REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE IBN KHALDOUN - TIARET

Projet de Fin d'Etude

Présenté à :

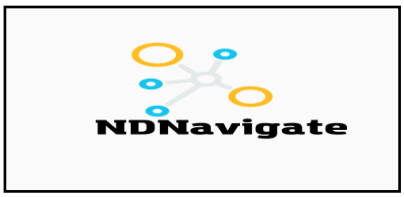
FACULTÉ DES MATHEMATIQUES ET DE l'INFORMATIQUE
DÉPARTEMENT D'INFORMATIQUE

Pour l'obtention du diplôme de Master

Spécialité : Réseaux et Télécoms

En vue de créer une startup

NDNavigate



Par :

BELGOUMENE Sara
SACKO Fatoumata

Sur le thème

Etude et simulation d'un réseau NDN

Soutenu publiquement le 24 / 06 / 2023 à Tiaret devant le jury composé de :

Mr AID Lahcen	MCA	Université Tiaret	Président
Mr Mostefaoui Sid Ahmed Mokhtar	MCB	Université Tiaret	Encadrant
Mr Meghazi Hadj Madani	MAA	Université Tiaret	Examinateur
Mme SADJI Fatima	Pr	Université Tiaret	Directrice de la Maison de l'Entreprenariat
Mme SELMANI Mourad	Directeur	de la poste et des télécoms Tiaret	R/ partenaire économique

2022 - 2023

" La vraie valeur d'un être humain réside dans sa capacité à donner, non pas dans sa capacité à recevoir. "

- Albert Schweitzer le célèbre médecin, théologien et philosophe.

Dédicace

À mes chers parents, mes frères et mes amis,

Il est difficile d'exprimer à quel point votre présence et votre soutien ont été précieux tout au long de mon parcours.

À mes parents, les deux êtres les plus précieux au monde, pour leur confiance inébranlable, leur patience infinie, leur amour inconditionnel, leur soutien inépuisable et leurs encouragements constants. Vous êtes mon guide et mon inspiration, et votre présence dans ma vie est un don inestimable.

À mes frères, pour leur précieuse aide et leur courage constant. Votre soutien indéfectible et votre présence dans ma vie ont été une source de force et de motivation inégalées.

À ma famille et à mes amies, avec qui j'ai partagé les moments les plus merveilleux de mon existence. Votre présence joyeuse, votre soutien inconditionnel et vos encouragements sincères ont illuminé mon parcours et ont rendu chaque étape encore plus précieuse.

Sara.

Dédicace

Avec l'expression de ma reconnaissance, je dédie ce travail :

A mes chers parents, qui se sont sacrifiés pour que je sois là où je suis aujourd'hui. Papa, maman merci pour votre amour vos encouragements, votre soutien, votre patience et vos prières. Nulle dédicace ne serait à la hauteur pour exprimer mon affection et mes gratitudes pour tout ce que vous faites pour moi. Puisse Allah vous garder très longtemps à mes côtés.

A ma seconde mère qui m'accompagne toujours avec sa prière.

A mes frères et sœurs en témoignage de l'amour qui nous attachent.

A tous mes amis. Et surtout Diakité Bintou, Dembélé Mariam et Berthé Astan.

A tous ceux qui m'ont soutenu tout au long de mes études.

Fatou.

Remerciements

Tout d’abord nous remercions Allah le tout puissant de nous avoir donné la volonté, le courage et la patience de mettre à terme notre travail.

Nos remerciements vont à l’endroit de notre encadrant **Mr Mostefaoui Sid Ahmed Mokhtar** qui nous a fait confiance en nous confiant ce sujet de mémoire et aussi pour son encadrement, sa disponibilité et ses conseils.

Nous tenons aussi à exprimer notre gratitude à toutes les personnes de près ou de loin avec lesquelles nous avons pu échanger sur ce travail, proches, amis, professeurs. Parmi ces personnes, on s’en voudrait de ne pas citer **Mr Nassane Samir** qui nous a été d’une aide précieuse pour la mise en place de notre simulation, merci de votre disponibilité, de votre accompagnement et de vos conseils motivant.

Un grand merci à nos très chers parents et à toute notre famille qui ont été des soutiens moraux tout au long de ce travail, merci à eux pour leur affection, leur ingéniosité, leur patience et leurs encouragements. Merci à tous nos amis de près ou de loin qui sont toujours présents pour nous.

TABLE DES MATIERES

LISTE DES FIGURES

LISTE DES TABLEAUX

RESUME

Le réseau NDN (Named Data Networking) est une architecture de réseau de communication qui vise à repenser la façon dont l'information est échangée sur Internet. Contrairement à l'architecture actuelle basée sur le protocole IP (Internet Protocol), qui se concentre sur l'acheminement des paquets de données basés sur les adresses IP, NDN se concentre sur l'acheminement de l'information basée sur son nom.

Ce mémoire pour obtenir le diplôme de master en informatique représente une étude approfondie d'un réseau NDN. Il examine essentiellement les principes fondamentaux tels que l'architecture du réseau, le routage, la sécurité et la mise en cache de contenu. L'objectif est d'évaluer et mets en évidence les avantages potentiels de cette architecture par rapport au modèle IP traditionnel qui sera limité. Des simulations sont aussi réalisées pour mesurer les performances, notamment le délai de transmission et l'utilisation du cache. Cette étude contribue à la compréhension et ouvre de nouvelles perspectives pour l'Internet du futur.

Mots-clés :

Réseaux Orientés Information, Réseaux Orientés Contenus, Named Data Networking (NDN).

ABSTRACT

The Named Data Networking (NDN) is a communication network architecture that aims to rethink the way information is exchanged over the Internet. Unlike the current IP-based architecture, which focuses on routing data packets based on IP addresses, NDN focuses on routing information based on its name.

This master's degree thesis represents an in-depth study of an NDN network. It primarily examines fundamental principles such as network architecture, routing, security, and content caching. The objective is to evaluate and highlight the potential advantages of this architecture compared to the traditional IP model, which is limited. Simulations are also conducted to measure performance, including transmission delay and cache utilization. This study contributes to the understanding and opens new perspectives for the future Internet.

Keywords:

Information-Centric Networking, Content-Centric Networking, Named Data Networking (NDN).

INTRODUCTION GENERALE

L'Internet actuel a considérablement évolué depuis sa création dans les années 1960 pour devenir un outil incontournable de la vie moderne, passant d'un simple réseau de communication à une plateforme pour des services en ligne tels que les réseaux sociaux, la vidéo en streaming, la banque en ligne, le commerce électronique, etc. Ces nouveaux services ont créé de nouveaux besoins pour les utilisateurs d'Internet, notamment la bande passante élevée et faible latence, la sécurité et la confidentialité, la mobilité, l'accessibilité, etc [1]. Ces défis ne sont que quelques exemples des nombreux défis auxquels Internet est confronté aujourd'hui.

Pour faire face à ces défis, une nouvelle architecture de réseau a été proposée pour compléter ou remplacer l'architecture IP connue sous le nom d'ICN (Information Centric Networking) [2].Ce dernier représente une nouvelle approche qui met l'accent sur le contenu plutôt que sur les hôtes. Alors, les contenus sont identifiés par des noms plutôt que par des adresses IP. Ces noms sont uniques et indépendants de l'emplacement ou du serveur qui les héberge.

En effet, ICN offre une meilleure efficacité de distribution de contenu, car le contenu peut être stocké dans plusieurs endroits et peut être récupéré à partir du plus proche nœud, réduisant ainsi la charge sur les serveurs centraux. Il offre également une meilleure sécurité de contenu, car le contenu est crypté et signé numériquement, et ne peuvent être récupérés que par les destinataires autorisés [2].

ICN est basé sur une idée simple : au lieu de demander des informations à une adresse spécifique, on demande simplement un contenu particulier. Lorsqu'un utilisateur demande un contenu spécifique, le système recherche le nom de ce contenu dans les routeurs et renvoie les données correspondantes. Ces données peuvent être stockées dans plusieurs endroits différents, ce qui permet d'améliorer l'efficacité et la disponibilité du réseau [3].

Il existe plusieurs architectures d'ICN, qui sont différents dans leurs conceptions et leurs approches de gestion des données comme le "Content-Centric Networking" (CCN) [4], le "Named Data Networking" (NDN) [5], la "Data-Oriented Network Architecture" (DONA) [6]et le "Network of Information" (NetInf) [7].

Dans ce travail nous nous intéressons au réseau NDN, nous allons faire une étude et un examen approfondi de ce réseau et de ses caractéristiques, de sa topologie, de ses mécanismes de routage et de sécurité. L'étude de ces éléments permet de mieux comprendre les performances et les avantages du réseau NDN.

Ce mémoire est organisé en quatre chapitres comme suit. Dans le premier chapitre, nous introduiront l'architecture NDN et nous analyserons ces concepts : le nommage, la résolution des noms et le routage. Le chapitre 2 est consacré à la mise en cache et le stockage permanent. Dans le troisième chapitre, en termes de sécurité, nous présenterons tous les fonctionnalités qui peuvent garantir l'intégrité, la confidentialité et l'authenticité des données échangées. Le quatrième chapitre contient une analyse et une évaluation des résultats obtenus après avoir mené une simulation de réseau NDN. Nous clôturerons le travail par une conclusion générale.

CHAPITRE 1

L'ARCHITECTURE NDN

INTRODUCTION :

L'Internet est basé sur le protocole de communication IP (Internet Protocol) qui a été conçu pour permettre à différents ordinateurs et périphériques de communiquer entre eux en utilisant des adresses IP uniques. Les données sont transmises sous forme de paquets de données qui sont routés via des serveurs intermédiaires jusqu'à leur destination.

Cependant, avec la croissance exponentielle des données et l'évolution des exigences de l'utilisateur, plusieurs défis se posent, en particulier la sécurité et la mobilité, etc. Ce qui rend le protocole IP actuel insuffisant pour répondre aux besoins actuels et futurs de l'Internet. C'est pourquoi de nouvelles technologies telles qu'ICN dont NDN fait partie sont développées.

Named Data Networking (NDN) est un nouveau modèle de communication de réseau qui utilise un nom de contenu pour identifier et router les données plutôt que l'adresse IP. Le concept est de remplacer la communication centrée sur l'adresse IP avec une communication centrée sur le contenu, où chaque paquet de données est un objet identifié par un nom unique [2].

Dans ce chapitre nous présenterons les limites de l'architecture de l'internet actuel et ces défis. Nous introduirons brièvement l'architectures de l'ICN Content Centric Networking (CCN) et nous nous concentrerons sur l'architecture NDN et ses principaux caractéristiques : Le nommage, la résolution des noms et routage.

1) Les limites de l'architecture actuelle d'internet :

- La distribution des contenus :

Avec l'avancée des appareils mobiles et la démocratisation de l'accès à haut débit, Internet a connu une croissance rapide en tant que moyen de distribution de grandes quantités de contenu aux utilisateurs [8]. Selon les études menées par Cisco [9], le trafic Internet mondial augmentera d'un

facteur de 64 par rapport à 2005 d'ici 2019, avec les vidéos représentant entre 80% et 90% de ce trafic. Afin de répondre à la demande croissante de contenu, des solutions telles que les réseaux de diffusion de contenu (CDN - Content Delivery Network) [10] et les réseaux peer-to-peer (P2P) [11] ont été proposées. Ces solutions ont amélioré la distribution de contenu en se basant sur la mise en cache dans le réseau [12]. Toutefois, elles restent des corrections partielles spécifiques aux applications ou aux fournisseurs et fonctionnent sur le protocole IP. Elles présentent également certaines limites [13].

Deux problèmes majeurs se posent lorsqu'il s'agit de distribuer efficacement du contenu sur Internet. Tout d'abord, il est difficile de sélectionner la meilleure paire d'utilisateurs en pair-à-pair (P2P) pour la distribution des contenus, ce qui entraîne un trafic coûteux entre les fournisseurs [14]. De plus, il est difficile d'exploiter de manière efficace le stockage en réseau, ce qui limite les possibilités de réduction des coûts dans les réseaux P2P et les réseaux de diffusion de contenu (CDN) [15].

Face à la demande croissante d'une distribution de contenu évolutive et efficace, les utilisateurs s'intéressent davantage aux contenus eux-mêmes plutôt qu'aux hôtes qui les stockent. Dans ce contexte, une nouvelle architecture qui modifie le modèle de communication, passant d'un modèle centré sur les hôtes à un modèle centré sur les contenus, semble plus adaptée à l'évolution de l'utilisation d'Internet. Cette architecture doit permettre une mise en cache native dans le réseau, afin de distribuer un contenu demandé à partir de la source la plus appropriée [2].

- Sécurité et confidentialité :

Au début, l'objectif de l'Internet était de connecter quelques hôtes distants de confiance. Cependant, le succès croissant de l'Internet a engendré de nombreux problèmes de sécurité et des attaques de plus en plus sophistiquées [16]. Afin de résoudre ces problèmes, plusieurs protocoles tels que TLS [17], IPsec [18] et DNSSEC ont été développés. Cependant, en plus des problèmes de performance induits par ces protocoles, chacun d'entre eux vise à sécuriser un protocole spécifique et leur combinaison ne garantit pas nécessairement un système sécurisé [19]. De plus, le modèle de sécurité actuellement utilisé dans le réseau IP lie la sécurité d'un contenu à la confiance accordée à l'hôte qui le stocke et à la connexion utilisée pour le récupérer (par exemple, en utilisant le protocole TLS) [20]. Étant donné que la connexion est temporaire, ce modèle de sécurité est vulnérable à certains problèmes [21]. En effet, un utilisateur qui stocke un contenu précédemment récupéré à partir de la source d'origine ne peut pas être sûr que ce contenu n'a pas été modifié (par

exemple, par un logiciel malveillant). De plus, un autre utilisateur souhaitant accéder au même contenu ne peut pas l'obtenir à partir du premier utilisateur. Pour avoir confiance dans ce contenu, il est nécessaire de le récupérer à partir de la source d'origine en établissant une connexion sécurisée.

Une alternative plus adaptée à une approche basée sur la sécurisation des connexions est un modèle de sécurité axé sur les contenus, qui intègre les mécanismes de sécurité directement dans le contenu lui-même. Cette approche offre une solution intéressante en permettant aux utilisateurs de vérifier la sécurité d'un contenu récupéré, peu importe sa source et à tout moment [21].

- Mobilité :

La mobilité représente un défi supplémentaire dans le contexte actuel de l'Internet. En effet, les adresses IP remplissent à la fois le rôle de localisateur et d'identifiant. Lorsqu'un hôte se déplace, le changement de localisateur entraîne également un changement d'adresse IP, ce qui entraîne une interruption de la connectivité. Plusieurs propositions ont été formulées pour résoudre ce problème, mais elles ne proposent pas de solutions radicales. Certaines de ces propositions nécessitent l'utilisation d'une adresse IP différente, ce qui implique une modification majeure de l'approche de la dénomination, tandis que d'autres compromettent la hiérarchie du routage et menacent ainsi sa scalabilité [22].

- Accessibilité :

Bien que la couverture d'Internet soit en augmentation constante, il y a encore des régions du monde qui n'ont pas accès à Internet ou qui ont un accès limité. Les nouveaux besoins incluent donc une meilleure accessibilité pour les personnes qui n'ont pas encore accès à Internet [23].

2) L'approche des réseaux orientés contenus : Une réponse aux problèmes de l'Internet actuel :

Le changement radical dans l'utilisation de l'Internet et les problèmes évoqués précédemment ont conduit au développement de l'approche des réseaux orientés contenus (ICN). Cette approche se concentre sur la distribution des contenus indépendamment des hôtes qui les hébergent. Elle considère le contenu nommé comme l'élément central du réseau et intègre nativement la mise en cache. Ainsi, une copie d'un contenu demandé peut être récupérée à partir du nœud le plus approprié du réseau, ce qui répond aux exigences identifiées pour une distribution de contenus plus efficace que celle de l'Internet actuel.

De plus, grâce aux noms de contenus qui jouent le rôle d'identifiants indépendants des localisateurs, la mobilité ne pose plus de problème. Enfin, pour répondre aux exigences de sécurité, l'ICN remplace le modèle traditionnel de sécurisation des connexions par un modèle axé sur les contenus, en intégrant des mécanismes cryptographiques dans le contenu lui-même et en utilisant un système de nommage adéquat.

3) Content Centric Networking CCN : L'origine de NDN :

Le NDN s'inspire de différentes technologies et concepts existants, tels que le Content Centric Networking (CCN). Le CCN a été développé à partir de 2006 au centre de recherche PARC (Palo Alto Research Center) par Van Jacobson, dans le but de résoudre plusieurs des limitations de l'architecture actuelle d'internet, en particulier celles liées à la gestion des données, à la sécurité et à la mobilité des dispositifs [24].

CCN conserve l'architecture en forme sablier (hourglass) de l'internet actuel, mais les données sont stockées et récupérées en utilisant leurs noms plutôt que leurs adresses IP. Cette architecture possède deux principales couches : une couche "strategy" qui permet la gestion des flux de données dans le réseau (les requêtes et les réponses). Et une couche "Security" pour garantir l'intégrité, la confidentialité et l'authenticité des données échangées entre les nœuds du réseau [25].

L'implémentation actuelle de l'architecture CCN est appelée CCNx. CCNx a été développé par Cisco pour étendre le modèle de CCN en ajoutant des fonctionnalités avancées telles que la prise en charge de la mobilité et la qualité de service (QoS).Il peut également être utilisé dans des applications telles que l'Internet des objets (IoT) pour faciliter la distribution efficace des données entre les appareils connectés [24] [26].

La figure ci-dessous montre les deux paradigmes des réseaux informatiques et ces architectures. L'architecture NDN est une évolution de CCN et de nombreuses similitudes peuvent être observées entre les deux architectures mais le NDN a été amélioré pour mieux répondre aux besoins de sécurité et de confidentialité dans les réseaux modernes.

