Si le « next hop » possède une route vers le nœud intermédiaire et la destination, la source établit la route reçu du nœud intermédiaire et commence l'envoi des données.

2) Si le « next hop » a une route vers la destination, mais n'a pas de route vers le nœud intermédiaire, la source suppose que le nœud intermédiaire est un nœud malicieux. Ensuite, elle initie l'envoi des données via la nouvelle route à travers le next hop et diffuse un message d'alarme dans le réseau afin d'isoler le nœud malveillant.

3) Si le « next hop » n'a pas de routes vers le nœud intermédiaire et la destination, la source lancera un nouveau processus de découverte de route, et envoie également un message d'alarme afin d'isoler le nœud malveillant.

Le mécanisme proposé est efficace dans la détection de l'attaque Blackhole, cependant, l'envoi d'un paquet FRREQ à partir du nœud source vers le « next hop» et l'attente du paquet FRREP du « next-hop » augmente la charge du routage « overhead » entre la source et le « next hop », surtout

quand ce mécanisme est appliqué sur un réseau à grande échelle et la distance entre la source et le nœud malicieux est longue.

En 2004 Al-Shurman[Al-Shurman et al, 2004] proposé deux solutions conçues pour cibler l'attaque BLACKHOL dans le protocole AODV. La première solution proposée consiste à trouver plus d'une route vers la destination (au moins trois routes différentes). La source envoie un paquet RREQ au nœud destination en utilisant ces trois routes. La destination, le nœud malicieux et les nœuds intermédiaires vont répondre à ce paquet. Le nœud expéditeur met ses paquets de données dans un tampon jusqu'à ce qu'il reçoit plus d'une réponse RREP; lorsque la source reçoit des RREP, si les routes à destination ont des nœuds partagés, la source peut reconnaître une voie sûre vers la destination, et les paquets vont être transmis. Si aucuns nœuds partagé sn semblent être dans ces routes redondantes, l'expéditeur attendra une autre RREP jusqu'à ce qu'un chemin avec des nœuds partagés identifié ou le temps d'attente soit expiré. Cette solution peut garantir à trouver une route sécurisé vers la destination, mais le principal inconvénient est le délai d'attente. Plusieurs paquets RREP doivent être reçues et traitées par la source. En outre, s'il n'y a pas de nœuds partagés entre les routes, les paquets ne seront jamais envoyés.

La seconde solution proposée exploite le numéro de séquence inclus dans l'en-tête de chaque paquet. Le nœud dans cette situation a besoin d'avoir deux tables supplémentaires; la première table comprend les numéros de séquence du dernier paquet envoyé à chaque nœud dans le réseau. La deuxième table contient le numéro de séquence reçu de chaque expéditeur. Pendant la phase de réponse de route, le nœud intermédiaire ou la destination doivent inclure le numéro de séquence du dernier paquet reçu de la source qui déclenche la demande de route. Une fois la source reçoit ce RREP, il va extraire le dernier numéro de séquence, puis le comparer avec la valeur enregistrée dans sa table. Si elle correspond, la transmission aura lieu. Si ce n'est pas, ce nœud est un nœud malveillant, alors un message d'alarme sera diffusé pour avertir le réseau sur ce nœud. Toutefois, les deux solutions ont le délai de bout en bout comme inconvénient.

En 2010 Hafi[HoudaHafi, 2010] propose un protocole basé sur l'utilisation d'un modèle de confiance capable d'assurer les échanges sécurisés dans les réseaux sans fil P2P. Dans le modèle proposé, et afin d'évaluer le degré de confiance d'un nœud, chaque nœud dans le réseau maintient une table d'activité, dans cette table il sauvegarde l'identifiant d'un nœud, le nombre des paquets de données, le nombre des paquets de demande de route(RREQ) et le nombre des paquets de réponse (RREP) reçus de ce nœud. Quand un nœud légitime reçoit un paquet, selon le type du paquet reçu, il augmente le nombre dans sa table d'activité. Si le paquet reçu est de type

RREP, il consulte sa table d'activité pour vérifier l'une des équations ci-dessous, selon les valeurs stockées dans cette table, il décide si le nœud est un nœud de confiance ou bien non.

A chaque fois qu'un nœud BLACKHOLE reçoit un paquet de données, il le supprime directement, ainsi quand il reçoit un paquet RREQ, il répond en envoyant une fausse RREP sans consulter sa table de routage et il ne rediffuse pas le RREQ vers les autres nœuds. En se basant sur ce comportement, un nœud légitime ne recevra aucun paquet de données ou bien un paquet RREQ d'un nœud malicieux, il reçoit que des paquets de réponse RREP, par conséquent, si on suppose que

NB-D : le nombre des paquets de données reçus d'un nœud X

NB-RREQ : le nombre des paquets RREQ reçus d'un nœud X

NB-RREP : le nombre des paquets RREP reçus d'un nœud X

Si (NB-D+NB-RREQ > NB-RREP) alors : X est un nœud de confiance

Si ((NB-D+NB-RREQ!=0) and (NB-RREP >NB-D+NB-RREQ)) alors : X est un nœud connu

Si (NB-D+NB-RREQ=0) alors : X est un nœud inconnu et peut être un nœud BLACKHOLE

Dans ce qui suit, nous présentons l'idée générale du protocole:

Step 1:Le nœud source S commence la phase de découverte de route

Step 2:Chaque nœud intermédiaire reçoit un RREQ stocke le numéro de séquence de la source (SSN)

Step 3:Quand un nœud intermédiaire reçoit un RREP, il vérifie d'abord si le nœud existe dans le BLACKHOL, si la condition est vraie, il le supprime directement. Sinon il passe à l'étape 4

Step 4:Dans cette étape il vérifie un bit rajouté au format du paquet RREP, pour éviter que plusieurs nœuds vérifient plusieurs fois le même paquet.

