République Algérienne Démocratique et Populaire

Ministre de l'Enseignement Supérieur et de la Recherche Scientifique

Université Abderrahmane MIRA de Bejaia

Faculté des Sciences Exactes

Département Informatique

Mémoire de fin de cycle

En vue de l'obtention du diplôme de Master Professionnel

En Informatique

Option : Administration et Sécurité des Réseaux

Thème :

Sécurité DTN : Etat de l'art et Solution DVD

Réalisé par :

BOUHARA Fatiha

CHERAFT Sihem

Soutenu devant le jury:

Président *M^r* AMAD Mourad

Examinateur *M^r* BAADACHE Abderrahmane

Examinatrice *M^me* BATTAT Nadia

Promoteur *M^r TOUAZI Djoudi*

Année 2011/2012

Remerciements

Je remercie le bon dieu de nous avoir procurée de l'aide afin de réaliser ce modeste travail.

Tout au long de ce projet, il a fallu souvent faire preuve d'efforts et de résistance sans relâche face à certaines difficultés à surmonter bien que le courage a toujours été présent, grâce aux personnes auxquelles nous souhaitons exprimer nos reconnaissances qui sont innombrables.

Nos vifs remerciements s'adressent également :

À notre promoteur Mr Touazi, de nous avoir encadrés dans la réalisation de ce mémoire, ses nombreux conseils, et pour la confiance qu'il nous a témoignée.

Aux membres de jury qui ont acceptés de juger notre travail, commençant par le président de notre soutenance Mr AMAD Mourad et les examinateurs Mr BADAACHE Abderrahmane et Mme BATTAT NADIA

Nous tenons, également à exprimer notre sincère reconnaissance et notre profonde gratitude à tous ceux qui ont contribué de près ou de loin à la réalisation de ce mémoire.

Et un merci tout particulier à tous ceux qui nous ont apporté leur soutien.

Dédicaces

Je dédie ce modeste travail en premier lieu à la mémoire de mon cher papa qui a espéré depuis ma naissance de faire des études supérieurs , et bien sûr à ma très chère maman pour tous ses sacrifices et pour les encouragements que j'ai eus de sa part ,pour cela j'implore le bon Dieu pour lui prêter une longue vie pleine de bonheur et de santé.

À mes chers frères : Azzedin , Hachemi, Ali, Samir, Khaled, Rahim

À mes sœurs : Kahina, Djida, Sabrina

À mes belles sœurs : Nassima, Adouda, Mina, Assia

À toute mes nièces : Elina, Sarah, Malek

À tous mes nouveaux : Alloua, Islam, Iliass

À ma chère binôme Fatty

Sans oublier mon cher ami Massi qui m'a toujours soutenu et encouragé durant toutes mes études supérieures.

Mes cousins et mes cousines :Hassiba, allal, Omar, Fatiha, Kahina, Fadila, Soraya

Tous mes amis sans exception : Alae, Lilia, Fouad, Kahina, Louiza, Zouina, Kahina Soraya, Souad, Mustafa, Lila,Tayakout, lilia, Kouciela, Sabrina……etc

Cheraft Sihem

Dédicaces

Je dédié cet événement marquant de ma vie :

A mes très chers parents que je ne pourrais jamais remercier assez, qui m'ont toujours aidé durant le parcours de mon travail.
A mes frères Sofiane, Bilal, Fayçal..
A ma binôme Sihem.
A mes grand parants.
A mes tantes Nabila, Hassina et Lila ainsi son mari et ses enfants.
A mes oncles : Mokhtare et Ali ainsi leurs femmes et leurs enfants, Slimane ainsi sa femme, Djamel.
A mes cousins et cousines : Hania, Sabrina, Mina , Lynda, Mima, Souad.
A toute ma famille
A mes meilleurs amis et camarades de la fac : Souad, Kahina, Souad, Ghania, Lila, Alae, Fouad et Mostapha.

Pour finir à tous ceux ou celles qui ont participé(e)s de prés ou de loin à la réalisation de ce travail.

BOUHARA Fatiha

Sommaire

Liste des tableaux

Chapitre I :

Liste des figures

Chapitre I

Chapitre II

Chapitre III

Chapitre IV

Dans nos jours, nous remarquons que la technologie Internet prend de plus en plus le succès dans l'interconnexion des équipements pour échanger des informations. En effet, la plupart des applications Internet sont basées sur un ensemble de protocoles homogènes appelés TCP/IP. Cependant, les services d'Internet actuels reposent sur quelques prés requis clés. Ils présupposent par exemple l'existence d'une liaison de bout en bout entre deux communicants.

Depuis quelque années, les chercheurs se sont penchés à s'intéresse aux communications à longue distancecomme la communication spatiale. En revanche, dans un tel environnement les protocoles de couche transport d'Internet (TCP et UDP)échouent, suscitant ainsi une question principale à savoir : pourquoi Internet n'est-ilpas capable de répondre aux besoins de tel environnement?

C'est là qu'intervient une nouvelle architecture de réseaux proposé par le DTNRG appelée : les réseaux tolérants aux délais (ou DTN : Delay Tolerant Network). Ces dernierssont définis comme étantdes réseaux de plusieurs réseaux homogènes, mais hétérogènes entre eux. Ils se caractérisent par une connectivité intermittente et une absence de communication de bout en bout. Ils implémentent un mécanisme de stockage et de retransmission des données. Tel que, si un nœud d'une région est temporairement déconnecté, les paquets de données seront stockés dans les buffers et quand la connexion apparaîtra, ces paquets seront délivrés à nouveau aux destinations.Ce mécanisme de stockage persistant est réalisé à l'aide d'une couche supplémentaire appelée la couche Bundle située au-dessus de la couche Transport du model TCP/IP.

Vu que les DTNs se comportent différemment et que les protocoles de routage traditionnels utilisés par les réseaux Internet ne s'y appliquent plus. De multiples recherches dans ce domaine sont alors menées, afin de développer des protocoles propres à ce nouvel environnement et adaptés à ses caractéristiques. Commele routage dans un réseauordinairepermet de définir le chemin à suivre pour les données avant d'arriver à la destination. Une telle étude dans un environnement intermittent, l'objectif n'est plus de trouver le chemin qui minimise certaines métriques (ex : le plus court chemin), mais il s'agit de repérer celui qui maximise la probabilité de délivrer un message en prenant en considération l'état du réseau à tout moment.

Introduction générale

Dans un réseau ordinaire, pour assurer la sécurité des messagesne vise qu'à vérifier l'identité de l'émetteur du message et à s'assurer de l'intégrité de ce dernier, sans se soucier de ce qui se passe au niveau des intermédiaires (routeurs). Du fait des longs délais de communications et des communications parfois opportunistes entre certains routeurs, les mécanismes traditionnels de sécurité sont inefficaces et incompatibles avec lesDTNs. Ces mécanismes ne peuvent pas être étendus à des réseaux où les nœuds sont déconnectés pour de longues périodes. La sécurité des réseaux DTN demande donc de faire face à deux principaux problèmes qui sont :

- L'établissement d'un canal sécurisé entre les nœuds.
- L'authentification mutuelle des nœuds.

Face à ces contraintes soulevées par le DTN, de nouveaux régimes de cryptages sont en cours de développement. Ils fonctionnent à l'aide de la distribution de clés publiques, et permettent de contourner les problèmes soulevés par le DTN. Ils donnent la possibilité de créer des canaux sécurisés et d'assurer l'authentification mutuelle.

Afin de bien expliquer toutes ces notions, notre étude comportera quatre axes principaux. Dans le premier chapitre nous allons nous focaliser à rappeler les principales caractéristiques du protocole TCP/IP sur lequel se base la technologie Internet puis ses limites. Ensuite nous avons enchainé avec une présentation générale des DTNs, le contexte de leur apparition, leur architecture ainsi que leur mode de fonctionnement.

Tandis que, le deuxième chapitre sera dédié à l'étude de protocoles de routage dans les réseaux tolérants aux délais. Nous présenterons, tout d'abord, certains protocoles utilisés dans les réseaux traditionnels, puis passer à la présentation des diffèrent classification de protocoles de routages existantes dans les DTNs.

Le troisième chapitre porte des généralités sur les politiques de la cryptographie existantes et appliqués dans les réseaux traditionnels pour assurer les différents services de la sécurité.

En finale, dans le dernier chapitre nous allons présenter une vue d'ensemble d'état de l'art de la sécurité des réseaux DTNs. Puis, d'proposer et d'identifier une nouvelle infrastructure de sécurité pour ces réseaux. Pour enfin terminer notre rapport par une conclusion générale et des perspectives.

Chapitre I

Réseaux tolérants aux délais :

Généralités

Introduction

Au cours de ce premier chapitre, nous allons présenter tout d'abord des rappels sur Internet dans son contexte actuel et ses limites. Ensuite, des généralités sur les réseaux tolérants aux délais connus dans la littérature comme *Delay Tolérant Networks* (DTN).

Comme leur nom l'indique, ces réseaux incluent des mécanismes qui permettent l'établissement des communications en présence des délais importants, non uniformes et d'interruption de liens dans le réseau empêchant l'établissement d'une connectivité de bout en bout entre les terminaux.

I-1- Internet : Rappels

La technologie Internet se base sur un grand nombre de protocoles de communications tel que le TCP/IP[1], qui est défini sur le style établi par l'Open System Interconnections (OSI).

I-1-1- Modèle de référence OSI :

C'est un modèle d'architecture fournit une structure commune pour le développement de standards d'interconnexion des systèmes.

Il définit les termes, les concepts liés à une architecture en couches et introduit sept couches spécifiques, tel que la couche 1 usuellement désignée comme la couche la plus basse à la couche 7, la couche la plus haute [8] [13]:

1. *La couche physique.*
2. *La couche liaison de données.*
3. *La couche réseau.*
4. *La couche transport.*
5. *La couche session.*
6. *La couche présentation.*
7. *La couche application*

Les sept couches [Annexe A] sont divisées en deux grandes catégories : les couches d'informations (Les trois couches supérieures) et les couches de données (Les quatre couches inférieures).

[1] Transmission Control Protocol/ Internet Protocol

Etant donné le modèle OSI[2] définit ci-dessus, nous pouvons aborder le modèle TCP/IP.

I-1-2- Modèle TCP / IP

Le TCP/IP est l'une des piles protocolaires les plus utilisées pour les communications réseaux. En effet, elle a des tâches beaucoup plus diverses que les couches du modèle OSI. La pile de protocole TCP/IP est structurée en quatre couches dont les rôles sont détaillés dans [Annexe A] [8] [13] :

1. ***Couche Application*** **:** Au plus haut niveau, cette couche construit les messages des utilisateurs.
2. ***Couche Transport*** **:** Elle fournit la communication de bout en bout entre applications. Au départ, cette couche divise le flux de données en segments et le réassemble à l'arrivée. Elle vérifie le flux de données et assure la fiabilité du transfert : les octets envoyés doivent être identiques à ceux reçus. C'est pourquoi, cette couche effectue des sommes de contrôle. Sur Internet, le protocole TCP (*Transmission Control Protocol)* est utilisé à cet effet une tâche importante effectuée au niveau de cette couche est le multiplexage/démultiplexage. C'est à dire faire transiter sur une même ligne des données provenant d'applications diverses ou en d'autres termes mettre en série des informations arrivants en parallèles. Ces opérations, sont réalisées grâce au concept de ports, c'est-à-dire un numéro associé à un type d'application, qui est combiné à une adresse IP (*Internet Protocol*) permet de déterminer de façon unique une application qui tourne sur une machine donnée.
3. ***Couche Internet*** **:** Cette couche fournit des services pour l'échange de données individuelles sur le réseau, entre les périphériques finaux identifiés. Pour effectuer le routage[3], il utilise quatre processus de base : l'adressage l'encapsulation, le routage, et la décapsulation.
4. ***Couche accès réseau*** **:** Cette couche fournit des outils de transmission des trames de bits à la couche supérieure et elle permet de contrôler les périphériques matériels et les supports qui constituent le réseau.

[2] Open System Interconnections

[3] Un mécanisme qui permet d'acheminer les données au récepteur

Modèle TCP/IP	**Modèle OSI**
Couche 4 : Application	Couche 7 : Application
	Couche 6 : Présentation
	Couche 5 : Session
Couche 3 : Transport (TCP)	Couche 4 : Transport
Couche 2 : Internet (IP)	Couche 3 : Réseau
Couche 1 : Accès réseau	Couche 2 : Liaison de données
	Couche 1 : Physique

Tab 2-1 : *Les couches de modèle OSI et TCP/IP*

I-1-3- Caractéristiques de TCP/IP

La communication sur Internet est basée sur la pile protocolaire TCP/IP qui est caractérisé par des propriétés suivantes :

I-1-3-1- Commutation de paquets

Pour décrire le principe d'échange d'informations sur Internet, nous décrivons la commutation de paquets. Tel que, ces derniers sont des morceaux d'un bloc complet de données utilisateurs, passants de la source vers la destination via un réseau de lien connecté par des routeurs.

Chaque paquet composant un message, peut emprunter n'importe quel chemin du réseau. Si un lien devient non disponible pour une quelconque raison, les paquets passeront par un autre. Ces derniers se composent de deux parties :

- Une partie données utilisateur appelée : partie de charge utile.
- Une partie constituant l'entête appelée : partie contrôle.

L'entête contient des informations aidant les routeurs à commuter les paquets d'un nœud à un autre jusqu'à atteindre sa destination.

Les paquets d'un message donné peuvent ne pas arriver dans l'ordre, un mécanisme de réassemblage se trouve au niveau d'un nœud de destination, il se charge de les réordonner.

Les performances d'Internet dépendent essentiellement de :

- ***Une connectivité de bout en bout :*** Une connexion bidirectionnelle est disponible entre la source et la destination supportant une interaction[4] de bout en bout.
- ***Un court délai de propagation :*** Un délai relativement court et conforme entre l'envoi d'un paquet de données et la réception de l'acquittement qui lui correspond.
- ***Un faible taux d'erreur :*** Peu de données perdues sur chaque lien [12].

I-1-3-2- Fiabilité et retransmission

Le TCP/IP utilise des mécanismes pour assurer la fiabilité des communications entre l'émetteur et le récepteur [5] [12]:

- Une conversation constante entre l'émetteur et le récepteur permettant d'adapter la communication dynamiquement aux éventuels problèmes.
- Etablissement d'un seul chemin (à un instant donné) entre les nœuds.
- Retransmission de données en cas d'erreurs.

I-1-4 Limites d'Internet

Les applications qui reposent sur la suite de protocole Internet ne convient pas correctement. Exemple, le cas de communication spatial, dont les données emploient un chemin sur lequel la connexion entre certains nœuds est intermittente[5], le délai de propagation du signal est très important de même, le taux d'erreur est très élevé.

La principale cause est le non fiabilité de son protocole de couche transport, mais aussi, le mode de fonctionnement du protocole de routage d'Internet n'est pas toujours satisfaisant. Donc, les protocoles TCP/IP ne sont pas adaptés pour tels environnements [8].

[4] Echange d'information

[5] Discontinu

I-2- Les réseaux tolérants aux délais

I-2-1- Notions de base

I-2-1-1- Historique

L'utilisation générale des protocoles sans fil développe le domaine réseau dans les années 1990. Tel que, la téléphonie mobile en réseau ad hoc (MANET[6]) et des véhicules ad hoc mise en réseau sont devenus des domaines d'un intérêt croissant.

A la fin des années 90, les activités de MANET a financé la NASA[7] pour but d'élaborer une proposition pour les communications interplanétaires [6]. Pionnier de l'Internet Vint Cerf, l'un des aventeurs du protocole TCP/IP, a développé l'architecture IPN (Internet Interplanétaires) initiale, a réfléchi à une nouvelle architecture permettant de faciliter les communications spatiales. Cette réflexion a été étendue à tout type de réseau offrant des caractéristiques similaires. En 2002, Kevin Full a commencé à l'automne adapter certaines des idées dans la conception IPN à des réseaux terrestres et il a inventé le terme délai tolérant et le sigle DTN [1].

I-2-1-2- Définition

DTN signifie Delay Tolerant Network, ce qui se traduit par réseaux tolérant aux délais. Un DTN est composé de plusieurs réseaux sujets à des connexions intermittentes. Ces réseaux ne sont pas nécessairement homogènes, ni en termes de technologies ni par rapport aux protocoles utilisés [2].

A travers un exemple simple, tentons de comprendre la portée du DTN, imaginons dans le désert un avion équipé d'un routeur sans fil qui n'a que des connexions intermittentes avec différents terminaux. En effet, une station de base de vie des chercheurs veut transmettre les résultats de ces recherches à un centre tutelle. Cet avion se déplacera entre ces deux stations, le routeur pourrait stocker et transmettre les résultats de recherches ou les communications envoyées à n'importe quel moment par ses chercheurs. Mais avec le protocole internet actuel ce n'est pas possible, car il présuppose l'existence d'une liaison de bout en bout entre deux

[6] Utiliser pour désigner un réseau ad hoc mobile

[7] National Aeronautics and Space Administration

terminaux (la base de vie de chercheurs et la base tutelle) à tout moment et donc ne prévoit pas le stockage des communications.

Il est tout à fait facile de concevoir un routeur qui exploite un autre protocole qui permettrait ce stockage, alors pour assurer le passage de ce mini-réseau au réseau Internet on utilise les DTNs.

I-2-1-3- Les caractéristiques

Parmi les différents réseaux traversés, certains offrent des contraintes extrêmes pour lesquelles les protocoles les plus couramment utilisés ne sont pas adaptés :

- ***Une Connectivité intermittente:*** Il n'existe pas de connexion continue entre l'émetteur et le récepteur. En effet, le caractère bidirectionnel de chaque tronçon de la connexion n'est pas assuré, donc la technologie TCP/IP ne peut pas être adaptée [5].

- ***Un délai long et variable :*** Dans l'espace, la distance qui sépare l'émetteur et le récepteur est très importante, pour parcourir cette distance, les données sont limitées par la vitesse de la lumière, que si elle parait instantanée sur Terre, se révèle lente dans le cadre des communications interplanétaires

- ***Une vitesse de transmission asymétrique:*** La communication spatiale se caractérise par une vitesse de transmission asymétrique, contrairement à l'Internet qui supporte une asymétrie modérée (ADSL). Mais, dans le cas d'asymétrie important, cela pénalise le bon fonctionnement de protocoles conversationnels [7].

- ***Un taux d'erreur important :*** Des erreurs d'envoi de donnée sur un lien du réseau exigent une retransmission de la donnée dans son intégralité, donc plus de trafic réseau. En effet, la retransmission dans les DTN se fait saut par saut et rarement de bout en bout.

I-2-2- Les spécificité des DTNs

I-2-2-1- L'architecture

La NASA étend sa portée sur la lune, donc pour mener à bien ces missions, cela a besoin d'une architecture réseau pour les environnements intermittents et spatiaux.

Le groupe de recherche des réseaux tolérant aux délais DTNRG[8], s'est penché sur le sujet et a proposé une architecture pour ces réseaux [9].

Les réseaux DTN sont des réseaux capables de transmettre des informations de bout en bout, même lorsque le réseau n'est pas connecté en permanence. La figure ci-dessous représente un exemple de DTN [3].

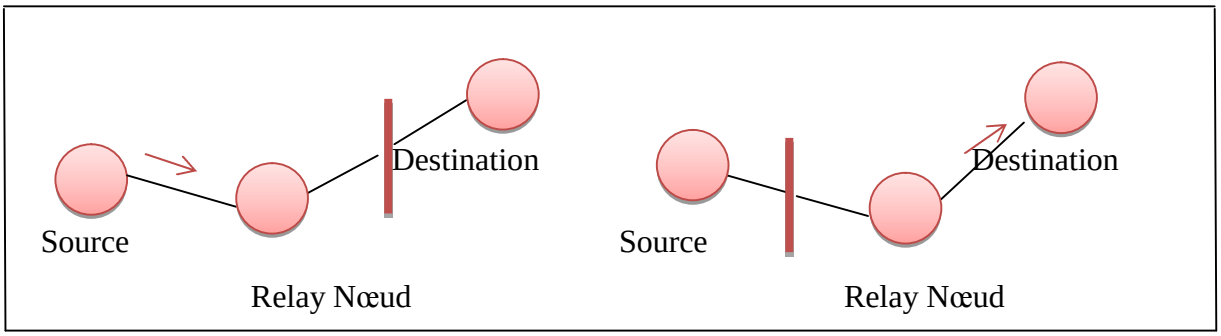

Figure (2-1) : Transfert en utilisant un nœud intermédiaire

En fonction de la mobilité des nœuds, le nœud relais est connecté soit à la source soit à la destination mais pas aux deux simultanément. Ce qui fait, il n'y a pas de connexion de bout en bout. Donc, on peut distinguer 3 catégories de DTN par à port à la mobilité des nœuds, cela fait à représenter 3 architectures :

1) ***Les nœuds ne bougent pas ou très peu de nœud sont mobiles :*** Dans la figure suivante, on remarque 3 régions principales, dans chaque région les liaisons sont fiables (filaires ou sans fil) mais pas entre les régions. En revanche les liaisons entre régions peuvent être assurées par des liens satellitaires dont la durée, la période et la bande passantes de cette connexion sont régulières, par des nœuds qui se déplacent entre *Gate1* et *Gate5*, par exemple un avion entre deux stations de recherche ou un bus entre deux villages ou par des liaisons radio (entre *Gate3* et *Gate4*) épisodiques ou peu fiable.

[8] Delay Tolerant Network Researche Group

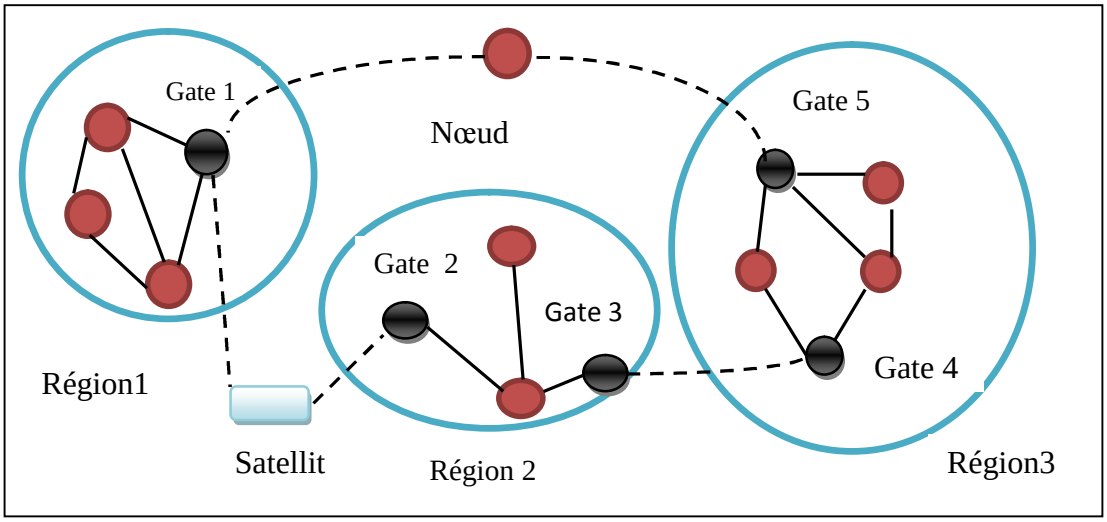

Figure (2-2): *La première architecture de DTN*

2) ***Tous les nœuds sont mobiles :*** Ils communiquent par les liens sans fil comme dans les réseaux Ad hoc, mais le réseau présente une densité hétérogène[9].