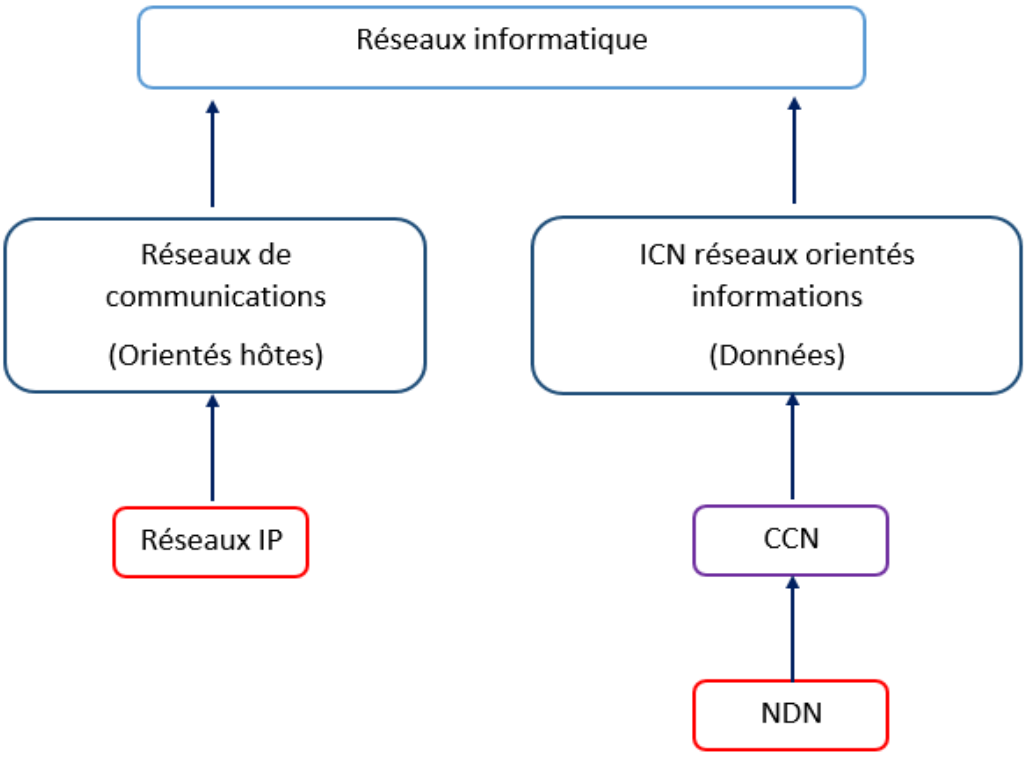


Figure 1 Le NDN et les principales architectures

4) NDN (Named-Data Networking) :

4.1) Présentation du projet :

Le projet NDN est l'un des cinq projets financés par la NFS (National Science Fondation) dans le cadre de l'architecture de l'internet de future. En 2009, le PARC (Palo Alto Research Center) a conçu l'architecture CCN. En 2013, le projet CCN a été scindé en deux projets la NSF-FIA (National Science Foundation‘s Future Internet Architecture) a financé le projet NDN et le PARC a financé le projet CCN. Les architectures CCN et NDN sont similaires à l'exception de quelques différences dans les perspectives de confidentialité [27].

4.2) L'architecture de NDN :

Bien que NDN représente une toute nouvelle proposition d'architecture, sa forme en sablier le rend compatible avec l'Internet d'aujourd'hui et conduit à une stratégie d'évolution claire et simple,(comme il est illustré dans la figure) .Dans cette architecture les contenus et leurs noms sont au cœur de la pile des protocoles de réseau au lieu des adresses IP .Elle comporte aussi autres

couches, la couche "strategy", la couche de sécurité, la couche de routage et la couche d'application. La couche "strategy" est responsable de l'acheminement des paquets de données nommés, tandis que la couche de sécurité fournit des mécanismes pour protéger les données contre les attaques malveillantes. La couche de routage est responsable de la prise de décisions de routage pour acheminer les paquets de données nommés vers leur destination, tandis que la couche d'application fournit des interfaces pour les applications utilisant NDN [28].

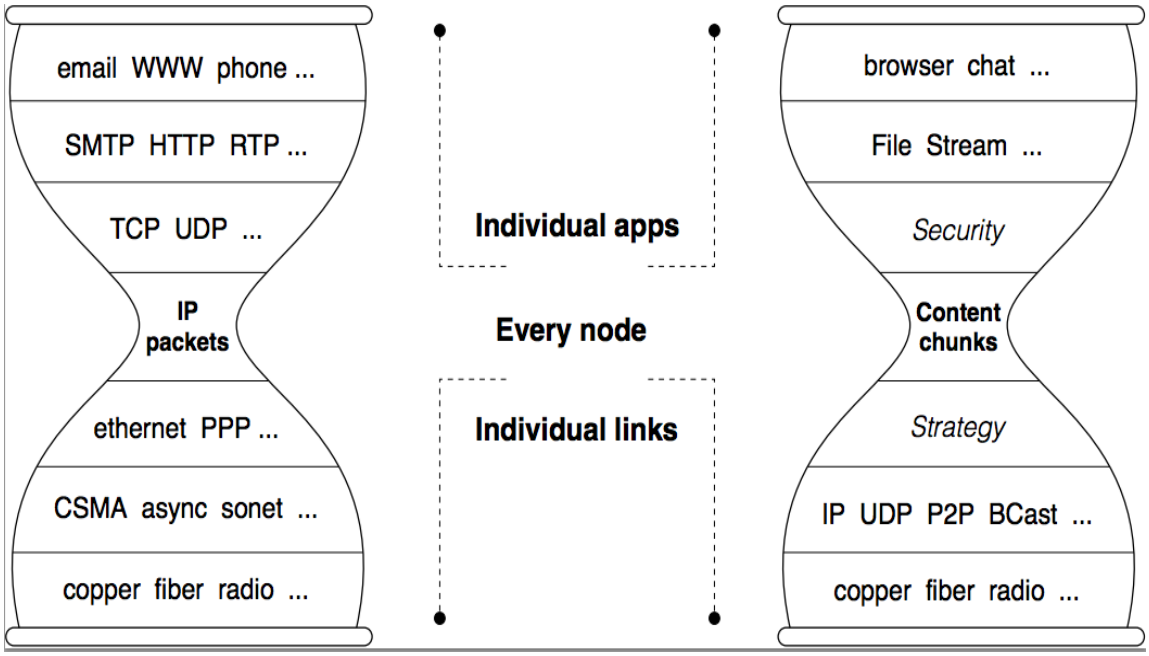


Figure 2 L'architecture Hourglass du NDN

L'architecture NDN comporte trois types d'entités principales :

- Les producteurs : Ils génèrent et publient les données dans le réseau. Les producteurs peuvent être des serveurs, des applications, des dispositifs IoT (Internet des objets) ou tout autre appareil capable de produire et publier des données.
- Les consommateurs : représentent les demandeurs des données dans le réseau qui envoient des requêtes. Les consommateurs peuvent être des ordinateurs, des téléphones portables, des tablettes, des utilisateurs finaux ou tout autre type de dispositif qui a besoin d'accéder à des données.

- Les routeurs : Les routeurs sont les entités qui acheminent les paquets de données et d'intérêt entre les producteurs et les consommateurs dans le réseau.

4.3) Le nommage :

NDN est un modèle de réseau de communication qui identifie les données par des noms plutôt que par des adresses IP, comme c'est le cas dans les réseaux TCP/IP traditionnels. Cela signifie que chaque nom NDN est indépendant de l'emplacement de la ressource et qu'il peut être utilisé pour identifier les mêmes données à différents endroits du réseau [29].

Un nom dans NDN a une structure hiérarchique et similaire à celle d'une URL (Uniform Resource Locator) ou d'une URI (Uniform Resource Identifier) dans le contexte d'Internet. Ce nom est divisé en composants, séparés par des caractères ("/"), Chaque composant est une chaîne de caractères non nulle, qui peut contenir des caractères alphanumériques, des tirets, des points et des caractères spéciaux. Ces composants sont ordonnés du plus général au plus spécifique, par exemple, un nom NDN pour un document spécifique peut ressembler à ceci:

univ-tiaret.dz/étudiant/mastérant/mémoire/Reseau_NDN.pdf

Dans cet exemple, le nom commence par le premier composant 'univ-tiaret.dz/étudiant/mastérant' qui représente le préfixe du nom et identifie l'institution qui a publié le document et le domaine d'intérêt. Le deuxième composant 'mémoire' identifie la catégorie de contenu du document. Le dernier composant 'Reseau_NDN.pdf' représente le document spécifique.

Un paquet d'intérêt pour '/univ-tiaret.dz/étudiant/mastérant/mémoire/Reseau_NDN.pdf' peut être satisfait par un paquet de données nommé 'univ-tiaret.dz/étudiant/mastérant/mémoire

/Reseau_NDN.pdf/1/1' où /1/1 signifie que c'est la première version du premier segment du mémoire.

Le segment fait référence à une partie d'une donnée qui peut être envoyée individuellement sur le réseau. Lorsque les données sont trop volumineuses; pour être transmis en une seule fois, il peut être divisé en plusieurs segments. Chaque segment est identifié par un nom unique qui est dérivé du nom de données plus large. La version fait référence à une itération particulière d'une donnée qui peut être modifiée au fil du temps. Lorsqu'une donnée est publiée pour la première fois, elle est considérée comme la version 1. Si le contenu de donnée est modifié et republié, la nouvelle version sera identifiée comme la version 2 et ainsi de suite [30].

Donc, un nom dans NDN peut être présenté de la manière suivante : la première partie du nom représente le nom globalement routable, la deuxième représente le nom organisationnel et la dernière partie fournit les informations de la version et du segment comme il est illustré dans l'exemple ci-dessous :

Figure 3 La structure des noms dans NDN

Voici quelques détails du nommage dans NDN [29] :

- Hiérarchie: Les noms dans NDN sont hiérarchiques, ce qui signifie qu'ils peuvent être imbriqués les uns dans les autres pour former une structure arborescente. Les noms peuvent être organisés selon une structure de répertoire, avec des noms de répertoire supérieurs qui contiennent des sous-répertoires et des fichiers.
- Structure arborescente : Les noms dans NDN sont basés sur une structure arborescente, où chaque nœud dans l'arbre représente un élément du nom. Les noms peuvent inclure des informations sur le contenu, telles que le type de contenu, l'éditeur, la date et l'heure de publication, ainsi que des informations de localisation. Par exemple, un nom pourrait ressembler à :

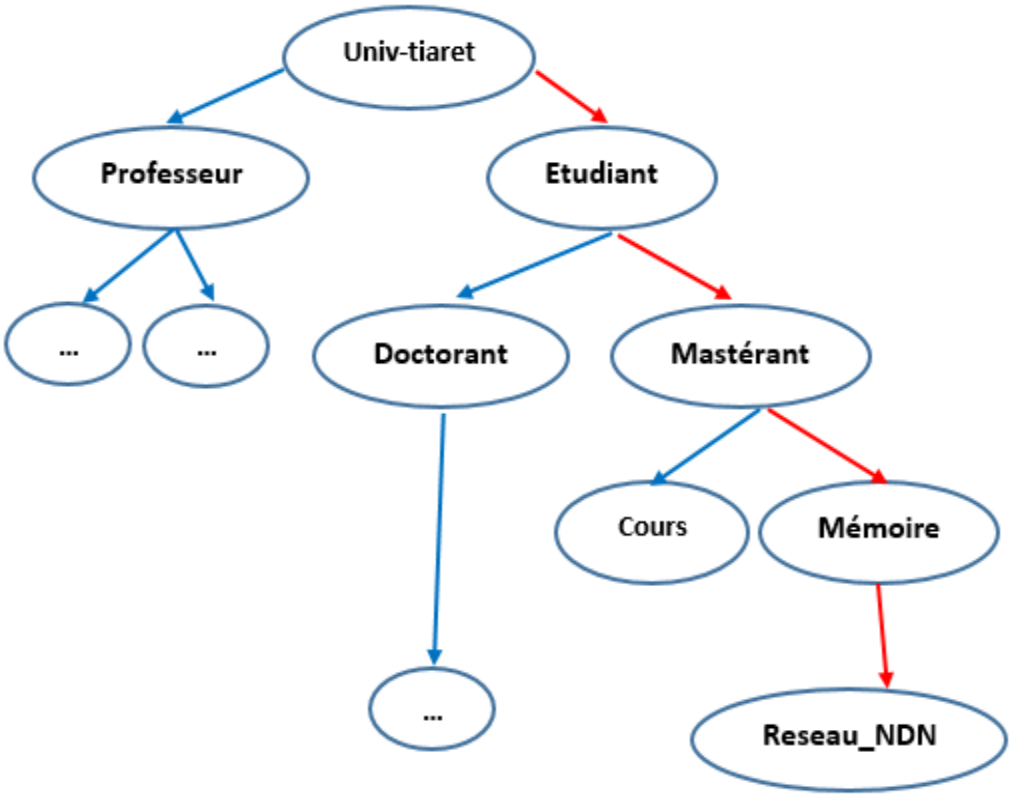


Figure 4 Le schéma de nommage dans l'architecture NDN

- Noms uniques : Les noms dans NDN sont uniques, ce qui signifie qu'un nom donné identifie une ressource de manière unique. Les éditeurs de données peuvent garantir l'unicité des noms en utilisant des identifiants de version pour que chaque version de la donnée ait un nom unique.

En utilisant des noms de segment et de version dans les noms des données, les utilisateurs peuvent récupérer des parties ou des versions spécifiques d'une donnée, plutôt que de la récupérer complète. Cela peut améliorer l'efficacité et la fiabilité de la distribution de contenu sur les réseaux NDN.

4.4) La résolution des noms et le routage :

Nous présentons un scénario simple de modèle de communication NDN dans la figure 5. L'exemple illustratif contient un producteur, deux consommateurs (C01, C02) et deux routeurs (R01, R02).

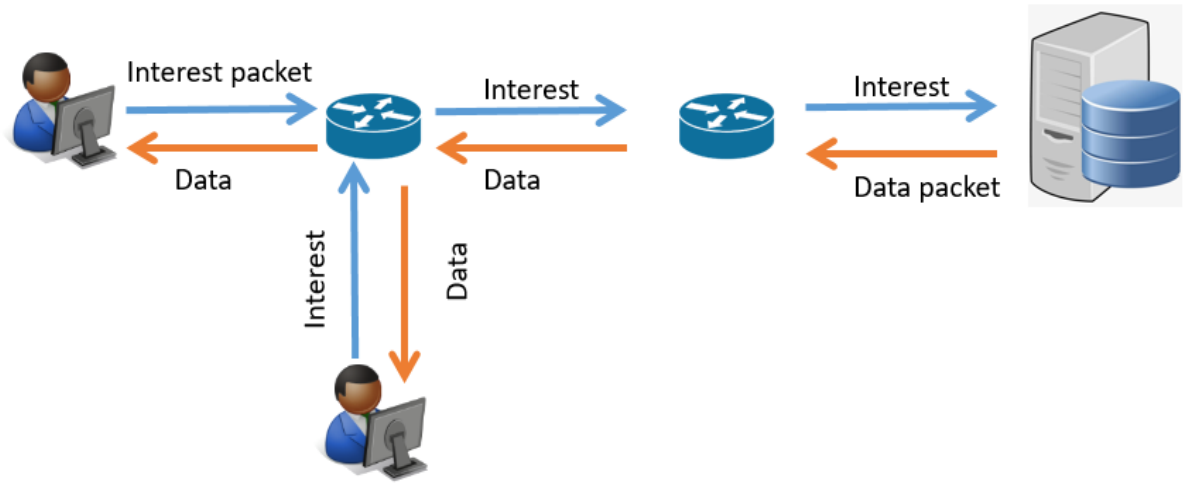


Figure 5 Le modèle de communication dans NDN

Les demandes de données sont exprimées sous la forme de paquets d'intérêt (Interest), qui contiennent le nom des données recherchées et sont diffusés dans le réseau. Les nœuds intermédiaires qui reçoivent les paquets d'intérêt peuvent répondre soit en envoyant un paquet de données (Data) correspondant au nom spécifié, soit en redirigeant la demande vers un autre nœud qui est plus proche du producteur des données. Les paquets de données contiennent le nom des données, les données elles-mêmes, ainsi que des métadonnées telles que des informations sur la signature pour garantir l'authenticité et l'intégrité des données. Les nœuds intermédiaires peuvent stocker en cache les paquets de données qu'ils ont reçus pour répondre plus rapidement aux futures demandes similaires [29].

4.4.1) La résolution des noms :

Pour transmettre les données dans NDN, il existe deux types de paquets [29] [5] :

1. Le paquet d'intérêt (Interest packet) : Il est envoyé par un nœud du réseau (ou un client) pour demander une donnée spécifique. Le paquet d'intérêt contient le nom de la donnée souhaitée.
2. Le paquet de donnée (Data packet) : Il contient la donnée elle-même ainsi que le nom de la donnée pour laquelle il a été demandé. Le paquet de donnée est envoyé par le nœud qui possède la donnée demandée par le paquet d'intérêt.

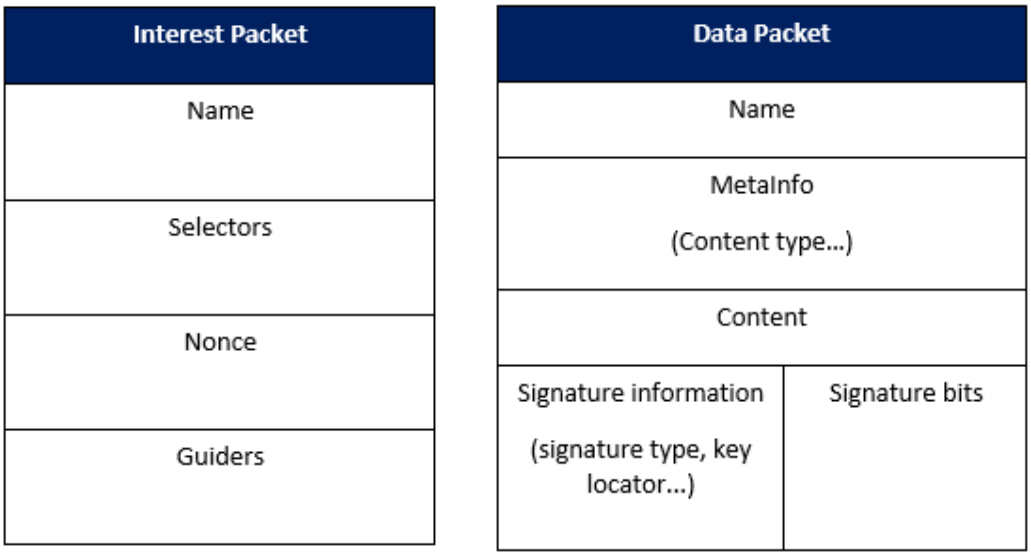


Figure 6 Le paquet Interest et Data de NDN

Le paquet d'intérêt comprend différents champs : le nom du contenu "content name", le sélecteur "selector", il contient également une valeur aléatoire "nonce".