Si (le bit = 1) alors :

- Le RREP a été déjà vérifié par un nœud et le nœud suivant n'aura plus besoin de revérifier le paquet (dans ce cas le nœud est jugé soit de confiance, soit connu)
- Rediffuser RREP vers la source

Sinon (le bit =0)

Switch Etat du nœud

Case 1: Le nœud est jugé de Confiance

- Mettre le bit = 1
- Rediffuser RREP vers la source

Case 2 : Le nœud est jugé Connu

- Mettre le bit = 1
- Rediffuser RREP vers la source

Case 3 : Le nœud est Inconnu (Route non sécurisé, et le nœud peut être un BLACKHOLE)

Si (DSN>>SSN) (pour confirmer)

- Il ne le renvoie pas à la source
- Ajouter le nœud au black List
- Supprimer le RREP

Sinon

- Mettre le bit = 1
- Rediffuser RREP vers la source

Finsi

En 2010 IRSHAD [IRSHAD ULLAH et al, 2010] fons une étude sur l'attaque de trou noire dans les réseaux Mobile Ad hoc (MANET). Ils proposent l'objectif qu'est étudié l'effet de l'attaque du trou noir sur le réseau Mobile Ad hoc à l'aide d'un protocole de routage proactive comme OLSR et un protocole de routage réactive comme AODV, ensuite compares les résultats dès les deux protocoles. Ils prennent la problématique qu'est " Les réseaux Mobile Ad hoc fonctionne sans un administrateur centrale, cette caractéristique plus vulnérables pour être exploiter par un attaquant au sein de réseaux". Les chercheures utilisent le simulateur OPNET comme l'outil de mesure de performance de réseau Ad hoc.

Le résultat de cette étude est Simulation de l'attaque de trou noir par l'AODV et OLSR et prendre les critères delay, Throughput, Network Load, comme des critères de mesure de l'effet de l'attaque de trou noir.

En 2011 Subash [Subash et al, 2011] présente un algorithme pour détecter l'attaque trou noir dans un MANET basé sur un prétraitement appelé Pre_Process_RREP, il est simple ainsi il ne change pas le fonctionnement de l'un des nœuds intermédiaires ou de destination. Il n'a même pas modifié le fonctionnement normal de l'AODV. Le processus continue à accepter les paquets RREP et appelle un processus appelé Compare_Pkts (p1 paquets, p2 paquet) qui

compare le numéro de séquence de destination des deux paquets et sélectionne le paquet avec un numéro de destination supérieur si la différence entre les deux numéros n'est pas sensiblement élevée. Le paquet contenant exceptionnellement un numéro de séquence de destination élevé est soupçonnée d'être un nœud malveillante un message d'alerte contenant l'identification du nœud est généré et diffusé vers les nœuds voisins de sorte qu'il peut être isolé du réseau et peut maintenir une liste de ces nœuds malveillants.

En 2011 Esmaili[H.A.Esmaili et al, 2011] font une étude sur le performance du protocole de routage AODV sous l'attaque de trou noir, ils proposes l'objectif qu'est la mesure de l'effet de l'attaque du trou noir sur le réseau ad hoc à l'aide AODV comme un protocole de routage et en suite définie une solution pour accroître la sécurité dans ces réseaux, à partir d'un problématique qu'est " Mobile ad hoc networks (MANETs) sont faible contre des nombreux types d'attaques comme l'attaque de trou noir". Les chercheures utilisent la simulation comme l'outil de mesure de performance de réseau Ad hoc, et il choisit l'outil de simulation de réseau OPNET.

Les résultats de cette étude est résumé dans les point suivants:

- Simulation d'un seul nœud malicieux dans un environnement de 46 nœuds mobiles
- Simulation de deux nœuds malicieuse dans le même environnement
- Simulation de trois nœuds malicieuse dans le même environnement
- Simulation de quatre nœuds malicieuse dans le même environnement

En 2013 Sharma[Romina Sharma et al ,2013]fons une étude sur le protocole de routage AODV dans les réseaux mobile Ad hoc, ils proposes l'objectif qu'est "modifier le protocole de routage AODV pour empêche l'attaque du trou noire et muserai l'impact de l'attaque du trou noire sur les réseaux mobile Ad hoc et compare avec le protocole modifie de AODV" à partir d'un problématique "à cause du vulnérabilité de sécurité de protocole de routage, les réseaux mobile Ad hoc ne sont pas protèges de l'attaque de malicieuse nœud, comme l'attaque de trou noire". Les chercheures utilisent le simulateur OPNET comme l'outil de mesure de performance de réseau Ad hoc.

Les résultats de cette étude est résumé dans les trois point suivant:

- Simulation du protocole de routage AODV sans l'attaque de trou noir.
- Simulation de l'attaque du trou noire dans les réseaux mobile Ad hoc
- Simulation de l'algorithme pour empêcher l'attaque de trou noire.

6. Conclusion

À partir de ce chapitre, on peut considérer que la sécurité des réseaux P2P consiste en cinq types d'opération: authentification d'un utilisateur, intégrité des données, la disponibilité, confidentialité des données, la non-répudiation. Malgré sa, les réseaux P2P restent toujours vulnérables à des attaque comme l'attaque de trou noir qui a un grand effet sur le déroulement de réseau à cause de l'environnement ouvert de ces réseaux. Pour cela, plusieurs recherche a été développé pour trouver des solutions à ce problème.

Dans le chapitre suivant, nous essayons de proposer un modèle de simulation pour l'attaque de trou noire, en utilisant le simulateur de réseau OPNET.

Chapitre : 03

Implémentation

1. Introduction

Comme nous avons vu dans le chapitre précédent, diverses solutions ont été proposées pour sécuriser les réseaux sans fil contre l'attaque de trou noir. L'objectif principal de ce chapitre est de présenter notre contribution dans le cadre de ce mémoire. Nous commençons par une brève définition de la simulation, ensuite en fait une grille d'analyse pour augmenter notre choix de simulateur, puis on donne une présentation sur OPNET, puis on va créer notre modèle de simulation, et on termine par l'analyse des résultats et une conclusion. .

2. La simulation comme un outil de dimensionnement

Les méthodes de simulation, conçues pour être utilisées en statistique et en recherche opérationnelle, ont connu et connaissent encore un développement rapide dû à l'extraordinaire évolution des ordinateurs. Des applications se rencontrent tant dans l'industrie qu'en économie, ou encore en sciences sociales, en physique des particules, en astronomie et dans de nombreux autres domaines.