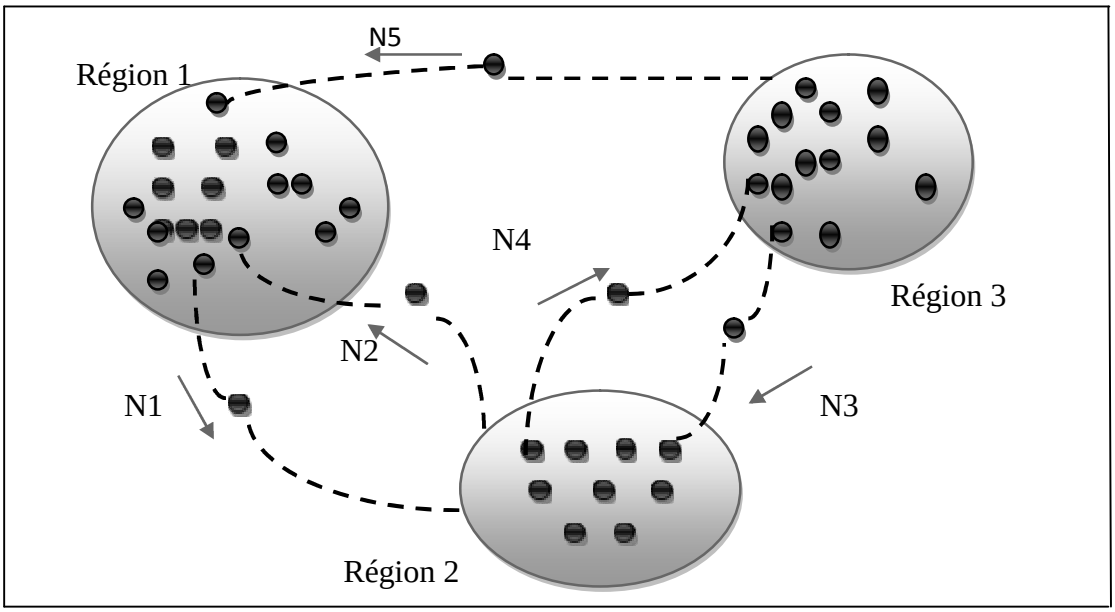

Figure (2-3) : *une deuxième architecture de DTN*

Dans la figure présentée, la densité de nœud est assez grande dans les trois régions. La connectivité interne de chaque région est assurée. Cependant, il n'y a pas de connexion

[9] Une quantité de nœud

permanente entre deux régions, la communication entre deux régions n'est dépendant que du déplacement de certains nœuds.

3) ***Tous les nœuds sont mobiles, mais la densité de nœuds est très faible :*** Il n'y a pas de connexion de bout en bout permanente et l'acheminement de message est effectué par le déplacement des nœuds. En effet, les deux nœuds se rencontrent, ils échangent certains messages qu'ils doivent acheminer. Les connexions intra-régions sont toujours stables et la plupart des connexions inter-régions sont prédictibles.

La deuxième catégorie peut être assimilée à un cas particulier de la troisième catégorie. Comme l'acheminement de messages dépend de la mobilité des nœuds, il est très difficile d'obtenir des informations globales et le routage devient une problématique intéressante.

I-2-2-2- Le fonctionnement

Le DTN résout tous les problèmes rencontrés par les protocoles de bout en bout, en fonctionnant sur une logique dites *store-and-forward message switching*.

I-2-2-2-1- Principe Stor-and-Forword Message Switching

- ***Stor-and-Forword (S&F):***

Durant le long chemin entre l'émetteur et le récepteur, ce mécanisme se base sur la transmission d'informations d'une zone de stockage à une autre, comme c'est montré dans la figure suivante [7] [8]

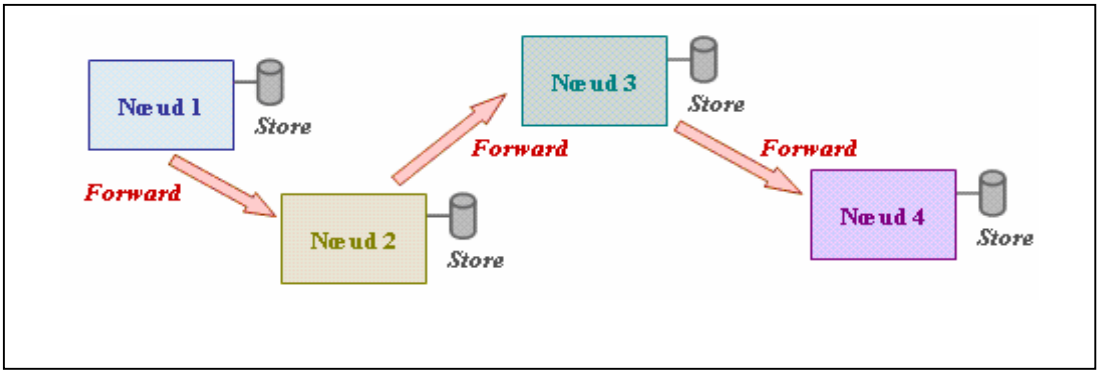

Figure (2-4): Mécanisme Stor-and-Forword (S&F)

Au niveau d'espace de stockage de chaque nœud du réseau, les données sont conservées indéfiniment, ce qui a fait un stockage persistant, contrairement avec les mémoires à court terme pour les routeurs utilisés dans les réseaux Internet.

Contrairement à l'internet, les réseaux DTN, ils utilisent des espaces de stockage plus importants (disque dur). En effet, pour les raisons ci-dessous, l'utilisation de stockage persistant est indispensable :

- ✓ L'absence de lien de communication entre la source et la destination pour une durée indéterminée.
- ✓ Un nœud dans une paire communicante peut envoyer ou recevoir des données beaucoup plus rapidement ou plus sûrement que les autres nœuds.
- ✓ La retransmission de message en cas d'erreur sur le réseau est obligatoire, ou si les informations ne sont pas acceptées pour être transférés [8].

❖ ***Message Switching:***

Message Switching signifie commutation de message lors du transfert de données. Depuis, un nœud du réseau vers le suivant, les communications sont orientées message, c'est à dire que toutes les données à envoyer sont regroupées dans une seule et même entité, comme ci montré dans la figure suivante :

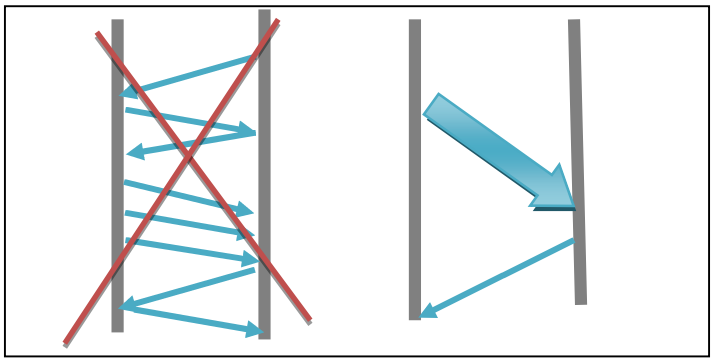

Figure (2-6): Commutation de message

Comme le montre cette figure, la technique commutation de message permet de réduire la conversation entre les nœuds qui peuvent être coûteuses en termes de délais et de débit [8].

I-2-3- Modèle de référence DTN

Afin de mettre en place le Store and Forward Message Switching, une nouvelle couche protocolaire a été mise en place appelée la couche Bundle. Dont, la fonction principale est de permettre à une application de communiquer à travers des différentes régions.

On parle alors de Bundle protocole, plus précisément, une seule Bundle layer est utilisée à travers les différents réseaux traversés. Tandis que, les couches qui se trouvent en dessous de la Bundle layer sont spécifiques à chaque région comme le montre la figure 6 [8].

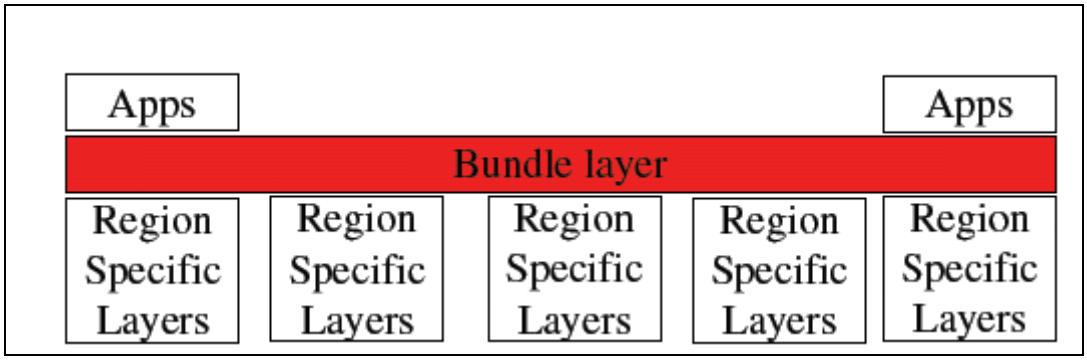

Figure (2-6): Bundle layer dans les réseaux DTN

I-2-4- Pile de protocole DTN

Etant donné le modèle de référence DTN représenté ci-dessus, nous allons aborder la pile de protocole DTN dans cette figure [5] :

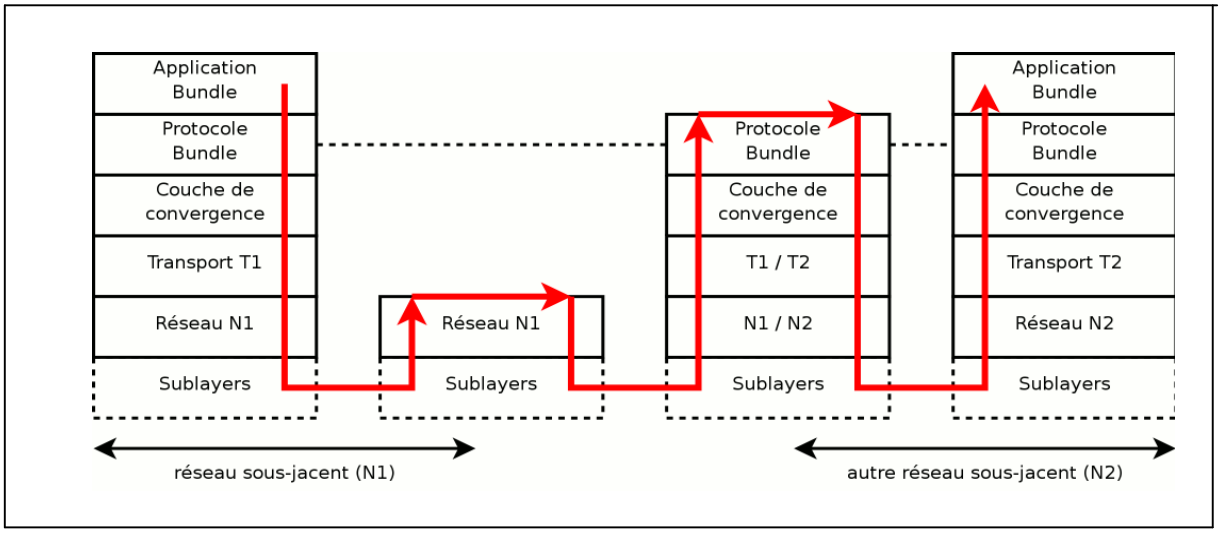

Figure (2-7): Exemple de réseau DTN

Dans le réseau DTN, le protocole Bundle est mise en place dans la couche Bundle, ce protocole réunie les données sous forme de message appelés Bundle et se charge de les transmettre. La pile de protocole DTN est organisée en cinq couches. Cependant, nous présentons uniquement les couches Transport et Bundle.

I-2-4-1- Couche Transport

Au niveau de cette couche, en plus de ces services offerts dans la pile protocolaire TCP/IP. En particulier, elle implémente le protocole LTP *(Licklider Transmission Protocol)* qui est un protocole fiable de couche de convergence fonctionnant en mode paire entre les nœuds DTNs adjacents.

Dans un tel scénario, LTP intervient directement au-dessus des protocoles de couche liaison de données. Lorsque c'est le cas, la correction des erreurs de transmission et/ou le mécanisme de somme de contrôle effectué par le protocole de liaison de données de la couche inférieure assure l'intégrité des données qui circulent entre les entités en communication [8].

I-2-4-2- Couche Bundle

Cette couche permet de s'abstraire des technologies rencontrées sur les différent réseaux du DTN, grâce à la couche de convergence utilisée pour faire le lien entre la couche Bundle et les couches inférieures (figure 7) [8].

La couche Bundle stocke et transmet tous les Bundles[10] entre les nœuds, elle supporte des transmissions de bout en bout. Les Bundles sont automatiquement transportés d'un nœud au nœud suivant, indépendamment des autres, bien qu'elle puisse fragmenter un Bundle en plusieurs fragments.

I-2-4-3- Services du protocole

Le protocole Bundle est un protocole de couche applicatif, donc il fournit un ensemble de six classes de services *(*COS *Classe Of Services)* [8] [7]:

- ***Le service transfert de garde (*CT :*Custody Transfert):*** Le nœud DTN qui a reçu le Bundle est chargé d'assurer la fiabilité de transmission, par l'envoie d'un message d'acquittement au nœud précédent.
- ***Le service d'accusé de réception (*RR :*Return Receipt) :*** C'est une confirmation à la source de la réception du Bundle par l'application destinatrice.
- ***Le service de Notification du transfert de garde (*CTN :*Custody-Transfret Notification):*** C'est une notification à la source, lorsqu'un nœud accepte la garde du transfert d'un Bundle.

[10] Message

- ***Le service de notification d'envoi de bundle (*BFN :*Bundle-Forwarding Notification) :*** C'est une notification à la source lors de la transmission d'un Bundle à un autre nœud.
- ***Le service de priorité de livraison (*PoD :*Priority of Delivery):*** La priorité que pour les messages d'un même émetteur sur nœud, le message d'un nœud A ne sera jamais plus prioritaire que ceux de B [3], alors ce service définit la façon avec laquelle le Bundle est envoyé. On distingue trois types de priorités:
  - Livraison en masse *(Bulk).*
  - Livraison normale *(Normal).*
  - Livraison accélérée*(Expedited).*
- ***Le service d'authentification (Authentification):*** Il permet de vérifier l'identité de la source du Bundle et l'intégrité du message.

La figure 9 ci-dessous met en valeur les différents types de classes de services.

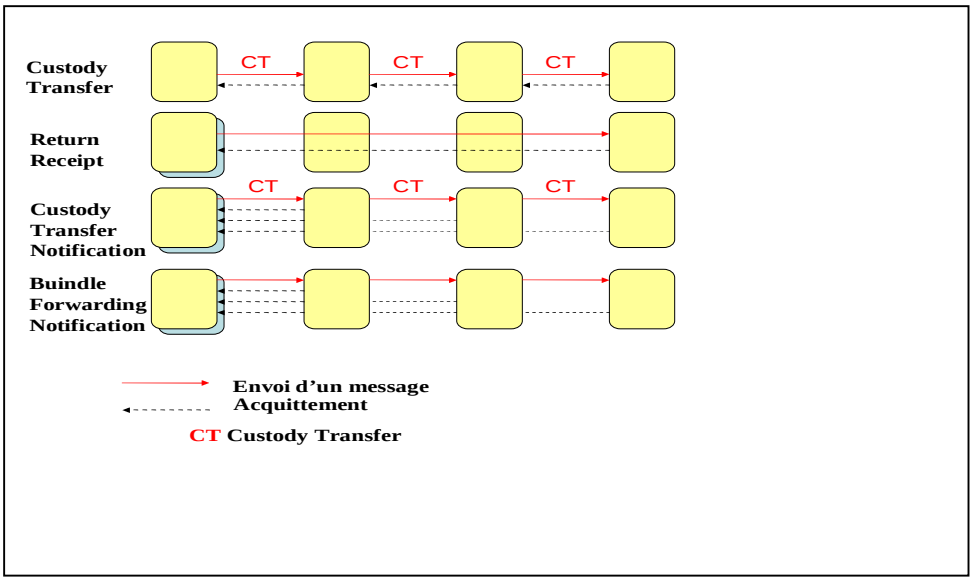

Figure (2-8): Les différentes classes de services

Au niveau de la couche transport, le protocole LTP fournit en plus des services offerts par la suite de protocole Internet un certain nombre de services :

- Le service de données unitaire *(*SDU *Service Data Unit)* : Il offre le moyen de contrôler la taille des blocs, ainsi on peut contrôler la majorité des accusés de

réception lorsque le block est reçu pour améliorer l'adaptation des taux de données asynchrones.

- Le service de contrôle de flux non conversationnel sur les liens interplanétaires En fait, le nombre maximal de session de transmissions simultanées géré par LTP, multiplié par la taille maximale d'un bloc définit la fenêtre de transmission (TW *Transmission Window)* [8].

I-2-4-4- L'entête d'un bundle

La couche bundle doit porter certaines informations de bout en bout selon les besoins de transmission. Ses informations sont insérées dans l'entête de chaque bundle. Elles sont résumées comme suit [40] :

- ***Version de l'identifiant :*** Protocole bundle de 8 bits.
- ***ID de l'entité destination :*** Champ à longueur variable contenant le tuple destination. Il est ajouté par l'application locale lorsque l'envoi nécessite le service bundle.
- ***ID de l'entité source :*** C'est l'identifiant de l'instance de l'application bundle de la source. Il est sous forme d'un tuple, ajouté par le service bundle local, car un hôte particulier peut avoir de multiples noms et un seul sera choisi en se basant sur les décisions de routage. L'ID de l'entité source peut être retourné à l'application afin de supporter le processus de « retour-réception ».
- ***ID de l'entité « Répondre à » (optionnel) :*** La source peut anticiper le fait qu'elle ne soit pas capable d'accepter les réponses et utiliser ce paramètre pour spécifier la destination des « retour-réception » et les enregistrements de délivrance.
- ***ID du gardien courant (optionnel) :*** C'est l'identifiant du gardien courant. Il est nécessaire pour identifier en amont le nœud qui a la garde courante du bundle, afin d'acquitter le transfert de garde ou le bundle ou le fragment d'un bundle.
- ***Classe de service drapeaux :***
    - ***Drapeaux :*** gardien, retour-réception, enregistrement de délivrance.
    - Sélecteur de la classe de service.
    - ***Sécurité :*** présence d'authentification et/ou de cryptage.

- **Estampille d'envoi :** C'est le moment où le bundle a été présenté par l'application d'envoi à la couche bundle pour la transmission.
- **Durée de vie :** Considérée en secondes à partir du moment d'envoi du bundle. C'est un paramètre qui indique le moment où le bundle doit être chassé du réseau DTN.
- **Information d'authentification (optionnelle) :** Ce sont des données d'authentification utilisées pour prouver que le bundle en question devrait être transmis dans le réseau.
- **Information de fragmentation (optionnelle) :** Utilisée pour un fragment d'un bundle indiquant à quel endroit du bundle original, le fragment appartient. Certains bundles (ou événements) provoquent une indication du statut, générée par la couche bundle. En effet, les indications de la couche bundle sont envoyées sous forme de bundles avec une partie des données utilisateur qui est remplacée par un « rapport de statut » qui consiste en les informations suivantes :
    - **ID de l'entité source du sujet bundle :** C'est une copie du tuple de la source du bundle.
    - **Estampille d'envoi du sujet bundle** : Utilisée pour lever l'ambiguïté des rapports de statuts pour les différents bundles provenant de la même entité source.
    - **Drapeaux de statuts :** Indiquant si les bundles ont été ou pas :
        - Reçus correctement par l'expéditeur du rapport de statuts.
        - Transférés en utilisant le transfert de garde à l'expéditeur du rapport de statuts.
        - Transmis par l'expéditeur du rapport de statuts.
    - **Temps de réception (optionnel) :** C'est le moment où l'expéditeur du rapport de statut reçoit le bundle.
    - **Temps de transmission (optionnel) :** C'est le moment où l'expéditeur du rapport de statut transmet le bundle.

I-2-5- Entités de communication

I-2-5-1- Nœuds DTN

Un réseau DTN est composé d'un ensemble d'entités communicantes appelées : Nœuds. Ce nœud, peut être un hôte, routeur, ou une passerelle, agissant comme une source, destination, ou une expéditeur de message (appelés aussi : Bundles).

- ***Hôte :*** Il envoi et/ou reçoit les Bundles, mais il ne les diffuse pas [Annexe A].
- ***Routeur :*** Il diffuse les Bundles au sein d'une seule région DTN et il peut optionnellement jouer le rôle d'un hôte.
- ***Passerelle :*** Elle diffuse les Bundles entre deux ou plusieurs régions DTNs .

I-2-5-2- Régions et Adressage dans les DTN

Un DTN est un réseau de réseaux dans lequel chaque réseau est appelé région, une région est constitué d'un ou de plusieurs réseaux dont les communications sont homogènes[11].

Chaque région DTN a un nom unique et connu, ou que l'on peut connaître parmi toutes les autres régions du DTN. Les Bundles DTN envoyés à l'origine des régions différentes vers la destination sont transmis en premier lieu via des passerelles, qui connectent la région source à une ou plusieurs d'autres régions.

Pour mettre en place le routage inter et intra régions, chaque nœud DTN a un nom sous forme d'un tuple composé de deux parties :

- ***L'identificateur de la région (ou nom de région)*** : <Identifiant Région>
- ***L'identificateur de l'entité (ou nom d'entité)*** : <Nom de l'Entité>

Dont la structure générale d'un tuple est :{<Identifiant Région>, <Nom de l'Entité>}.
Le routage des messages entre régions est basé sur les identités des régions qui sont liés à leurs adresses correspondantes dans tout le DTN.

Le routage interne est basé que sur les identités des entités qui sont liés à leurs adresses correspondantes au sein de la région.

Les passerelles appartiennent à deux ou plusieurs régions et déplacent les bundles entre ces régions, ainsi ces passerelles possèdent plusieurs identités région.

[11] Même plate-forme

L'objectif d'organisation hiérarchique des noms de région DTN permet de réduire les tables des transporteurs DTN, les noms des entités n'ont pas de structure particulière. Cependant, la résolution de ce nom doit pouvoir être faite dans la région source (origine) ou dans la région de destination [10] [8]. Le principe d'adressage est alors illustré par la figure 9 montrée ci-dessus [10]:

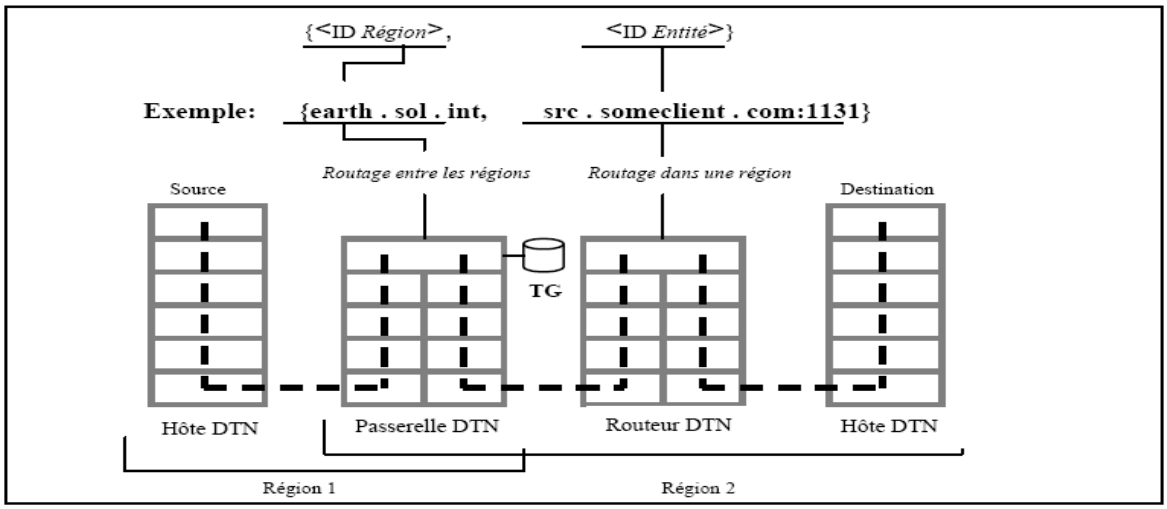

Figure (2-9): Adressage dans un DTN

I-3-5- Application

Les deux groupes qui s'intéressent et développent les DTNs et les protocoles associés :

- ***Applications spatiales:*** L'aérospatiale est à l'origine du concept de DTN. C'est donc, dans ce domaine qu'on trouve les premières applications. Toutefois, tout est encore au stade expérimental. Un premier test des DTNs pour les communications spatiales a été réalisé en septembre 2008 par la NASA.