- Content Name : représente le nom du contenu désiré.
- Selector : ce champ indique à quelle distance se trouve le paquet d'intérêt. Il peut avoir l'une des trois valeurs prédéfinies (0, 1 ou 2). La valeur 0 signifie ne pas diffuser le paquet d'intérêt sur le démon NDN local. La valeur 1 signifie la diffusion du paquet d'intérêt à la couche application du nœud NDN actuel. La valeur 2 signifie ne pas diffuser le paquet d'intérêt vers le prochain saut.
- Nonce : C'est un nombre aléatoire généré pour chaque paquet Interest émis par un émetteur. Ce champ permet de garantir l'unicité des paquets d'intérêt émis.

Le paquet de donnée comprend différents champs : le nom de contenu "Content Name", "Signature", des métadonnées telles que "Freshness" et "Type".

- Content Name : ce champ contient le nom du contenu.
- Signature : est une signature à clé publique créée par le producteur de contenu. Il fournit également une référence par nom pour vérifier la clé publique.
- Freshness : il contient le temps recommandé pour mettre en cache le contenu défini par le producteur.
- Type : définit le type de contenu.

4.4.2) Le routage :

Le routage dans NDN (Named Data Networking) est différent du routage dans le réseau IP (Internet Protocol). Dans le réseau IP, les paquets sont routés en utilisant des adresses IP qui identifient les hôtes sources et de destination. En revanche, dans NDN, les paquets sont routés en utilisant des noms de données, qui identifient les données elles-mêmes plutôt que les hôtes, ce qui permet à cette architecture de se libérer des problèmes habituellement rencontrés dans l'architecture IP, tels que la limitation du nombre d'adresses, le NAT et la mobilité des nœuds.

- Contrairement à l'architecture IP, il n'y a pas de limitation sur le nombre d'adresses disponibles dans NDN car son espace de noms est hiérarchique et ne comporte aucune restriction.
- De plus, dans NDN, les hôtes n'ont pas besoin de communiquer leurs adresses pour échanger des données, donc le NAT n'est pas nécessaire. La mobilité des nœuds n'affecte pas les communications, pourvu qu'elles utilisent des noms de données cohérents.
- Dans les réseaux NDN, il n'est donc pas nécessaire d'assigner et de gérer les adresses logiques, ce qui est particulièrement utile pour les objets connectés dans un environnement domestique, par exemple [31].

Le fonctionnement du protocole de routage dans NDN peut être comparé à celui de l'IP, mais avec une différence significative. Au lieu d'échanger des préfixes d'adresses IP, les routeurs NDN échangent des préfixes de noms de données. Les protocoles de routage traditionnels de l'IP tels qu'OSPF et BGP peuvent être adaptés à NDN pour manipuler des noms de données plutôt que des adresses IP. Ces annonces de routage sont propagées dans le réseau pour permettre à chaque routeur de construire sa table FIB. Le protocole de routage principal utilisé dans NDN est le protocole de routage à état de lien nommé (NLSR - Named-data Link State Routing Protocol) [32].

Chaque routeur dans le réseau NDN maintient trois structures de données principales :

- La table de routage (FIB, Forwarding Information Base) : contient des informations sur les préfixes de noms de données et les interfaces de sortie associées à ces préfixes. Cette table permet aux routeurs de déterminer le prochain saut pour un paquet Interest en fonction de son nom.
- La mémoire tampon (CS, Content Store) : contient des copies des données récemment reçues par le routeur, ainsi que les informations associées telles que la date d'expiration. Cette table permet aux routeurs de répondre rapidement aux paquets Interest en envoyant directement les données stockées dans le cache.

- La table d'attente (PIT, Pending Interest Table) : contient des informations sur les paquets Interest en attente de réponse. Pour chaque paquet Interest reçu, le routeur ajoute une entrée à la PIT qui contient des informations sur le nom de la donnée demandée, l'interface d'entrée et les interfaces de sortie correspondantes. Lorsqu'un paquet Data est reçu en réponse à un paquet Interest en attente, le routeur utilise les informations stockées dans la PIT pour acheminer le paquet Data vers le nœud qui a émis l'Interest.

Lors du processus de routage dans les réseaux NDN, les routeurs peuvent être confrontés à deux types de paquets différents, comme évoqué dans [33] [34]. Si le routeur reçoit un paquet de type "Intérêt" (Interest), sa tâche est alors de localiser les données demandées afin de répondre à la requête.

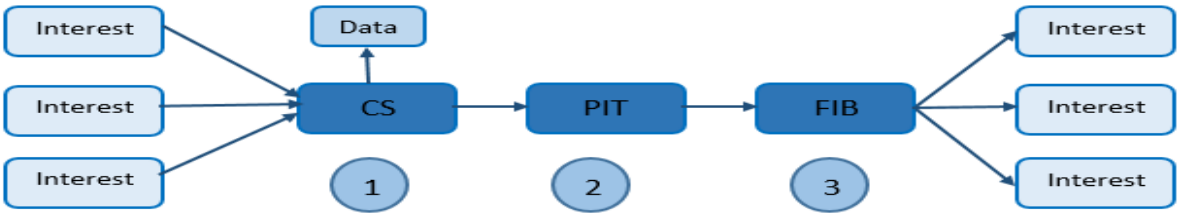


Figure 7 Le routage NDN lors de la réception d'un Interest

La figure 7 ci-dessus illustre comment un routeur NDN traite un paquet d'intérêt (Interest). Tout d'abord (étape 1), le routeur vérifie si la donnée correspondant à l'intérêt est présente dans son cache de stockage (CS). Si tel est le cas, il envoie la donnée sous forme de paquet de données (Data) à travers l'interface d'arrivée du paquet d'intérêt reçu. Sinon, le routeur examine la table PIT (étape 2). S'il y a déjà une demande pour cette donnée, le routeur ajoute simplement l'interface d'arrivée de l'intérêt à l'entrée correspondante dans la PIT. Sinon, le routeur crée une nouvelle entrée dans la PIT et passe à la table FIB (étape 3) pour trouver le chemin menant à la donnée demandée. Des paquets d'intérêt seront alors envoyés sur toutes les interfaces correspondant au chemin le plus précis dans la FIB.

Lorsqu'un routeur reçoit un paquet de type "Data", il est nécessaire qu'il le transmette aux interfaces qui ont initialement émis la demande pour cette donnée.

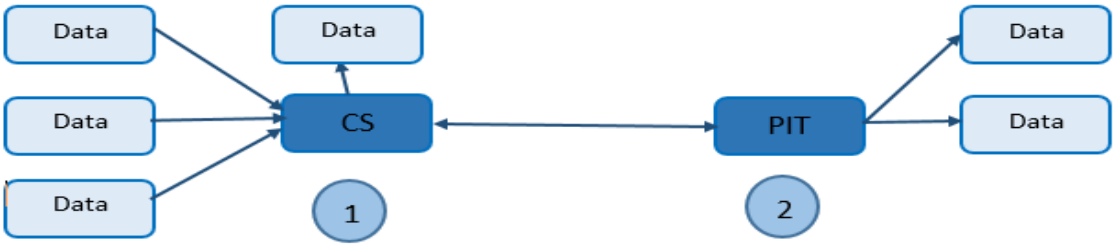


Figure 8 – Le routage NDN lors de la réception d'une donnée

Le traitement des paquets Data par un routeur NDN est illustré dans la figure 8 ci-dessus. Tout d'abord, le routeur vérifie si la donnée demandée existe déjà dans son cache de stockage (CS) (1). Si c'est le cas, le paquet est rejeté. Ensuite, le routeur vérifie s'il existe une entrée correspondante dans la table PIT (2). Si aucune entrée n'est trouvée, le paquet est abandonné. En revanche, si une entrée est trouvée, la donnée est transmise à toutes les interfaces enregistrées dans l'entrée correspondante de la PIT et stockée dans le CS. Il est important de noter que la table de forwarding information base FIB ne joue aucun rôle dans ce processus.

Pour mieux comprendre le fonctionnement de ce routage, prenons un exemple :

Lorsqu'un routeur reçoit un paquet Interest, il recherche la donnée demandée dans sa propre cache (CS). Si la donnée est présente, le routeur peut répondre immédiatement avec un paquet Data à l'Interest et ce dernier sera ensuite éliminé. Sinon, il recherche dans la PIT. S'il existe déjà un paquet Interest exactement sous le même préfixe du nom, l'interface source de ce paquet est ajoutée et le paquet sera ensuite éliminé. Si la CS et la PIT ne présente aucune donnée correspondante, il recherche dans la FIB. S'il existe une entrée correspondante au préfixe du nom du paquet Interest, ce paquet est transmis vers les interfaces indiquées dans la FIB.

Le routeur transmet l'Interest à ses voisins en utilisant son propre mécanisme de routage. Les routeurs peuvent utiliser différents algorithmes de routage, tels qu'OSPF (Open Shortest Path First) ou BGP (Border Gateway Protocol), pour décider du meilleur chemin à emprunter pour transmettre l'Interest.

Lorsqu'un nœud possède la donnée demandée, il envoie un paquet Data qui contient la donnée elle-même ainsi que le nom de la donnée. Le paquet Data est transmis directement au nœud qui a émis l'Interest.

Lorsqu'un nœud reçoit un paquet Data, il vérifie si le paquet correspond à l'Interest stocké dans sa propre cache. Si c'est le cas, la donnée est extraite du paquet Data et stockée dans le cache du nœud. Si le paquet Data ne correspond pas à un Interest stocké dans la cache, le paquet est ignoré.

Ce processus de transmission des paquets Interest et Data continue jusqu'à ce que la donnée soit trouvée et transmise à l'émetteur de l'Interest. Si la donnée n'est pas disponible dans le réseau, l'Interest sera transmis à tous les nœuds connectés jusqu'à ce que la donnée soit trouvée ou jusqu'à ce qu'un délai limite soit atteint.

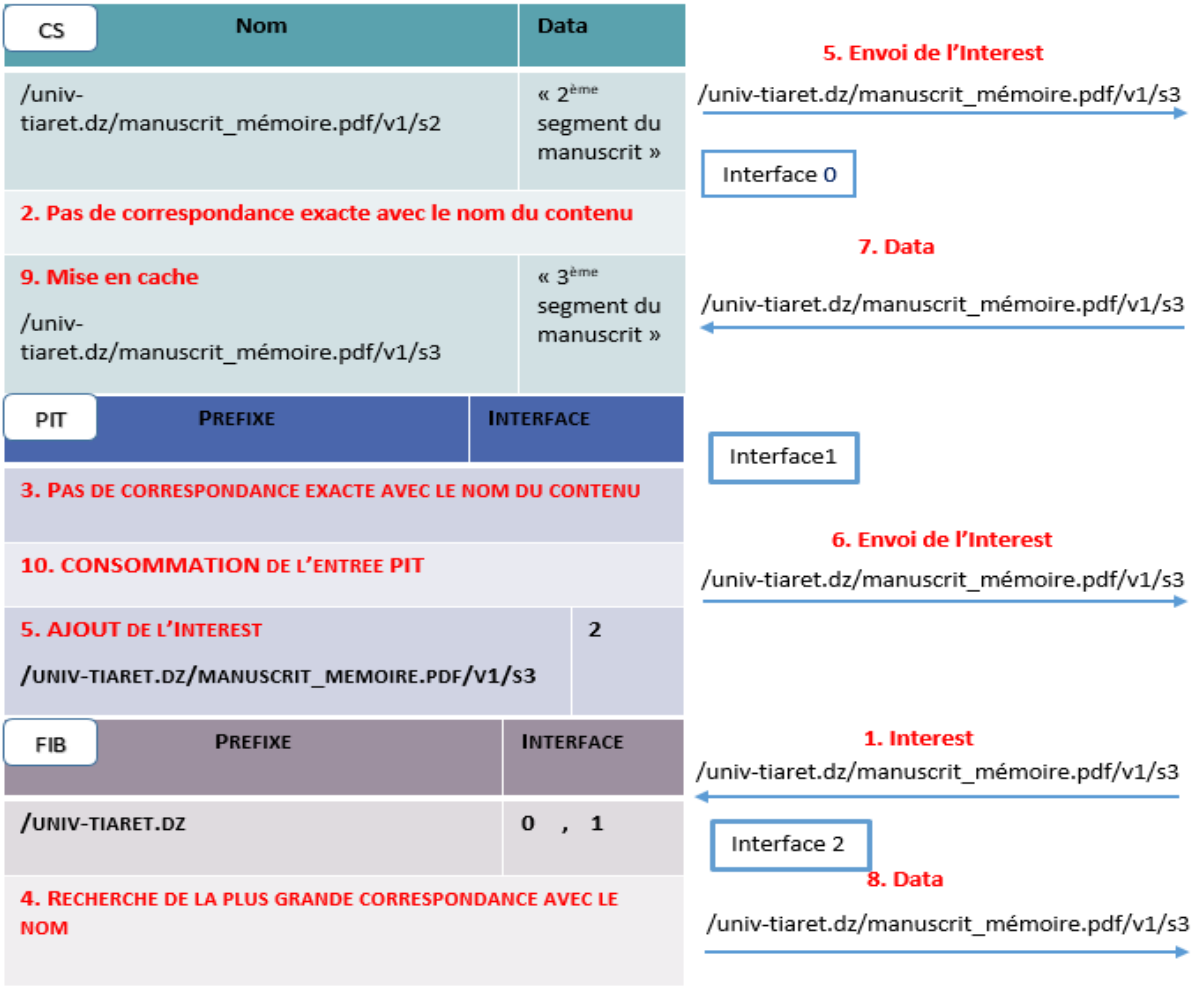


Figure 9 La transmission des paquets Interest et Data dans NDN

4.5) Sécurité :

Au lieu de transmettre des paquets à des destinataires identifiés par des adresses IP, NDN permet aux utilisateurs de demander des données souhaitées en utilisant des noms. Cette approche permet à NDN de sécuriser les données directement au niveau du réseau en rendant le contenu de chaque paquet de données vérifiable et, si nécessaire, confidentiel [35].

La méthode utilisée repose principalement sur l'inclusion d'une signature numérique qui lie le nom au contenu dans chaque paquet de données. Cette signature est générée en prenant en compte l'ensemble du paquet, y compris le nom du contenu, les métadonnées, les données et les informations relatives à la signature, grâce à l'utilisation de la clé privée du producteur. La vérification de la signature numérique permet de garantir l'intégrité des données en s'assurant qu'elles n'ont pas été altérées et qu'elles correspondent bien au nom indiqué dans le paquet Interest, qui doit être le même que celui du paquet Data pour assurer l'authenticité des noms. Cette vérification permet également d'authentifier le producteur en utilisant sa clé privée, ainsi que d'identifier la source et de déterminer si elle est acceptable pour le contenu, ce qui garantit la provenance des données. Toutefois, pour vérifier la signature du paquet Data, il est nécessaire d'utiliser la clé publique du producteur, qui peut être obtenue à partir du champ KeyLocator inclus dans les informations de la signature. Pour assurer la confiance dans ce mécanisme, il est nécessaire de disposer d'un système permettant aux demandeurs de décider si une clé publique est valide et en mesure de vérifier la signature d'un paquet Data. NDN ne force pas l'adoption d'un modèle de confiance spécifique, mais permet aux applications de faire leur propre choix [36].

En outre, la sécurité de NDN est assurée par l'utilisation de mécanismes cryptographiques autres que les signatures, ainsi que par les propriétés des noms. Les données sensibles peuvent être chiffrées et seules les entités autorisées ont connaissance des clés utilisées pour chiffrer et déchiffrer ces données, garantissant ainsi à la fois le contrôle d'accès et la confidentialité. De plus, le nom contenu dans un paquet Interest peut contenir des informations importantes sur le contenu, étant identique à celui du paquet Data associé. En récupérant le paquet Data correspondant, le demandeur peut être sûr que le contenu reçu est bien conforme à sa demande, ce qui garantit la pertinence des données [37].

CONCLUSION :

Les problèmes et les difficultés auxquels L'internet est confronté sont le résultat de son architecture initiale qui n'a pas été conçue pour répondre à l'explosion de l'utilisation et du contenu. Pour cette raison, les chercheurs proposent une nouvelle architecture Internet ICN.

NDN est une implémentation spécifique d'ICN considéré comme une approche prometteuse pour l'avenir des réseaux de communication. C'est un réseau de nouvelle génération qui vise à améliorer la manière dont les données sont transmises sur l'internet. Contrairement à l'Internet actuel qui est basé sur l'adresse IP et qui est principalement conçu pour transférer des données entre deux hôtes, NDN se concentre sur la communication basée sur le contenu, plutôt que sur les adresses IP.

Dans ce chapitre, nous avons présentés quelques limites de l'internet actuel, nous avons vu l'architecture NDN avec ses différentes fonctionnalités et ses principes comme le nommage, la résolution des noms, le routage et la sécurité. En outre, pour mieux détailler l'architecture NDN et scruter les performances et les avantages de ce réseau, ils nous faut comprendre et étudier les stratégies de cache que les routeurs NDN peuvent utiliser pour déterminer quelles données stocker et pendant combien de temps et nous allons voir est-ce que ces stratégies peuvent maximiser l'efficacité du cache. C’est tout ceci que nous allons étudier dans le deuxième chapitre.

CHAPITRE 2

LA MISE EN CACHE ET STOCKAGE PERMANENT

INTRODUCTION :

La mise en cache est l'une des révolutions de l'architecture réseau. Elle permet de remédier à l'augmentation du trafic des contenus en stockant des copies de ces contenus dans un emplacement de stockage temporaire, afin d'avoir un accès rapide en cas de besoin.

La mise en cache dans l'architecture NDN est plus avantageuse que celle de l'architecture traditionnelle TCP/IP. Les routeurs IP et NDN mettent en mémoire tampon les contenus. La différence est que les routeurs IP ne peuvent pas réutilisés les données après les avoir transférées tandis que ceux de NDN peuvent être réutilisés par les routeurs grâce à leur identification par les noms.

Dans ce chapitre, nous allons vous amener à comprendre la mise en cache dans le réseau Named Data Network, quelles sont les différentes stratégies de placement et de remplacement intervenant dans cette mise en cache.

1) Mise en cache dans NDN :

La mise cache dans NDN consiste à stocker les données dans les routeurs par lesquelles elles passent, pour qu'à chaque besoin de ces données on ait une réponse rapide. La mise en cache NDN se passe comme suit :

- L'utilisateur va envoyer un paquet d'intérêt, sur le chemin chaque routeur vérifiera son magasin de contenu pour vérifier si cette demande y existe. Si ce n'est pas le cas, il l'ajoutera à sa table PIT et la demande sera acheminée vers le producteur qui la satisfera.