Dans beaucoup de situations, que ce soit de la vie courante ou dans la recherche scientifique, le chercheur est confronté à des problèmes dont il recherche des solutions sur la base de certaines hypothèses et contraintes de départ. Pour résoudre ce type de problème, il existe des méthodes analytiques applicables à des situations où le modèle permet de traiter les différentes variables par des équations mathématiquement maniables, et des méthodes numériques où la complexité du modèle impose un morcellement du problème, notamment par l'identification des différentes variables qui entrent en jeu et l'étude de leurs interactions. Cette dernière approche s'accompagne souvent d'une importante masse de calculs. Les techniques de simulation est des techniques numériques: simuler un phénomène signifie essentiellement reconstituer de façon fictive son évolution.

3. Choix de simulateur

Au cours de cette recherche sur le choix du simulateur réseau, nous avons été amenés à définir une grille d'analyse fonctionnelle d'un simulateur pour argumenter notre choix et permettant de proposer une implémentation d'un simulateur. Pour ce faire, nous avions dressé une liste des simulateurs de réseau qu'ont trouvé dans [S. Mehta, 2010], et en termine par la sélection d'un outil parmi aux.

3.1. Grille d'analyse d'un simulateur

Notre grille comporte six simulateurs: NS2, GloMo-Sim, J-Sim, OMNet++, OPNet, QualNet et dix critères: l'applicabilité, Les modules disponibles, la mobilité, L'interface graphique, Contrat, Evolutivité, parallélisme, la documentation, extensibilité. On résume la comparaison dans la table suivant[S. Mehta, 2010]

Les outils / LesCritères	NS-2	GloMo-Sim	J-Sim	OMNet++	OPNet	QualNet
Applicabilité	Net/Sys	Net/Sys	Net	Net/Sys	Net/Sys	Net/Sys
Les modules disponibles	T/W/Ad /WSNA	T/W/Ad	T/W/Ad/ WSNA	T/W/Ad	T/W/Ad/ WSN	T/W/Ad/ WSNA
Mobilité	Supporté	Supporté	Supporté	Non	Supporté	Supporté
Interface graphique	Non	Limiter	Bien	Trèsbien	Excellent	Trèsbien
Parallélisme	Non	SMP/Beawulf	RMI-based	MPI/PVM	Oui	SMP/Beawulf
Contrat	Open Source	Open Source	Open Source	Gratuit pour l'utilisation académique	Contrat académique Gratuit pour l'utilisation limité	Commercial
Evolutivité	Petit	Large	Petit	Large	Moyenne	Très large
Documentation	Excellent	Pauvre	Pauvre	Bien	Excellent	Bien
Extensibilité	Excellent	Excellent	Excellent	Excellent	Excellent	Excellent

Table 3.1: Comparaison entre différents simulateurs réseaux [S. Mehta, 2010]

On déclarant les abréviations utilise suivant:

Net: Network, Sys: System

T: Les modèles traditionnelles (eg. TCP/IP, Ethernet)

W: Wireless Support (eg. Propagation model, IEEE 802.11)

Ad: Ad-Hoc Support (eg. AODV, DSR)

WSN: Wireless Sensor Networks Support (eg. S-MAC, Direct Diffusion)

WSNA: Advance Wireless Sensor Networks Support (eg. Zigbee, Energy Model)

Pour choisir l'outil adéquate nous avons utilisé la méthode ***"Making a Decision By Weighing Up DifferentFactors***" qui nous avons trouvé dans [www.mindtools.com]. On résume les étapes de cette méthode dans les paragraphes sous dessous suivant:

On prépare une liste des options que on va choisir une parmi celle, et on les place en colonnes d'une table, et une liste des facteurs que nous devons considérer dans les lignes. Ensuite on va évaluer chaque option/facteur association par une note comprise entre 0 (faible) et 5 (très bon).

La prochaine étape est de travailler sur l'importance relative aux facteurs dans notre décision. On va allouer à chaque facteur un coefficient de 0à 5, où 0signifie que le facteur est absolument négligeable dans la décision finale, et 5signifie qu'il est très important. (Il est parfaitement acceptable d'avoir des facteurs ayant la même importance)

Ensuite, on va multiplier chaque option/facteur par le coefficient du facteur associe, Cela donne un score pondéré pour chaque option/facteur combinaison

En fin, on va additionner ces scores pondérés pour chacun des options. L'option qui a obtenu le plus grand nombre gagne, et elle doit être sélectionnée.

Dans notre cas la liste des options est:[NS2, GloMo-Sim, J-Sim, OMNet++, OPNet, QualNet] ce sont les simulateurs réseaux qu'on va choisir un parmi eux, el la liste des facteurs est: [applicabilité, Les modules disponibles, la mobilité, L'interface graphique, Contrat, Evolutivité, parallélisme, la documentation, extensibilité]. On applique la méthode précédant sur ces donnes et on a le résultat suivant:

	Coefficient	NS-2	GloMo-Sim	J-Sim	OMNet++	OPNet	QualNet
Applicabilité	5	5	5	2,5	5	5	5
Les modules disponibles	4	5	3	5	3	4	5
Mobilité	4	5	5	5	0	5	5
Interface graphique	5	1	2	3	4	5	4
Parallélisme	3	0	3	2	3	5	3
Contrat	4	5	5	5	4	3	1
Evolutivité	3	2	4	2	4	3	5
Documentation	5	5	1	1	3	5	3
Extensibilité	4	5	5	5	5	5	5
Total	37	141	133	124,5	129	167	148

Table3.2: Grille d'analyse d'un simulateur

3.2. Le simulateur retenu

Après avoir analysé et comparé plusieurs simulateurs disponibles, et après le résultat obtenu dans le tableau 3.2, notre choix de simulateur d'implémentation c'est porté sur le simulateur OPNET (Optimized Network Engineering Tools), Ce choix est motivé par ces propriété qu'on à vu dans la table 3.1 tel que l'interface graphique et la mobilité …

4. L'implémentation

4.1. Présentation du Simulateur OPNET

[S. Mehta, 2010] OPNET (OPtimized Network Engineering Tools) Modeler est un simulateur de réseau à événements discrets, a été proposé premièrement par Massachusetts Institute of Technology (MIT) en 1986 et écrit en langage C++. Il est bien établi et une suite commerciale professionnelle pour la simulation de réseau. Actuellement, il est l'environnement de simulation commercial le plus largement utilisé. Toutefois, il peut être utilisé gratuitement par les chercheurs s'appliquant aux programmes d'université. Contrairement NS-2 et GloMoSim,

OPNET soutient l'utilisation de la modélisation de réseau différent et matériel spécifique, comme lien physique émetteurs-récepteurs et d'antennes.