  La sonde Dee Impact, qui dispose d'une implémentation du Bundle Protocol a émis un message en direction de la Terre. Ce message a été relayé par neuf nœuds-relais, tous utilisant les mécanismes de DTNs, avant d'arriver à la destination. Bien que, ces nœuds étaient en réalité des simulations fonctionnant sur Terre, le test a été un succès et a permet de mettre en avant l'intérêt des DTNs dans ce type de communication. La NASA prévoit d'installer en juillet

2009 un nœud DTN dans la Station Spatiale Internationale, afin de servir de relais pour les futures communications.

- ***Applications militaires :*** L'armée américaine est le second organisme à s'intéresser de près aux DTNs, le DARPA travaille effectivement sur son propre DTN (signifiant ici Disruption Tolerant Network) depuis 2005. L'objectif est d'améliorer les communications entre les unités sur le champ de bataille. Ici, il ne s'agit pas de mettre en place un réseau tolérant aux délais mais plus aux perturbations (plus particulièrement le brouillage) bien que ces dernières entrainent à leur tour des délais [10].

Conclusion

Toute au long de ce premier chapitre, nous avons tenté d'aborder l'architecture des réseaux tolérants aux délais, de donner une vue partielle de toutes les possibilités offertes par cette architecture, et ces spécifications dérivées qui permet de mettre en place les communications intermittentes, à forte délais où les protocoles Internet tel que TCP/IP peuvent être inadaptés.

Le principe de routage dans les DTNs, fera l'objet du chapitre suivant dans lequel nous allons s'intéresser aux algorithmes de routage et définir les différents protocoles utilisés.

Chapitre II

Routage dans les réseaux tolérants aux délais

Introduction

Dans ce chapitre, nous allons s'intéressés à la couche réseau du système OSI, c'est à dire, à la couche numéro trois. Nous rappelons que le rôle principal de cette couche est le routage des paquets.

Le routage est l'art d'évaluer la qualité des trajets possibles et de sélectionner le chemin le plus approprié pour une transmission donnée. Etant donné les particularités des DTNs et leurs incompatibilités avec les mécanismes des réseaux traditionnels, la problématique du routage constitue une part importante du problème de transmission.

Pour cela, dans ce deuxième chapitre, nous allons présenter des approches de routage classiques qui sont inadaptées dans les DTNs. Ensuite, nous allons aborder des stratégies de routages qui ont été proposées pour les réseaux intermittents, pour but d'assurer le fonctionnement correct de routage au sein des DTNs. Enfin, nous détaillerons les protocoles participants à la notion de routage, et leurs classifications.

II-1- Internet : Routage

II-1-1- Rappels

Les routeurs [Annexe B] sont des équipements qui assurent la tache de routage[1] [Annexe B].Un routeur conserve des informations dans une table de routage [Annexe B] qui lui permet de prendre une décision sur le prochain saut à suivre pour envoyer le paquet de données afin qu'il puisse atteindre sa destination finale. Cette décision est prise selon plusieurs critères : le plus court chemin en coût, ou en délai.

II-1-2- Types de routage

Comme le routage n'est que la spécification de direction pour naviguer de réseau en réseau. Tel que, ces directions peuvent être indiquées d'une façon dynamique ou statique.

II-1-2-1- Routage statique

Il consiste à indiquer l'adresse IP des réseaux de destinations. Nous associons à chaque adresse, le nom d'interface du routeur ou l'adresse IP du routeur voisin se situant sur la route

[1] Mécanisme qui permet d'acheminer les données à la destination

vers les réseaux de destinations et pour prévenir à tout disfonctionnement[2], il faut effectuer une surveillance permanente et reconfigurer chaque routeur dans le cas échéant.

II-1-2-2- Routage dynamique

Puisque le routage statique centralise la configuration du routage dans les mains d'un individu dont le temps de réaction est fatalement long et les risques d'erreurs importants.

Le routage dynamique utilise une route qu'un protocole de routage a modifiée automatiquement en fonction des changements de topologie ou de trafic.

II-1-3- Protocoles de routages

Les protocoles de routage [Annexe B] les plus utilisés dans le réseau Internet peuvent être classés à base des stratégies intra-domain et inter-domain.

II-1-3-1- Protocoles basés sur l'intra-domain

Un protocole de routage interne vise à maintenir des routes sans cycle à l'intérieur d'un Système autonome[3] [Annexe B]. Il construit les meilleurs chemins au sens d'une métrique donnée, il prend également en compte la disparition des routes, qui peuvent être résulté de la disparition d'un sous-réseau ou de la disparition d'un lien. Il distribue également à l'intérieur d'un système autonome les informations de routage qui lui sont transmises par les routeurs de bordure[4], ces derniers exécutent deux protocoles de routage à la fois externe et interne. En effet, il existe deux grandes familles de protocoles de routage interne : Protocoles de routage à base de vecteur de distance et protocoles de routage à état de liens [Annexe B].

II-1-3-2- Protocoles de routages basés sur l'inter-domain :

Dans les protocoles de routage externe, ce sont les routeurs aux frontières des systèmes autonomes qui s'échangent périodiquement des informations de routage. Il va permettre l'échange des adresses contenues dans les systèmes autonomes. Il va aussi propager des routes apprises depuis un autre système.

[2] Panne d'un routeur, ligne coupée, etc.

[3] Est constitué d'un ensemble de routeurs situés sous le même domaine d'administration.

[4] Extrémité.

Le but de tel protocole est de faire propager des nouvelles routes vers d'autres systèmes autonomes toute en permettant d'appliquer des restrictions[5] décidées par l'administrateur de chaque système autonome. Plus de détails dans [Annexe B].

II-2-Le routage dans les DTNs

II-2-1- Modélisation d'un DTN

Pour implémenter des protocoles de routage pour les réseaux DTN, Warthman a basé sur la théorie des graphes [Annexe C], afin de modéliser un DTN avec un multi graphe [14] dans le quel plusieurs liens peuvent être existés entre deux nœuds.

II-2-1-1- Nœuds et arêtes

Une paire de nœuds peut être connectée par plus d'une arête[6]. Ceci permet de choisir entre deux types de connexion différents pour transmettre des informations entre une même paire de nœuds. Le graphe ci-dessous représente un modèle du réseau DTN [14] [10] :

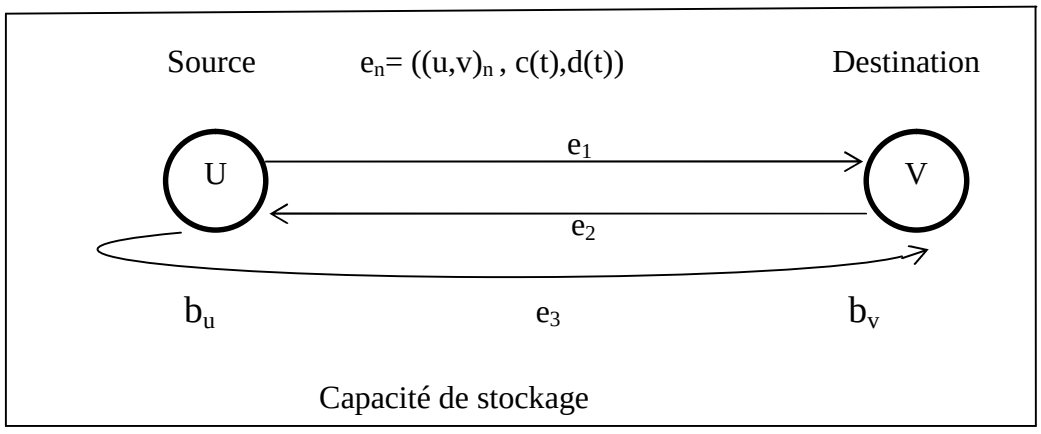

Figure (2-1): Liens (ou arcs) dans un graphe

II-2-1-2- Contacts

Un contact est l'opportunité d'envoyer des données à travers une arête [10]. Sur le schéma chacun des nœuds u et v utilise l'opération *store-and-forward message switching* et possède une capacité de stockage b_u et b_v.

[5] Filtrage de routes

[6] Appelée aussi un lien

Un lien e_n est paramétré par les nœuds source et destination, une capacité c (t) et une fonction de délai d(t). Lors d'un contact, où, lorsque l'opportunité d'envoyer des informations sur un lien se présente, la capacité du lien est strictement positive, il peut être [10] [14] :

- ***Persistant :*** Toujours disponible, c'est-à-dire qu'il n'exige pas d'action d'initiation de connexion.
- ***A la demande* :** Nécessite une action de demande de connexion puis fonctionne comme un contact persistant lorsque celle-ci est bien établie.
- ***Prévu intermittent :*** Ce qui est une sorte d'accord d'établissement de connexion à un temps particulier et pour une durée définie.
- ***Opportuniste intermittent :*** C'est-à-dire qu'il n'est pas prévu mais se présente de lui-même, comme dans les communications infrarouges et Bluetooth entre deux nœuds.
- ***Prédit intermittent* :** N'est fondé sur aucun ordonnancement fixe mais résulte des prévisions des temps, et des durées des contacts basées sur l'historique observé précédemment, ou sur d'autres informations.

Les routes dans les contacts prédits peuvent être choisies en se basant sur des informations tirées d'un assez haut niveau de confiance [10]. En ce qui concerne les messages, ceux-ci sont représentés par un tuple (u, v, t, m), où u représente la source du message, v la destination, t le moment où le message est injecté dans le système et m la taille du message [10]. En outre, chaque nœud DTN possède un buffer afin de pouvoir mettre en application la technique de store-and-forward. Enfin, les techniques de routage vont se charger de déterminer par quels nœuds le message va transiter, les messages stockés qui ne seront pas immédiatement transférés devront attendre d'être assignés par l'algorithme de routage lorsqu'il est possible qu'un contact ait lieu [10].

II-2-1-3- La fragmentation des messages

La fragmentation des messages [Annexe B] est d'autant plus intéressante dans les réseaux DTN, car les messages peuvent être arbitrairement gros et il se peut qu'un message ne puisse pas être transmis entièrement en un seul contact. Cependant, fragmenter un message complique la tâche de routage car il faut d'une part déterminer la taille des fragments, et d'autre part déterminer les chemins correspondants à chacun des fragments [7].

II-2-2- Notions de base du routage dans les DTNs

Etant donné les particularités des DTNs et leurs incompatibilités avec les mécanismes de routages des réseaux traditionnels, il est nécessaire d'avoir un mécanisme particulier permettant de caractériser les routes dans un DTN.

II-2-2-1- Scénario du routage

Dans le cas général, pour trouver les chemins à suivre pour les messages dans un DTNs, le scénario du routage se déroule en quatre étapes [15] :

a) ***Attendre une opportunité de transfert :*** Pour un nœud qui désire transférer un message vers un nœud destinataire, il sauvegarde le message jusqu'à l'apparition de contacts entre la source et la destination.

b) ***Echange d'entête de messages :*** A la rencontre de deux nœuds, ils échangent les listes des messages qu'ils possèdent.

c) ***Appliquer l'algorithme de routage :*** Sélectionner les messages à envoyer selon l'algorithme adopté.

d) ***Echange des contenus des messages :*** Pour chaque message sélectionné dans un nœud, le contenu est transféré à l'autre nœud.

II-2-2-2- Approches du routage

Le but majore de routage dans les réseaux traditionnels[7], consiste à sélectionner le meilleur chemin vers la destination, qui minimise certaine métrique, mais pour les DTNs, l'objectif n'est pas si évident [10]. Vu les caractéristiques des réseaux DTN, la notion de chemin de topologie est différente, puisque les contacts peuvent être intermittents et les nœuds sont mobiles. Alors, on a une topologie variable dans le temps, et les protocoles de routage traditionnels se révèlent inefficaces [10].

Les objectifs du routage dans les réseaux DTNs sont [8] [3] **:** De diminuer le taux de perte ou d'échec dans l'acheminement des paquets , de maximiser la probabilité de livraison, de minimiser le délai de bout en bout et de diminuer le nombre total de transmissions nécessaires d'un paquet.

[7] Réseau Internet

Le premier but du routage est de transmettre le paquet d'une source à une destination. Donc, le taux de perte est toujours le paramètre le plus important pour le routage. Cependant, pour certaines applications, un paquet qui arrive trop tard n'a aucune valeur, on doit donc réduire le délai de bout en bout.

Donc, pour améliorer la performance du système, il faut réduire le nombre total de transmission de paquets et le nombre de copies de chaque paquet, ainsi que minimiser la charge liée à l'échange des informations de routage.

II-2-2-2-1- Routage réactif & Routage proactif

- ***Routage proactif :*** La plupart des protocoles de routages d'Internet standards, et quelques protocoles Ad Hoc tels que DSDV (Destination-Sequenced Distance Vectoring) et OLSR (Optimized Link State Routing) adoptent le routage proactif. Dans ce cas, les routes sont calculées de façon automatique et indépendamment de tout trafic arrivant [10] [3]. Dans les réseaux DTN, le routage proactif ne calcule les routes que pour les nœuds actuellement connectés, parce que les liens ne sont pas toujours disponibles, les messages de topologie envoyés entre les routeurs auront du mal à circuler, et l'algorithme ne pourra pas converger [3]. Ces protocoles échouent lorsqu'il faut trouver le chemin menant à un nœud qui n'est pas accessibles [8]. Malgré ce désavantage, le routage proactif est rapide et il peut fournir des éléments utiles aux algorithmes de routage DTN, en leur désignant l'ensemble des nœuds accessibles pour le choix du prochain saut [7] [10].
- ***Routage réactif :*** Le principe de ce type de routage consiste à découvrir les routes à la demande pour chaque nouvelle destination, il est plus adapté aux connexions intermittentes. Ce routage est utilisé par certains protocoles de réseaux Ad Hoc tels que AODV et DSR [3] et il ne fonctionne que sur les nœuds actuellement connectés et pourra ne pas trouver de route vers la destination s'il n'existe pas de chemin de bout en bout à l'instant de la recherche. Il faut par ailleurs, que la route découverte soit maintenue suffisamment longtemps pour permettre d'y acheminer les messages [10].

II-2-2-2-1- Routage source & Routage par saut

- ***Routage source :*** Il consiste à déterminer le chemin complet que doit suivre le message, depuis le nœud source, tel que ce chemin est codé dans le paquet du

message, il est déterminé une fois et ne change pas lorsque le message traverse le réseau [10].

- ***Routage par saut :*** Le prochain nœud du message est déterminé à chaque saut tout le long du chemin. Cette technique de routage permet au message d'utiliser l'information sur les contacts disponibles et les files d'attente à chaque saut, ce qui est généralement indisponible à la source. Ainsi ce routage peut conduire à des meilleures performances. Cependant, en raison de sa nature locale, il peut conduire à des boucles lorsque les nœuds ont différentes vues de topologie [10]. Pour cela, différentes approches ont été trouvées permettant de résoudre ces problèmes [8].

II-2-2-3- Classification des protocoles de routages

Les stratégies de routage proposées pour les DTNs, sont divisées en deux catégories. Elles sont basées sur la réplication et d'autres stratégies sont basées sur la connaissance [8].

- **La réplication *(replication)* :** Les protocoles basés sur cette stratégie ne tiennent pas en compte le fait que les nœuds contiennent des informations pouvant être utilisées pour déterminer le chemin. La source envoie plusieurs copies d'un même message à un ensemble de nœuds. Ces derniers, vont garder le message jusqu'à ce que la connexion avec le destinataire soit établie [8]. Cette stratégie de routage utilise de multiples copies pour chaque message afin d'augmenter la chance qu'au moins une copie soit délivrée, ou pour réduire la latence de livraison. Certainement, l'approche la plus fiable est de faire porter à chaque nœud une copie du message, dans ce cas, ce dernier n'est considéré perdu que si tous les nœuds qui le portent sont incapables de le délivrer. En revanche, ceci consomme la bande passante et les ressources de stockage de manière proportionnelle au nombre de nœuds dans le réseau [10].

- **La connaissance *(acknowledge)* :** Les stratégies de routages basés sur la connaissance adoptent une approche traditionnelle pour router les données, elles exigent plus d'informations sur la topologie du réseau pour sélectionner le meilleur chemin et transmettre ensuite les données via ce dernier [8]. Ces stratégies emploient des règles statiques qui sont configurées initialement, et tous les nœuds vont les livrer. L'inconvénient est que cette stratégie ne peut pas être

adaptée à tous les réseaux ou à toutes les conditions, ainsi elle ne prend pas des décisions optimales [10].

Cette classification en deux catégories a été proposée par Jain & Al [10]. Elle se base sur deux critères, le critère d'inondation et le critère d'expédition où le concept d'oracles de connaissances a été intégré.

- ***L'inondation*** : Consiste à la délivrance de multiples copies de message pour un ensemble des relais[8]. Ces derniers stockent les messages jusqu'ils se connectent avec la destination où les paquets de données seront délivrés.
- ***L'expédition*** : les stratégies de cette famille nécessitent quelques connaissances supplémentaires sur la topologie du réseau DTN, pour sélectionner le meilleur chemin et envoient un seul message le long de celui-ci. Ainsi, elles évitent d'utiliser la réplication sur lequel le message est alors envoyé en allant d'un nœud à l'autre [10].
- ***Les oracles de connaissance*** : Le problème de routage DTN a beaucoup de variables d'entrées, par exemple : les caractéristiques de la topologie dynamique et la demande de trafic. La connaissance complète de ces variables facilite le calcul des routes optimales. Cependant, avec des connaissances partielles, la capacité de calcul des routes optimales est saturée et les performances du routage résultant s'avèrent inférieures. Afin de comprendre cette interaction fondamentale entre performances et connaissances, un ensemble abstrait d'oracles[9] de connaissances a été créé. Ces oracles sont des éléments utilisés pour encapsuler des connaissances particulières sur le réseau, requises par différents algorithmes. Alors, nous pouvons distinguer 4 types d'oracles :
    - ***Oracle de l'état des contacts*** : La connaissance de connaître ces paramètres permet de connaitre des statistiques générales à propos des contacts, il fournit en particulier, le temps d'attente moyen jusqu'au prochain contact [14]. Ainsi, l'oracle de l'état des contacts ne fournit que le temps invariant, ou un résumé des caractéristiques des contacts [10].

[8] Un ensemble de nœud

[9] Des connaissances particulières sur le réseau

- ***Oracle de contact*** : Cet oracle permet de résoudre n'importe quelle question concernant les contacts entre deux nœuds à n'importe quel moment [14]. Ceci est équivalent à la connaissance du multi-graphe DTN dans un temps variant, il est possible que l'oracle de l'état des contacts être construit à base de l'oracle contact mais le réciproque n'est pas vrai.
- ***Oracle de file d'attente*** : Cet oracle donne des informations sur l'occupation instantanée des buffers à n'importe quel moment et sur n'importe quel nœud [14] [10]. A la différence avec les autres oracles, l'oracle de la file d'attente est affecté par les nouveaux messages qui arrivent au système, et le choix fait par l'algorithme de routage lui-même.
- ***Oracle de demande de trafic*** : Cet oracle permet de répondre à n'importe quelle question concernant la demande de trafic présente ou future. Grâce à ce paramètre, il devient possible de connaître l'ensemble des messages injectés dans le système à n'importe quel moment [10].

II-2-2-4- Algorithmes du routage

II-2-2-4-1- Algorithmes basés sur l'inondation

Parmi les protocoles de routage basés sur cette stratégie on trouve :

i. ***Inondation Tree-based* :** Dans cet algorithme, le nœud source génère une copie du message au niveau d'un relais qui lui génère un autre nombre de copies au niveau des relais qui le suivent. Cette stratégie est nommée *Tree-based*, car l'ensemble des relais forme un arbre dont la racine est le nœud source. L'algorithme basé sur l'inondation Tree-based peut fournir des messages à des destinations qui sont loin de plusieurs sauts [10]. En revanche, le fait d'inonder le réseau, implique une consommation énorme de ressources de stockage et de bande passante [7].

ii. ***Routage épidémique* :** Le principe de cet algorithme est le plus simple [3] car il ne nécessite aucune connaissance sur le réseau pour la livraison des messages. Chaque nœud a une seule file d'attente [3]. En effet, quand un message est envoyé, il est étiqueter par un identifiant unique et placé dans la file d'attente, lorsque deux nœuds entrent en contact, chacun envoie à l'autre sa liste de tous les identifiants des messages qu'il a dans sa fil. Cette liste est appelée « vecteur d'état ». En utilisant ce vecteur d'état, les nœuds s'échangent les messages qu'ils

ne possèdent pas, après cette opération, tous les nœuds ont les mêmes messages [10]. Dans le routage Epidémique, chaque nœud peut être le gardien (custody) ce qui rend la probabilité que le message soit délivré très élevé, cependant l'inconvénient est de consommer une énorme quantité de ressources, qui est dû au grand nombre de copies, ce qui nécessite une grande quantité d'espace en terme de buffer, de bande passante et d'énergie [8] [10].

iii. ***Probabilistic Routing Protocol using History of Encounters and Transitivity (PRoPHET)***: Le principe de PRoPHET[10] est similaire à celui du routage épidémique, lorsque deux nœuds se rencontrent, ils s'échangent les vecteurs d'état qui dans ce cas contiennent aussi l'information sur la prévisibilité de délivrance d'un message qui est stocké dans les nœuds [10]. Pour cela, afin d'obtenir une meilleure performance du routage, il semble évident qu'il faut transmettre les messages vers le nœud qui a une plus grande prédictibilité en fonction de la destination. Sachant que, la prédictibilité est la probabilité qu'un message arrivé à la destination via un nœud intermédiaire donné [8]. En effet, *PROPHET* utilise une stratégie très simple, lorsqu'un message arrive à un noud, il peut ne pas y avoir de chemin disponible vers la destination. Ainsi, le nœud doit le garder dans le buffer, et à chaque rencontre d'un autre nœud qui a une prédictibilité plus grande pour le message, il transmet ce message à ce nœud, et garde encore ce message pour le transmettre à d'autres nœuds dans le futur [10]. Le problème est que, lorsque le nœud original du message a une très faible prédictibilité pour la destination, il va transmettre ce message vers tous les nœuds qu'il rencontre, jusqu'à ce message soit supprimé par la file d'attente (souvent, le nœud original garde ses messages pendant longtemps). Ce processus prend beaucoup de ressources, même si l'on peut ajouter un contrôle afin d'éviter de transmettre le message au même nœud plusieurs fois. Par contre, si le nœud original de message a une très grande prédictibilité, ce message va être distribué rarement, très peu de nœud pouvant avoir une prédictibilité plus grande que lui. Ce message va donc rester dans le nœud original longtemps. Par exemple, le nœud original vient de rencontrer la destination, et part plus loin. Sa prédictibilité pour la destination diminuera lentement [3]. Vu les inconvénients

[10] Probabilistic Routing Protocol using History of Encounters and Transitivity

précédents de l'approche PRoPHET, en revanche, il garantit plusieurs avantages suivants [10] :

- Il utilise l'historique des nœuds rencontrés avant de prendre la décision de remettre un message à un autre nœud.
- Il utilise la transitivité dans sa fonction de calcul de prédictibilité. En effet, si le nœud A rencontre fréquemment le nœud B, et le nœud B rencontre fréquemment le nœud C, alors le nœud C est probablement bon pour transmettre des messages destinés au nœud A.
- Les simulations ont montré que PRoPHET donne des performances similaires et parfois meilleures que le routage épidémique.

iv. ***Spray &Wait :*** Spyropoulos et Al ont proposé le protocole de routage « Spray and Wait », dont il n'y a pas de table de routage [10], qui a pour principe la distribution de seulement un petit nombre de copies à chaque relais différent. Chaque copie est alors portée tout le long du chemin vers la destination par le relais désigné. L'algorithme « *Spray* and *Wait* » comport 2 phases :

a. ***La phase Spray (pulvérisation)*** : le nœud source envoie rapidement *L* copies de message à *L* autres nœuds quelconques.

b. ***La phase Wait (Attente)*** : Si la destination n'a pas été trouvée dans la phase « Spray », chaque nœud parmi ces *L* nœuds garde le message jusqu'à ce qu'il rencontre la destination. Donc, chaque message va ne toucher que L nœuds intermédiaires, *L* dépend de la dimension du réseau et du délai moyen que l'on veut obtenir [3].