- Sur le chemin de la livraison de la demande, des copies de cette demande se feront sur les routeurs en fonction de la stratégie de placement souhaitée.

Pour assurer la disponibilité des contenus, NDN met en place un nouvel élément de communication appelé repo, assurant le stockage permanent de tout type de données NDN [38]. Repo stocke permanemment tous les demandes pour avoir accès à ses demandes en cas besoin.

La mise en cache NDN est basée sur deux stratégies fondamentaux la stratégie de placement et la stratégie de remplacement.

La mise en cache des contenus NDN dans le réseau résout les inconvénients de l'architecture internet actuelle [39].

Le réseau NDN utilise trois processus de mise en cache :

a) La mise en cache du réseau :

Elle consiste à mettre le contenu dans un emplacement proche de l'utilisateur qui le demande.

b) La mise en cache sur le chemin :

Dans cette mise en cache, un morceau du contenu est mis en cache sur le chemin de son demandeur [40].

c) La mise en cache hors chemin :

Dans cette mise en cache, le contenu peut ou ne peut pas être mise en cache tout au long du chemin de livraison de la demande.

2) Stratégie de la mise en cache de NDN:

Le réseau de données nommées utilise deux stratégies de décision de mise en cache à savoir : stratégie de placement et de remplacement que nous allons expliquer ci-dessous.

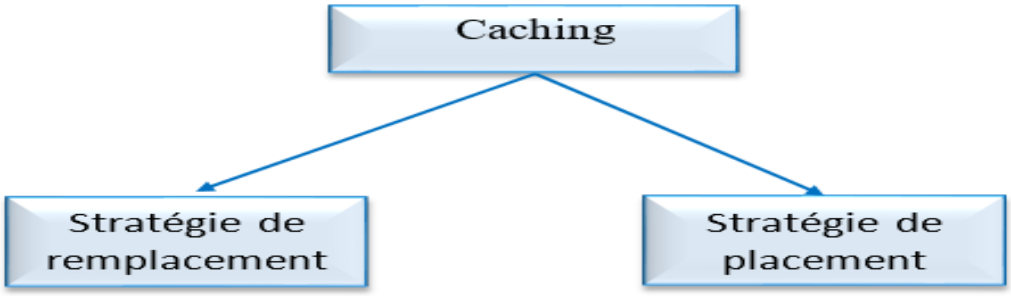


Figure 10 Les classifications des stratégies de mise en cache

Stratégie de placement : où le contenu doit être stocké.

Stratégie de remplacement : comment le contenu doit être changer pour mettre de la place aux nouveaux.

2.1) Stratégie de placement de cache :

Elle permet de déterminer où le contenu doit être stocké en utilisant plusieurs algorithmes dont les plus courants sont ce que nous allons décrire ci-dessous.

2.1.1) Leave Copy Everywhere(LCE) :

LCE est la stratégie par défaut qu'utilise l'architecture NDN. LCE stocke une copie du contenu demandé sur chaque routeur qui se trouve le long du chemin de la demande. Il permet d'avoir une réponse rapide du même contenu à la prochaine demande. LCE utilise LRU comme stratégie de remplacement par défaut pour faire de la place de stockage lorsque le contenu est plein. La stratégie de mise en cache LCE se déroule comme suit :

- Un consommateur envoie un paquet d'intérêt vers le producteur, sur le chemin chaque routeur va vérifier si le paquet d'intérêt est dans son magasin de contenu. Si cela n'est pas le cas il va l'envoyé au routeur suivant après l'avoir ajouté à sa table PIT.
- Lorsque le producteur reçoit le contenu il va envoyer le paquet de donnée sur le même chemin en sens inverse de l'intérêt, chaque routeur stocke une copie de cette donnée et la transmet au prochain routeur en aval.

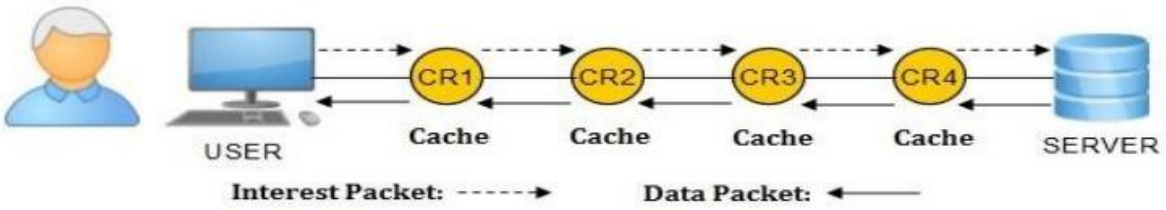


Figure 11 La stratégie de mise en cache LCE [41]

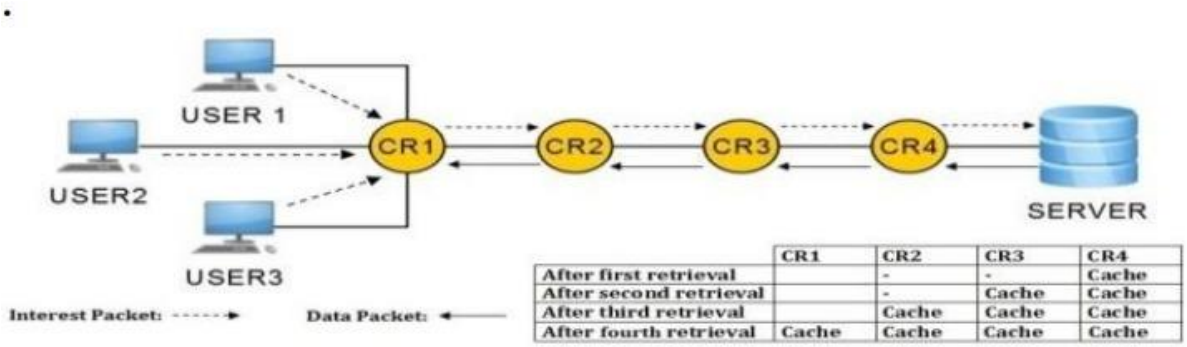
LCE réduit le temps de réponse en satisfaisant les prochaines demandes par les précédentes qui ont été mise en cache sur les routeurs-caches se trouvant en aval.

L'inconvénient de LCE est la duplication du contenu sur tous les routeurs-caches, cela consomme beaucoup de ressource du réseau et parfois n'est pas nécessaire. Le contenu le plus demandé peut être remplacé par le contenu le moins demandé. C'est cette redondance sur le chemin de livraison qui fait que la stratégie LCE est inefficace.

2.1.2) Leave Copy Down(LCD):

La stratégie de mise en cache LCD stocke une copie du contenu demandé sur le premier routeur qui se trouve sur le chemin de livraison de la demande. Comme la stratégie LCE, LCD aussi fait appelle à LRU comme mécanisme de remplacement par défaut pour supprimer des contenus en cas de saturation du stockage. Le processus de mise en cache LCD se fait comme suit :

- Un consommateur envoie un paquet d'intérêt vers le producteur, sur le chemin chaque routeur va vérifier si le paquet d'intérêt est dans son magasin de contenu. Si cela n'est pas le cas il va l'envoyé au routeur suivant après l'avoir ajouté à sa table PIT.
- Lorsque le producteur reçoit le contenu il va envoyer le paquet de donnée sur le même chemin en sens inverse de l'intérêt. Dans ce cas seul le premier routeur va faire une copie du paquet et le paquet sera acheminé vers le consommateur. A la prochaine demande de ce contenu, la copie se fera en aval sur le routeur qui suit celui qui a fait un cache la demande précédente.



	CR1	CR2	CR3	CR4
After first retrieval		-	-	Cache
After second retrieval		-	Cache	Cache
After third retrieval		Cache	Cache	Cache
After fourth retrieval	Cache	Cache	Cache	Cache

Figure 12 La stratégie de mise en cache LCD [41]

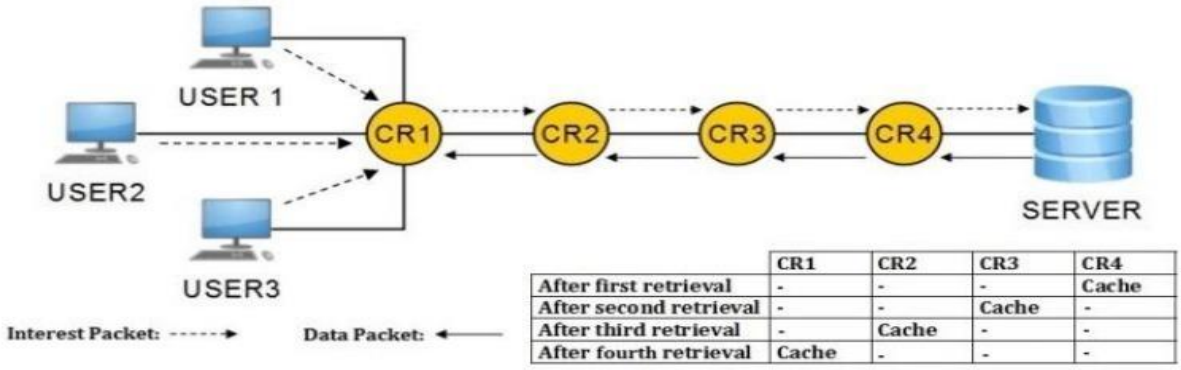
LCD a pour objectif de réduire la redondance du cache sur le réseau en faisant à chaque fois une copie de la donnée récupéré sur le premier routeur-cache qu'il rencontre sur le chemin de livraison. Mais elle consomme une grande partie de la bande passante en couvrant les caches du routeur sur le chemin de livraison et met une durée énorme pour mettre les données près de l'utilisateur. Il entraine une redondance inutile le long du chemin de livraison, ce qui affecte ses performances de mise en cache [39].

2.1.3) Move Copy Down(MCD) :

La stratégie de mise en cache MCD est un mécanisme de mise en cache coopératif et populaire [39]. MCD a été pour la première fois proposé par l'architecture internet actuelle, et après a été ajusté pour l'architecture de réseau centrée sur l'information. Il fonctionne de la même façon que la stratégie LCD, sauf qu'au lieu de faire une copie sur le premier routeur, il le fait sur le prochain routeur en aval. Le processus de mise en cache MCD se fait comme suit :

- Un consommateur envoie un paquet de d'intérêt vers le producteur, sur le chemin chaque routeur va vérifier si le paquet d'intérêt est dans son magasin de contenu. Si cela n'est pas le cas il va l'envoyé au routeur suivant après l'avoir ajouté à sa table PIT.
- Lorsque le producteur reçoit le contenu il va envoyer le paquet de donnée sur le même chemin en sens inverse de l'intérêt. Dans ce cas seul le prochain routeur cache va faire une copie du paquet et le paquet sera acheminé vers le consommateur. A la prochaine demande de ce contenu, la copie se fera en aval sur le routeur qui suit celui qui a fait un cache la demande précédente.

N.B : MCD ne duplique pas le contenu il le supprime du routeur actuelle pour le stocker sur le prochain routeur.



	CR1	CR2	CR3	CR4
After first retrieval	-	-	-	Cache
After second retrieval	-	-	Cache	-
After third retrieval	-	Cache	-	-
After fourth retrieval	Cache	-	-	-

Figure 13 La stratégie de mise en cache MCD [41]

MCD permet de réduire la redondance sur le chemin de livraison et de libérer une espace importante du magasin de stockage. Mais, MCD augmente la durée des demandes à cause de la suppression du contenu sur le routeur-cache, en le dupliquant sur le routeur suivant. Les ressources du réseau sont consommées par les demandes répétitives.

2.1.4) Caching avec Probabilité (PROB(P)) :

Similaire à LCE, cette stratégie met en cache le contenu avec une probabilité donnée p et ne le met pas en cache avec la probabilité 1-p. Lorsque le routeur-cache est atteint par le paquet de donnée, des nombres aléatoires comprises entre 0 et 1 seront diffusés par ce routeur. Si ce nombre est inférieur à p alors le paquet de donnée sera caché par le routeur, sinon il sera diffusé par le routeur sans qu'il soit stocké. Comme LCE, PROB(P) aussi utilise LRU comme stratégie de remplacement par défaut. Le processus de cette mise en cache se déroule de la façon suivante :

- Un consommateur envoie un paquet d'intérêt vers le producteur, sur le chemin chaque routeur va vérifier si le paquet d'intérêt est dans son magasin de contenu. Si cela n'est pas le cas il va l'envoyé au routeur suivant après l'avoir ajouté à sa table PIT.
- Lorsque le producteur reçoit le contenu, le router-cache va générer une valeur cache qui sera insérée dans le paquet de données puis sera transmis en sens inverse de l'intérêt. Chaque routeur se trouvant le long de ce chemin va vérifier la valeur du paquet entrant. Si cette valeur est inférieure ou égale à p alors une copie du paquet de donnée entrant sera stockée par le routeur et

ensuite il envoie le paquet vers l'aval. Dans le cas contraire, il enverra le paquet en aval sans stockage de copie.

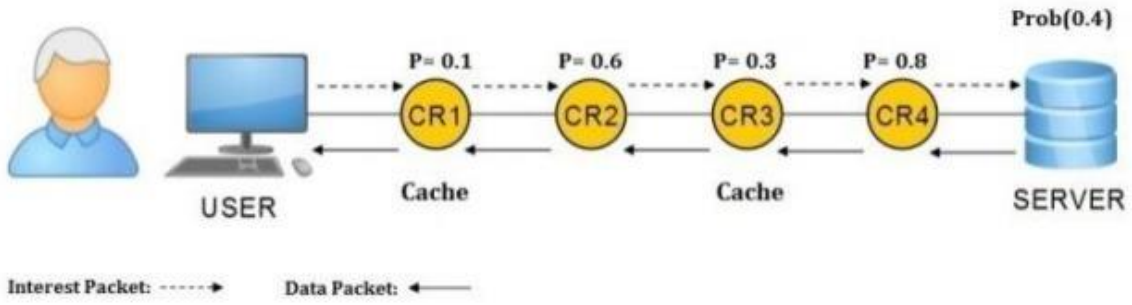


Figure 14 La stratégie de mise en cache PROB(P) [41]

PROB(P) stocke plusieurs paquets de données sur chaque routeur qu'il rencontre tout au long du chemin en aval. PROB(P) permet l'amélioration de l'efficacité du cache. La performance de PROB(P) dépend de la valeur donnée à p, si la valeur p égale à 1 PROB(P) se comportera comme LCE.

2.1.5) Probcache :

Probcache est une stratégie de mise en cache probabiliste appartenant à Information-Centric Network (ICN). Probcache cache dans les nœuds des routeurs se trouvant sur le chemin de la livraison avec des probabilités différentes pour chaque nœud. Probcache se base sur deux facteurs; le premier facteur est TimesIn, qui est la quantité de trafic qu'il doit servir, le second est le poids du cache, ce qui signifie le taux de distance entre l'utilisateur et le routeur de contenu et la distance entre l'utilisateur et le serveur [41]. Pour calculer la probabilité de mise en cache Probcache(x), Probcache va d'abord calculer le TimesIn et le Weight cache en fonction des valeurs du Time-Since-Inception(TSI) et du Time-Since-Born(TSB), puis va multiplier le TimesIn par le weight cache ce qui donne la valeur de Probcache(x).

$$ProbCache(x) = TimesIn(x) \times CacheWeight(x)$$

Avec:

$$\text{TimesIn(x)} = \frac{\sum_{i=1}^{b-(a-1)} Ni}{T_{fc}\mathrm{N_a}}$$

Où :

b : est le TSI (temps depuis le début) ;

a : est le TSB (temps depuis la naissance) ;

Ni: Nombre de contenu d'un routeur cache

T_{fc}: Temps de conservation du contenu sur le chemin de livraison. Elle est estimée à 10s.

$\mathrm{N_a}$: Taille moyenne que peut avoir une cache le long du chemin ;

$\sum_{i=1}^{b-(a-1)} Ni$: Somme du résultat de la soustraction TSI moins TSB qui prend en compte que les caches restantes au lieu de toutes les caches du consommateur au producteur.

Le poids du cache pour l'entrée est calculé pour obtenir une allocution équitable des ressources sur le chemin de livraison [39].

$$CacheWeight(x) = \frac{a}{b}$$

Probcache aussi utilise LRU comme stratégie de remplacement par défaut.

Le routeur ayant la Probcache(x) la plus grande mettra en cache le contenu avec une probabilité plus grande, comme le montre la figure.

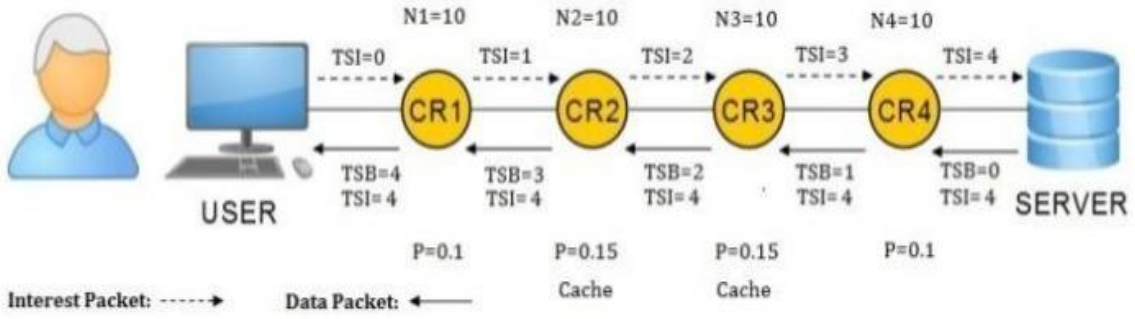


Figure 15 La stratégie de mise en cache Probcache [41]

Probcache vise à minimiser la redondance de la mise en cache et à assurer une allocation équitable des ressources de cache le long du chemin de livraison.

Les calculs sur les routeurs font l'objet de la consommation des ressources des routeurs-caches et favorise l'augmentation du retard.

2.1.6) Randomly copy one(RCOne) :

Similaire à LCD, la stratégie de mise en cache RCOne sélectionne au hasard le routeur-cache sur lequel la copie sera placée contrairement à LCD qui fait la copie sur le premier routeur après un saut. RCOne utilise LRU comme stratégie de remplacement par défaut. Cette stratégie de mise en cache se fait comme suit :

- Un consommateur envoie un paquet d'intérêt vers le producteur, sur le chemin chaque routeur va vérifier si le paquet d'intérêt est dans son magasin de contenu. Si cela n'est pas le cas il va l'envoyer au routeur suivant après l'avoir ajouté à sa table PIT.
- Lorsque le producteur reçoit le contenu, une copie de celui-ci est stockée par un seul routeur-cache sélectionnée au hasard sur le chemin de livraison. Les autres routeurs-caches ne feront que transmettre la demande.