OPNET modeler dispose d'un environnement de développement interactif permettant la conception et l'étude des réseaux, des dispositifs, des protocoles et des applications. Pour ce faire, une longue liste de protocoles est supportée. En particulier, les protocoles MAC comprennent (wifi) IEEE 802.11a/b/g et ceux de Bluetooth. OPNET peut également être utilisé pour définir les formats de paquets personnalisés. Le simulateur aide les utilisateurs au développement des différents modèles par le biais d'une interface graphique. L'interface peut également être utilisée pour modèle, graphe, et d'animer le résultat obtenu. Une des caractéristiques les plus intéressantes d'OPNET est sa capacité à exécuter et suivre plusieurs scénarios d'une manière simultanée. Cependant, OPNET souffre également des mêmes problèmes d'évolutivité orienté objet comme NS2. OPNET Modeler fonctionne sur Windows XP/2K, Windows 7, Windows 8, Linux et Solaris.

OPNET est fonctionne en quater étapes, proposer du modèle, spécification des statistiques, exécution de la simulation, obtenu les résultats. Si les résultats ne sont pas corrects il faut retourner à la première étape et fait les corrections du modèle puis continue les autres étapes. La figure 3.1 représente le fonctionnement général d'OPNET.

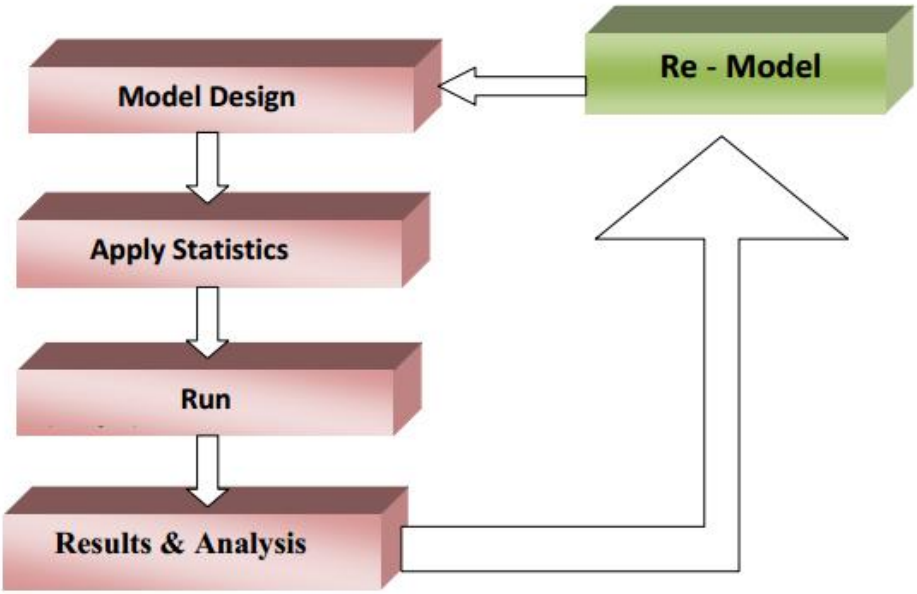

Figure 3.1: Fonctionnement d'OPNET

4.2. Préparation de l'Environnement d'Implémentation

La préparation de l'environnement d'implémentation consiste à installer le simulateur de réseau OPNET sous le système d'exploitation Windows 7. Nous avons utilisé la version académique d'OPNET 14.5. Avons l'installation d'OPNET on a besoin d'installer **Microsoft Visual Studio**10.

L'installation d'OPNET s'effectue sur les étapes suivantes:

1. Ajouter les variables suivant dans le variable d'environnement du système

Nom de variable	Valeur de variable
DevEnvDir	C:\Program Files\Microsoft Visual Studio10\Common7\IDE;
Framework35Version	v3.5
FrameworkDir:	C:\Windows\Microsoft.NET\Framework;
FrameworkSDKDir:	v2.0.50727;
Include	C:\Program Files\Microsoft Visual Studio10\VC\atlmfc\include;C:\Program Files\Microsoft Visual Studio10\VC\include;C:\Program Files\Microsoft SDKs\Windows\v7.0A\include\
LIB	C:\Program Files\Microsoft Visual Studio10\VC\atlmfc\lib\;C:\Program Files\Microsoft Visual Studio10 \VC\lib\;C:\Program Files\Microsoft SDKs\Windows\v7.0A\lib\
LIBPATH	C:\Windows\Microsoft.NET\Framework\v3.5\;C:\Windows\Microsoft.NET\Framework\v2.0.50727\;C:\Program Files\Microsoft Visual Studio10\VC\atlmfc\lib\;C:\Program Files\Microsoft Visual Studio 10\VC\lib\
Path	C:\Program Files\Microsoft Visual Studio10\VC\bin;C:\Windows\Microsoft.NET\Framework\v3.5\;C:\Windows\Microsoft.NET\Framework\v2.0.50727\;C:\Program Files\Microsoft Visual Studio10\VC\vcpackages\;C:\Program Files\Microsoft Visual Studio10\Common7\IDE\;C:\Program Files\Microsoft Visual Studio 10\Common7\Tools\;C:\Program Files\Microsoft SDKs\Windows\v7.0A\Bin\;

VCINSTALLDIR	C:\Program Files\Microsoft Visual Studio 10\VC\
VS100COMNTOOLS	C:\Program Files\Microsoft Visual Studio 10\Common7\Tools
VSINSTALLDIR	C:\Program Files\Microsoft Visual Studio10\
WindowsSdkDir	C:\Program Files\Microsoft SDKs\Windows\v7.0A\

Tableau 3.3.Varibles d'environnement d'OPNET

2. Le logiciel OPNET contient trois fichiers exécutables OPNET Modeler.exe, OPNET Modeler_docs.exe et OPNET Modeler_library.exe. On commence par installer l'un après l'autre respectivement.
3. Avant d'exécute OPNET il faut d'abord lancer license maker.exe, puis on clique sur OK pour générer (file license) dans la partition C, cela pour la version académique seulement, donc il faut lancer OPNet Modeler en tant que administrateur.