Le mécanisme de cet algorithme combine la rapidité du routage épidémique (première phase), avec la simplicité et l'économie en ressources de la transmission directe(deuxième phase). Cependant il présente quelque inconvénient tels que : Le fait que la mobilité des nœuds est faible et localisé, l'algorithme Spray&Wait perd ses performances [10]. Si la mobilité de chaque nœud est restreinte à une région locale alors aucun des nœuds transportant le message ne pourrait voir la destination.

En résume, les approches de routage basées sur l'inondation ont la particularité de diffuser un grand nombre de copies des messages, d'assurer un haut niveau de fiabilité dans la livraison des données et de garantir des faibles latences. Cependant, elles sous entendent

l'utilisation non seulement de beaucoup d'espace mémoire au niveau des nœuds mais aussi l'utilisation excessive de la bande passante.

II-2-2-4-2- Algorithmes basés sur l'expédition

L'ensemble des algorithmes de routage basés sur le critère d'expédition sont :

a) ***Routage à connaissance zéro :*** Ces algorithmes n'utilisent aucune connaissance, leurs performances sont assez pauvres, parmi eux [8] :

- ***First Contact (FC)* :** Examinons l'algorithme FC, il utilise n'importe quel contacte disponible. En effet, un message est transmis au long d'un lien choisi aléatoirement parmi les contacts actuel, si tous les liens sont indisponible, le message est alors sauvegardé et ensuite envoyé au premier contact qui sera disponible. De plus, cet algorithme réalise de faibles performances dans des environnements complexes vu que le choix du saut prochain est totalement aléatoire et l'acheminement du message à travers le lien sélectionné peut faire aucun progrès pour atteindre la destination. L'algorithme FC n'est pas très efficace, mais très facile à implémenter. Cependant, cet algorithme peut subir des améliorations différentes, par exemple, il est possible d'introduire un sens à la trajectoire entre la source et la destination afin que le message soit routé dans une direction plus proche de la destination. Pour éviter les boucles, une trace du chemin peut lui être ajoutée [10].

b) **La connaissance partielle *(partial knowledge)*:** Les algorithmes de la classe Partial Knowledge, n'utilisent pas les informations sur le trafic, ils utilisent les connaissances en termes de contacts et de files d'attente. De plus, chaque message Bundle est routé indépendamment de la future demande de trafic [8]. Tous ces algorithmes font intervenir des coûts qui sont assignés aux liens et cherchent à calculer les chemins dont le coût est minimal. Ces coûts sont utilisés afin de donner une estimation du délai lorsque le message passe par tel ou tel nœud [14]. En voici, quelques-uns :

- ***Minimum Expected Delay (MED)* :**La caractéristique principale de MED est qu'il minimise le temps moyen d'attente et par conséquent les coûts. Cependant, cet algorithme ne permet pas d'exploiter des liens possédant de meilleures caractéristiques qui deviendraient disponibles

après que la route ait déjà été calculée [14]. En plus, il utilise le même chemin pour tous les messages ayant la même paire source-destination [10]. L'algorithme MED n'utilise aucun mécanisme pour éviter la congestion ou la suppression du message si l'espace de stockage n'est pas disponible. Des améliorations ont été proposées pour cette approche, parmi elle, celle qui consiste à trouver de multiples chemins disjoints avec des couts différents, et choisir au hasard parmi eux celui qui pourrait améliorer l'équilibrage de la charge et réduire la congestion [10]. La route pré calculée pourrait alors être modifiée lors de la transmission lorsqu'un meilleur lien deviendrait disponible, cet algorithme aurait alors un comportement plus réactif [8].

- ***Earliest Delivery (ED)*** **:** Cet algorithme se base sur l'oracle des contacts, il cherche à minimiser la date de livraison d'un bundle sans prendre en considération les informations concernant la file d'attente, et les chemins sont calculés sans tenir compte de la disponibilité de l'espace de stockage aux nœuds intermédiaire. Ce qui peut conduire à une chute lorsque les buffers sont trop pleins. Cependant il est optimal dans le cas où les capacités des contacts et lorsque les files d'attentes des nœuds qui se situent dans le chemin sélectionné sont vide, alors ED aussi est optimale [10].
- ***Earliest Delivery with Local Queuing(EDLQ)*****:** Dans cet algorithme, les informations concernant les files d'attente locales sont prises en compte afin d'estimer les délais dus aux liens, et ce de la manière suivante [8]: La fonction qui permet d'assigner les coûts dépend du nœud qui est en charge de calculer la route. Cela peut entraîner la formation de boucles et que des messages déplacent indéfiniment dans le système. Pour éviter de telles mésaventures, il est possible, lorsqu'une boucle est détectée, d'utiliser un vecteur de distance et de refaire les calculs en utilisant des routes fixes, qui ont par exemple été calculées en utilisant l'algorithme ED. Enfin, comme pour ED, il se peut que des messages soient perdus en raison de buffers trop pleins.

- ***Earliest Delivery with All Queues (EDAQ)*:** Cet algorithme utilise les informations concernant les files d'attente afin de déterminer instantanément la taille des files d'attente à travers tout le réseau, et non simplement localement, à n'importe quel endroit du réseau et à n'importe quel moment. EDAQ ne tient pas compte des capacités des buffers et la perte de messages reste encore possible. Introduire des contraintes de stockage dans cet algorithme est une opération difficile à réaliser et il faudrait alors utiliser d'autres algorithmes ou mettre en place un contrôle de flux dynamique [14].

c) La connaissance complète (*Complete Knowledge*) : Les algorithmes de cette classe utilisent tous les oracles (contacts, files d'attente, et trafic) et représentent la première formulation complète du problème du routage [8].

- ***LP (Linear Program)*** : C'est la première formulation de problème de routage dans les DTNs qui prend en considération toutes les informations (oracles) pour déterminer le routage optimal afin de minimiser le délai moyen sur le réseau.

Le schéma ci-dessous traduit le compromis recherché entre performance et connaissance du système [14]

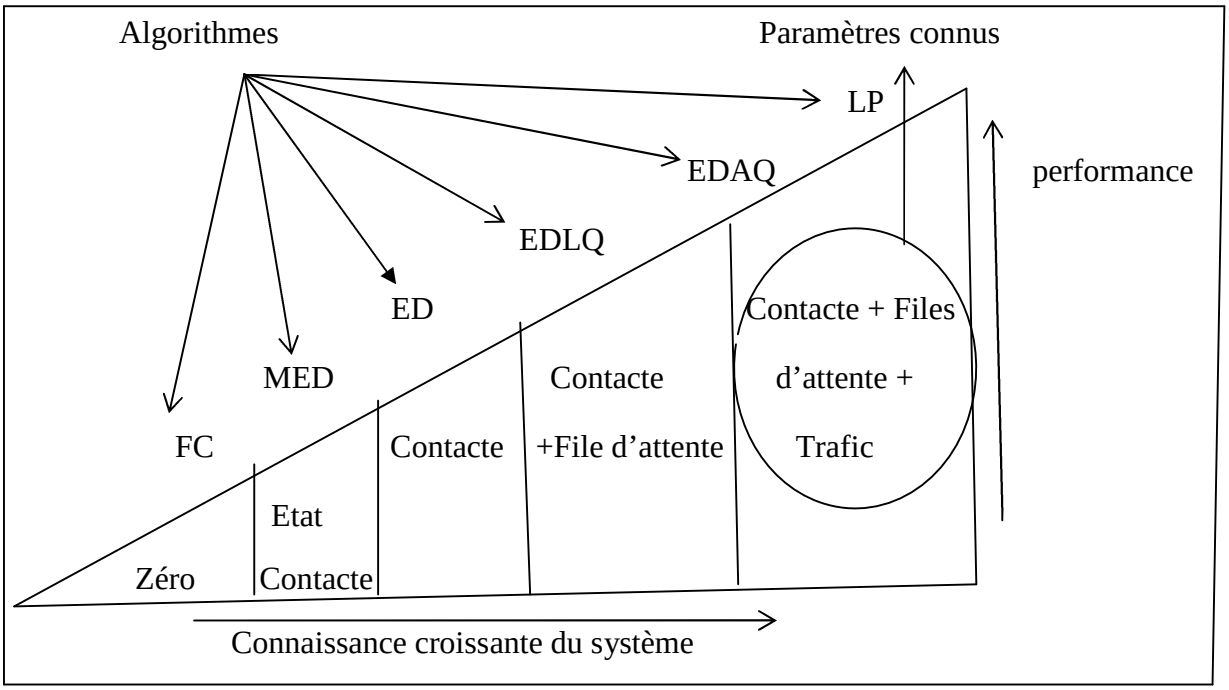

Figure (2-2): *Compromis recherché entre performance et connaissance du système*

Le schéma précèdent traduit bien, le fait qu'une bonne performance ne peut être obtenue qu'au prix d'une connaissance très précise du système. Au-dessus de chaque zone de connaissance, on représente les différents algorithmes en utilisant les paramètres correspondants.

II-2-2-4- Schéma récapitulatif de cette classification :

Après avoir présenté quelques protocoles de routage, nous les regroupant dans un seul diagramme afin de faciliter d'avantage la lecture, et de mieux orienter l'utilisateur. La figure ci-dessous montre les algorithmes de routage dans les DTN que nous avons recensés, et les classes à les quelles appartiennent selon les deux propriétés : l'expédition et l'inondation [10].

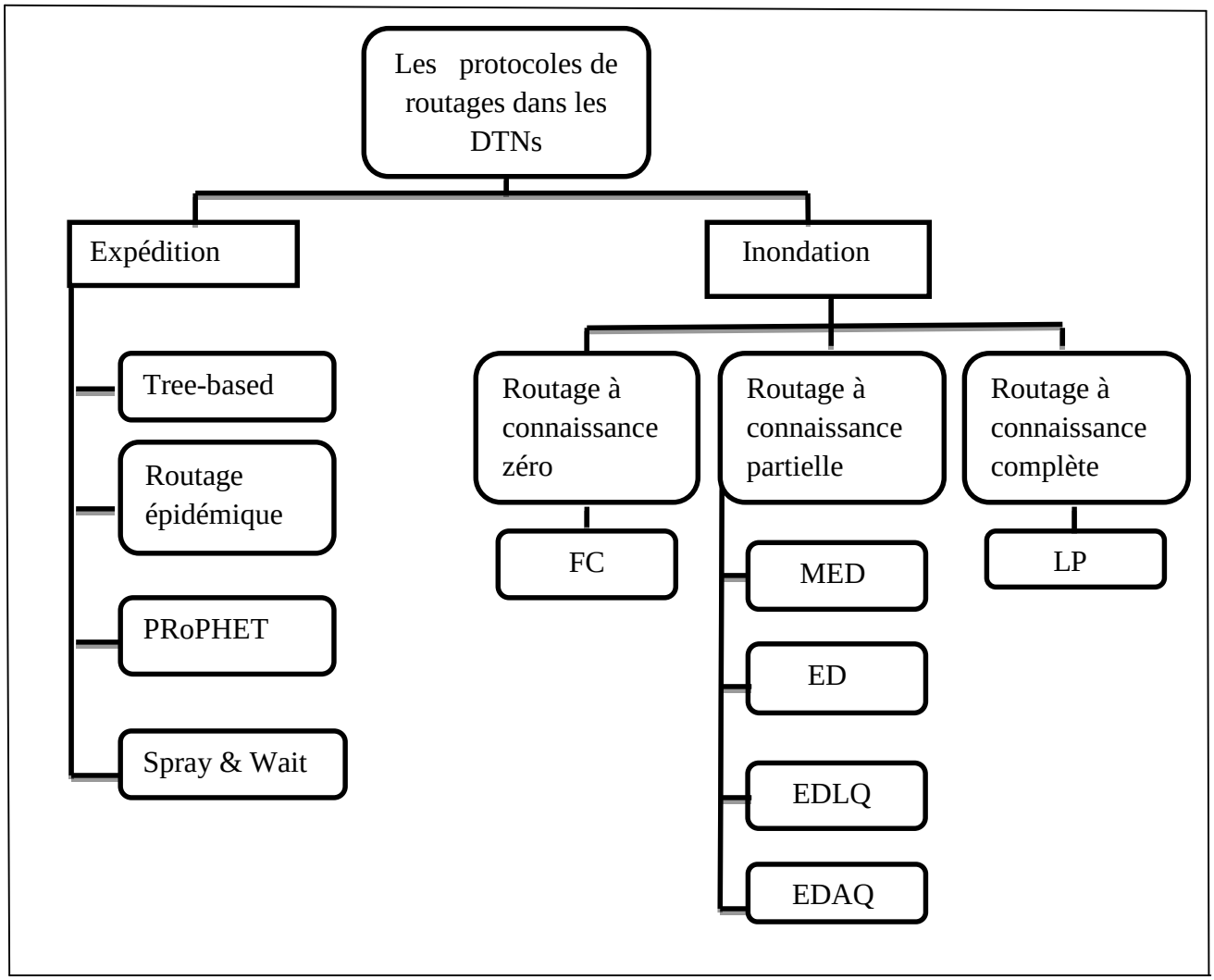

Figure (2-3) **:** *Organigramme résumant la classification de protocoles de routage des DTNs.*

Conclusion

Dans ce chapitre, nous avons décri les mécanismes de routage dans les réseaux classiques tel que Internet, comme ces approches ne fournissent pas une fiabilité dans les réseaux tolérants aux délais, nous avons tenté de rependre à cette problématique, en comparant les deux approches de routages, puis, en montrant et en proposant des stratégies de routages adoptés dans les communications intermittentes.

Et aussi, dans le monde de réseau Infrastructure, la sécurité vise à vérifier l'identité de l'émetteur du message et à s'assurer de l'intégralité de ce dernier, sans se soucier de ce qui se passe au niveau des routeurs. Vu aux connections intermittentes dans les DTNs, les mécanismes traditionnelles sont incompatibles et inefficaces, et dans les deux chapitre suivants, nous allons aborder des généralités sur la sécurité informatiques, et proposer une approche de sécurité pour assurer la protection de transfert des messages dans les DTNs.

Chapitre III

Sécurité et Cryptographie

Introduction

Les problèmes rencontrés sur le salon de toutes les technologies des réseaux existants aujourd'hui, est que la sécurité doit être une considération très importante.

Ce chapitre constitue à présenter un aperçu générale sur les différents mécanismes cryptographiques existantes et les plus utilisées dans les réseaux informatiques, dans le but d'assurer les principaux services de la sécurité.

III-1- Définition de la cryptographie

Le mot cryptographie est dérivé d'un mot grec **kruptos** (caché) et **graphian** (écrire). C'est la science qui utilise les mathématiques pour chiffrer et déchiffrer des données. Il s'agit de transformer les lettres composantes le message en une succession de chiffre sous forme de bits. La cryptographie permet de stocker les informations sensibles pour qu'elles ne puissent pas être lues par personne à l'exception du destinataire [23].

III-1-1 La confidentialité

La confidentialité des données est la priorité par laquelle l'information n'est pas rendue disponible ou n'est pas révélée aux individus, aux entités ou aux processus non autorisés [24].

La confidentialité des données dans une communication réseau fournit une protection contre l'analyse du trafic. Tel que, les données transportées ne peuvent pas être lues par un adversaire espionnant les communications. Elle est assurée en utilisant le chiffrement.

- **Chiffrement** : Il est définit comme une transformation de massage à partir d'un texte claire à un texte chiffré, pour le rendre incompréhensible. En effet, la forme de ce dernier dépend d'une clé de chiffrement [25].
- **Déchiffrement** : C'est une méthode qui permet de reconstruire le message en claire à partir d'un message chiffré. Cette reconstitution requiert une deuxième clé dite clé de déchiffrement [25]

II-1-1-1- La cryptographie symétrique

La cryptographie symétrique est aussi appelée les algorithmes à clés privées. En effet, lorsque on crypte[1] un message à l'aide d'un algorithme symétrique avec une clé secrète, le destinataire utilisera la même clé secrète pour le décryptage[2]. Il est donc nécessaire que les deux interlocuteurs se soient mis d'accord sur une clé privée auparavant, par courrier, par téléphone ou lors d'un entretien privé. Cette technique a besoin d'un canal pour échanger des informations sures [26].

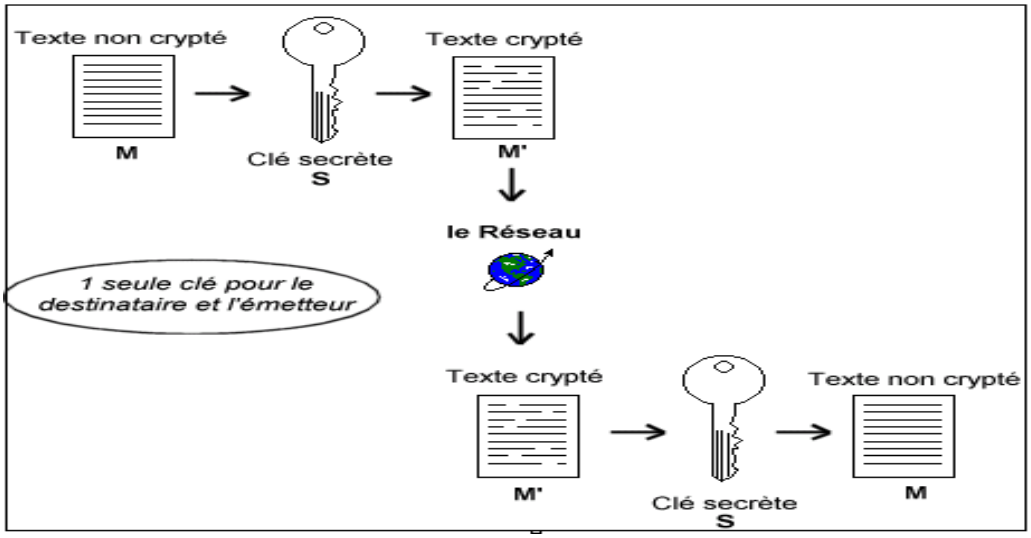

Figure (1-1) : Assurer la confidentialité avec le chiffrement à clé symétrique

Le chiffrement à clé privé a l'avantage d'être rapide. Cependant, il peut être assez coûteux en raison de la difficulté de la distribution sécurisée de la clé. Comme exemple l'algorithme de chiffrement symétrique. On trouve DES (Data Encryption Standard) [27], AES (Advanced Encryption Standard) et IDEA (International Data Encryption Algorithme) [27] [29] [30].

III-1-1-2- La cryptographie asymétrique

La cryptographie asymétrique a été inventée par Whitfield Diffie et Martin Hetlman en 1976 pour éviter le problème d'échange de clé secrète préalable [30].

[1] Chiffrer

[2] Déchiffrer

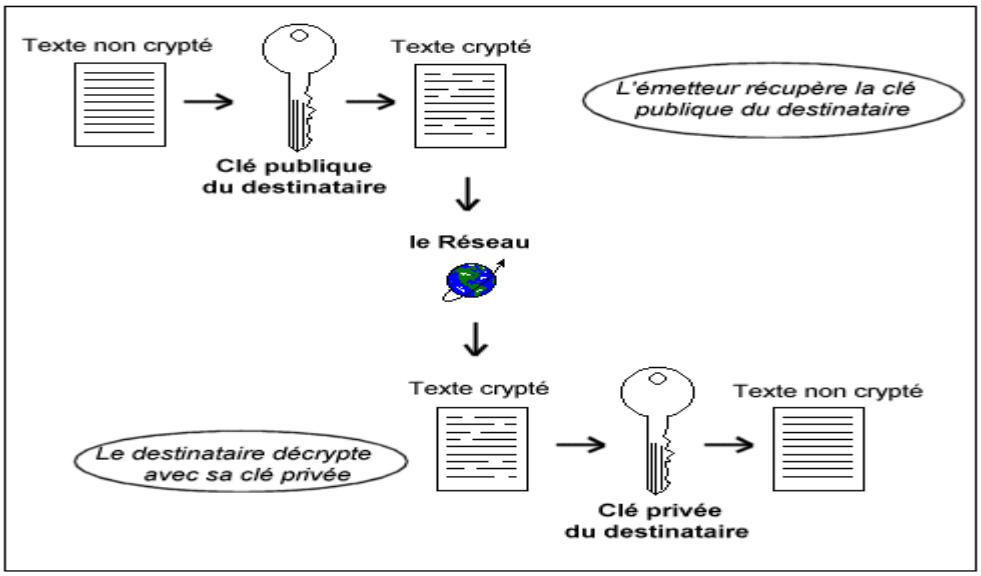

Figure (1-2) **:** *Assurer la confidentialité avec le chiffrement asymétrique*

En effet, la cryptographie asymétrique est aussi appelée les algorithmes à clés publiques. C'est à dire que chaque interlocuteur[3] possède une paire de clé (clé publique et privé), la clé publique peut être connue par d'autres interlocuteurs et la clé privée reste secrète.

L'utilisateur crypte un message à l'aide de la clé publique du destinataire, qui sera le seul à pouvoir le décrypter à l'aide de sa clé privée [26].

III-2- Intégrité des données

L'intégrité des données est la propriété par laquelle on s'assure que les données n'ont pas été altérées[4], détruites ou perdues d'une façon non autorisée , ou accidentelle durant la transmission [24]. Elle est rassurée par des fonctions cryptographiques de hachages.

III-2-1- Fonction de hachage

Une fonction de hachage est appelée aussi fonction de hachage à sens unique. Dans ce type de fonction, on chiffre le texte de telle sorte qu'on aura le chiffrement facile à calculer et le déchiffrement difficile ou même impossible. Le résultat d'une fonction de hachage est appelé le haché ou bien le condensé. Soit *H* une fonction de hachage, *m* le message à hacher tel que *H* (*m*) = *h* (*h* le condensé) alors :

[3] Utilisateur

[4] Modifier

- Etant donné *m*, il est facile de calculer *h*.
- Etant donné *h*, il est difficile de retrouver *m*.
- Etant donné *m*, il est difficile de retrouver un autre message *m'* tel que *H* (*m*)=*H* (*m'*).

Cette fonction est très utilisée en cryptographie, principalement pour réduire la taille de données à traiter par la fonction de cryptage. En effet, une fonction de hachage à sens unique utilise une entrée de longueur variable et produit une sortie de langueur fixe.