Cette stratégie réduit la duplication, permet de varier les contenus et réduit les frais.

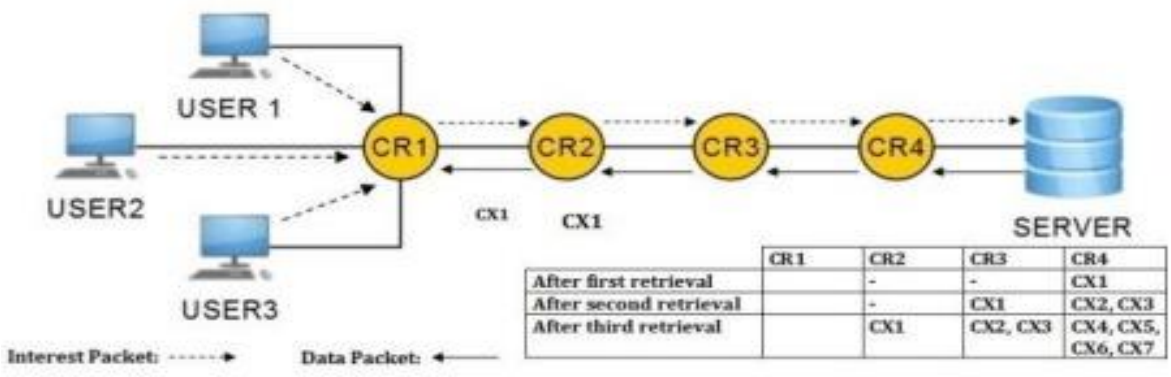
Son inconvénient est que sa manière de choisir l'emplacement des copies joue sur l'efficacité de NDN.

2.1.7) Wave :

Similaire à LCD, la différence est que le mécanisme de mise en cache wave est basé sur la division de contenu en plusieurs morceaux. Un nœud suggère explicitement au nœud suivant quel contenu doit être stocké [42]. Wave utilise LRU comme stratégie de remplacement par défaut. Le processus de mise en cache wave se passe comme suit :

- Lorsqu'un consommateur demande un morceau de contenu, celle-ci sera acheminée vers le producteur. Sur le chemin de la demande, il peut y avoir un routeur-cache qui stocke ce morceau, si c'est le cas celui-ci satisfera la demande sinon elle sera transmise au producteur.

- La mise à jour du nombre de contenu à stocker dépendra du nombre d'accès. Le stockage du nombre de morceaux de contenus dépendra de la suggestion du producteur ou du routeur-cache. Le producteur ou le routeur-cache recommandera de stocker un morceau dans son routeur-cache en aval en marquant le morceau de contenu [39]. Le contenu peut être soit mise en cache ou soit ignoré par le routeur-cache. Chaque routeur-cache prend sa propre décision de mise en cache sans consulter les autres routeurs-caches.



	CR1	CR2	CR3	CR4
After first retrieval		-	-	CX1
After second retrieval		-	CX1	CX2, CX3
After third retrieval		CX1	CX2, CX3	CX4, CX5, CX6, CX7

Figure 16 La stratégie de mise en cache wave [41]

La stratégie de placement wave est une proposition permettant l'amélioration de l'utilisation du cache et de la livraison du contenu.

Wave a les mêmes inconvénients que NDN. Le stockage des morceaux de contenus prend beaucoup de temps avant d'être effectué.

2.2) Stratégie de remplacement du cache :

La taille du CS est limitée pour pouvoir stocker de nouveaux contenus si nécessaire. La stratégie de remplacement permet d'y remédier en évacuant les contenus obsolètes pour faire de la place à de nouveaux contenus. Plusieurs politiques de remplacement sont recensées dans cette stratégie. Ces stratégies sont adaptées aux spécificités et caractéristiques de ces environnements [43]. Cinq stratégies de mise en cache ont été mise en évidence () à savoir :

- Les stratégies de remplacement de cache basées sur la récence
- Les stratégies de remplacement de cache basées sur la fréquence
- Les stratégies de remplacement de cache basées sur la taille.

- Les stratégies de remplacement de cache basées sur les fonctions
- Les stratégies de remplacement de cache dédiées aux environnements mobile.

Nous allons nous intéresser aux deux premières stratégies et d'autres qui ne font pas partie de ces catégorie.

2.2.1) Les stratégies de remplacement de cache basées sur la récence :

- Least Recently Used (LRU): LRU est la stratégie la moins récemment utilisée, elle consiste à supprimer le contenu le moins récemment utilisé pour permettre aux nouveaux contenus d'avoir de l'espace pour leur mise en cache. C'est la stratégie de remplacement la plus utilisée. Il est principalement utilisé en raison de son exécution et de sa proportion de succès en cache [40].
- LRU-Threshold [44]: qui est une extension de LRU. Dans cette politique tant que la taille du contenu dépasse un seuil donné il ne sera pas stocké, sinon il se comportera comme LRU.
- LRU-Hot [45]: qui est aussi une extension de LRU, contrôle deux listes LRU : une pour les contenus chauds (populaires) et une pour les contenus froids (pas aussi populaires) [43]. Si un contenu a une fréquence d'accès au-dessus d'un seuil donné on dit qu'il est chaud. Le client reçoit cette information avec le contenu. C'est grâce à cette information que le contenu est stocké dans la liste qu'il faut. Le traitement de ces listes se fait différemment. Cette politique utilise deux compteurs qui sont tous initialisés à zéro : un compteur de base et un compteur pour les contenus chauds. Après chaque envoie d'intérêt le compteur de base est augmenté d'un et un ajout d'un se fait après chaque α requêtes (α > 1). Quand un contenu est reçu, il est stockée au début de sa liste correspondante, et une valeur d'accès lui est affectée et est égale à la valeur actuelle du compteur de base. Sur un remplacement, le cache recalcule les valeurs des deux documents se trouvant dans les queues des deux listes [43].

$$hot\_value = tail_{hot} - hot\,reference\,counter$$

$$cold\_value = tail\_cold - cold\,reference\,counter$$

Ces politiques sont simples à mettre en œuvre grâce à la liste LRU que la plupart utilise. Cette liste stocke les nouveaux contenus en tête de liste et en cas d'un hit il est remplacé et mis à la fin de la liste.

L'inconvénient de cette politique est qu'elle ne prend pas en compte la fréquence.

2.2.3) Les stratégies de remplacement de cache basées sur la fréquence :

- Least Fréquent Used(LFU): LFU est la stratégie la moins fréquemment utilisée. Elle consiste à évacuer le contenu le moins fréquemment utilisé pour permettre la mise en cache des nouveaux contenus.
- LFU-Aging [46]: est une extension de LFU. Cette politique permet d'éviter la pollution de cache qui est le cache des contenus populaires qui ne sont plus sollicités. LFU-Aging utilise un seuil, si la valeur de tous les compteurs est supérieure à ce seuil, ils seront tous divisés par deux.
- HYPER-G [47] : est une combinaison de LRU et LFU et fait recours aussi à la taille des contenus. HYPER-G est une stratégie de remplacement hybride. Premièrement, il utilise la stratégie LFU. S'il voit que plusieurs contenus ont la même fréquence, il choisit le contenu le moins récemment utilisé. Si cela aussi ne répond pas aux critères alors il choisit le plus grand contenu.

Une stratégie de remplacement hybride est une stratégie basée sur plusieurs critères.

Ces stratégies prennent en compte la fréquence et la récence qui sont des facteurs très importantes.

Cette politique peut avoir pour inconvénient la pollution du cache dont pour y remédier on fait appelle à la méthode Aging. Les contenus peuvent avoir la même fréquence.

2.2.4) Les stratégies de remplacement de cache basées sur la taille :

- **LRU-Min** [44]**:** C'est une variante de la stratégie LRU qui essaye de minimiser le nombre de documents à remplacer [43]. Elle se déroule en quatre étapes. Prenons A et t représentants respectivement une liste et un seuil.

1ére étape : t va recevoir un contenu de taille N.

2ème étape : A comprendra tous les documents qui ont une taille N inférieure ou égale à t (A peut ne rien contenir c'est-à-dire vide).

3ème étape : A utilisera la stratégie de remplacement LRU jusqu'à ce qu'elle soit pleine ou qu'elle ait une taille de cache équivaut à au moins t.

4ème étape : si cette taille de cache n'est pas au moins t, t recevra t/2 et un retour se fera à l'étape deux.

- **SIZE** [47] **:** Cette stratégie remplace le plus grand document [43]. Pour les contenus ayant la même taille, on applique la stratégie LRU.

L'avantage de ces stratégies est qu'elles combinent la récence et la fréquence, s'ils sont bien définis, chaque stratégie peut éviter les inconvénients des deux stratégies [43].

Elles ont pour inconvénient la mauvaise gestion du cache car, celui-ci nécessite la prise en compte de la taille et de la fréquence. Une modification de la valeur de la fréquence peut entraîner une réorganisation des listes, parce que l'objet correspondant doit être inséré dans une nouvelle liste [43].

2.2.5) Les stratégies de remplacement de cache basées sur les fonctions :

- **LRFU** [48]**:** est une stratégie de remplacement hybride prenant en compte la fréquence et la récence. Elle combine les stratégies LRU et LFU. LRFU associe à chaque bloc une valeur appelée CRF (Combined Recency and Frequency) valeur et qantifie la probabilité que le bloc soit référencé dans un avenir proche [48].Chaque valeur donné à un bloc une CRF. Cette valeur est déterminée par une fonction F(x) qui est une fonction de pesage c'est-à-dire basée sur le poids. LRFU choisie la valeur CRF minimale pour remplacer un bloc.

$$\mathbf{F(X)=}\left(\frac{1}{2}\right)^{\lambda x}$$

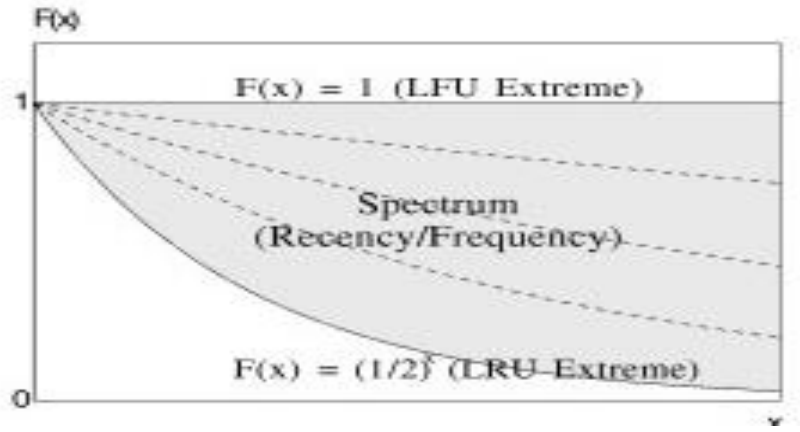


Figure 17 Les spectres de LRFU selon la fonction F (X) *[48]***.**

La figure 17 permet de bien se situer dans LRFU.

- Si F(x)=1, LRFU devient LFU (λ=0).
- Si F(x)=$^1/_2$, LRFU devient LRU (λ=1).

Avec x = (temps_courant – temps_précédent).

- **TSP (Taylor Series Prediction)** [49]**:** Hi étant la valeur caractéristique d'un document, TSP la calcule comme suit :

$$H_i = \frac{f_i \times C_i}{S_i \times T_t}$$

et

$$T_t = t_p - t_c$$

où Ci est le coût de chargement du document i depuis son serveur ;

S_i est la taille de document i ;

f_i est la fréquence de document i ;

T_t décrit "l'accroissement" temporelle de la requête vers le document i ;

t_p est une prédiction de temps prévu de la prochaine requête pour ce document i ;

t_c est le temps courant. Le t_p est déterminé avec la série de Taylor de second degré.

Figure 18 Le calcul de Hi avec TSP.

L'avantage des stratégies basées sur la fonction est qu'elles n'exigent pas une combinaison fixe des facteurs utilisés, à travers un choix approprié des paramètres, on peut optimiser n'importe quelle métrique de performance. Elles prennent en considération un certain nombre de facteurs qui permettent de manipuler différentes situations de charge de travail [43].

L'inconvénient de ces stratégies est l'utilisation du poids dans les paramètres pour le remplacement. Cette utilisation est une tâche très difficile qui peut causer des problèmes de performance.

A ces politiques, on peut ajouter :

- First In First Out(FIFO) : FIFO est la stratégie du premier entré premier sorti et la plus simple. Elle consiste à mettre tous les contenus mise en cache dans une file d'attente dans laquelle le plus ancien contenu mise en cache sera en tête de la file. En cas de saturation de cette file, le contenu le plus ancien sera évacué pour faire de la place au nouveau contenu.
- RAND (aléatoire) : RAND est la sélection aléatoire d'un contenu. Elle consiste à sélectionner aléatoirement un contenu afin de l'évacuer et de faire de la place aux nouveaux.

CONCLUSION :

Dans ce chapitre, nous avons abordé les points essentiels de la mise en cache du réseau NDN. Nous avons soulevés les stratégies importantes de la mise en cache de NDN en faisant une explication de leur idée principale, en détaillant leur fonctionnement et en soulevant certains avantages et inconvénients.

La mise en cache est l'une des facteurs causant des failles dans le réseau. Pour remédier à ces failles, il faut une sécurité solide du réseau. Le chapitre à venir fera l'objet d'une explication détaillée sur la sécurité et les attaques DDos dans le réseau NDN.

CHAPITRE 3

LA SECURITE DANS LES RESEAUX NDN : LES ATTAQUES DDOS

INTRODUCTION :

Les attaques par déni de service distribué (DDoS) sont devenues une menace majeure pour la sécurité sur Internet. Ces attaques visent à submerger les serveurs cibles avec un trafic excessif, ce qui entraîne l'indisponibilité des services en ligne pour les utilisateurs légitimes. Les conséquences peuvent être dévastatrices, entraînant des pertes financières, une dégradation de la réputation et une atteinte à la confiance des utilisateurs.

À la différence de l'Internet actuel, où les mesures de sécurité sont ajoutées après sa conception, NDN a pour objectif principal d'intégrer dès les premières étapes de conception des fonctionnalités de sécurité et de confidentialité. Notamment, afin de préserver la vie privée des utilisateurs, aucune adresse source n'est incluse dans les paquets [50]. Les routeurs enregistrent dans la table PIT l'interface d'origine des paquets d'intérêt, qu'ils utilisent ensuite pour transmettre les données aux utilisateurs. NDN offre également intrinsèquement une protection contre les données non sollicitées en adoptant un modèle de récupération de données piloté par le destinataire [51] .

Cependant, malgré les avantages de sécurité mentionnés précédemment, NDN est vulnérable à de nouveaux types d'attaques par déni de service distribué (DDoS) [52]. L'une de ces attaques les plus complexes est l'attaque DDoS sur les tables PIT, où un attaquant inonde le réseau avec un grand nombre de faux paquets d'intérêt. Chaque paquet de ce type pousse le routeur à créer et à conserver une entrée dans sa table PIT, ce qui gaspille les ressources de stockage du routeur et peut même provoquer un débordement de la table PIT. Ce type d'attaque est connu sous le nom d'attaque par submersion d'intérêt (IFA) [53], et s'il n'est pas correctement contré, il peut sérieusement perturber le fonctionnement normal d'un système NDN.

Dans cette perspective, ce chapitre se concentrera sur les attaques DDoS et les mesures de sécurité qui sont mises en œuvre en dehors du contexte du réseau NDN. Nous explorerons l'attaque IFA (Interest Flooding Attack), ainsi que le mécanisme de détection basé sur le mécanisme d'attention avec LSTM.

1) Les attaques DDoS : Un défi persistant pour la stabilité de l'Internet

La croissance exponentielle du nombre d'utilisateurs et l'évolution des services disponibles sur Internet ont engendré d'importants avantages tant sur le plan économique que social. On peut notamment penser à la création de nouveaux marchés et opportunités professionnelles, à la facilité déconcertante d'accès à l'information, ainsi qu'à la disponibilité de plates-formes numériques d'agrégation qui permettent une communication instantanée avec n'importe qui, n'importe où dans le monde.

Cependant, cette opportunité comporte également des dangers pour les entreprises fournissant des services numériques en ligne, ainsi que pour les utilisateurs eux-mêmes. Chaque secteur technologique est exposé à des risques et menaces spécifiques (voir figure 19), tels que les logiciels malveillants, le hameçonnage, les attaques DDoS et les actes de cyber-activisme, souvent perpétrés par des groupes soutenus par des États (connus sous le nom d'APT : Menaces Persistantes Avancées).

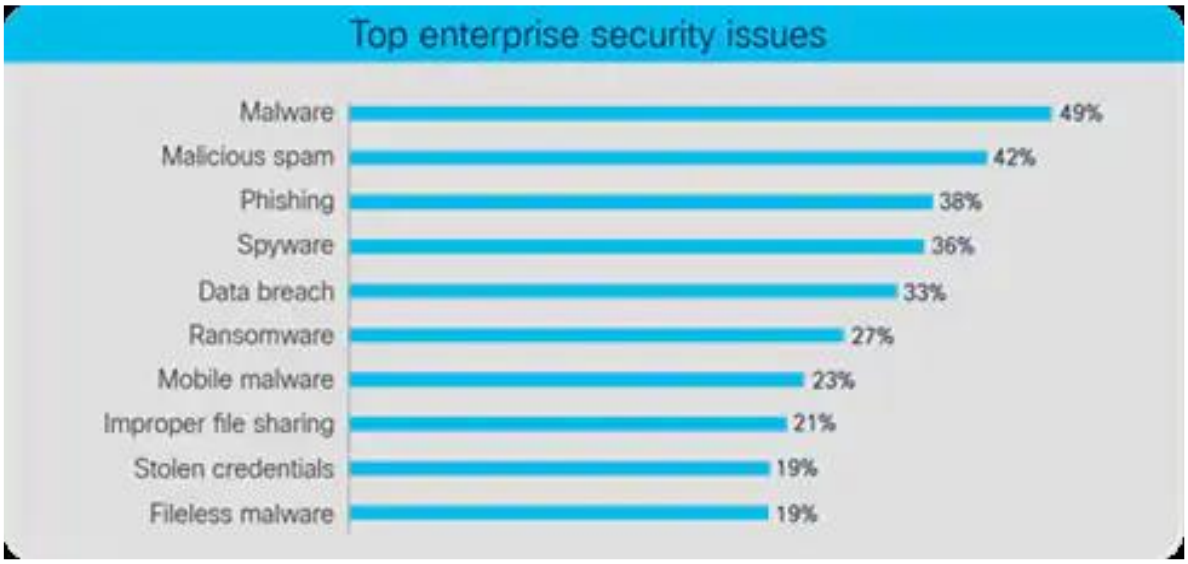


Figure 19 Les principaux problèmes de sécurité rencontrés dans les entreprises [54].