5. La simulation

Pour étudier l'impact de l'attaque du trou noire sur les réseaux mobile P2P, on va créer deux scenarios sur OPNET, dans le premier on va simuler le réseau sans attaque et dans le deuxième on va implémenter l'attaque, ensuite en va comparer les résultats.

La figure 3.1 représente l'environnement de la simulation qui contient 10 nœuds mobiles se déplacent dans un espace de 100×100m avec une vitesse variée entre 2 et 5 m/s,Packet Inter-Arrival Time (sec) est exponential (1),packet size (bits) est exponential (1024), data rates est 11 Mbps, transmitting power of 0.005 watts. Randomway point mobility est selecte. Tous les nœuds supportent AODV comme un protocole de routage, le nœud Source va envoyer des paquets au nœud Destination.

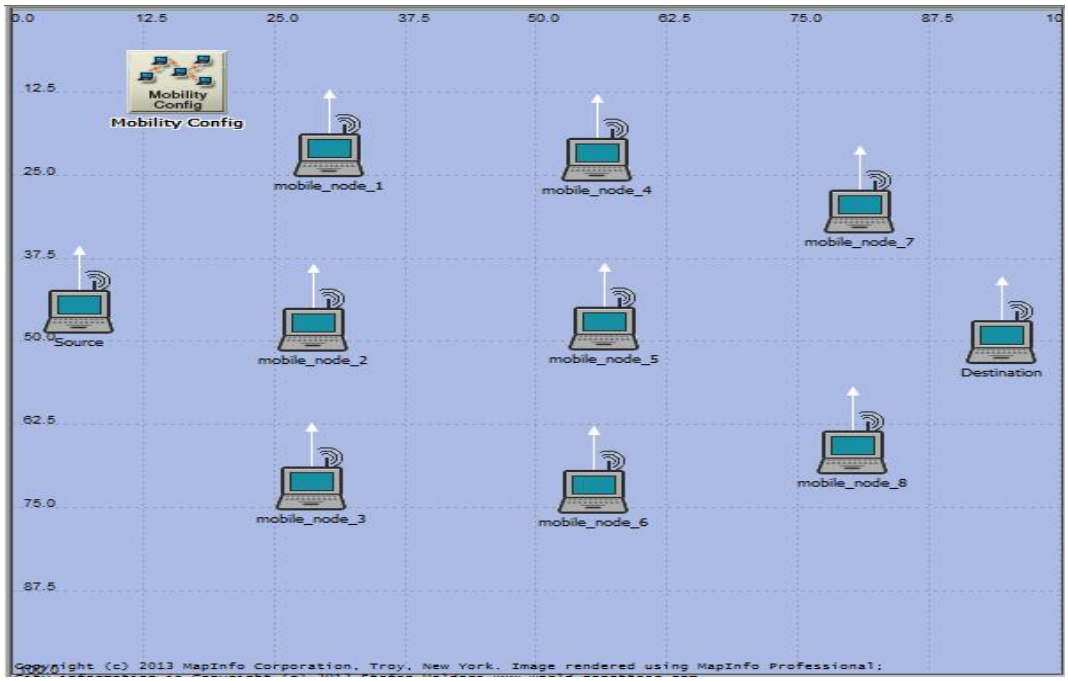

Figure 3.2: L'environnement de simulation

Mobility configuration: est utilisé pour spécifier le modèle de mobilité pour les nœuds dans le réseau et fournit des paramètres qui permettront de contrôler le mouvement des nœuds tels que la vitesse, le temps de départ, le temps d'arrêt.

Le tableau suivant résume les paramètres de notre modèle de simulation

SIMULATION PARAMETERS	
Simulateur	OPNET 14.5
Protocole de routage	AODV
Temps de simulation	1000 seconds
Nombre des nœuds	10
Pause Time	10 seconds
Terrain de simulation	100×100
MAC(protocol sans fil)	802.11

Tableau 3.4 : Paramètres de simulation

Les Performances métriques: les performances métriques que nous choisissons pour l'évaluation de l'attaque du trou noir sont **packet end-to-end delay, network throughputet network load**.

Packet end-to-end delay:c'est le temps moyen pour transférer un paquet à l'intérieur de réseau. Cela comprend le temps de générer le paquet de la source jusque la réception par la destination et exprimée en secondes. Cela comprend l'ensemble des retardes de réseaux, y compris les files d'attente de mémoire tampon, le temps de transmission et les retards induits en raison de activités de routage.

Network throughput: c'est le rapport de la quantité totale de données qui arrive à la destination de la source vers le temps nécessaire pour que la destination pour recevoir le dernier paquet. Il est représenté en bits par seconde ou paquets par secondes. En MANET débit est affectée par divers changements de topologie, une bande passante limitée et une puissance limitée. Douteux communication est aussi un des facteurs qui nuisent le paramètre de débit.

Network load: c'est le trafic total reçu par l'ensemble du réseau à partir de couche supérieure de MAC qui est accepté et en attente de transmission. Il indique la quantité de la circulation dans tout le réseau. Il représente le trafic total de données en bits par secondes reçues par l'ensemble du réseau à partir de la couche supérieure sont acceptés et en attente de transmission. Il n'inclure tout le trafic de données de couche supérieure a rejeté sans file d'attente en raison de la grande taille des paquets de données.