III-3- Authentification de l'origine des données

L'authentification de l'origine des données garantit que les données reçues proviennent de l'expéditeur déclaré [24].

Le MAC (Message Authentification Code) est une fonction cryptographique de hachage utilisant un deuxième paramètre d'entrée qui est une clé cryptographique pour le calcul du haché. Cette fonction est pour assurer l'authentification de l'origine des données et l'intégrité en même temps. Si deux interlocuteurs (a) et (b) désirent authentifier les messages entre eux, ils doivent préalablement partager une clé secrète K (ab).

- ***Etape (1):*** Emetteur (a) calcule le haché h= MAC (K (ab), m) du message (m) et de la clé partagée.
- ***Etape (2):*** Il envoie le massage m avec le haché h.
- ***Etape (3) et (4):*** L'or de la réception du message m avec le condensé h, le récepteur vérifie l'origine du message reçu comme suite :
    - Il calcule le haché du message reçu en utilisant la clé secrète k (ab).
    - Il le compare avec le haché reçu.
    - Si les deux hachés sont égaux, alors le message est dit authentique, sinon le message reçu a été modifié.

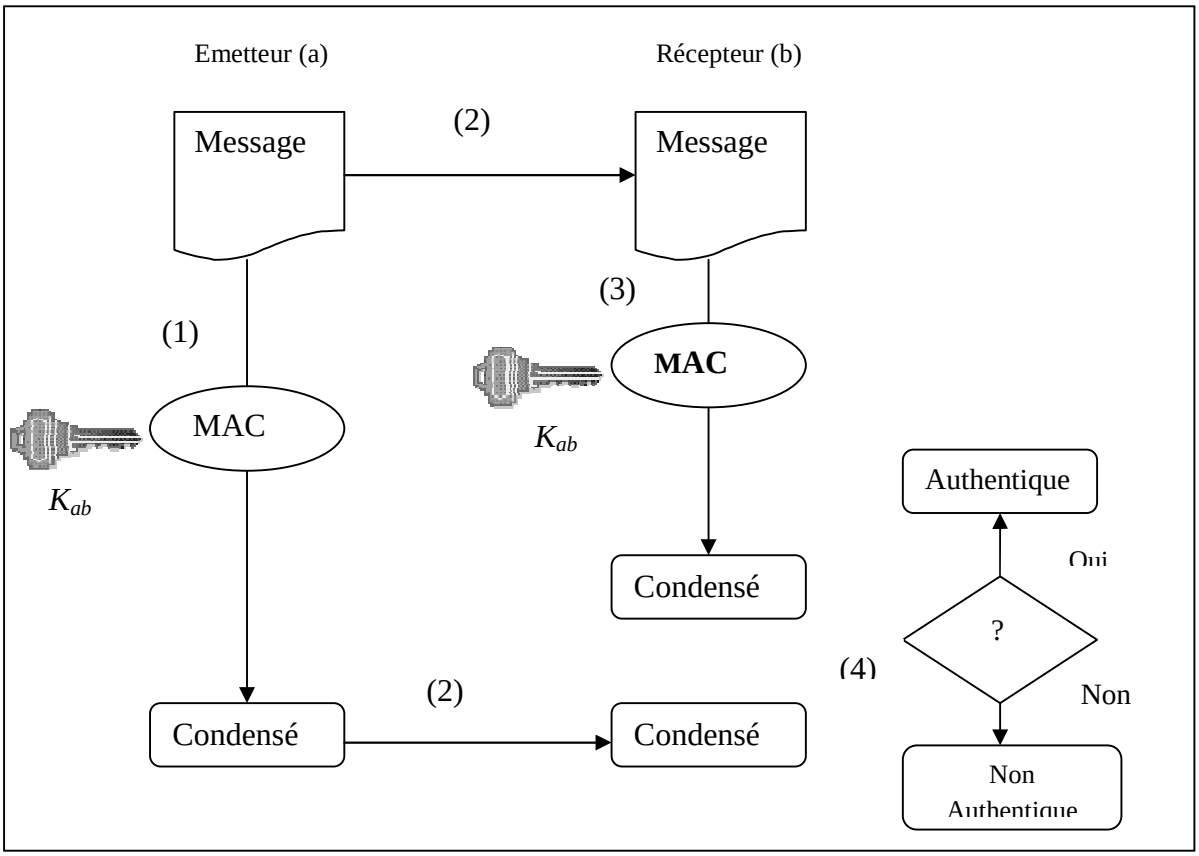

Figure (3-3) : Le MAC (Message Authentification Code)

III-4- Non répudiation avec preuve de l'origine des données

Le non répudiation avec preuve de l'origine des données, fournit au destinataire une information qui peut être utilisée comme preuve de l'origine des données reçues. Elle protège ainsi le destinataire contre une tentative de nier l'envoi des données par l'origine [24].

Notons que le MAC ne peut pas être utilisé comme preuve d'un message qui provient d'une entité spécifique. En effet, considérant un émetteur (a) et un récepteur (b) qui partagent une clé secrète K (ab). Si (a) nie d'avoir envoyé un message m, le récepteur (b) ne peut pas utiliser le MAC reçu avec m comme preuve de l'origine du message m, parce que (a) va dire que (b) pourrait avoir créé lui-même le MAC du m. Enfaite, la cryptographie asymétrique est la solution de base pour la non répudiation.

III-4-1- la signature numérique

Avec la cryptographie asymétrique, l'information envoyée avec le message comme preuve de l'origine de données est calculée en utilisant la clé privée de l'expéditeur, le

récepteur vérifie cette information en utilisant la clé publique de l'émetteur, par ce que seul l'émetteur peut calculer cette information. Ce dernier, peut être utilisé comme preuve de l'origine de données. En effet, ce mécanisme cryptographique est appelé signature numérique.

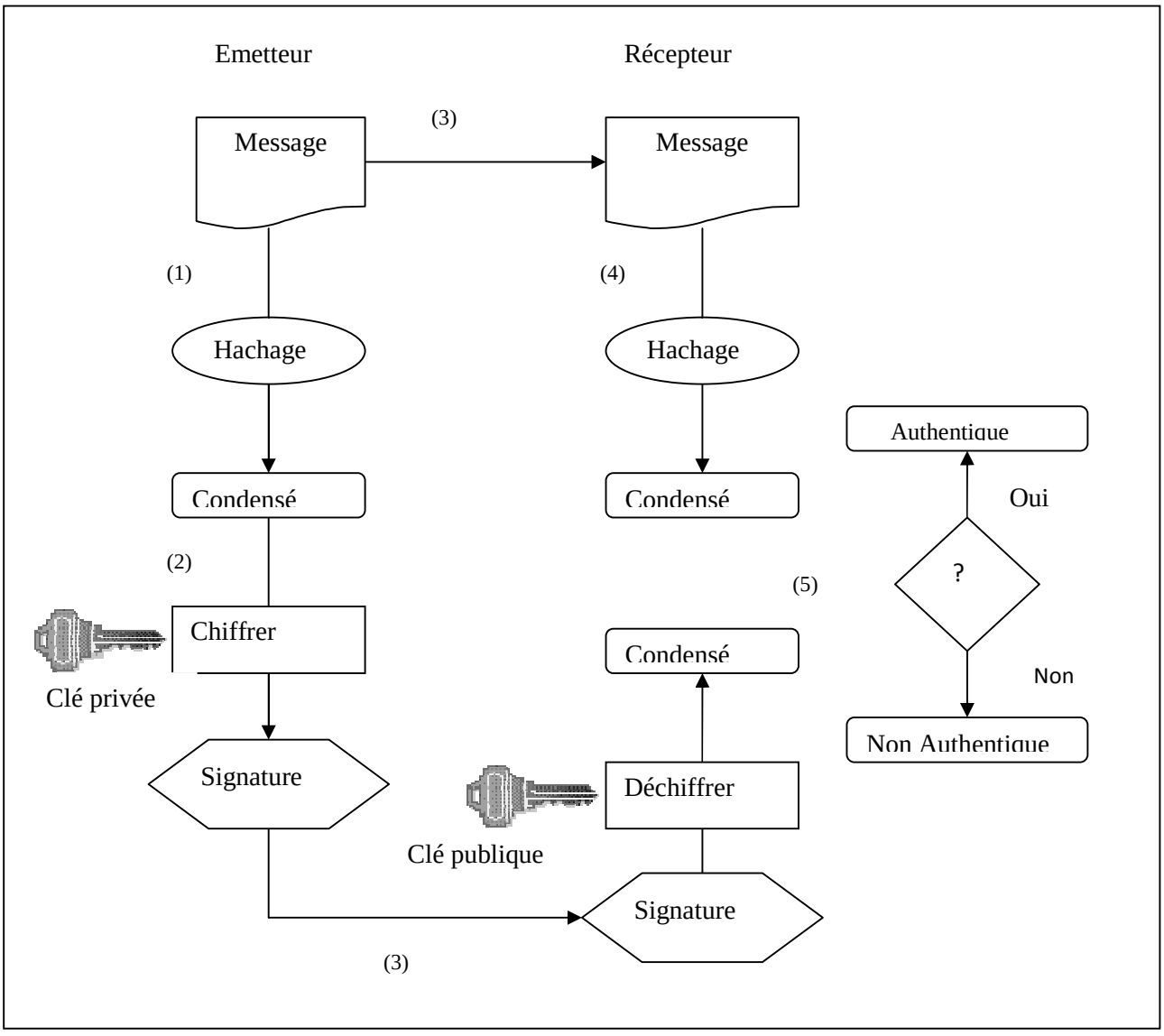

Figure (4-4) : <u>La signature numérique</u>

La signature numérique utilise un système cryptographique asymétrique pour signer un message m, l'émetteur :

- Calcule le haché h de m en utilisant une des fonctions de hachage usuelles H tel que h= H (m). (étape (1)).
- Chiffre le haché h avec sa clé privée le résultat de cette transformation appelé signature numérique du message m. (étape(2)).

- Envoi le message m avec la signature numérique. (étape (3)).

Lors de la réception du message et de la signature, le récepteur :

- Vérifie la signature en déchiffrant la signature en utilisant la clé publique de l'émetteur. (étape (4)). ;
- Calcule le haché du message reçu. (étape (4)).
- Vérifie la correspondance entre le haché reçu et le haché calculé. (étape (5)).
    - Si la signature est valide, alors on peut prouver que le message et son origine sont authentiques et on garantit le non répudiation de l'origine des données.
    - Sinon le message n'est pas authentique.

L'approche de signature numérique fournit les services suivants : l'authentification de l'origine des données, l'intégrité des données et le non-répudiation de l'origine des données. RSA (Rivest Shamir Adleman) [32] et DSA (Digital Signature Algorithm) [32] sont deux exemples de la signature numérique digitale.

III-4-2- Certificat à clé publique

Afin de vérifier une signature, le récepteur doit s'assurer que la clé publique utilisée pour la vérification correspond à la clé privée du l'émetteur supposé signé et non produit par un intrus[5] qui essaye de prendre l'identité de cet émetteur. Le document électronique qui assure ceci est appelé certificat à clé publique [Annexe C].

Conclusion

Dans ce troisième chapitre, nous avons tenté d'aborder les notions de base liées à la cryptographie à clé publique, outre à clé secrète, la signature numérique et la fonction de hachage.

Le chapitre suivant constitue le cœur de notre cas d'étude : la sécurité dans les DTNs. L'objectif est de comprendre pourquoi les mécanismes de la cryptographie traditionnels sont inapplicables dans les DTNs, et essayer de proposer une nouvelle infrastructure sécurisée pour tel environnement.

[5] Un utilisateur malveillant

Chapitre IV

Etat de l’art de la sécurité du DTN

Introduction

Le besoin de la politique de sécurité pour les réseaux tolérants aux délais est apparu dès les premières études sur les problématiques de la confidentialité et de l'intégrité. En effet, les techniques cryptographiques classiques basées sur PKI (Infrastructure des clés publiques) supposent un réseau d'accès continu, ces techniques sont inapplicables dans les DTNs. Ce qui rend, la gestion des clés publiques un problème ouvert.

Dans ce dernier chapitre, nous allons proposer un modèle d'infrastructure de sécurité pour assurer les différents services de sécurité dans les réseaux intermittents, en basant sur un modèle de graphe dynamique et virtuelle (DVD) pour l'étude de distribution de clés publiques. Ensuite, nous allons présenter un schéma basé sur un processus de cryptographie à deux canaux.

IV-1- Sécurité des réseaux tolérants aux délais

IV-1-1- Encapsulation des Bundles : Le Bundle se représente sous forme trois types d'information [34] :

- Les données utilisateur d'une application-source.
- Le contrôle des informations fournies par l'application source à la demande de destination, décrivant la façon de traiter, stocker la donnée d'utilisateur.
- L'entête Bundle [Annexe C] inséré au niveau de la couche Bundle.

IV-1-2- Menaces de sécurité : Les principales menaces trouvées dans les réseaux tolérants aux délais sont [35] :

- La modification des Bundles en transitant sur le réseau pour des causes malveillantes
- L'utilisation non autorisée des ressources rares de DTN.
- Le déni du service, par exemple en montant des attaques amplifiées dans lesquelles un nœud malveillant emploie les propriétés de réinterprète des protocoles de DTN, ainsi tremper les nœuds afin de produire un grand trafic sur le réseau.

L'histoire a prouvé que trois secteurs sont généralement plus susceptibles d'être attaqués: la couche réseau, la couche transport et la couche application [Annexe C].

Pour faire face à ces menaces, une architecture de sécurité est nécessaire dans laquelle les services de sécurité [Annexe C] peuvent être fournis à la base de nœud en nœud et de bout en bout.

IV-1-3- Spécifications de protocole de sécurité des Bundles

Les spécifications de protocole de sécurité dans un DTN, décrivent trois entêtes qui peuvent être ajoutés aux Bundles pour assurer les exigences de sécurité [36]:

i. **L'entête d'authentification du Bundle (BAH) :** Il fournit l'authentification pour un simple saut, en ajoutant un message de code d'authentification ou une signature au Bundles.

ii. **L'entête de sécurité de charge utile (PSH) *:*** Il est employé pour fournir l'authentification de bout en bout d'une manière semblable.

iii. **L'entête de confidentialité (CH) *:*** Il est employé pour encapsuler la charge utile de chiffrage au cours du trajet entre la source et la destination.

Chaque entête de message de sécurité contient l'information sur la sécurité de la source, l'information sur la sécurité de destinataire et un texte chiffré. Le texte chiffré définit les algorithmes qui vont être employés pour traiter la sécurité des entêtes reçus. La partie sécurité de l'expéditeur et l'information du texte chiffré déterminent l'ensemble des clés qui vont être employées [36].

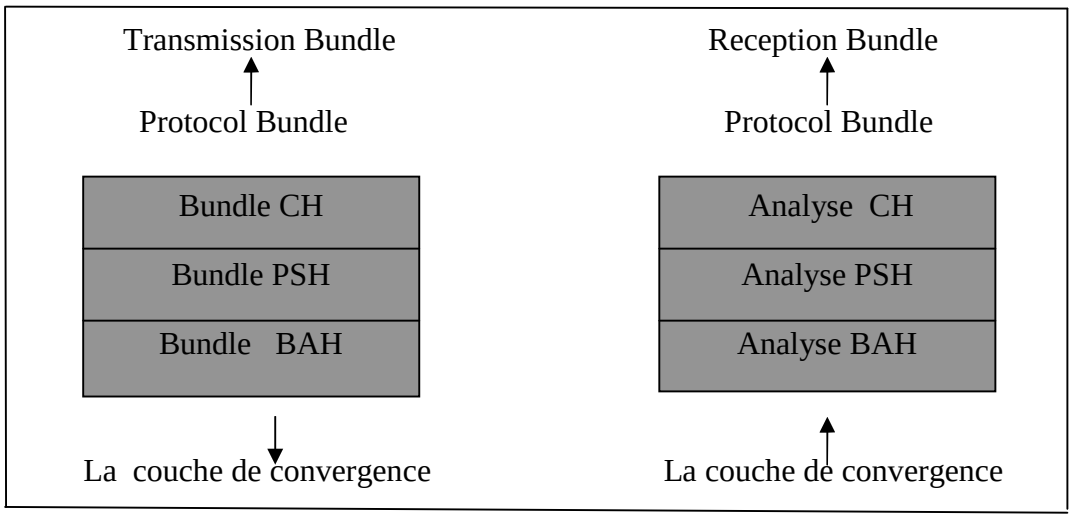

Figure (1-1): La pile de protocole

Dans la figure1, nous avons présenté une vue plus détaillée de la mise en œuvre d'en-tête de sécurité.

Au côté d'envoi de Bundle, les entêtes sont préparés par les format_header () qui est une fonction de la classe Bundle Protocol. La séquence de format d'en-tête doit suivre ce qui est représenté dans la figure1, le CH est le premier, suivie par le PSH ainsi le BAH. Cet ordonnancement est nécessaire, car le BAH s'appuie sur les informations de PSH, CH et la charge utile. Lorsque CH est activé, la charge utile est cryptée.

Ensuite, le PSH peut être calculé depuis le MAC PSH où la signature est calculée en fonction de la charge utile et de l'information CH.

Enfin, le BAH peut être appliqué, si cette option est activée, comme il fournit l'intégrité pour le Bundle entier, y compris tous les autre entêtes de sécurité. Une fois le formatage entête est terminé, le Bundle peut être transmis à la couche de convergence approprié.

Au côté de la réception, la couche de convergence transmet les données qu'elle tire du réseau à des parse_headers () qui est la fonction de la classe Bundle Protocol. Lors de l'analyse, les entêtes présentés dans le Bundle sont indiquées dans l'ordre.

Ainsi, le récepteur calcule d'abord le BAH. Ensuite, le PSH, et finalement le CH où la charge utile du bundle peut être déchiffrée. Après le calcul de chiffrement, le cas échéant des hachages ou de signatures calculées ne correspondent pas à la valeur extraite de l'en-tête, un événement de défaillance de la sécurité sera généré par l'agent DTN.

Si les contrôles passent, puis un événement Bundle reçu sera émis donc, le Bundle sera traité avec succès [36] [37].

IV-1-4- Protection de l'infrastructure DTN

Pour la protection de l'infrastructure DTN, des services de sécurité des agents Bundles sont : le contrôle d'accès, la vérification de l'intégrité des données saut-par-saut, l'authentification des terminaux et le manque de détection de la réplication dans les routeurs arbitraires.

IV-1-4 -1- Le contrôle d'accès

Le contrôle d'accès est effectué pour s'assurer que, seules les demandes légitimes de l'autorité et les permissions approprié sont autorisés à injecter des Bundles dans le réseau. Quand l'agent Bundle d'un hôte source reçoit un *Send*. Cette première étape est prise pour

vérifier l'autorisation de l'application demandé et de limiter ou imposer le contrôle d'accès basé sur l'autorisation de l'application source et la politique local. Le choix d'une suite de chiffrement est effectué dans la politique de sécurité spécifique. La construction d'entête de sécurité et son traitement est illustré dans la figure ci-dessus :

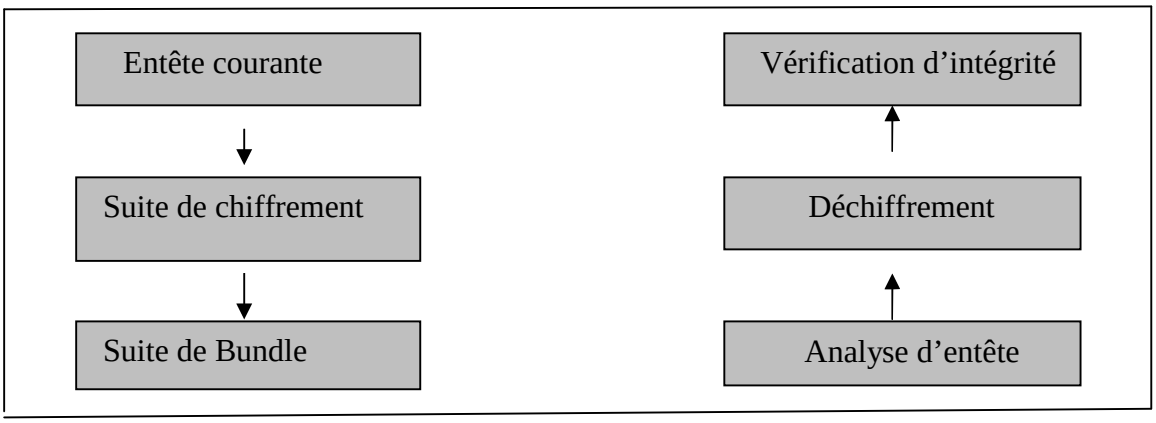

Figure (1-2): Traitement d'un entête de sécurité

Au côté de l'envoi, la première étape est de remplir les champs d'en-tête qui sont définis par la politique de sécurité lors de l'assemblé initiale du Bundle. Une fois que le Bundle est dans la forme finale appropriée, le résultat du calcul de chiffrement est ensuite ajouté à l'ensemble. Cette forme finale sécurisée sera transmise sur le réseau.

Au côté de la réception, les entêtes de sécurité n'ont pas besoin d'être définis par la politique de sécurité. Au lieu de cela, ils sont notés comme les Bundles analysés par les entêtes habituels. Pendant l'analyse d'entêtes des Bundles, le déchiffrement est appliqué à l'ensemble des bundles (avec les mêmes considérations que le scénario d'envoi) et un résultat est calculé.

L'étape finale du processus de réception est de vérifier l'intégrité de l'expéditeur basé sur la valeur de la signature ou le haché calculé et l'envoyé. Si aucune violation de l'intégrité n'a eu lieu, le Bundle est livré à la couche supérieure [35].

IV-1-4-2- Vérification de l'intégrité des données saut par saut :

Le protocole Bundle supporte l'intégrité des données et des services d'authentifications des nœuds le long de chaque saut. Ces services peuvent être fournis sur un lien DTN soit par

l'utilisation de l'entête BAH sur le lien ou par la couche de convergence d'hôte récepteur assurant l'authenticité le long de ce lien.

- Le bundle est envoyé au récepteur.
- A chaque saut l'agent calcule le haché, signe avec sa clé privé et transmis au saut suivant.
- Agent receveur de Bundle vérifie la validité du haché signé envoyé en le comparant avec le haché déterminé.
- Calculer à nouveau le haché signé par l'agent receveur avant de retransmettre le Bundle.

Le fait que l'agent receveur peut décrypter le haché signé, il déduit que la valeur de haché calculé et la valeur de haché reçu sont égales. Alors, cela peut authentifier l'intégrité du Bundle [37].

IV-1-4-3- Manque de détection de réplication au niveau des routeurs :

Les réseaux DTNs n'incluent pas le mécanisme de détection et de rejeter les Bundles répliqués dans les nœuds. Cela veut dire qu'un attaqueur peut espionner le trafic DTN, enregistrer les Bundles légitimes durant la transmission et les injectés plus tard dans le réseau DTN [37]. La réplication ne sera pas détectée jusqu'à ce que le Bundle atteigne le nœud destinataire. La réplication des Bundles injectés dans les réseaux DTNs causera des surcharges sur le chemin jusqu'à ce que le Bundle expire sachant que les liens sont précieux.

IV-1-5- Protection des applications DTNs

La protection des applications DTNs sont assurées par les différents services de sécurité qui sont : La confidentialité des données, l'intégrité des données et l'authentification des terminaux [37].

IV-1-5-1- Confidentialité des données

Les utilisateurs DTNs sont libres d'utiliser le protocole Bundle pour supporter une confidentialité de bout-en-bout pour les données des applications, mais le chiffrement des informations les quelles sont transmises comme des unités de données d'application est accompli par la couche application avant d'être passés à la couche Bundle.