Le courrier électronique constitue le principal vecteur d'attaque lorsqu'une entreprise ou un utilisateur est victime d'une violation de sécurité. Il est souvent utilisé pour inciter la victime à divulguer des informations d'identification ou à installer des logiciels malveillants, compromettant ainsi d'autres services ou systèmes.

Parmi les menaces les plus préoccupantes pour les fournisseurs d'accès à Internet (FAI) [54], figurent les attaques DDoS (Déni de Service Distribué), qui consistent à submerger les serveurs de la victime de nombreuses requêtes provenant d'un vaste réseau d'appareils compromis, communément appelés "zombies" ou "robots-zombies".

L'état actuel de ces opérations pose un problème pour les organisations, car les machines attaquées voient leurs ressources s'épuiser au point qu'elles ne peuvent plus fournir les services en ligne aux utilisateurs.

La plus grande attaque DDoS jamais enregistrée a été observée par Google en 2017 et rendue publique le 16 octobre 2020 [55]. La société américaine a réussi à contrer le trafic malveillant d'une capacité de 2,5 Tbps provenant de centaines de milliers de machines infectées, soit le double de l'attaque contre GitHub en 2018 [56] .

L'augmentation du nombre d'appareils IoT mentionnée précédemment est étroitement liée aux problèmes de cybersécurité. Bien que l'adoption mondiale de solutions intelligentes apporte de nombreux avantages pour les utilisateurs, elle comporte également des risques liés à leur mise en œuvre. Les logiciels embarqués et les services Web fournis par les fournisseurs de services IoT ne sont pas suffisamment sécurisés. Une fois compromis, ces appareils sont utilisés pour former des botnets et mener des attaques DDoS, comme le célèbre Mirai [57].

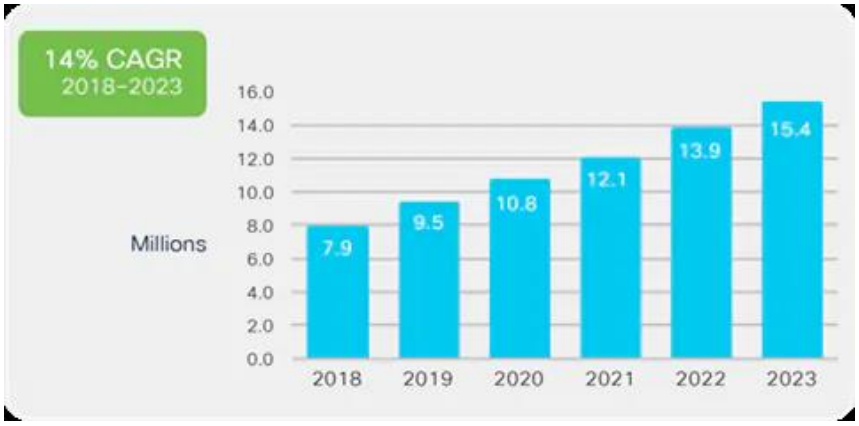


Figure 20 Le nombre (en millions) d'attaques DDoS attendues jusqu'en 2023 [54]**.**

Comme le montre la figure 20, ce phénomène est en forte croissance, et des études prévoient que le nombre d'attaques DDoS en 2023 pourrait doubler par rapport à celui enregistré en 2018.

Il est donc impératif que les communautés de fabrication et de recherche se concentrent sur la promotion de processus de développement sécurisés et de mesures efficaces pour atténuer ces attaques.

2) Les attaques DDoS dans NDN :

2.1) IFA (Interest Flooding Attack) :

Les utilisateurs malveillants ou compromis peuvent exploiter le mécanisme de transfert basé sur la table PIT de NDN pour lancer des attaques d'intérêt submergé (Interest Flooding Attack - IFA), considérées comme l'un des types les plus graves d'attaques DDoS sur NDN [58]. Dans le cadre de l'IFA, l'utilisateur malveillant (ou un groupe d'utilisateurs) envoie un grand nombre de faux paquets d'intérêt. À chaque réception de ces paquets, chaque routeur crée une entrée dans sa table PIT et transfère le paquet au nœud suivant (routeur ou source de contenu). Selon les règles de NDN, une entrée est supprimée de la table PIT dans deux cas :

- L'entrée expire (par exemple, une durée d'expiration typique est de 1 seconde [59]).
- Le routeur reçoit le paquet de données correspondant avant l'expiration de l'entrée.

Ainsi, la meilleure stratégie d'attaque consiste à émettre des paquets d'intérêt pour un contenu qui n'existe pas. Dans ce scénario, les fausses entrées restent dans la table PIT aussi longtemps que possible. L'objectif de l'attaquant est de remplir rapidement la table PIT et de la maintenir pleine, afin que les paquets d'intérêt émis par les utilisateurs légitimes finissent par être abandonnés.

Dans la Figure 21 ci-dessous, nous présentons un exemple simple d'IFA dans NDN. Supposons que la capacité de la table PIT de chaque routeur soit de 3 entrées. La stratégie de l'attaquant est d'envoyer 3 faux paquets d'intérêt pour du contenu inexistant (différent). Ces paquets remplissent les tables PIT des deux routeurs. La source abandonne ces paquets car ils demandent un contenu qui n'existe pas. Cependant, les entrées correspondantes demeurent dans les tables PIT jusqu'à leur expiration. Après l'expiration, l'attaquant émet 3 nouveaux paquets d'intérêt dans le but de maintenir les tables PIT constamment pleines. Ainsi, certains, voire tous les paquets d'intérêt des utilisateurs légitimes, seront abandonnés.

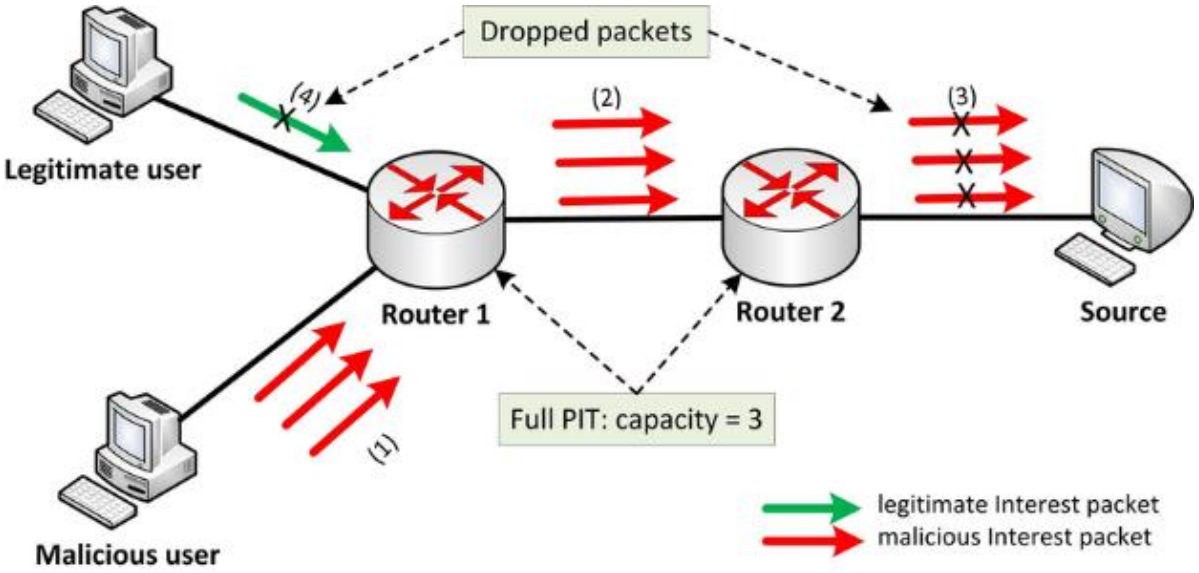


Figure 21 L'IFA (Interest flooding attack) dans NDN

2.2) Autres attaques DDos :

Dans cette partie, nous abordons brièvement d'autres types d'attaques DDoS possibles dans NDN :

a. Cache poisoning/pollution attack : L'attaquant cherche à réduire l'efficacité du cache en le remplissant de contenus impopulaires, voire même de contenus falsifiés. Cela peut être réalisé en demandant de manière répétée le même contenu impopulaire. L'objectif est d'augmenter les erreurs de cache et de forcer les paquets d'intérêt à atteindre la source de contenu. Ce type d'attaque est difficile à atténuer, car l'utilisateur malveillant peut se faire passer pour un utilisateur légitime pendant une longue période.

b. mobile interest flooding attack : L'attaquant peut visiter périodiquement différents routeurs et émettre des paquets d'intérêt frauduleux. Cette attaque est plus difficile à détecter et à atténuer que l'IFA classique. La raison en est que la retransmission de paquets d'intérêt en cas de mobilité est une procédure normale dans NDN. Ainsi, pour détecter un attaquant mobile, un schéma complexe impliquant un grand nombre de routeurs coopérants serait nécessaire.

c. Attaque sur le mécanisme de transfert : Un routeur potentiellement compromis peut sérieusement affecter les performances du réseau en redirigeant les paquets d'intérêt dans la

mauvaise direction. En cas d'attaquants coopérants, cela pourrait même être exploité pour créer des boucles de transfert dans le réseau.

L'attaque IFA présente de graves risques et une dissimulation intense. Les chercheurs ont exploré différentes méthodes de défense, principalement basées sur l'apprentissage automatique et les techniques statistiques. En raison des caractéristiques du trafic réseau, il est difficile d'identifier précisément les attaques sur un seul intervalle de temps, ce qui entraîne une faible précision de détection des attaques. Dans ce mémoire, nous utilisons des données passées à travers une fenêtre glissante et un modèle proposé basé sur l'attention et la mémoire à court terme (LSTM) [60] pour détecter l'IFA. Une fois l'IFA détectée, la distance de Hellinger est utilisée [61] pour identifier le préfixe malveillant.

3) Mécanisme de détection basé sur le mécanisme d'attention avec LSTM :

Cette section présente une vue d'ensemble du mécanisme de défense, du mécanisme de détection et du mécanisme de mitigation proposés. Nous avons choisis le modèle LSTM parce qu'il est l'un des modèles les plus récents et les plus avancés dans le domaine de l'apprentissage automatique et du traitement des séquences.

3.1) Aperçu :

Le mécanisme de défense comprend principalement cinq parties : le module de collecte des données, le module de prétraitement des données, le module de détection, le module de réponse et le module d'atténuation, comme illustré dans la Figure 19.

Dans le module de collecte de données, les données de trafic sont collectées et ensuite entrées dans le module de prétraitement. Dans ce dernier, les caractéristiques du trafic sont extraites. Ces caractéristiques sont utilisées pour détecter l'IFA dans le module de détection. Une fois l'IFA détecté, le module de réponse se met en action pour identifier le préfixe malveillant. Enfin, le module d'atténuation utilise ce préfixe malveillant afin de limiter les paquets d'intérêt malveillants.

3.2) Long-Short-Term-Memory (LSTM) :

Le deep learning est largement utilisé et trouve des applications dans divers domaines. Les Réseaux Neuronaux Récurrents (RNN) [62] sont une famille de méthodes de deep learning qui peuvent être utilisées pour détecter des anomalies. Cependant, les RNN rencontrent un problème de disparition de gradient [63]. La Mémoire à Court Terme Longue (LSTM) [60] est une version améliorée des RNN qui résout ce problème. La structure LSTM est illustrée dans la Figure 23. Elle

est principalement composée de trois éléments : la porte d'entrée, la porte d'oubli et la porte de sortie, qui permettent de mettre à jour la cellule LSTM de la manière suivante [60]:

$$
\begin{aligned}
f_t &= \sigma\big(W_f\,[h_{t-1}, x_t] + b_f\big), \\
i_t &= \sigma\,(W_i[h_{t-1}, x_t] + b_i\,, \\
\tilde{C}_t &= \tan h(W_c\,[h_{t-1}, x_t] + b_c)\,, \\
C_t &= f_t * C_{t-1} + i_t * \tilde{C}_t\,, \\
o_t &= \sigma\,(W_o[h_{t-1}, x_t] + b_o\,), \qquad et \\
h_t &= o_t * \tan h\,(C_t),
\end{aligned}
\tag{1}
$$

- W (weights) : les poids,
- b (bias) : le biais,
- h_t (hidden state at time step t) : l'état caché à l'instant t,
- x_t (input at time step t) : l'entrée à l'instant t.

3.3) Mécanisme d'Attention :

Le mécanisme d'attention, inspiré du comportement d'attention humaine, est largement utilisé dans le domaine de deep learning.

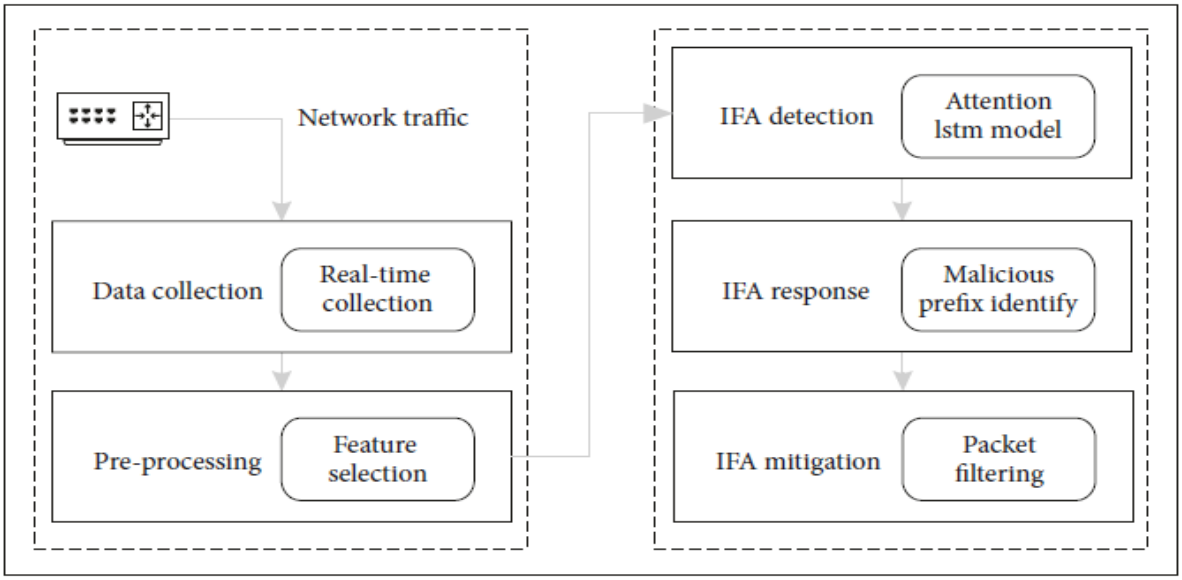


Figure 22 L'architecture du mécanisme de défense.

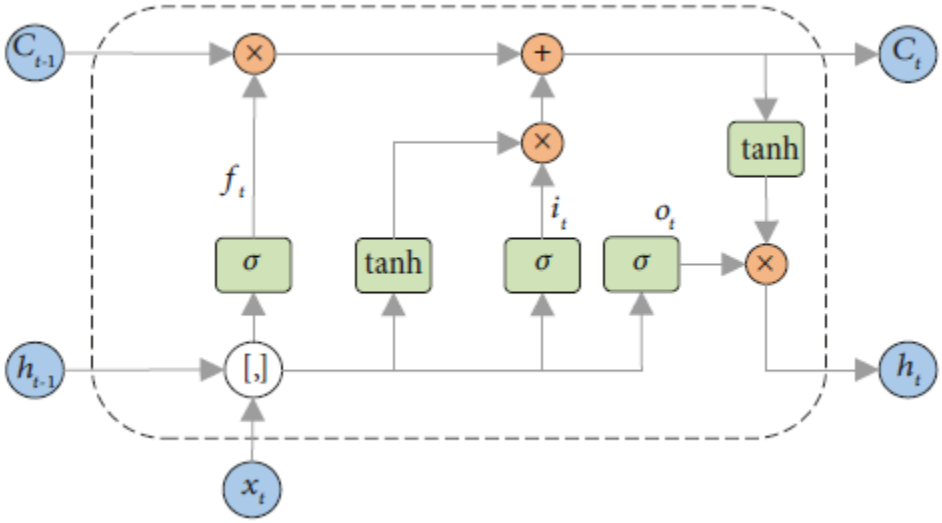


Figure 23 La structure d'une cellule LSTM [9].

Dans l'article [64], le mécanisme d'attention a été proposé. En considérant une entrée

$X = [\, x_1, x_2, \dots, x_N] \epsilon\, R^{D*N}$, où N représente la longueur de l'entrée, $x_n \epsilon\, R^D, n \,\epsilon\, [1\,, N]$.

D correspond au nombre de dimensions à chaque étape temporelle, le calcul du mécanisme d'attention se déroule en deux étapes : tout d'abord, on calcule la probabilité d'attention pour chaque élément de l'entrée, puis on effectue une moyenne pondérée des informations d'entrée en utilisant la probabilité d'attention correspondante.

3.4) Mécanisme de Détection :

Cette section expose en détail le mécanisme de détection. Dans un premier temps, nous répertorions les notations utilisées et définissons certaines caractéristiques. Les notations utilisées sont présentées dans le Tableau 2.

Définition 1. (Taille d'utilisation du PIT du routeur). Elle représente le nombre d'entrées PIT présentes dans le PIT pendant une période de temps donnée.

$$U(t_i\,, R_j) = e\,(t_i\,, R_j). \tag{2}$$

Définition 2. (Ratio de satisfaction des intérêts du routeur). Cela représente le rapport entre le nombre de paquets de données reçus et le nombre de paquets d'intérêt reçus pendant une période de temps spécifique.

$$S(t_i, R_j) = \frac{\varphi(\phi(t_i, R_j))}{\phi(t_i, R_j)} \quad (3)$$

Définition 3. (Fréquence des demandes d'intérêt du routeur). Il s'agit du nombre de paquets d'intérêt reçus pendant une période de temps spécifique.

$$I(t_i, R_j) = \phi(t_i, R_j) \quad (4)$$

Définition 4. (Fréquence de réponse des données du routeur). Il s'agit du nombre de paquets de données répondus pendant une période de temps spécifique.

$$r(t_i, R_j) = \varphi(\phi(t_i, R_j)) \quad (5)$$

Le calcul des caractéristiques est présenté dans l'algorithme 1.