Configuration du trou noir:

Pour simuler l'attaque de trou noir, l'environnement reste tout jour le même, mais on ajoute un nœud corrompu, qu'on considère comme un trou noir, la configuration est représentée dans le tableau suivant:

Paramètres	Valeur (Normal Nœud)	Value (corrompunœud)
Route DiscoveryParameters	Default	Custom Level
Route Request Retries	5	0*
Route Request Rate Limit (packets/Sec)	10	0*
Gratutious Route Reply Flag	Enabled	Enabled
Destination only Flag	Enabled	Enabled
AcknowledgementRequired	Enabled	Enabled
Active Route Timeout	3	3
Hello Interval	Uniform (1,1.1)	Uniform (1,1.1)
Net Diameter	35	100*
Timeout Buffer	2	0*
TTL	Default	Default
Packet Queue Size (packets)	Infinity	0*

Tableau3.5 : AODV paramètres pour corrompu et normale nœud

*ces paramètres désignent la déférence entre le nœud normal et le nœud corrompu

La figure suivant illustre le réseau avec le trou noir

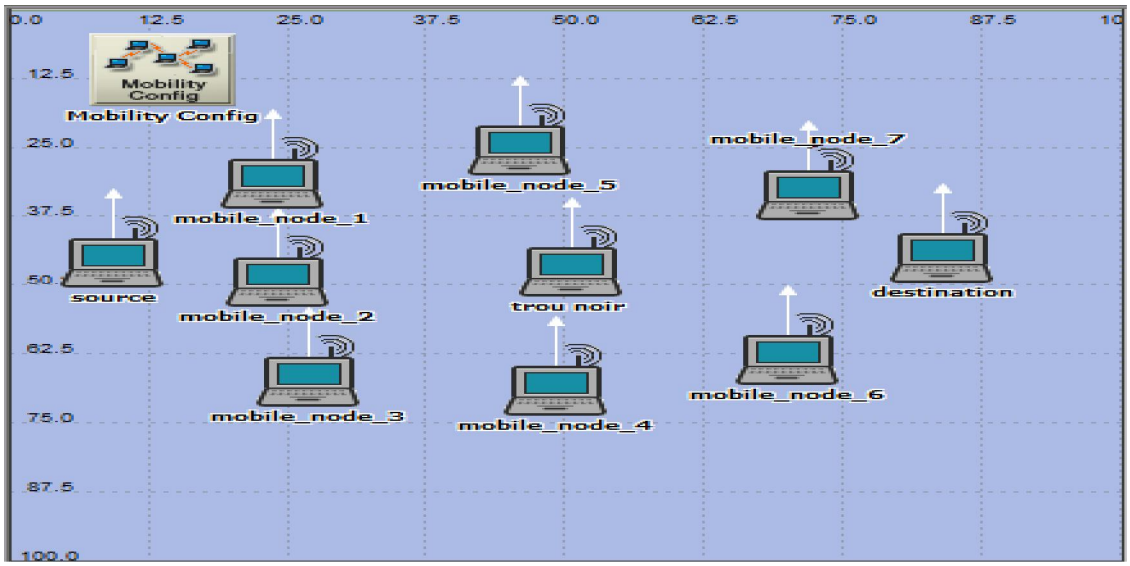

Figure 3.3 : L'environnement de simulation avec trou noir

6. Lesrésultats

Après la simulation des deux scénarios les résultats sont

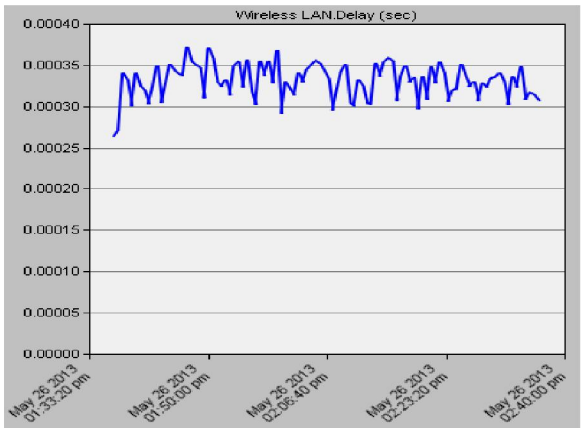

Figure 3.4: End-to-end delay sans attaque

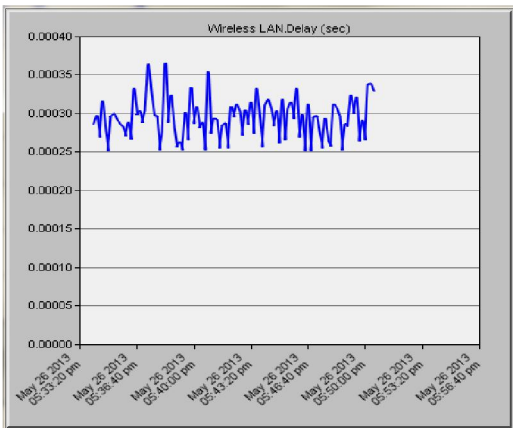

Figure 3.5: End-to-end delay avec l'attaque

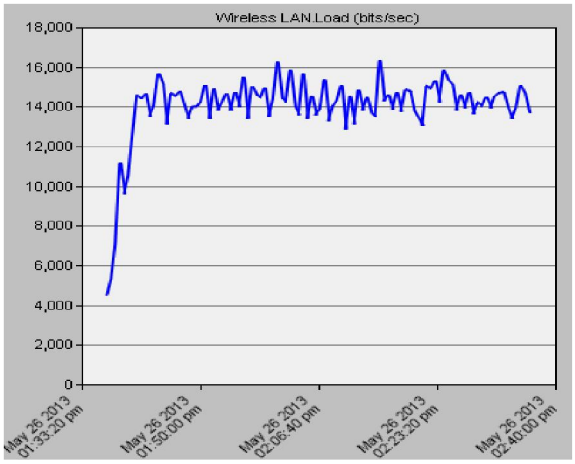

Figure 3.6: Network Load sans attaque

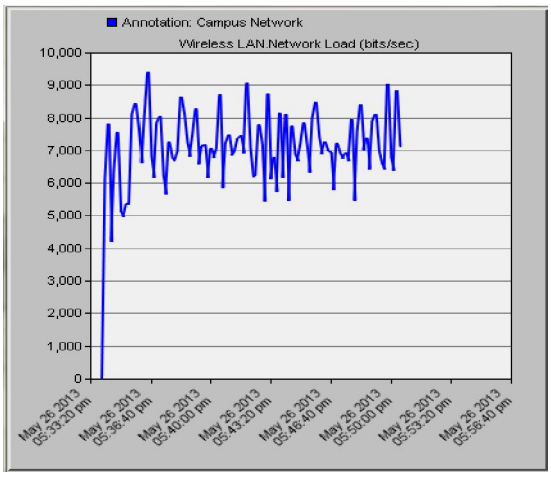

Figure 3.7: Network Load avec l'attaque

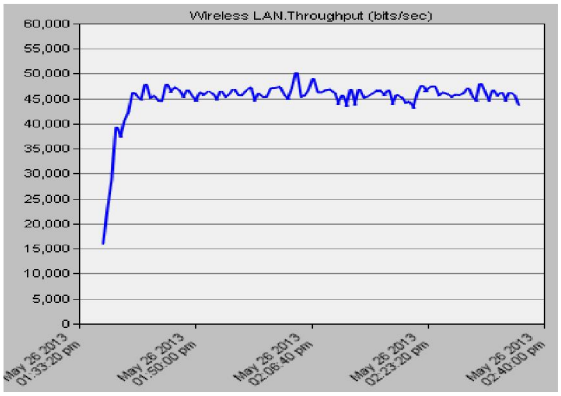

Figure 3.8: Throughput sans attaque