De même, le déchiffrement des unités des données d'application reçus au niveau d'hôte destinatrice doit être accompli par l'application de destinataire plutôt que la couche Bundle de destinataire. La couche application signale à la source ou à la destination, quel algorithme et quelle clé de chiffrement va-t-il utiliser pour chiffrer les données de l'application. Cela permet une flexibilité dans l'utilisation des différents algorithmes.

IV-1-5-2- Intégrité des données et Authentification des terminaux

L'entête PSH du protocole Bundle est utilisé pour assurer une intégrité des données de bout en bout et l'authentification des terminaux pour un Bundle entier, ce qui signifie qu'il prévoit un mécanisme par lequel l'agent destinataire peut vérifier que le Bundle reçu n'a pas été modifié durant le transfert. Il peut également permettre à l'agent destinataire de vérifier que le Bundle est envoyé pour cette destination et non pas à d'autres (la valeur de haché signé a été calculée sur le contenu de champ de la destination dans l'entête primaire du Bundle).

En fin, il peut permettre à l'agent destinataire de vérifier que le Bundle provient d'un terminal ID listé dans le champ de la source (car la valeur du haché signé a été calculée sur le contenu de champ de la source dans l'entête primaire du Bundle). Aussi que, soit le champ de la source ou quelques autres champs d'entête de Bundle ont été utilisé pour rechercher la clé publique approprié pour déchiffrer le haché signé. Car un déchiffrement correct du haché signé signifie que la clé privée correspondante a été utilisé pour signer le haché et que la source connait bien sa clé privée. Cela authentifie que soit les terminaux ID listé dans le champ de la source ou l'entité lié à la clé utilisé pour déchiffrer le haché.

Ces services sont prévus en ayant calculé le haché sur tout le Bundle par l'agent source du Bundle, utilisé la clé privée de la source pour signer le haché et placé la valeur du haché signé dans le champ d'information de sécurité de la charge utile d'entête de sécurité. Dès la réception du Bundle, l'agent destinataire du Bundle applique la clé publique de la source au haché signé, ce qu'il déchiffre sa valeur original au haché non signé.

Le destinataire calcule son haché du Bundle et compare la valeur du haché calculé avec la valeur du haché (actuellement non signé) reçu. Si les deux valeurs sont équivalentes alors le destinataire de la couche Bundle peut s'assurer que le contenu du Bundle n'a pas été modifié depuis son envoie par la source.

Le PSH permet à l'application destinatrice de déterminer d'une manière fiable si le Bundle reçu a été modifié pendant la transition, même dans le cas où un ou plusieurs routeurs DTNs sont compris sur le chemin de la source vers la destination [37].

IV-1-6- Identity-Based Encryption (Cryptage Basé sur l'Identité)

IV-1-6-1- Définition et principe

Dans le cryptage traditionnel, la clé publique de destinataire (Bob) est une chaîne aléatoire sans rapport avec son identité. En revanche, un chiffrement basé sur IBC est un système de cryptographie à clé publique dont n'importe quelle chaîne est une clé publique valide. Par exemple, les adresses électroniques.

Quand l'expéditeur (Alice) désire envoyer un message à Bob, elle doit d'abord obtenir la clé publique de Bob « bob@berkeley.edu », elle chiffre le message en utilisant la chaîne « bob@berkeley.edu » comme clé publique. Il n'est pas nécessaire pour Alice d'obtenir le certificat de la clé publique de Bob. Quand, ce dernier reçoit le courrier chiffré, il contact un tiers de confiance appelé un générateur de clé privée (PKG), pour obtenir sa clé privée après s'authentifier au PKG, afin de déchiffrer le message (voir figure 1). Nous examinons brièvement ci-dessous le principe d'IBC [38] :

Un schéma d'IBC utilise le PKG qui génère un secret maître *s*, et il publie certains paramètres de système *params*, il inclue une clé publique du client et le masque *s*. Le PKG peut avoir de nombreux clients, chaque client a une pièce d'identité ID, qui est simplement une chaîne qu'il identifie.

Les principaux algorithmes d'IBC sont les suivant :

i. ***Configuration:*** Le PKG génère des paramètres du système mondial (Pk_{PKG}) et un maître-clé. Ces paramètres doivent être distribués à tous les hôtes au départ.
ii. ***Extrait:*** Le PKG utilise le maître-clé pour générer la clé privée (Sk_{IDBob}) correspondant à la chaîne d'identité de Bob (ID_{Bob}).
iii. ***Chiffrer:*** La source (Alice) crypte le message (M) en utilisant l'identité publique (ID_{Bob}) de la destination (Bob).
iv. ***Décrypter:*** Bob déchiffre le message (C) d'Alice en utilisant la clé privée correspondante (Sk_{IDBob}) qu'il a obtenu du PKG.

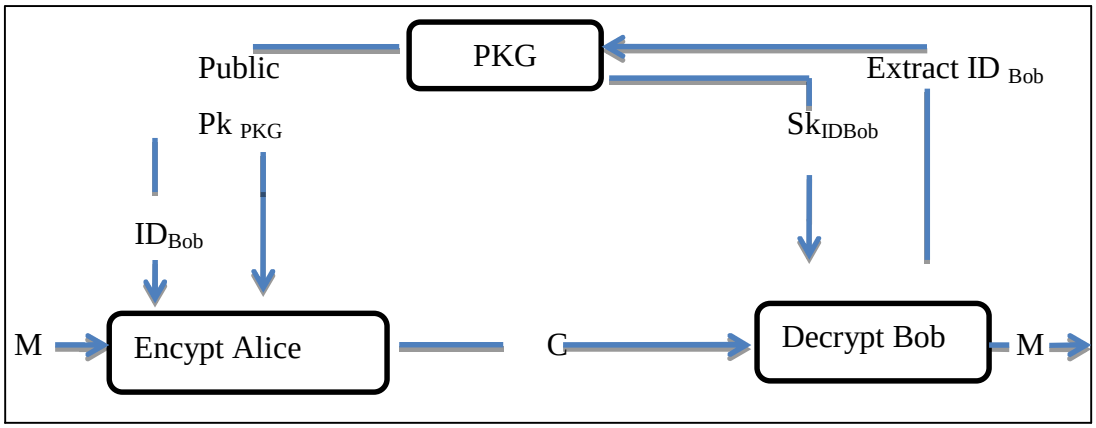

Figure (1-3): Schéma d'algorithmes d'IBC

IV-1-6-2- Phases de transmission Bundle

Les étapes de base nécessaires lors de l'envoi d'un Bundle représentées dans la figure 4 :

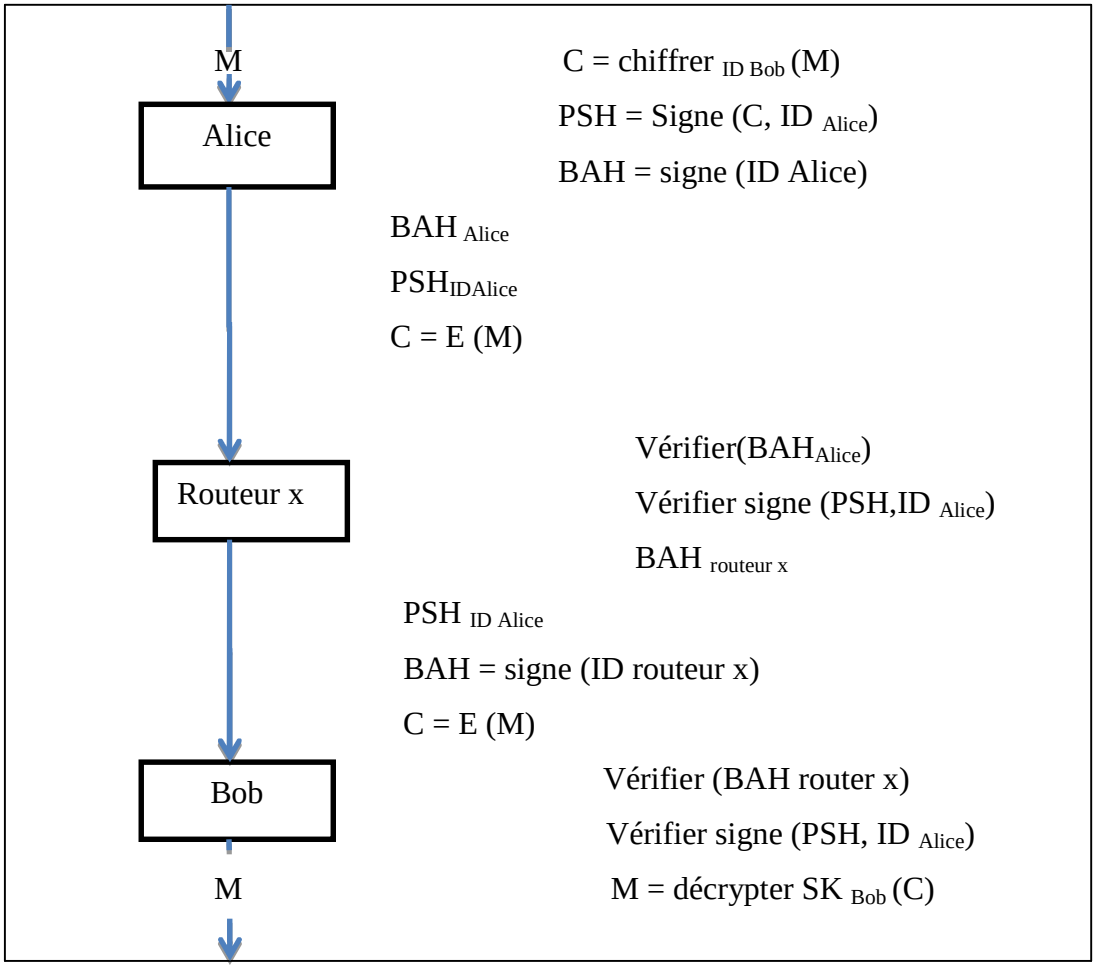

Figure (1-4) : Les étapes de transmission d'un Bundle

Les formats détaillés pour la charge utile de Bundle et la sécurité liés à l'en-tête (en-tête de sécurité de charge utile, PSH et Authentication Header Bundle (BAH) sont discutés dans Section (IV.1.3) [38].

- A la source (Alice):
    1. Pour chiffrer le message Bundle, la source (Alice) utilise d'abord la chaîne d'identité publique de la destination (ID_{Bob}). Ce chiffrement de texte forme la charge utile de paquet Bundle. Nous avons ensuite montré comment cette chaîne (ID_{Bob}) peut être construite.
    2. Ensuite, la source crée le PSH en signant avec sa chaîne d'identité (ID_{Alice}). L'opération de signature nécessite la clé privée correspondant à la chaine d'identité (ID_{Alice}). Cette chaîne d'identité encapsule l'autorisation nécessaire d'un contrôle d'accès. L'intégrité peut être vérifiée et l'identité de la source peut être authentifiée par tous les routeurs.
    3. Enfin, la source crée le BAH.
- Les routeurs intermédiaires:
    1. La première étape consiste à vérifier le BAH pour assurer l'intégrité de la transmission à partir de saut précédent et également pour authentifier le tronçon précédent.
    2. Le routeur peut aussi éventuellement vérifier la signature PSH pour authentifier la source origine (Alice) de Bundle.
    3. Enfin, le routeur crée son propre BAH et transmet le Bundle au prochain saut.
- Au Destinations:
    1. La première étape est de vérifier le BAH afin d'assurer l'intégrité.
    2. Ensuite, la destination peut vérifier la signature PSH pour authentifier la source (Alice) et également pour assurer l'intégrité de bout en bout.
    3. Maintenant la destination détermine qu'elle est la clé de déchiffrement nécessaire pour déchiffrer le texte chiffré (charge utile de Bundle). Si elle ne l'avait pas déjà, la destination demande à son parent PKG la clé privée ($skID_{Bob}$).
    4. La destination peut décrypter le texte chiffré avec la clé secrète.

IV-1-6-2- Inconvénients d'utilisation d'un système IBC

- ***Distribution de clés***: Dans un système IBC, le PKG génère des clés privées pour tous les utilisateurs du système, cela nécessite à l'utilisateur (Bob) de s'authentifier au niveau de PKG, ainsi cette opération nécessite un canal sécurisé à travers lequel il peut envoyer les clés privés aux utilisateurs, ce qui rend la distribution de ces clés est difficile et il peut nécessiter l'utilisation d'un mécanisme supplémentaire de coopération entre le PKG et les utilisateurs.
- ***Diffusion d'informations sécurisées***: Une installation d'IBC à besoin de bootstrap sécurisé de toutes les entités finaux avec les paramètres publics de système du PKG. Cela pourrait devenir un plus gros problème si nous voulons avoir de multiples installations PKG indépendante dans le DTN, comme il n'existe aucun moyen connu pour partager le même ensemble de paramètres du système entre eux.
- ***Révocation d'identité***: En raison de la liaison inséparable entre l'identité d'une entité et sa clé privée dans les systèmes basés sur IBC, il est plus difficile de révoquer la "clé publique" d'une entité, en particulier si l'identité représente juste un nom (comme une adresse e-mail). Cela conduit à l'utilisation de révocation implicite en utilisant des périodes de temps et d'autres informations dans la chaîne d'identité.
- ***Question de normes***: Depuis que nous avons essayé de coder la révocation de contrôle (date, etc) et des identificateurs de contrôle d'accès dans la chaine ID, toutes les entités du DTN doivent se mettre d'accord sur un format commun.
- Le PKG possède la clé principale et dans un grand réseau, il aurait un emploi lourd pour générer des clés privées pour tous les utilisateurs du système.
- Le PKG sait la clé privée de l'utilisateur Bob, c'est à dire, il peut déchiffrer le message destiné à Bob [38].

IV- 2 La Solution proposée

Dans notre cas d'étude, la solution proposée pour assurer la sécurité des Bundles dans les réseaux tolérants aux délais est de prendre en considération la topologie dynamique des nœuds DTNs. En basant sur la théorie des graphes, nous allons proposer un modèle de graphe dynamique et virtuel DVD (Dynamic Virtuel Digraphe) et des techniques de cryptographie basées sur un schéma de distribution de clés publiques qui se repose sur deux canaux sécurisés.

IV- 2-1 Distribution des clés publiques basées sur une cryptographie à deux canaux

Il est en mesure d'utiliser des canaux manuels pour transmettre les informations de vérification, et des canaux sans fils traditionnels pour transmettre la clé publique. Ainsi, la clé publique peut être échangée entre les propriétaires en toute sécurité et remis à d'autres nœuds DTNs par des nœuds intermédiaires.

IV-2-2- Préliminaires

Dans cette partie, nous allons présenter quelques techniques préliminaires de cryptographies basées sur deux canaux, qui servent comme un arrière-plan important pour le schéma proposé à la distribution de clé publique [39].

- L'adversaire peut lire, modifier et retarder tout message envoyé sur le canal à large bande non sécurisé. Il peut aussi empêcher un message d'être livré ou insérer un nouveau message à n'importe quel point dans le temps.
- L'adversaire ne peut que lire, retarder ou supprimer mais il ne peut pas modifier tout message transmis sur le canal étroit authentifié.
- Sur le canal étroit authentifié, le destinataire va savoir qui est l'expéditeur.
- L'adversaire ne peut pas initier un flux, bien qu'il soit capable de renvoyer un message précédemment envoyé.

Le type de canal de communication à deux canaux fonctionne comme suit (voir fig. 5). Nous allons présenter la cryptographie à deux canaux basés sur eTCR (enhanced target collision resistant) qui est une famille d'une fonction de hachage. Soit $H: \{0, 1\}^k \times \{0, 1\}^{<m} \rightarrow \{0, 1\}^n$ est une (T,ε) _eTCR [40] , où m est la taille maximale d'une longueur de message d'entrée (par exemple, $m= 2^{64}$).

Le modèle de communication de cryptographie à deux canaux basée sur la famille de fonction de hachage eTCR entre un demandeur Alice et le vérificateur Bob, se présente comme suit (voir figure 6).

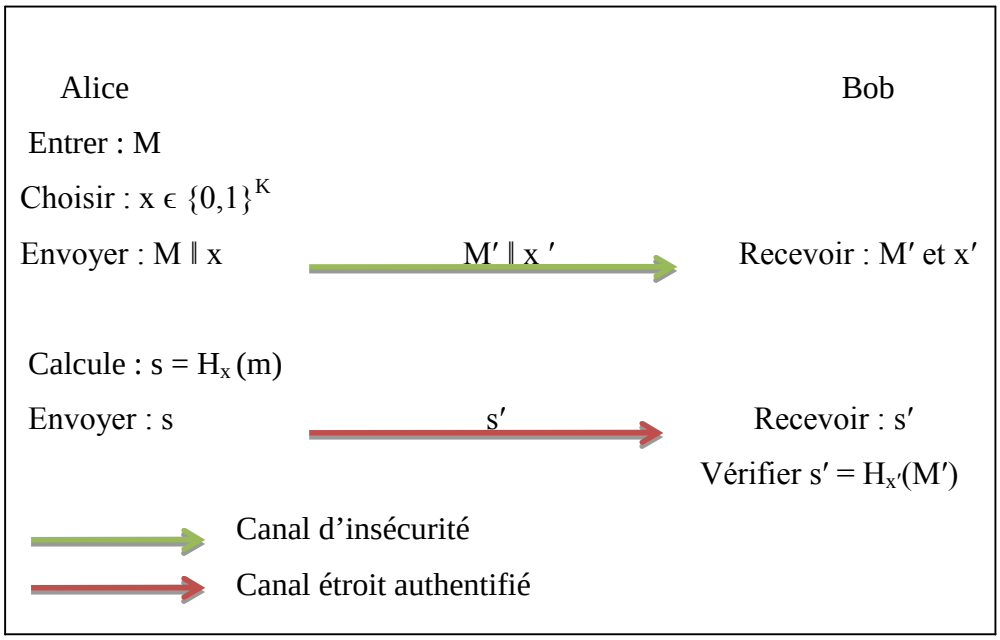

Figure (2-5) : Deux canaux de communication basée sur la fonction de hachage eTCR

(a) A la saisie de message M, Alice choisit d'une manière au hasard la valeur $x \epsilon \{0,1\}^k$ et calcule $s = H_x(M)$.

(b) Alice envoie (M, x) à Bob sur le canal d'insécurité et envoie $s = H_x(M)$ sur le canal authentifié.

(c) Quand Bob reçoit (M′, x′) via le canal d'insécurité et s via le canal authentifié, il sort (Alice, M). Si $s' = H_{x'}(M')$ Bob accepte M. Sinon, il le rejette [39].

IV-2-3- Modèle de distribution de clés

En raison de la caractéristique de déplacement de nœuds DTN. EG (Evolving Graphe) est considéré comme une théorie idéale pour décrire la topologie variante des DTNs dans le temps. Avec cette théorie, un chemin intermittent de la source à la destination peut être exprimé par une série de nœuds et pas de temps. Cependant, il ne peut pas désigner la relation de confiance définit par les clés publiques. Afin de traduire le nombre reçus de clés publiques en toute sécurité à partir des autres sur le degré d'un nœud, nous avons étendu la théorie des graphes en définissant une nouvelle terminologie définit dans la section suivante :

IV-2-3-1- Définitions

- ***Dynamic virtuelle digraphe (DVD)*** : Un graphe virtuel et dynamique peut être défini comme une paire (V, E), où V est l'atout de nœuds dynamiques qui peuvent être en mouvement à tout moment, et E est l'atout du bord virtuel dirigé entre les nœuds E c {(u, v) /u, v ϵ V}. Les paires de nœuds aux extrémités d'un bord virtuel ne sont pas nécessairement d'être typologiquement adjacents [39].
- ***Virtual directed edge*** : Dans un DVD (V, E), l'extrémité virtuelle e ϵ E est un arc d'un nœud u dynamique vers un autre nœud dynamique v, où u,v ϵ V. Il y 'a une arête virtuelle à partir du nœud u au nœud v si et seulement si le nœud u a obtenu la clé publique de v de manière authentifiée. Le bord virtuel dirigé est tout à fait différent de celui dans un graphe traditionnel dans lequel les nœuds sont statiques et la topologie du graphe n'est pas du tout changée. En DVD, les nœuds peuvent se déplacer et la topologie du graphe peut être modifiée à tout moment. Les bords traditionnels entre deux nœuds ne peuvent pas être prospectés, mais le bord virtuel dirigé défini ici, n'est pas affectée par le changement de topologie du graphe [39].
- ***Adjacence virtuelle*** : Deux nœuds sont adjacents s'ils ont un navire de relation adjacent virtuelle. Entre deux nœuds adjacents, un canal sécurisé peut être construit sur des réseaux publics tolérants aux délais.
- ***Virtual out-degree*** : Le degré sortant virtuel d'un nœud donné u, est le nombre des nœuds dont la clé publique a été reçu et cru légitime par le nœud u.
- ***Virtual in-degree*** : Il désigne le nombre de nœuds qui a obtenu et a approuvé la clé publique de nœud u donné.
- ***Virtual mean-degree*** : Dans un DVD, comme un bord d'entrée en un sommet doit être un avantage reliant à un autre, le demi degré (virtual out-degree) et le demi degré virtuelle(virtual in-degree) sont égaux. Il y a donc, le degré moyen virtuelle in-degree ou out-degree de tous les nœuds DTN.

- ***Chemin d'accès virtuel*** : Un chemin d'accès virtuel à partir de nœud u_I à u_J, à travers au moins un nœud intermédiaire v_1, v_2,… v_k est une séquence connexe de bords

virtuels dirigées à partir de nœud u_I et terminant à un nœud u_J, où u_i, u_j, v_1, v_2, . . . , $V_k \in V$. Si il existe un chemin d'accès virtuel ui, v_1, v_2, v_k, u_j du nœud u_i au u_j, sa indique que la clé publique du nœud uj est obtenue et reconnu par v_k. La clé publique du nœud vk est obtenue et reconnu par v_{k-1},….,la clé publique du nœud v_1 est obtenue et reconnu par u_i .

- ***Virtual Connected Component*** : Un composant virtuelle connecté c'est des nœuds définis V′, V′∈V, dans lequel il est au moins un chemin virtuel entre toute paire de nœuds u et v [39].

IV-2-3-2- Schéma proposé pour la distribution des clés publiques

- ***Terminologie et Hypothèses*** :

Dans ce paragraphe, nous définissons quelques terminologies et faire des hypothèses supplémentaires suivantes :

i. Les terminologies:

- Pki: la clé publique du nœud i d'un DTN.
- Ski: la clé privée du nœud i d'un DTN.
- IDI: l'identification du nœud i.
- $H_x()$: La fonction de hachage eTCR .
- ‖: La chaîne de caractère de concaténation.
- ϴ: paramètre du système.

ii. Hypothèses:

- Lorsque les nœuds DTN se déplacent dans la proximité géographique proche les uns des autres, il est possible d'utiliser un manuel canal, comme le canal sans fil d'habitude. En d'autres termes, le modèle de cryptographie à deux canaux de communication peut être utilisé pour authentifier l'intégrité du message.
- Chaque nœud DTN a généré sa propre paire de clés {pk, sk}.
- Chaque nœud DTN est initialisé avec la fonction de hachage ETCR et l'algorithme de signature.
- Chaque nœud DTN maintient une liste de clés publiques valides (VPL). Le stockage légitime des clés publiques, les informations de leurs propriétaires, et

une liste de révocation de clés publiques (PRL), le stockage Key ID (ID de la clé peut être calculée par une variété de méthodes, par exemple :
Key ID = Public Key mod 2^{64}) des clés publiques qui ne sont pas expirées, mais ont été révoqués.