Le mécanisme de détection détecte l'IFA à travers une fenêtre glissante, comme illustré dans la Figure 23.

Le trafic réseau est formellement considéré comme une série temporelle :

$Z = [z^1, z^2, \dots, z^i, \dots, z^F]$, Qui comprend F étapes temporelles. $z^i (1 \leq i \leq F)$ Représente la i-ème étape temporelle. Pour chaque fenêtre glissante, composée de φ étapes temporelles, le modèle de détection est utilisé pour classer la fenêtre glissante comme étant légitime ou malveillante.

La Figure 24 montre le LSTM avec mécanisme d'attention pour la détection de l'IFA. Le mécanisme d'attention peut améliorer les performances du LSTM en utilisant de manière discriminante chaque étape d'information d'état caché [65]. Par conséquent, cet article utilise le LSTM traditionnel avec mécanisme d'attention pour détecter l'IFA. Les états cachés de chaque étape sont pondérés par les poids d'attention. Dans la couche LSTM, l'entrée de chaque étape est transformée en un état caché.

$$h_i = LSMT(z_i), \qquad i \in [1, F] \quad (6)$$

Où h_i représente l'état caché à l'étape i et z_i représente l'entrée à l'étape i.

Dans la couche d'attention, l'état caché de chaque étape est utilisé en tant qu'entrée pour une couche d'attention ultérieure. Elle prend la forme suivante [66]:

$$\mathrm{H} = \sum_{t=1}^{N} \alpha_t \, h(t), \qquad et \tag{7}$$

$$\alpha_t = \frac{\exp(g_t(W_t, h(t)))}{\sum_{t=1}^{N} \exp(w_t, h(t))},$$

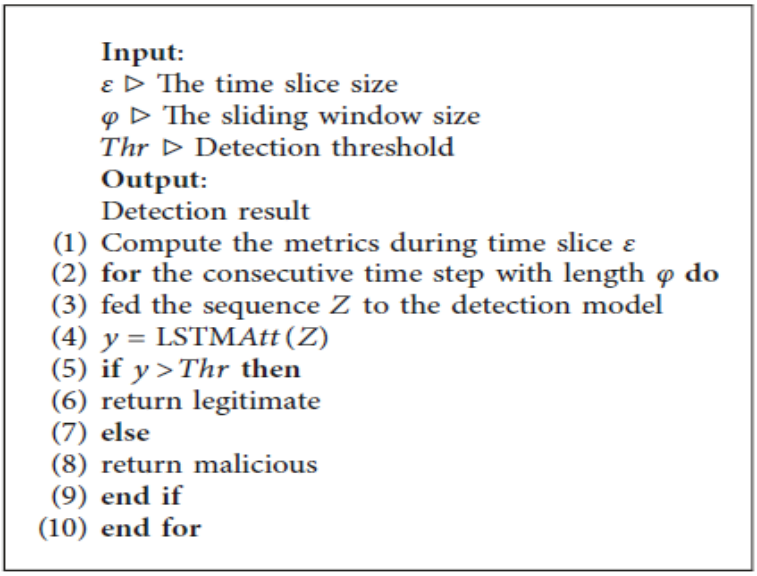
Notation	Description
t_i	La i-ème tranche de temps
R_j	Le j-ème routeur
$\phi(t_i, R_j)$	Le nombre de demandes d'intérêt reçues par le routeur j-ème dans la i-ème tranche de temps.
$\varphi(\phi(t_i, R_j))$	Le nombre de paquets de données correspondants reçus
$e(t_i, R_j)$	Le nombre d'entrées PIT du routeur j-ème dans la i-ème tranche de temps

Table 1 Les notations utilisées

Input:
ε ▷ The time slice size
Output:
i ▷ The request frequency
r ▷ The reply frequency
s ▷ The satisfaction ratio
(1) **procedure** *IncomingInterest(slice ε)*
(2) $i \longrightarrow i + 1$
(3) **end procedure**
(4) **procedure** *IncomingData(slice ε)*
(5) $r \longrightarrow r + 1$
(6) **end procedure**
(7) $s \longrightarrow r/i$
(8) **return** i r s

Figure 24 L'ALGORITHME 1 :

Calcul des caractéristiques d'intérêt.



Input:
ε ▷ The time slice size
φ ▷ The sliding window size
Thr ▷ Detection threshold
Output:
Detection result
(1) Compute the metrics during time slice ε
(2) **for** the consecutive time step with length φ **do**
(3) fed the sequence Z to the detection model
(4) $y = \text{LSTM}Att(Z)$
(5) **if** $y > Thr$ **then**
(6) return legitimate
(7) **else**
(8) return malicious
(9) **end if**
(10) **end for**

Figure 25 L'ALGORITHME 2 :

Détection basée sur le LSTM avec mécanisme d'attention.

Où α_t représente le poids pour chaque étape temporelle et $g_t(.)$ est une couche entièrement connectée avec une activation ReLU et des paramètres W_t .

L'illustration du mécanisme d'attention est présentée dans la Figure 8.

Dans la couche de sortie, la couche d'attention H fournit une entrée à une couche entièrement connectée avec une activation sigmoïde pour obtenir le résultat final.

output = simoid(v).

Le mécanisme de détection est présenté dans l'Algorithme 2.

L'algorithme fonctionne selon les étapes suivantes :

Étape (1) : compter les informations de trafic dans la tranche de temps ε en utilisant l'Algorithme 1.

Étape (2) : lorsque la taille de la fenêtre glissante est φ, alimenter le modèle de détection et obtenir la sortie y.

Étape (3) : si le résultat de détection est légitime, faire avancer la fenêtre glissante et revenir à l'étape (2).

Étape (4) : si le résultat de détection est malveillant, déclencher le mécanisme d'identification des préfixes malveillants.

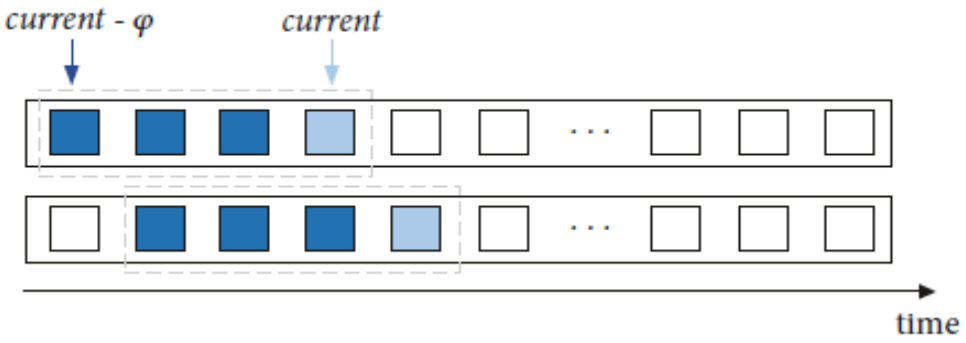


Figure 26 Une fenêtre glissante

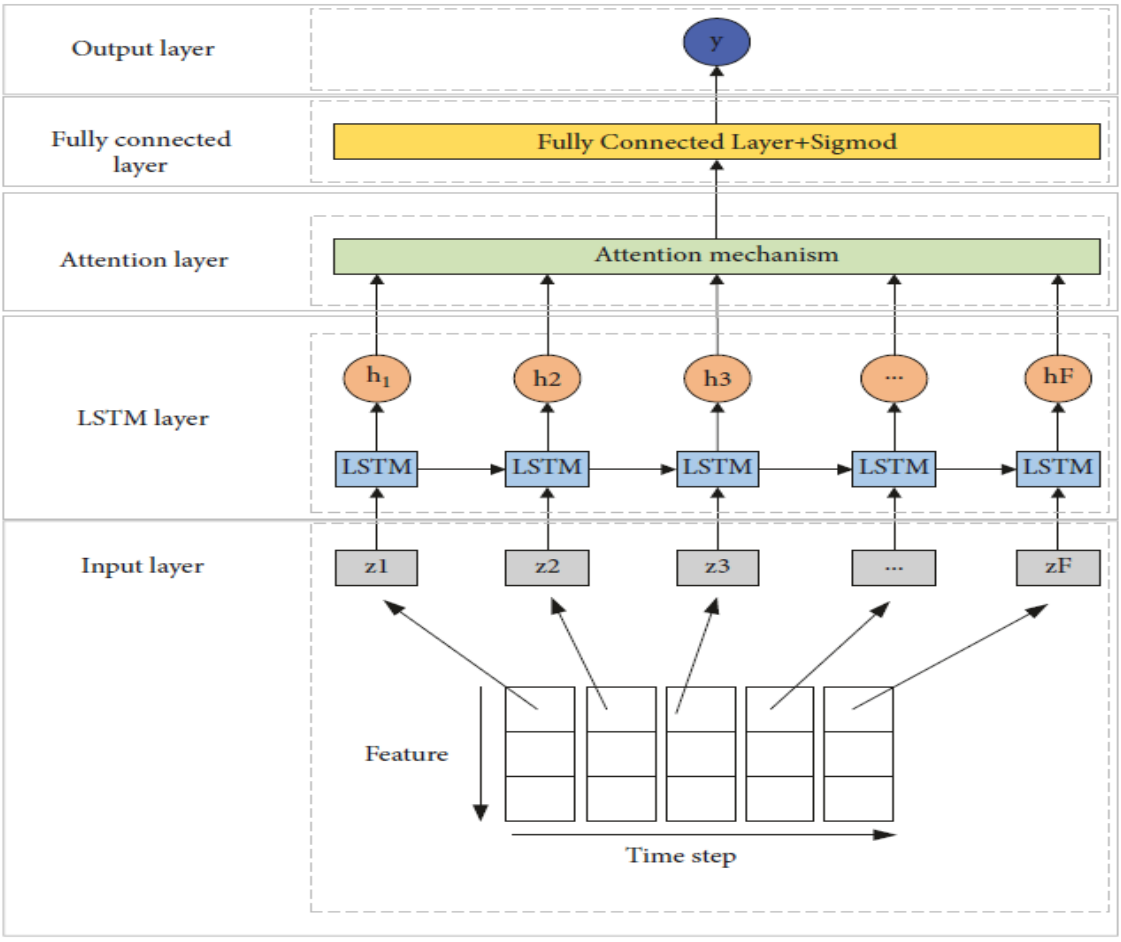


Figure 27 Le LSTM avec mécanisme d'attention.

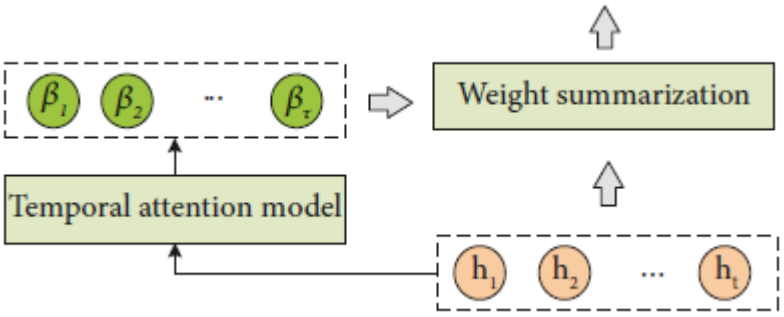


Figure 28 L'illustration du mécanisme d'attention temporelle

3.5) Mécanisme de réponse :

Cet article utilise la distance de Hellinger [61] pour détecter les préfixes d'intérêt malveillants. La distance de Hellinger permet de mesurer l'écart entre deux distributions de probabilité, indépendamment de leurs paramètres.

La distance de Hellinger est définie comme suit :

$$H(P,Q) = \frac{1}{\sqrt{2}}\sqrt{\sum_{i=1}^{n}(\sqrt{p_i}-\sqrt{q_i})^2}\,, \qquad p_i \geq 0;\ q_i \geq 0,$$

Où P et Q représentent deux distributions de probabilité, et P et Q sont des n-uplets $(p_1, p_2, \dots, p_n)$ et $(q_1, q_2, \dots, q_n)$, respectivement. Les valeurs de p_i et q_i doivent être supérieures ou égales à zéro, et la somme des p_i et des q_i doit être égale à 1.

Le processus de reconnaissance des préfixes malveillants est illustré dans l'Algorithme 3.

Input:
Interest prefix distribution when IFA is detected: $\mathbb{P}$
Interest prefix distribution before IFA is detected: $\mathbb{Q}$
Interest prefix set: I
Output:
Malicious prefix set
(1) $\mathbb{Q}' = \mathbb{Q}$
(2) **for** prefix$_i \in I$ **do**
(3) $\mathbb{Q}'_i = \mathbb{P}_i$
(4) calculate the Hellinger distance $H(\mathbb{Q}'_i, \mathbb{Q})$
(5) **if** $H(\mathbb{Q}'_i, \mathbb{Q}) > thr$ **then**
(6) add prefix$_i$ to malicious prefix set
(7) **end if**
(8) **end for**
(9) **return** malicious prefix set

Figure 29 La reconnaissance de préfixes malveillants basée sur la distance Hellinger

3.6) Mécanisme de Mitigation :

Lorsque des préfixes malveillants sont identifiés, le routeur envoie un paquet de notification contenant ces préfixes malveillants au routeur situé en aval, comme indiqué dans la Figure 30. Les routeurs en aval extraient les préfixes malveillants et limitent leur taux d'envoi lorsqu'ils reçoivent le paquet de notification.

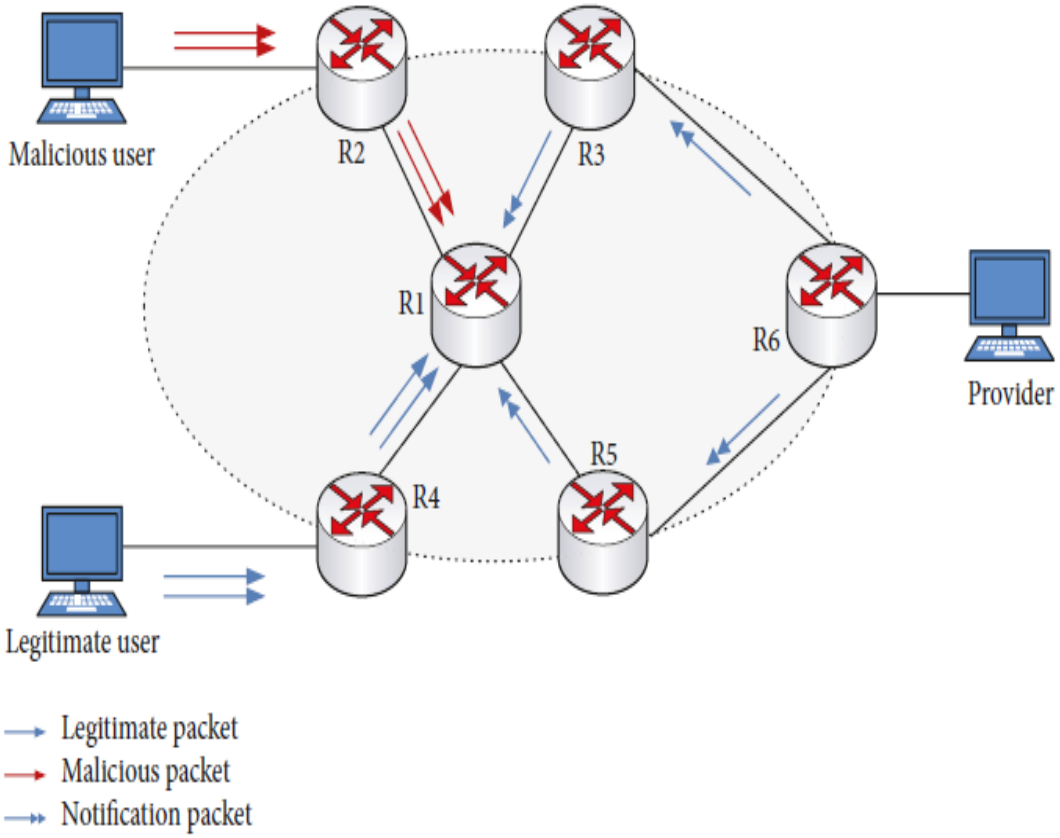


Figure 30 Un exemple de mitigation de l'IFA.

CONCLUSION :

Ce chapitre représente un mécanisme de défense contre les attaques IFA dans NDN. La défense se divise en trois parties : la détection, la réponse et l'atténuation. Pour détecter les attaques de submersion d'intérêt, un LSTM avec un mécanisme d'attention est utilisé. Une fois l'attaque détectée, la distance de Hellinger est utilisée pour identifier le préfixe malveillant des paquets d'intérêt. Enfin, ce préfixe malveillant est transmis aux routeurs en aval pour une coopération visant à limiter l'attaque.

En adoptant ce mécanisme de défense, les réseaux NDN peuvent renforcer leur sécurité en limitant les conséquences néfastes des attaques de submersion d'intérêt. Ces avancées sont cruciales dans un contexte où les réseaux informatiques sont de plus en plus vulnérables aux attaques malveillantes.

Les attaques DDoS peuvent cibler spécifiquement les mécanismes de mise en cache pour perturber les performances du réseau, donc il est crucial de développer une stratégie de mise en cache plus efficace.

Dans le prochain chapitre, nous mènerons une simulation des stratégies de mise en cache dans NDN, cette simulation nous permettra de modéliser divers scénarios et d'observer comment les différentes stratégies de cache se comportent dans chacun d'entre eux.

CHAPITRE 4

SIMULATION ET INTERPRETATION

INTRODUCTION :

Parmi les architectures d'ICN, l'architecture NDN est considérée comme la plus prometteuse pour l'avenir. Elle apporte des améliorations significatives en termes de qualité de service (QoS), notamment en ce qui concerne la bande passante, le délai, l'utilisation des ressources réseau, la congestion et la charge du serveur.

Pour exploiter pleinement les avantages de l'architecture NDN, il est essentiel de développer une stratégie de mise en cache plus efficace. De nombreuses études ont été menées afin de définir les meilleures stratégies de mise en cache, mais jusqu'à présent, aucune solution satisfaisante n'a été trouvée.