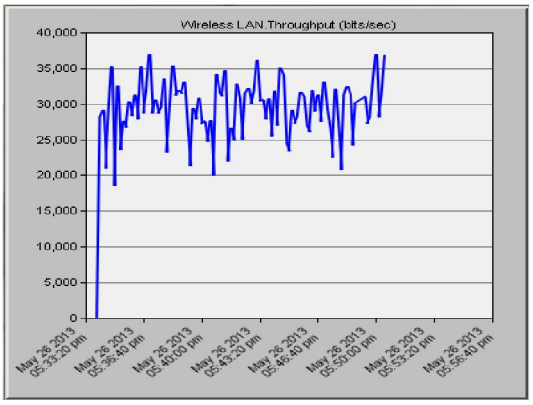

Figure 3.9: Throughput avec attaque

Pour observe l'effet de l'attaque du trou noir de façon plus claire on ajoute les métriquessuivants : Traficreçus, etTraficenvoyé

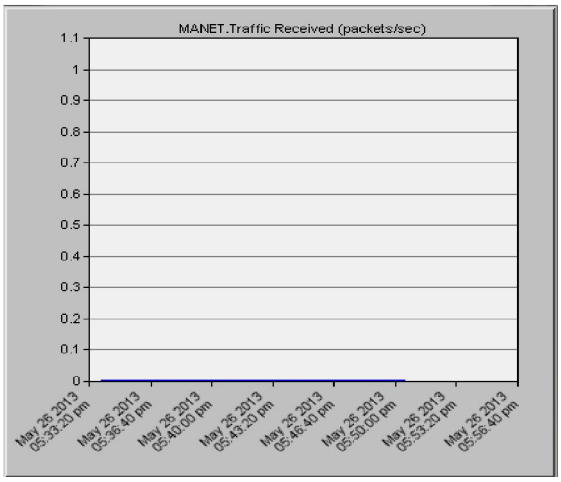

Figure 3.10: Trafic reçu par la destination

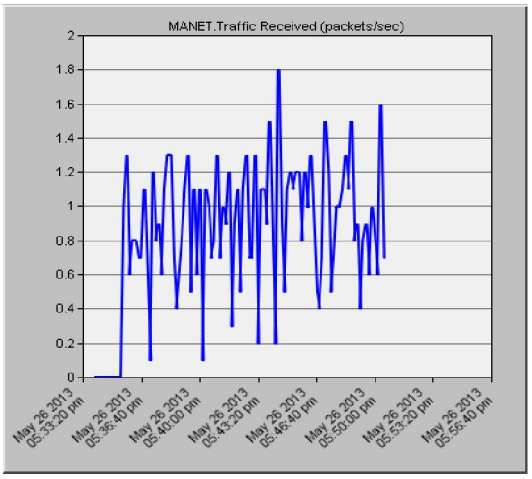

Figure 3.11: Trafic reçu par le trou noir

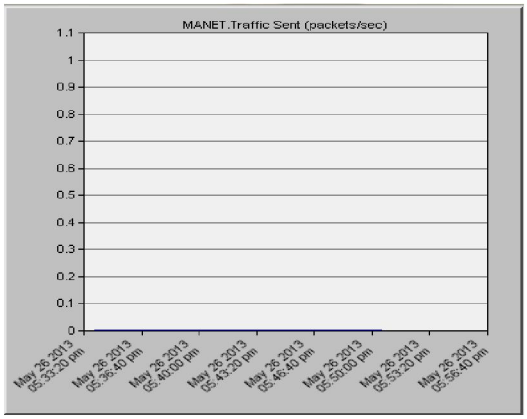

Figure 3.12: Trafic envoyé par le trou noir

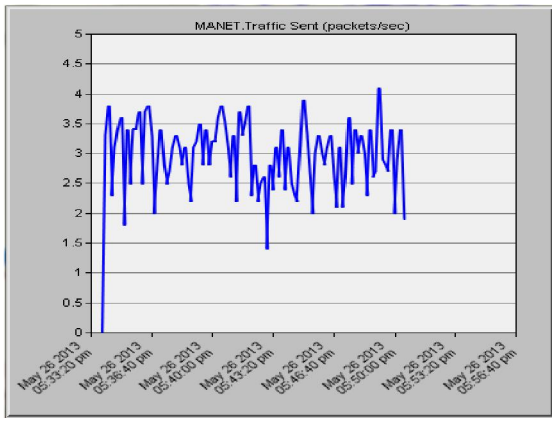

Figure 3.13 : Trafic envoyé par la source

7. Analyse de résultats

Quand nous observons dans la figure 3.5 nous comprendrons que le transfert des paquets dans le réseau, a fait un retard par contre dans le cas normale (sans attaque) le transfert des paquets est bien soulagé.

Dans le cas normal (sans attaque) nous observons dans la figure 3.6 la moyenne de trafic totale reçu (network load) est égale à 14 bits/second par contre dans la figure 3.7 (le cas de trou noir) est égale à 7 bits/second.

Dans le cas normale (sans attaque) nous observons dans la figure 3.8 la moyenne de la quantité totale des données qui arrive à la destination de la source (Throughput) est égale à 45 bits/second par contre dans la figure 3.9 (le cas de trou noir) est égale à 30 bits/second.

Dans la figure 3.13 le nœud source envoie des paquets a le nœud mobile_node_2 qu'l ensuite envoyé a le nœud trou noire (figure 3.11) qui garde ces paquets comme la figure 3.12 dite, et ne pas envoyer a le nœud destination (figure 3.9).