- Les nœuds DTN en proximité géographique souhaitent échanger leurs clés publiques.
- Chaque nœud DTN souhaite stocker, transporter et transférer des clés publiques directement à partir de leurs propriétaires.

❖ ***La distribution des clés :*** Quand un nœud détecte qu'il y a d'autres nœuds au sein de sa gamme manuel de communication, il restera une certaine quantité de temps, 120s par exemple, pour échanger des clés publiques (voir Fig. 6). La figure 6 montre qu'il y a trois nœuds DTN au sein de la gamme manuelle de communication les uns des autres. Ces nœuds peuvent échanger leurs clés publiques sur des canaux sans fil et transmettre des messages de confirmations sur les canaux manuelles. Ainsi, lorsque les clés publiques sont directement de leurs propriétaires, en exploitant des techniques de cryptographie à deux canaux et selon nos hypothèses que les nœuds rencontrés devraient échanger leurs clés publiques valables mutuellement, puis la légalité des clés publiques peut être confirmée facilement. Toutefois, lorsque les clés publiques ne viennent pas de leurs propriétaires, il y a quelques difficultés à confirmer la légitimité des clés publiques. Par exemple (voir fig. 7)

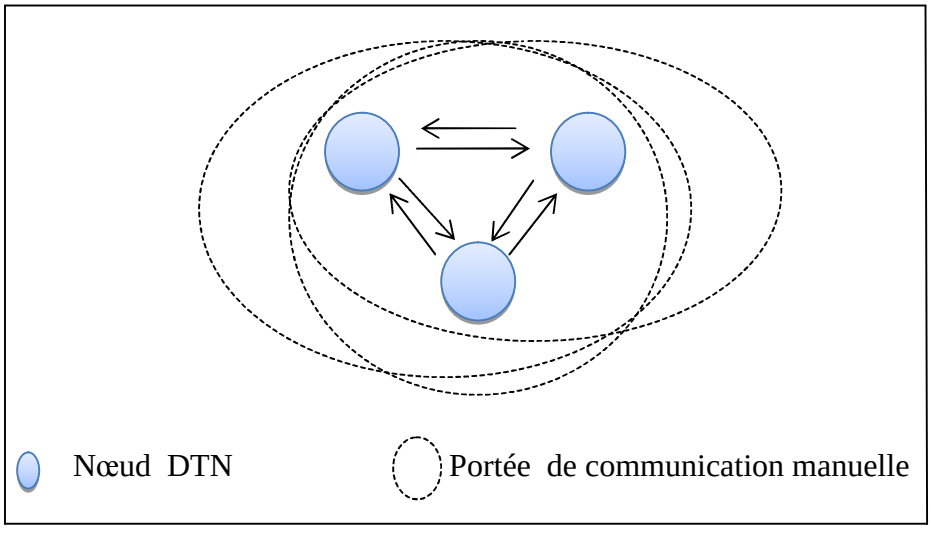

Figure (2-6) : Communication manuelle

Les nœuds h, i et l échangent leurs clés publiques à l'instant t. Chacun d'eux vas ranger et transporter les deux clés publiques d'autres nœuds quand ils se déplacent autour de la zone fermée. Ainsi, au moment (t +µ), les clés publiques des nœuds h et l peuvent être du nœud i et les clés publiques des nœuds h et i peuvent être du nœud l. Dans ce cas, nous disons que les clés publiques sont de leurs transporteurs. Il sera un grand défi pour authentifier ces clés publiques qui sont de leurs transporteurs, et non de leurs propriétaires.

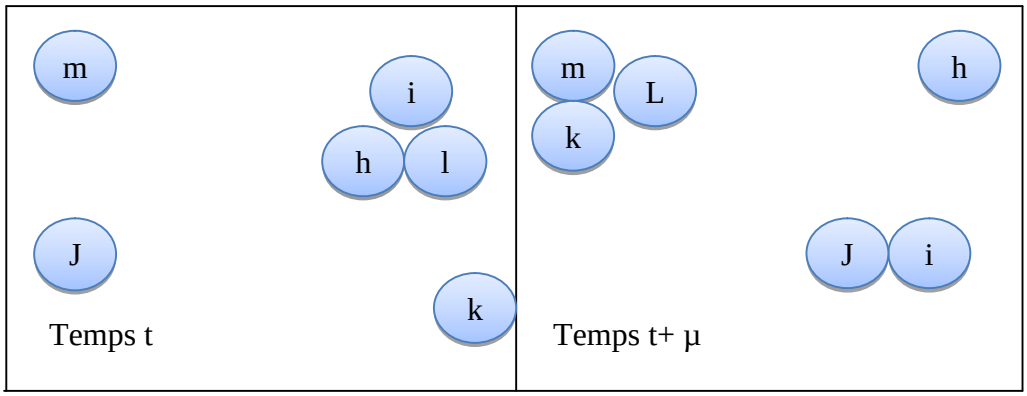

Figure (2-7) Délivrance des clés

Dans cette partie, nous discutons d'un régime de distribution des clés publiques comme suit : Tout d'abord, nous décrivons le processus d'échange de clés publiques entre leurs propriétaires, d'autre part, nous discutons de la conception d'échange de clés publiques entre leurs transporteurs, enfin, nous présentons une méthode d'approbation de clé publique afin d'identifier les clés publiques qui ne viennent pas directement de leurs propriétaires [39].

IV-2-3-3- Echange de clés publiques entre les propriétaires

Supposant qu'il existe deux nœuds, Alice et Bob, chacun d'eux est équipé uniquement de leur propre clé publique, respectivement, et ils sont dans le domaine de la communication manuelle. Ils peuvent obtenir et vérifier les clés publiques des autres à partir des procédures suivantes (figure 8).

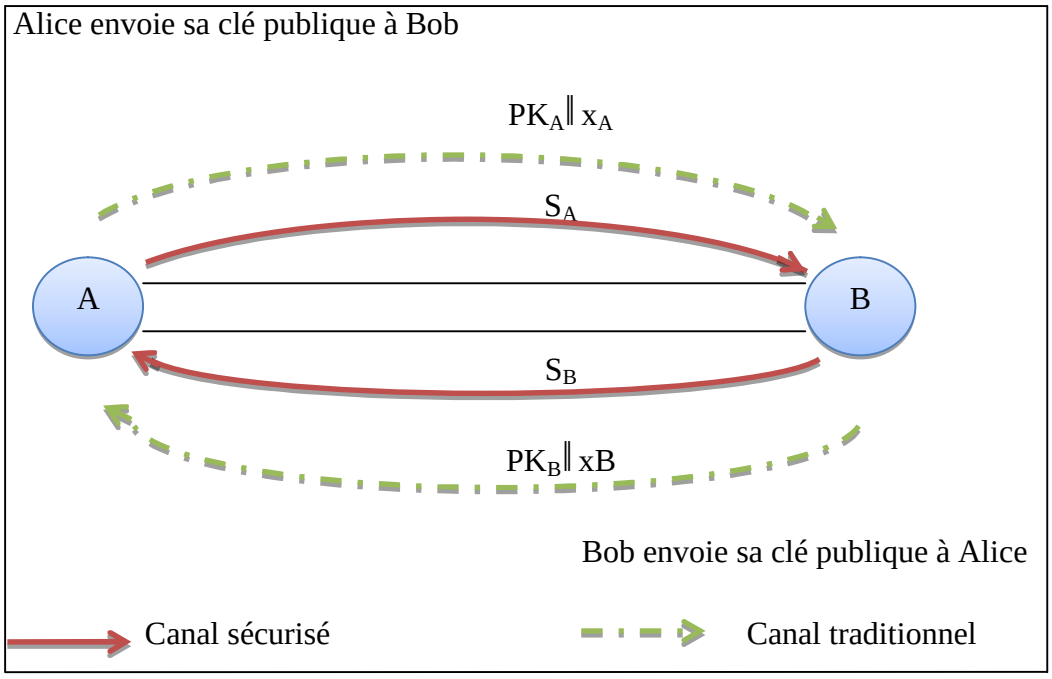

Figure (2-8): Echange de clés publiques entres les propriétaires

a) L'expéditeur, Alice, sélectionne au hasard une valeur aléatoire $x_A \epsilon \{0,1\}^K$ et l'utilise comme la clé de l'entrée de hachage. Dans la pratique, nous pouvons transformer x en utilisant une fonction de hachage.

b) Alice calcule $S_A = H_{XA}(PK_A)$.

c) L'expéditeur, Alice, concatène sa clé publique PK_A avec x_A, et il l'envoie au destinataire Bob sur le canal sans fil traditionnel.

d) Alice envoie à Bob S_A sur le canal sécurisé.

e) A la réception du message $PK'_A \| X'_A$ et S'_A à partir de Alice sur le fil traditionnels et les canaux sécurisé, respectivement, Bob vérifie l'équation $S'_A = H_{X'A}(PK'_A)$.

Si l'équation est vérifié, il accepte la clé publique PK_A d'Alice et lui donne directement un drapeau de croyance, sinon, il la rejette.

f) Afin que Bob envoi sa propre clé publique à Alice, il suivra les mêmes procédures que Alice [39].

IV-2-3-4- Echange de clés publiques entre les transporteurs : Dans ce paragraphe, nous allons discuter de mécanisme de la distribution de clés publiques entre ses transporteurs. Supposant deux nœuds, Alice équipé de clés publiques $C_1's$, $C_2's$,…. , $C_m's$, et nœud Bob équipé de clés publiques $D_1's$, $D_2's$,…. , $D_n's$ sont dans leur zone de communication manuel et l'échange des clés publiques réalisée avec eux. Dans la figure 9, nous allons montrer en détail comment échanger et vérifier les clés publiques entre les transporteurs, et la différence avec l'échange de clé publique entre les propriétaires.

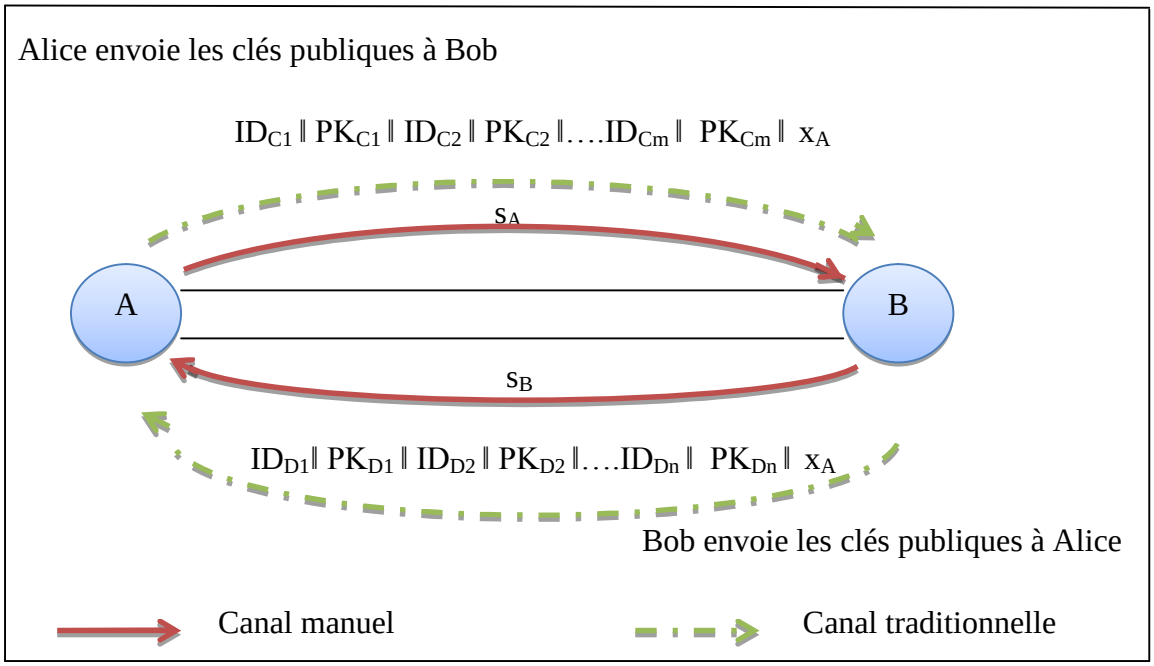

Figure (2-9) : Echange de clés publiques entre les transporteurs

(a) Alice choisit au hasard une valeur aléatoire $x_A \in \{0,1\}^K$ et il l'utilise comme une clé de l'entrée de hachage.

(b) Alice concatène ID_{C1}, PK_{C1}, ID_{C2}, pk_{C2},…., ID_{Cm}, pk_{Cm}, ensemble: $S = ID_{C1} \| pk_{C1} \| ID_{C2} \| pk_{C2} \| \ldots ID_{Cm} \| pk_{Cm}$.

(c) Alice calcule $s_A = H_{XA}(S)$.

(d) Alice envoie $S \| x_A$ à Bob sur le canal classique sans fil.

(e) Alice envoie à Bob s_A sur le canal manuel.

(f) A la réception de $S' \| x'_A$ sur le canal sans fil et s'_A sur le canal manuel, Bob vérifie l'équation $s'_A = H_{X'A}(S')$. Si l'équation est vérifiée, il stocke ces clés publiques, sinon, il rejette ces clés.

(g) Afin que Bob envoi la clé publique qu'il portait à Alice, il suivra les mêmes procédures que Alice.

IV-2-3-5- Clé publique d'approbation

Dans la partie ci-dessus, nous allons discuter d'une autre méthode de distribution de clés publiques entre les transporteurs. Cependant, pour déterminer la validité de la clé publique n'est pas une affaire facile si elle ne vient pas de son propriétaire et les transporteurs peuvent générer une paire de clés et de déclarer que le propriétaire de la clé publique est Carol, par conséquent, nous devons développer une technique d'identification afin d'aider les nœuds DTN à déterminer les propriétaires réels de clés publiques.

Supposant que chaque nœud se déplacera dans la zone fermée et tous les deux nœuds peuvent se rencontrer. Ainsi, étant donné les deux nœuds donnés, dit Bob et Carol, il est tout à fait possible à Bob de recevoir la clé publique de carole PK_{CAROL} auprès des transporteurs différents, C_1, C_2,…et C_k. Ces transporteurs peuvent être des amis de Bob, chacun a un niveau de confiance différent et Bob pourra attribuer une valeur de poids ti au transport Ci (i = 1, 2, …., k), de sorte que Bob peut évaluer la clé publique Pk Carol par la méthode suivante [39]:

```
Begin
    T=0; (Le point de confiance globale)
    Si  pk carrol.KeyID ∉ PRL   alors
        Pour (i=1, i< = K, i++) {
            Si  Pk_Ci.Flag (Drapeau) = = " DIRECT"
                T = T + ti  (Le point de confiance locale) ;
    Fin si }
        Si  T > ɵ   alors,  Pk carol. flag = =  " APROVAL"   Fin si.
Fin.
```

Si l'indicateur d'une clé publique a été fixé à " APPROVAL", cela signifie que Bob est convaincu que la clé publique est de Carol et elle n'est pas en PRL. Donc un bord direct virtuel de Bob vers Carol sera créé.

IV-2-3-6- Révocation de la clé publique

Dans la technique d'approbation, nous avons besoin de déterminer si la clé publique reçue est dans la liste PRL ou non. Par conséquent, une question cruciale de la gestion des clés publiques dans tous les DTNs est de s'assurer que la clé publique reçue est sur la liste révoquée. En fait, les systèmes de distribution et la technique d'approbation présentées dans ce précède qui sont également applicables à la distribution du message de révocation de la clé publique. Nous allons discuter dans deux scénarios différents comme ci-dessous:

Tout d'abord, un nœud DTN peut fournir un ID de clé de sa propre clé publique révoquée directement à l'ensemble de ses rencontres quand il se déplace autour de la zone fermée. Dans ce cas, nous pouvons adopter la méthode de distribution pour l'échange de clé publique entre les propriétaires tels que décrits dans la section IV.2.2.3 en remplaçant pk avec ID de la clé. A la réception de l'ID de clé, le nœud récepteur va le vérifie. Si il est correcte, le nœud récepteur met ID de clé (KeyID) de récepteur et l'identifiant de clé du propriétaire dans son PRL.

Deuxièmement, un nœud DTN peut porter le reçu d'ID de clé révoqué pour d'autres nœuds DTNs en utilisant la méthode de distribution pour l'échange de clé publique entre les transporteurs tels que décrits dans la section IV.2.2.4. Dans ce cas, nous venons de remplacer Pk_{Ci} avec $KeyID_{Ci}$. À la réception des identifiants de clé révoqués par des transporteurs, nous pouvons appliquer la technique d'approbation tel que discuté dans la section IV.2.2.5 afin d'assurer que la clé publique a été révoqué. Par exemple, nous avons mis ID de la clé de Carol (KeyID) la clé publique révoquée et l'ID de Carol (ID_{CAROL}) dans PRL. Si la valeur de confiance T, a dépassé la valeur de seuil ɵ. Pour des raisons de sécurité, le message de révocation doit être propagé plus vite que la clé publique, ce qui peut être fait facilement par une portée d'une plus grande qualité de service pour la révocation de message lors de sa transmission. Parce que l'effet de livrer les messages urgents, peuvent obtenir une vitesse plus rapide que la diffusion des messages généraux si la couche des nœuds DTN peut obtenir

des récompenses plus importantes par l'acheminement de premier puis l'acheminement du dernier [39].

IV-2-4- Analyse de la sécurité

Ce n'est que lorsque la clé publique est distribuée en toute sécurité et les signatures générées par sa clé privée correspondante peut être vérifiée, un canal sécurisé sur le réseau DTN basé sur le crypto-système de clé publique peut être construit. Par conséquent, la sécurité du système de distribution de clé publique est très cruciale.

IV-2-4-1- Echange de clés publiques entre les propriétaires

Dans ce cas, la technique à deux canaux sera de garantir la légitimité des clés publiques que chaque utilisateur détient. Dans notre situation où la cryptographie à deux canaux est utilisée, la clé publique et la valeur aléatoire x_A peut encore être lu, retardé et modifié. Toutefois, la valeur s_A envoyé sur le canal manuel ne peut pas être modifié, même si elle peut être lue, retardés ou supprimés. En outre, le malveillant ne peut pas initialiser une session sur le canal authentifié.

Ainsi, lors de la réception d'une clé publique, le destinataire connaîtra qui est le propriétaire de la clé et si la clé publique est authentique, la méthode similaire peut également être appliquée pour échanger des messages publics de révocation de la clé publique entre les propriétaires. En conséquence, le récepteur peut identifier qui entame la conversation et quand les clés publiques sont distribuées, et aussi de garantir l'authenticité du message de révocation en utilisant la technique à deux canaux. Par conséquent, l'authentification et l'intégrité de clé publique de révocation peut également être garantie.

IV-2-4-2- Echange de clés publiques entre les transporteurs

Une des hypothèses retenues dans le schéma proposé est que chaque nœud DTN portera les clés publiques reçues dans sa propre gamme de communication manuel, et transmettre ces clés à d'autres nœuds qu'il peut rencontrer dans le futur. Au cours de la transmission de la clé publique de son support à des destinataires, l'authenticité de la clé publique peut être garantie en employant la technique de cryptographie à deux canaux, mais, nous ne pouvons pas empêcher un transporteur malveillant de se propager de fausses clés publiques.

Par exemple, si quelqu'un génère une paire de clé publique / clé privée, et déclare qu'elle appartient à Alice, elle pourrait avoir deux conséquences:

- Toutes les informations chiffrées avec cette clé publique peuvent être lu par le transporteur malveillant.
- Le transporteur malveillant peut changer l'identité d'Alice en signant avec sa clé privée correspondante.

Pour résoudre ce problème, nous avons développé la technique d'approbation de la clé publique comme dans la section IV.2.3.5.

Nous allons signer un poids de confiance t_i pour la porteuse donnée C_i (i = 1,2, … ,K). La valeur du poids de confiance t_i est déterminée par le destinataire basé sur la clé publique sur un certain rapport social entre des nœuds DTN. Si $T>\theta$, où θ est un paramètre du système qui représente un ensemble d'expériences, $T = \Sigma$ ti, i ϵ (1, 2,. . . , K) la clé publique donnée peut être reconnu par le destinataire. En conséquence, l'attaque par l'adversaire peut être défendue, si un nœud malveillant veut ajouter assez de poids de confiance en vue de générer une paire de clés publique / privée et de se propager plus vite, il faut tricher assez d'amis et de payer plus cher pour les relais intermédiaires. Un coût potentiellement énorme risque de décourager et de dissuader les agresseurs de fausses clés.

Dans le cas où un nouvel utilisateur se connecte au réseau, le nouvel utilisateur sera progressivement accepté par la communauté et le poids de confiance de sa clé publique augmentera en conséquence. Lorsque la clé publique est approuvée, un bord virtuel dirigé sera construite à partir de son récepteur au propriétaire de la clé publique, puis un chemin virtuel est généré à partir du récepteur au propriétaire de la clé publique à travers le support. Ci-après, un canal sécurisé entre le propriétaire et le récepteur peuvent être construits.

De même, si un message de révocation de clé publique appartient aux transporteurs plutôt que le propriétaire, en utilisant la méthode décrite dans la section IV.2.3.6. Le récepteur peut déterminer si le message de révocation est digne de confiance par la technique de l'approbation tel que décrit dans la section IV-2-3-5. L'authenticité du message de révocation peut être garantie par la technique de deux canaux. L'attaque de la collusion peut être évitée par la mise en paramètres appropriés t_i et θ basé sur certaine information sociale.

Conclusion

Dans ce dernier chapitre, nous avons proposé un modèle DVD pour étude de la distribution de clés publiques en étendant la théorie des graphes et nous avons présenté un schéma de distribution de clés publiques pour les DTNs basé sur une cryptographie à deux canaux.

Le schéma proposé peut être utilisé pour l'échange de clés publiques entre les propriétaires et entre les transporteurs en exploitant notre méthode d'approbation de la clé publique**.** Grace à cette méthode d'échange des clés publiques et des messages, le destinataire assure l'authentification et l'intégrité des messages mais le problème qui reste, l'expéditeur ne peut pas savoir si le message est reçu ou pas.

Conclusion et perspectives

Ce travail nous a permis d'apprendre et d'avoir une connaissance majeure sur un type de réseaux important dans nos jours, dite les réseaux tolérants aux délais (DTN).Tel que, un tel type de réseaux offre un tout nouveau développement dans le monde de la recherche sur les réseaux, il offre l'espoir de connecter des entités qui ont étaient incapables de communiquer entre eux, ou cela rend énormément couteux. De même, connaitre un domaine revient à connaitre son véritable mode de fonctionnement.

Afin d'atteindre cet objectif nous avons d'abord tenté d'aborder les limites présentées par les protocoles standards Internet, puis l'environnement des DTNs, tel que ces réseaux sont principalement caractérisés par lefait que la connectivité entre les entités soufre de rupture, nous observons des liens intermittents, des taux d'erreurs élevés et des délais de propagation à la fois longs et variables. Ensuite, nous avons détaillé la couche protocolaire et expliquer le principe sur lequel est fondé le protocole Bundle. A l'échelle du réseau, l'hétérogénéité des liens et des piles de communications font en sorte que, les solutions proposées pour l'Internet échouent. La classe des réseaux tolérants aux délais s'offre pour principal objectif la résolution de ce problème.

Puis nous avons enchainer une partie importante pour les réseaux tolérants aux délais qui s'agit de détailler les algorithmes de routage pour but de sélectionner les meilleurs chemins à suivre et garantir les meilleurs performances de livraison pour les messages, puis de classifier les nombreux protocoles existants à utilisés afin de réaliser un routage correct dans les environnements intermittents.

La dernière partie constituant notre centre d'intérêt, qui porte sur les problèmes de la sécurité. Ce dernier consiste en un problème d'une très grande importance dans le monde des réseaux tolérants aux délais. En effet, une bonne stratégie de sécurité appliquée sur un environnement intermittent forme la clé de la bonne transmission de données. Actuellement, il existe plusieurs stratégies cryptographiques qui sont adoptées pour atteindre les bonnes propriétés de sécurités telles que la confidentialité, l'authentification et l'intégrité des données.

Conclusion et perspectives

Notre principale contribution s'insère donc à ce niveau où la mobilité des nœuds dans ce type de réseaux DTNs, tel que nous l'avions montré dans le premier chapitre. Cela nous a permet de penser à une nouvelle solution d'infrastructure sécurisée en prenant compte beaucoup plus la mobilité des nœuds. Pour cela, nous avons basé à étendre la théorie des graphes pour proposer un graphe dynamique et virtuel (DVD) afin de représenter les nœuds d'un DTN et d'utiliser une cryptographie basé sur deux canaux sécurisé. Un canal traditionnel sans fil pour transmettre les clés publiques et un deuxième canal étroit authentifié pour transmettre des messages de confirmations. Grace à cette méthode nous avons arrivé à proposer un mécanisme d'authentification efficace pour atteindre les principaux services de sécurité pour les réseaux tolérants aux délais.

Avec notre cas d'étude, une des perspectives qu'on envisage est de faire une étude d'un cas réel, de bien étudier ces caractéristiques et d'implémenter la solution DVD afin d'assurer les différents services de sécurité et d'élaborer de nouvelles théories sur le DVD, de plus en vérifiant notre solution de distribution de clé publiques dans les différents environnements DTNs.

1. ***La couche physique :*** Elle est chargée de transmettre les signaux physiques entre les différents systèmes, les services correspondant à cette couche sont l'émission et la réception de bits.
2. ***La couche liaison de données :*** Elle gère les communications entre deux systèmes directement relies par un support physique, elle manipule des paquets de bits appelés trames, contrôle leur synchronisation et détecte les erreurs.
3. ***La couche réseau :*** Elle est chargée pour gérer les communications entre deux systèmes, elle gère les communications d'un système source à un système destination. Cela inclut le routage, l'adressage des paquets et leur séquencement.
4. ***La couche transport :*** Elle gère les communications entre les processus, c.à.d. le transport des données d'une application à une autre. En plus elle est chargée de gérer, entre autre, les erreurs de transmissions.
5. ***La couche session :*** Elle gère la synchronisation des échanges au travers de l'ouverture, du maintien et de la fermeture de connexions.
6. ***La couche présentation :*** Cette couche code les données en chaines d'octets pour qu'elles soient transmises, ainsi elle est responsable de la syntaxe des informations transmises et assure l'indépendance des données par rapport au format utilisé par le réseau.
7. ***La couche application :*** Elle est l'interface avec l'utilisateur.

- ***Hôte :*** Il envoi et/ou reçoit les Bundles, mais il ne les diffuse pas [Annexe A]. Ce qui nécessite un stockage persistent durant les longs délais dans lesquels les Bundles seront alignés jusqu'à ce que les liens soient disponibles.

- ***Passerelle :*** Elle diffuse les Bundles entre deux ou plusieurs régions DTNs et peut optionnellement jouer le rôle d'un hôte, elle opère sur la couche transport et se base sur la commutation de messages plutôt que sur la commutation de paquets. Cependant, elle fournit l'interopérabilité entre des protocoles spécifiques pour une région et ceux qui sont spécifiques pour une autre.

- **Routage :** Le routage est le cœur de chaque réseau de donnée faisant passer les informations dans un inter-réseau, de la source à la destination [17].

- **Routeur :** Un routeur est un dispositif matériel ou logiciel qui examine les paquets rentrants (couche Internet dans le modèle TCP/IP), il permet de relier un réseau à un autre. Le routeur est donc responsable de transmission des paquets à travers les différents réseaux [17].

- **Fonctionnement d'un routeur :** Un routeur exécute en parallèle 3 processus distincts: la commutation**,** le routage et la gestion des paquets. Les paquets commutés contiennent des données à destination d'hôtes distants. Tel que, ces paquets sont reçus sur un port d'entrée i, transféré vers un port de sortie j et enfin émis sur ce port j. Le transfert nécessite la consultation d'une table de routage qui indique le port de sortie correspondant à l'adresse de destination du paquet [17].

- **Table de routage :** C'est un regroupement d'informations permettant de déterminer le prochain routeur à utiliser, pour accéder à un réseau précis sur lequel se trouvera la machine destinatrice [17].

- **Protocole de routage** : Le protocole de routage est un type de communication établis entre les routeurs. Il permette à un routeur de construire, tenir et partager des tables de routage avec d'autres routeurs sur les réseaux qu'ils connaissent ainsi que sur leurs proximités.

- **Système autonome :** Un system autonome est constitué d'un ensemble de routeurs situés sous le même domaine d'administration

- **Protocole de routage à vecteur de distance :** Les protocoles de routage à base de vecteur de distance tirent leur nom du fait qu'il est possible de calculer les plus courts chemins quand la seule information échangée est un vecteur de distance. En outre, l'information n'est échangée qu'entre routeurs adjacents. Initialement, chaque routeur ne connait que le coût de ses propres liaisons. Ces information sont stockées dans sa table de routage, chaque entrée de cette table contient le prochain routeur où envoyer le paquet, afin d'atteindre sa destination finale. Le protocole de routage à vecteur de distance est une version distribuée de l'algorithme Bellman-Ford [18]. En effet, il est basé sur l'échange périodique d'informations de routage entre routeurs adjacents,

quand un routeur reçoit une information de routage de son voisin, il effectue les traitements suivants :

Pour chaque entrée du vecteur de distance reçue il vérifie :

- Si l'entrée n'est pas dans sa table, il la rajoute.
- Si le cout de la route proposée plus le cout de la route pour atteindre le voisin est plus petit que celui de la route stockée, alors il met à jour sa table de routage pour prendre en compte cette nouvelle route.
- Sinon, il n y'a pas de changement.

Le protocole de routage à vecteur de distance force les routeurs à diffuser périodiquement des informations de routage. En revanche, un routeur détectera un problème quand il ne recevra pas pendant une période de temps fixée (Time Out) des informations de routage de l'un des routeurs adjacents, il mettra à l'infini les entrées correspondant à ce routeur dans sa table de routage et poursuivra l'algorithme [18].

- **RIP *(Routing Protocol):*** RIP est un exemple populaire de protocole de routage à base de vecteur de distance, il est principalement destiné à une utilisation en tant qu'IGP (*Interior Gateway Protocol*) dans les réseaux raisonnablement homogènes de taille modérée. Ce protocole est limité à 15 sauts. En effet, une métrique de 16 signifie l'infini, cela peut paraitre petit, mais il permet de faire converger rapidement l'algorithme lorsqu'un routeur tombe en panne. Ses principales caractéristiques sont les suivantes [17]:
  - Il utilise le nombre de sauts comme mesure de sélection d'un chemin.
  - Si le nombre de sauts pour un réseau est supérieur à 15, le protocole RIP ne peut pas fournir de route à ce réseau.
  - Par défaut, les mises à jour de routage sont diffusées ou multi-diffusées toutes les 30 secondes.

- **Protocole de routage à état des liens**

L'algorithme de routage à vecteur de distance peut conduire à des boucles qui ralentissent sa convergence. Cela est dû au fait que les routeurs ont une connaissance partielle de la topologie du réseau. Pour éviter la production des boucles dans un protocole de routage

à état des liaisons, il faut que chaque routeur ait une connaissance complète de la topologie du réseau.

- **OSPF (*Open Shortest Path First*):** OSPF est un protocole de routage interne de type "état des liens". Il converge aussi rapidement en cas d'apparition ou de disparition d'un lien. Par contre, il est considérablement plus complexe que RIP. OSPF est utilisée dans des réseaux de grande taille (une centaine de routeurs).

- **Protocole de routage à Path vector :** L'information de routage échangée dans ce type de protocole doit contenir le chemin (Path) complet de tous les numéros d'un système autonome (ASN est un identifiant unique d'un système autonome dans Internet) par lesquels transite une annonce de route. Cette liste ASN est mémorisée dans un attribut ASPATH.
  - **BGP *(Border Gateway Protocol*):** BGP est un protocole de routage à base de Path Vector, il permet d'échange des routes entre les différents systèmes autonomes, cet échange se fait dans une session TCP de port 179 établie entre deux routeurs voisins. Ces routeurs négocient des paramètres de session (version de protocoles, time out…) en utilisant des messages « OPEN ».

- **Fragmentation de messages** : Lors de la transmission des messages, ces derniers sont fragmentés, c'est-à-dire que les différents fragments sont routés le long de différents chemins. Cette technique est utilisée afin de réduire les délais de transmission et d'améliorer la charge entre les différents liens.

- **Les couches attaquées dans les DTNs :**

  Les principales couches qui sont attaquées par les malveillants sont [35] :

  - **Exploits la couche réseau :** On peut attaquer un réseau à la tentative de réorienter le trafic ou de créer le déni de service (DoS) ou de perturber le réseau.
  - **Exploits la couche transport :** Le protocole de transport Licklider définit des extensions de sécurité pour LTP, généralement prévu pour aider à combattre des attaques DoS. Celles-ci incluent des options pour la mise en œuvre de l'authentification cryptographique d'un segment.
  - **Exploits la couche application :** La couche application semble être la couche du choix pour exploiter un système au moins dans l'Internet comme démontré par la vaste quantité de logiciel d'anti-virus et d'anti-spyware. Très probablement c'est parce qu'il fournit le plus grand profit monétaire (par exemple vol d'identité, vol de l'information). En outre, il se peut être le secteur le plus facile pour attaquer, en raison, d'un nombre vaste d'applications
  - **Exploits d'exécution de Code :** La nature du protocole bundle ajoute les vulnérabilités potentielles supplémentaires qui devraient être adressées. En raison, des nombreux champs de longueur variable, l'analyse de champ texte sur le terrain, et d'autres opérations bundle de traitement, il peut y avoir des risques dû aux implémentations de bugs (par exemple les dépassements de tampon) qui n'existent pas avec les champs de largeur fixe et les formats binaires (par exemple IP).Ils peuvent être probablement des attaques sur l'hôte, l'unité centrale de traitement et la mémoire en envoyant les bundles et les dossiers administratifs de manière malveillante. Les implémentations doivent considérer avec soin les ressources, dont ils exposent les algorithmes pour les gérer, y compris le stockage local, l'accès à la liaison, la mémoire pour la gestion des contacts et les minuteries,... etc. l'expérience Internet montre qu'il est souvent possible d'exploiter les décisions d'implémentation de ces algorithmes, si le protocole ne les protège pas.

❖ **Déni de service :**

On distingue habituellement deux types de dénis de service :

- Les dénis de service par saturation, consistant à submerger une machine de requêtes, afin qu'elle ne soit plus capable de répondre aux requêtes réelles
- Les dénis de service par exploitation de vulnérabilités, consistant à exploiter une faille du système distant afin de le rendre inutilisable.

Le principe des attaques par déni de service consiste à envoyer des paquets IP afin de Provoquer une saturation ou un état instable des machines victimes et de les empêcher ainsi d'assurer les services réseau qu'elles proposent. Lorsqu'un déni de service est provoqué par plusieurs machines, on parle alors de « déni de service distribué » (noté DDOS pour Distributed Denial of Service). Les attaques par déni de service distribué les plus connues sont Tribal Flood Network (notée TFN).

❖ **Définition et types de DVD :**

- ***Adjacence virtuelle*** : Deux nœuds sont adjacents s'ils ont un navire de relation adjacent virtuelle. Entre deux nœuds adjacents, un canal sécurisé peut être construit sur des réseaux publics tolérants aux délais.
- ***Virtual out-degree*** : Le degré sortant virtuel d'un nœud donné u, est le nombre des nœuds dont la clé publique a été reçu et cru légitime par le nœud u.
- ***Virtual in-degree*** : Il désigne le nombre de nœuds qui a obtenu et a approuvé la clé publique de nœud u donné.
- ***Virtual mean-degree*** : Dans un DVD, comme un bord d'entrée en un sommet doit être un avantage reliant à un autre, le demi degré (virtual out-degree) et le demi degré virtuelle(virtual in-degree) sont égaux. Il y a donc, le degré moyen virtuelle in-degree ou out-degree de tous les nœuds DTN.

- ***Chemin d'accès virtuel*** : Un chemin d'accès virtuel à partir de nœud u_I à u_J, à travers au moins un nœud intermédiaire v_1, v_2,… v_k est une séquence connexe de bords virtuels dirigées à partir de nœud u_I et terminant à un nœud u_J, où u_i, u_j, v_1, v_2, . . . , $V_k \in V$. Si il existe un chemin d'accès virtuel ui, v_1, v_2, v_k, u_j du nœud u_i au u_j, sa indique que la clé publique du nœud uj est obtenue et reconnu par v_k. La clé publique du nœud vk est obtenue et reconnu par v_{k-1},….,la clé publique du nœud v_1 est obtenue et reconnu par u_i .

- ***Virtual Connected Component*** : Un composant virtuelle connecté c'est des nœuds définis V′, V′∈V, dans lequel il est au moins un chemin virtuel entre toute paire de nœuds u et v [39].

A

ACK	**A**ccusé de réception
ADSL	**A**symmetric **D**igital **S**ubscriber **L**ine
AES	**A**dvanced **E**ncryption **S**tandard

B

BAH	**B**undle **A**uthentication **H**eader
BFN	**B**undle **F**orwarding **N**otification
BGP	**B**order **G**ateway **P**rotocol

C

CA	**C**ertificat **A**utorit
CH	**C**onfidentiality **H**eader
COF	**C**lasse **O**f **S**ervices
CT	**C**ustody **T**ransfert
CTN	**C**ustody **T**ransfret **N**otification

D

DTN	**D**elay **T**olerant **N**etwork
DES	**D**ata **E**ncryption **S**tandard
DSA	**D**igital **S**ignature **A**lgorithme
DVD	**D**ynamic **V**irtuelle **D**igraphe
DoS	**D**enial **o**f **S**ervice

DTNRG **D**elay **T**olerant **N**etwotk **R**esearch **G**roup
DARPA **D**efense **A**dvanced **R**esearch **P**rojects **A**gency

E

E

ED **E**arlist **D**elivery
EDLQ **E**arlist **D**elivery with **L**ocal **Q**ueuing
EDAQ **E**arlist **D**elivery with **A**ll **Q**ueuing
eTCR **e**nhanced **T**arget **C**ollision **R**esistant

F

F

FC **F**irst **C**ontact

H

H

HMAC **H**ashed **M**essage **A**uthentication **C**ode

I

I

IP **I**nternet **P**rotocol
IPN **I**nternet **I**nterplanétaires
IGP **I**nterior **G**atway **P**rotocol
IDEA **I**nternational **D**ata **E**ncryption **A**lgorithm
IBE **I**dentity **B**ased **E**ncryption

L

L

LTP **L**icklider **T**ransmission **P**rotocol

LP **L**inear **P**rogram

M

MAC **M**essage **A**uthentification **C**ode
MD **M**essage **D**igest
MED **M**inimum **E**xpected **D**elay

N

NASA **N**ational **A**eronautics and **S**pace **A**dministration

O

OSPF **O**pen Shortest Path First
OSI **O**pen Systems Interconnection

P

PSH **P**ayload **S**ecurity **H**eader
PKG **P**ublic **k**ey **G**enerator
PRL **P**ublic **R**evocation **L**ist
PKI **P**ublic **K**ey **I**nfrastructure
PoD **P**riority **o**f **D**elivery

R

RIPEMD **R**ipe **M**essage **D**igest

RSA **R**ivest **S**hamir **A**dleman
RIP **R**outing **I**nformation **P**rotocol
RR **R**eturn **R**eceipt

S

S

SHA **S**ecure **H**ash **A**lgorithm
SDU **S**ervice **D**ata **U**nit

T

T

TCP **T**ransmission **C**ontrol **P**rotocol
TW **T**ransmission **W**indow

U

U

UDP **U**ser **D**atagram **P**rotocol

V

V

VPL **V**alid **P**ublic **L**ist

[1] Samet Olfa, **« Apport et complémentarité des satellites avec d'autres technologies terrestres émergentes»,** projet de fin d'études sous le thème, 2006/2007.

[2] Hugo CRUZ SANCHEZ **« Routage Store and Forward dans les constellations de satellites »,** Septembre 2008.

[3] BAI Meng, « **le routage dans les DTN**», DTN_raport_final-ENST-P.

[5] Simon Paillard, **« Architectures réseaux pour communications interplanétaire »,** rapport de stage**,** Aout 2006.

[6] http://www.nasa.gov.

[7] Solène Alos, Georges-Rémy Fouad, Patrick Perouse « **Etat du l'art du Delay Tolerant Network »,** Juin 2006.

[8] Olfa Samet, Francin Kreif, **« Apport des satellites et de l'architecture DTN dans les réseaux ad hoc** », Rapport Travail Personnel Encadré (TPE)**,** 2006/2007.

[9] Tsafack Chetsa, Ghislain Landry **« Émulation de réseau interplanétaires et validation de protocoles tolérants aux délais »,** Juillet 2009.

[10] Asma Benmessaoud, « **Classification des protocoles de routage dans les Réseaux Tolérants aux Délais (DTN) »,** 2008/2009.

[11] Kevin Fall, Intel Research, Berkeley, « **A Delay-Tolerant Network Architecture for Challenged Internets »,** Juillet 2009.

[12] Vinton Cerf, Scott Burleigh, Adrian Hooke, Leigh Torgerson, Robert Durst, Keith Scot , Kevn Fall, Howord Weiss « **Delay-Tolerant Network (DTNs) »,** Mars 2003.

[13] DESS DCISS, « **Les réseaux : Introduction** (Vocabulaire, Modèle OSI, Ethernet) », Année 2002/2003.

[14] Sushant Jain, Kevin Fall, Rabin Patra, **« Routing in a Delay Tolerant Network »,** Année 2004.

[15] M^{me} BOUTRID née AMEZA Samia, mémoire de Magister « **Etude des réseaux tolérants aux délais DTNs et proposition d'une technique de routage », Année** 2007.

[16] BAI Meng, rapport de stage «**Le routage dans les DTNs** »

[17] CCNA2 exploration « **Protocole et conception du routage** » version 4.

[18] http://fr.wikipedia.org/wiki/Vecteur_de_distances.

[19] C.Hedrick "**Routing Information Protocol**", RFC 1058, June 1988.

[20] G. Mahajan, "**RIP Version 2**", RFC 2453(Standard), November 1998.

[21] http://cisco.goffinet.org/s2/vecteur_distance

[22] L. Toutain. **« Réseaux locaux et Internet, des protocoles à l'interconnexion** », 2eme édition, Année 1999.

[23] http://www.ebook-cours.com/cryptographie-cour-gratuit.html

[24] T.Ebraimi, F.Leprévost et B.Warusfel, **« Cryptographie et sécurité des systèmes et réseaux »,** sous la direction dirigée par Jean-charles Pomerol. ISBN 2-7462-1260-9, Année 2008.

[25] R. Shirey. « **Internet Security Glossary »**. RFC 2828, may 2000.

[26] Ghislaine, Labouret **« introduction a la cryptographie** » groupe Hervé Schauer Consultants(HSC), Année 1999/2001.

[27] N. Bennai et N. Belmouri sous le thème **« Sécurité dans les réseaux tolérant aux délais- DTN** », Université A. Mira, mémoire de fin de cycle.

[28] FIPS PUB 46-3, "**Data Encryption Standard (DES).Federal Information Processing Standards Publication"**, October 1999.

[29] FIPS PUB 197, "**Advenced Encryption Standard (AES)"**.Federal Information Processing Standards Publication, November 2001.

[30] D. Harkins and D. Carrel. "**The Internet Key Exchange (IKE) ".** RFC 2409,(Standard Track), Nouvembre 1998.

[31] W. Diffie and M. E. Hellman, "**New directions in cryptography IEEE Transactions of information Théory"**, IT-22: 644-654, Nouvenbre 1976.

[1] http://www.ebook-cours.com/cryptographie-cour-gratuit.html

[32] T. Ebrahimi, F. Leprévost et B. Warusfel, « **Cryptographie et sécurité des systèmes et réseaux »,** sous la direction dirigée par Jean-Charles Pomerol. ISBN 2-7462-1260-9, Année 2008.

[33] H.Krawezyk, M. Bellare, and R. Canetti. HMAC: **Keyed-Hashing for Message Authentification**. RFC 2104, February 1997.

[34] Forrest Warthman, "**Delay-Tolerant Networks (DTNs)",**Associés Warthman, Version1.1, Mai 2003.

[35] William D. Ivancic, "**Security Analysis of DTN Architecture and Bundle Protocol Specification for Space-Based Networks",** NASA Glenn Research Center, Année 2009.

[36] W. Scheirer, M. Chuah, "**DTN Security Features Technical Report"**. Department of Computer Science and Engineering, Lehigh University, Année 2005.

[37] Susan Symington, « **Secure Multidestination Delivery in DTN**", March 6, 2005.

[38] C. Gentry and A. Silverberg, "**Hierarchical ID-Based Cryptography. *Proceedings of Advances in Cryptology"***, *Asiacrypt*, Année 2002.

[39] Zhongtian Jia , Xiaodong Lin , Seng-HuaTan , Lixiang Li , Yixian Yang , Article info,**« Public key distribution scheme for delay tolerant networks based on two-channel cryptography" ,** Mars 2011.

[40] Mashatan A, Stinson DR. Practical unconditionally secure two channel message authentication. Designs, Codes and Cryptography 2010.

[41] V. Cerf, S. Burleigh, A. Hooke, L. Torgerson, R. Durst, K. Scott, K. Fall and H. Weiss "**Delay-Tolerant Network Architecture"**, September 2003.

Résumé

Depuis quelques années les communications à longues distance font l'objet de l'attention des chercheures. En effet, la technologie Internet et les protocoles utilisés fonctionnent mal dans tel environnement, pour résoudre ce problème, il a été une nouvelle architecture de réseau appelé les réseaux tolérants aux délais (DTN).

Un DTN est un réseau interconnectant des réseaux régionaux, il se situe comme une nouvelle couche au-dessus de l'ensemble des réseaux régionaux, y compris Internet. Du fait que cette technologie soit récente, alors divers problèmes sont encore au stade de recherche parmi lesquels nous citons le problème de la sécurité, qui est l'objet de notre projet de fin d'étude.

Les problèmes de la sécurité pour les DTNs varient en fonction de l'environnement, si l'authentification et la confidentialité sont souvent critiques. Ces garantis de sécurité sont difficiles à établir dans un réseau sans connexion avec les techniques cryptographiques classiques. L'objet de ce travail alors, est de proposer un nouveau modèle d'infrastructure de sécurité pour les DTNs.

Mots clés : Internet, DTN, Sécurité, Authentification, Confidentialité.

Abstract

In recent years, the long distance of communications is subject to the attention of researchers. Indeed, the Internet technology and protocols used in this environment, to solve this problem is dysfunctional; we propose new network architecture called the delay tolerant networks (DTN).

DTN is a network interconnecting regional network, it is as a new layer above all the regional networks, including the Internet. Because this technology is new, then various problems are still under research, among which we mention the problem of security, which is the subject of our final project study.

The problems of security for DTNs vary with the environment, if authentication and confidentiality are often critical. These are guaranteed security in difficult to establish a wireless connection with conventional cryptographic techniques. The purpose of this work then is to propose a new model of security infrastructure for DTN.

Keywords: Internet, DTN, Security, Authentication, Confidentiality.