A partir les résultats obtenu on peut dire que le nœud corrompu fait son objectif qui est :

- ✓ Gérer le flot de données sur le réseau,
- ✓ Laissé le déroulement de trafic à lui-même.

8. Conclusion

Dans ce chapitre, nous avons créé un modèle qui consiste un système P2P et aussi on a créé deux scenarios, dans le premier on a simulé le réseau sans attaque et dans le deuxième on a implémenté l'attaque par l'intégration d'un nœud malveillant (trou noir), on a testé le processus de découverte de route et le trafic des données, après nous avons comparé et analysé les résultats.

Conclusion générale

Conclusion générale et perspectives

Les réseaux pair-à-pair (P2P) sont devenus très populaires. Cette popularité vient des bonnes caractéristiques offertes par ces systèmes, mais également ont des caractéristiques particulières rendent ces réseaux très vulnérables à plusieurs formes d'attaques. Un exemple spécifique de l'une de ces attaques est l'attaque de trou noir. Ce type d'attaque peut représenter une menace importante pour le bon fonctionnement du réseau.

Ce travail a été principalement axé sur la sécurité de ces réseaux, qui représente un grand défi. Dans ce mémoire, nous avons proposé un modèle de simulation pour l'attaque de trou noir. Nous sommes intéressés à la sécurité au niveau routage, plus précisément nous avons basé notre étude sur le protocole AODV.

Dans ce mémoire, nous nous sommes intéressés à l'analyse de l'attaque trou noir, nous avons proposé un modèle permet de mesurer l'effet de cette attaque sur le fonctionnement de ces réseaux, et nous avons implémenté la sous le simulateur de réseau OPNET. Ensuite, nous avons effectué un ensemble de simulations et nous avons présenté et interprété les résultats obtenus.

Ce projet nous a offert l'occasion d' étudier les réseaux mobiles P2P, la sécurité des réseaux en général et les réseaux P2P en particuliers, découvrir et enrichir nos connaissances sur des domaines de recherche très vastes, découvrir l'outil de simulation de réseaux OPNET.

L'étude de problème du trou noire et son effet sur les réseaux mobile P2P est une tache ambitieuse, en particulier vu le temps imparti d'une mémoire. La problématique présentée dans ce mémoire ouvre plusieurs perspectives de recherche concernant les solutions de cette attaque. Nos perspectives à court terme visent particulièrement à compléter ce travail pour étudier toute les solutions proposées pour ce problème et faire une comparaison entre ces solutions.

Par ailleurs, dans les prochaines études, on va essayer d'étudier tous les problèmes lie à la sécurité dans les réseaux mobile P2P et de proposer un modèle pour sécuriser ces réseaux contre les attaques et les menaces qui peut perturber le déroulement général de ces réseaux.

Références bibliographiques

[Al-Shurman et al, 2004] Al-ShurmanM, S Moo Yoo and S.Park, "Black hole Attack in Mobile Ad Hoc Networks", ACM Southeast Regional Conference, 2004.

[Androutsellis. S et al, 2004] Androutsellis.S -Theotokis and D. Spinellis. "A survey of peer-to-peer content distribution technologies", ACM Computing Surveys, December 2004.

[Deng et al, 2002] Deng H., Li W. and Agrawal, D.P., "Routing security in wireless ad hoc networks", Communications Magazine IEEE, October 2002.

[Guillaume D et al, 2010] Guillaume D, Juliette D, Rida Kh, "Approche Collaborative pour la détection d'attaques dans les réseaux Pair à Pair", Groupement -GIS 3SGS-, délivrable1, LORIA–INRIA, 2010.

[Guy Pujolle, 2008] Pujolle G, "Les Réseaux", EYROLLES, Paris,-France, 1128, Edition 2008.

[H. A. Esmaili et al,2011] H. A. Esmaili, M. R. Khalili, Hossein gharaee, "Performance Analysis of AODV under Black Hole Attack through Use of OPNET Simulator", World of Computer Science and Information Technology Journal (WCSIT) Vol. 1, 2011.

[HoudaHafi, 2010] Houda Hafi, "Protocole pour la sécurité des réseaux sans fil peer to peer ", thèse de Magister, université de UKM Ouargla, 2010.

[Irshad. U et al, 2010] Irshad. U, Shoaib UR Rehman, "Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols", Master thesis, School of Computing Blekinge Institute of Technology, Sweden, 2010.

[K. Lakshmi et al, 2010] K. Lakshmi et al, "Modified AODV Protocol against Blackhole Attacks in MANET", International Journal of Engineering and Technology Vol.2 (6), 2010, p 444.

[Liorens etal, 2003] C. Liorens et L. Levier, “Tableaux de bord de la sécurité réseau”, Eyrolles, Paris-France, 2003.

[Nathalie. B et al,2003] Nathalie B, Benoit T, Stéphane V,"Nouvelles Technologies Réseaux Les réseaux peer-to-peer", thèse ingénieur Informatique Réseaux, 2003

[Patrick Marlier, 2007] Patrick MARLIER, “Sécurité du Peer-to-Peer”, [en ligne], www.labo-asso.com, 2007

[Radad Al king,2010] : Raddad AL KING, "Localisation de sources de données et optimisation de requêtes réparties en environnement pair-à-pair", thèse de doctorat, université de Toulouse, 2010.

[RominaSh et al ,2013] RominaSh, Rajesh Sh, "Modified AODV Protocol To Prevent Black Hole Attack in Mobile Ad- hoc Network", International Journal OF Innovative Research & Development, Vol 2 Issue 4, April 2013.

[S. Mehta et al, 2010] S.Mehta,H.Kabir,"Network and System Simulation Tools for Next Generation Networks: a case study", Inha University Korea, 2010

[Subash et al, 2011] Subash Chandra Mandhata, Dr.Surya Narayan Patro, “A counter measure to Black hole attack on AODV- based Mobile Ad-Hoc Networks”, International Journal of Computer & Communication Technology (IJCCT), 2011.

Page Web [www.mindtools.com] http://www.mindtools.com/pages/article/ newTED_03. Html , Last accessed 28/03/2013