Dans ce chapitre, nous explorerons en détails les différentes étapes et aspects liés à la mise en place de simulations. Nous commencerons par présenter les outils spécifiques utilisés pour ces simulations et détaillerons les étapes nécessaires à leur installation.

Nous nous concentrerons ensuite sur la configuration et le lancement du simulateur, en mettant en évidence les paramètres clés à prendre en compte pour obtenir des résultats précis et fiables. Nous aborderons les diverses options de configuration disponibles, telles que la topologie du réseau.

Une fois les simulations lancées, nous procéderons à une interprétation approfondie des résultats obtenus. Nous nous intéresserons particulièrement à la mise en cache en utilisant les stratégies sélectionnées, et nous analyserons les métriques pertinentes, telles que le taux de réussite (hit ratio). Cette analyse comparative nous permettra de tirer des conclusions sur l'efficacité des différentes stratégies de mise en cache dans le contexte de l'architecture NDN.

1) Les outils de simulation et leur installation :

Pour la réalisation de notre simulation, nous avons utilisé le simulateur ccnSim qui est un simulateur de CCN écrit en C++ et utilisé sous le framework Omnet++. Ces applications ont été installées sur un PC Intel Core i5 avec la distribution Linux Ubuntu 22.10 LTS 64 bit.

1.2) Omnet++ :

Omnetv5.0 est un environnement utilisant le langage C++ permettant la simulation des réseaux. Il se caractérise par [67] :

a. un ensemble de classes C++ de base, qui peuvent être étendues afin de personnaliser l'environnement simulé;

b. un langage de description de réseau simple (NED) utilisé pour décrire les interactions entre les modules;

c. un langage msg définissant les messages échangés entre les nœuds du réseau.

L'un des ingrédients fondamentaux de cette infrastructure en sont une composante architecture pour les modèles de simulation. Les modèles sont assemblés à partir de réutilisables composants appelés *modules*. Les modules bien écrits sont vraiment réutilisables, et peut être combiné de différentes manières comme les blocs LEGO [67].

Pour l'installation d'omnet++ version 5.0 :

1. Téléchargez l'archive OMNeT++ 5.0 sur (https://omnetpp.org/omnetpp).
2. Extraire le fichier tar.gz téléchargé dans un répertoire de votre choix.
3. Ouvrez un terminal et accédez au répertoire où vous avez extrait le fichier.
4. Exécutez la commande suivante pour installer les dépendances nécessaires : sudo apt-get install build-essential gcc g++ bison flex perl qt5- default tcl-dev tk-dev libxml2-dev zlib1g-dev libwebkitgtk-3.0-dev libssl-dev
5. Ensuite, exécutez la commande suivante pour configurer OMNeT++ : ./configure
6. Enfin, exécutez la commande suivante pour compiler OMNeT++ : Make
7. Vous pouvez maintenant exécuter OMNeT++ en utilisant la commande suivante : Omnetpp

1.3) ccnSim v.04 :

ccnSim v0.4 est un simulateur du Content Centric Networks (CCN) écrit en C++ et utilisé sous Omnet++. Son intégration avec Omnet++ permet de voir un aperçu des stratégies de transfert et de mise en cache, stratégies de décision de mise en cache, modèle de demande de contenu, et ainsi de suite [68].Grâce à sa conception modulaire et ses optimisations, ccnSim permet d'effectuer des simulations événementielles classiques de réseaux CCN à grande échelle, c'est à dire jusqu'à M $=10^9$contenu, avec des budgets CPU et mémoire modérés [68].

Les commandes suivantes servent à installer ccnSim sur omnet++ :

cd $CCNSIM_DIR

cp ./patch/omnet-5x/ctopology.h $OMNET_DIR/include/omnetpp

cp ./patch/omnet-5x/ctopology.cc $OMNET_DIR/src/sim

cd $OMNET_DIR && make && cd $CCNSIM_DIR

./scripts/makemake.sh

make.

2) La configuration et lancement du simulateur :

2.1) Le démarrage du simulateur :

Les étapes suivantes décrivent comment lancer notre simulateur :

1. Ouvrir un terminal et tapez omnetpp pour l'ouverture d'omnet++.
2. Accédez au dossier ccsim se trouvant dans projet.
3. Choisir network pour choisir et modifier une topologie.
4. Pour la compilation choisir ED_TTL-omnetpp.ini et ajouter les paramètres qu'il vous faut et ensuite lancer la configuration.

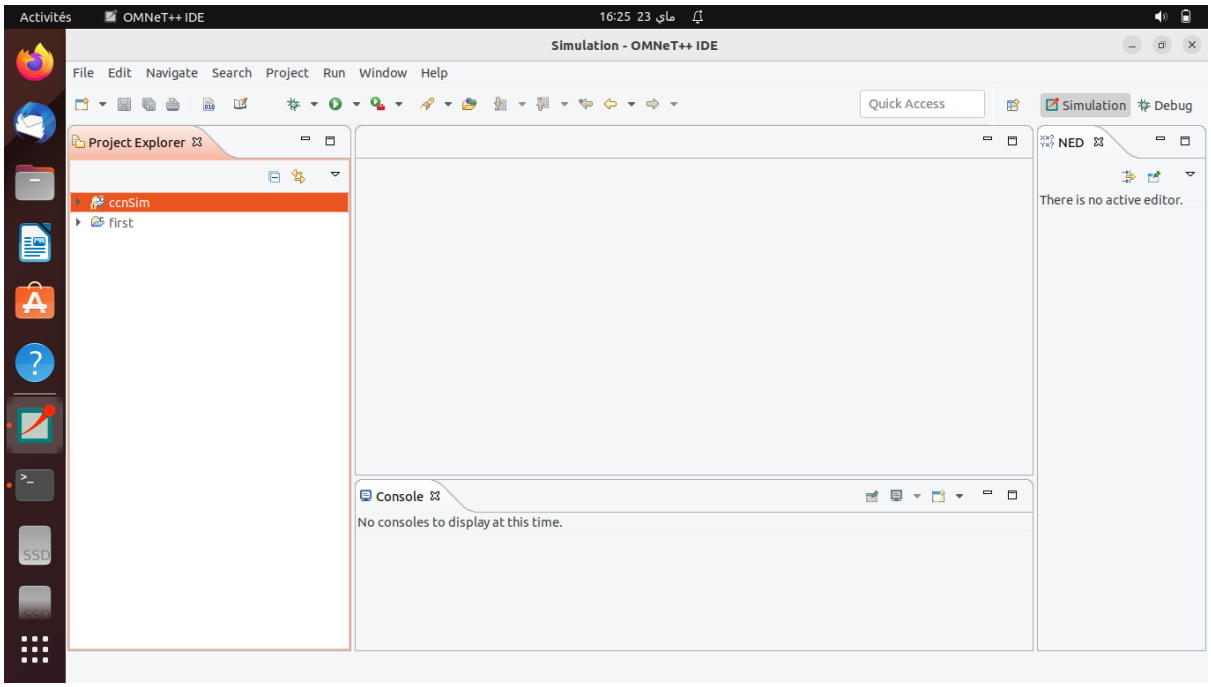


Figure 31 L'ouverture d'omnet++ et l'accès au projet ccnsim

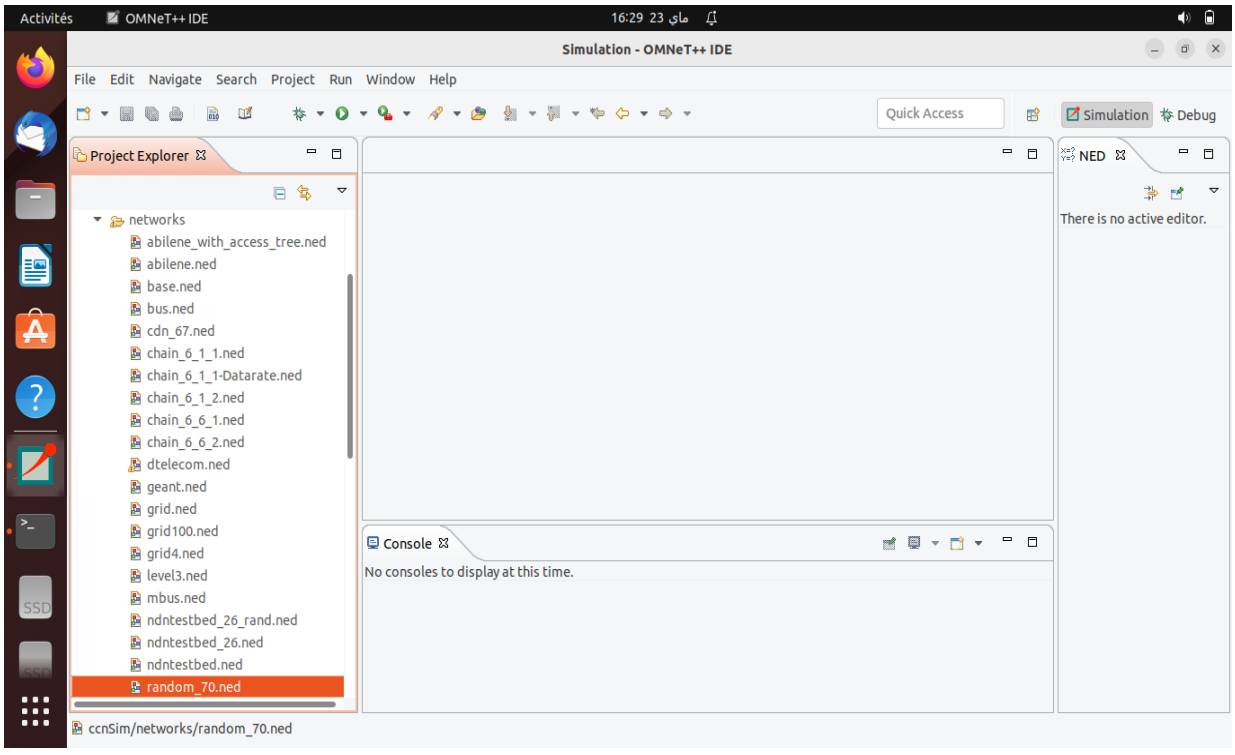


Figure 32 Les différentes topologies dans network

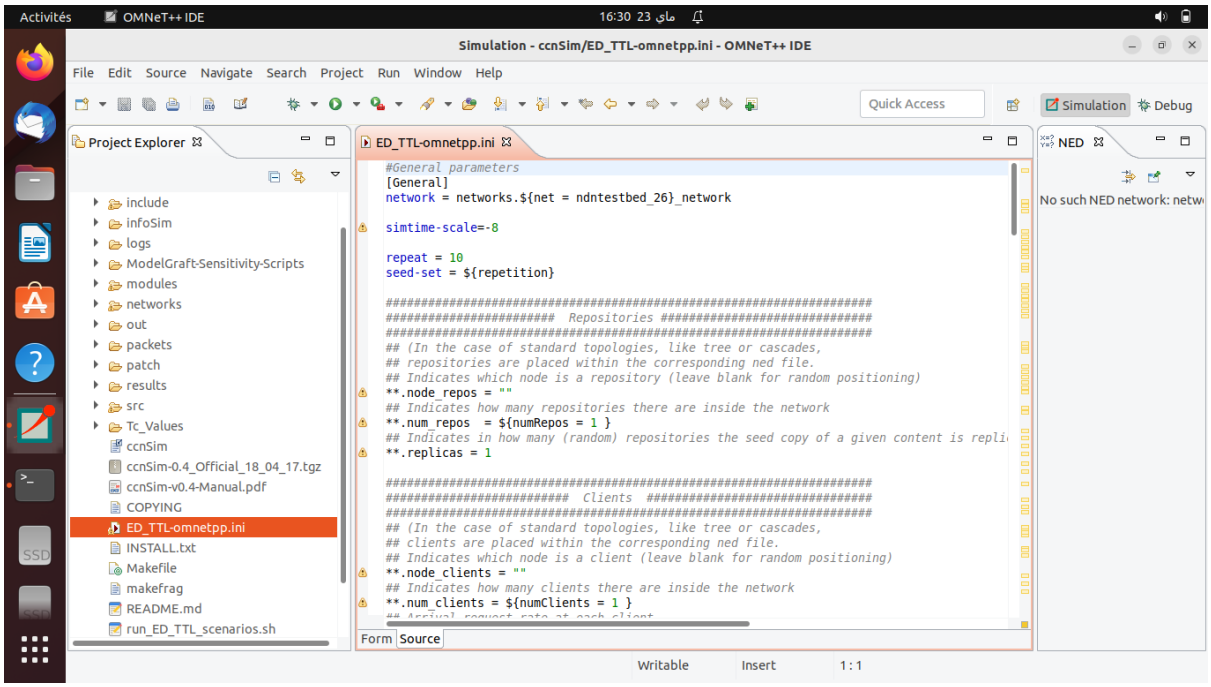


Figure 33 Lancement de simulation

2.2) L'ajout des nouvelles stratégies de remplacement :

Le simulateur ccnSim donne la possibilité d'ajouter de nouvel algorithme dans son environnement. C'est dans ce cadre que nous avons mis en place de nouvelles stratégies de remplacement et les avons ajoutées à notre simulateur. Ces stratégies sont :

- **RandLRU :** est une combinaison de random et lru. Elle consiste à sélectionner aléatoirement deux contenus et ensuite on remplace le moins récemment utilisé parmi eux.
- **RandLFU :** est une combinaison de random et lru. Elle consiste à sélectionner aléatoirement deux contenus et ensuite on remplace le moins fréquemment utilisé parmi eux.
- **RandLRFU :** est une combinaison de random et lru. Elle consiste à sélectionner aléatoirement deux contenus et ensuite on remplace le moins récemment et le moins fréquemment utilisé parmi eux.

En ajoutant ces nouvelles stratégies de remplacement au simulateur ccnSim, nous pourrons évaluer leurs performances et mieux comprendre leur comportement dans différents scénarios d'utilisation. Voici un récapitulatif des avantages potentiels de chaque stratégie :

- **RandLRU :** Cette stratégie permet de maintenir la diversité des contenus dans le cache tout en accordant une importance particulière dans son choix aléatoire de contenus. Ce choix se fera en fonction des contenus récemment utilisé. Cela peut être bénéfique dans les situations où l'on souhaite avoir une variété de contenus tout en s'assurant que les contenus récemment utilisés restent accessibles.
- **RandLFU :** Cette stratégie est utile pour conserver les contenus les plus fréquemment utilisés dans le cache. Dans son choix aléatoire de contenus fréquemment utilisé, la stratégie RandLFU peut être avantageuse lorsque certains contenus sont demandée plus fréquemment que d'autres, car elle garantit leur présence dans le cache, ce qui réduit les temps d'accès et améliore les performances.
- **RandLRFU :** Cette stratégie combine à la fois l'aspect de récence (LRU) et la fréquence d'utilisation (LFU), ce qui fait que le choix aléatoire des contenus se fera en fonction de la récence et aussi de la fréquence des contenus. Cette approche peut être bénéfique lorsque l'on souhaite équilibrer ces deux critères lors du remplacement des contenus dans le cache.

En évaluant les performances de ces nouvelles stratégies, nous serons en mesure de déterminer les combinaisons les plus adaptées à nos besoins spécifiques en termes d'efficacité et de performances du cache.

L’ajout se passe comme suit :

1. Tout d’abord on crée le fichier par exemple randlru.cc dans le dossier source src, et randlru.h dans le dossier include.
2. Après on ajoute le nom de la stratégie dans le cache.ned se trouvant dans le cache de module.
3. Et enfin on ajoute dans makefile de ccnsim.

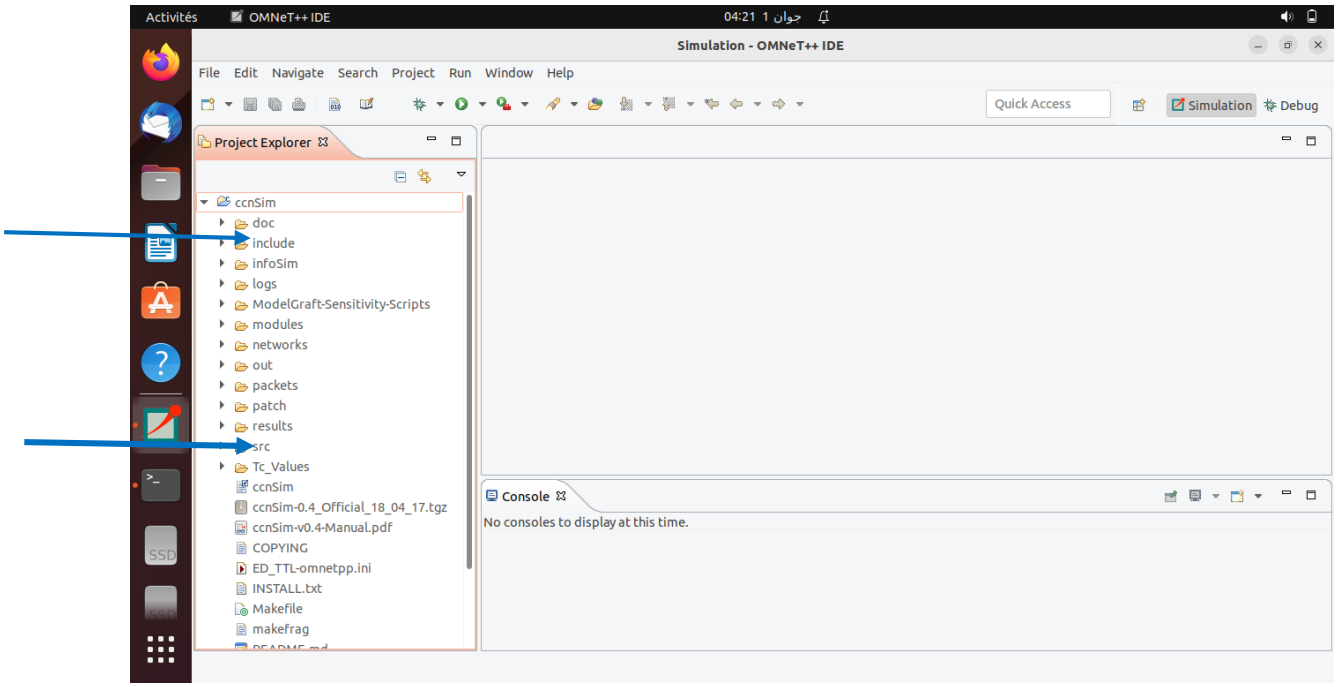


Figure 34 Le dossier où on ajoute la nouvelle stratégie

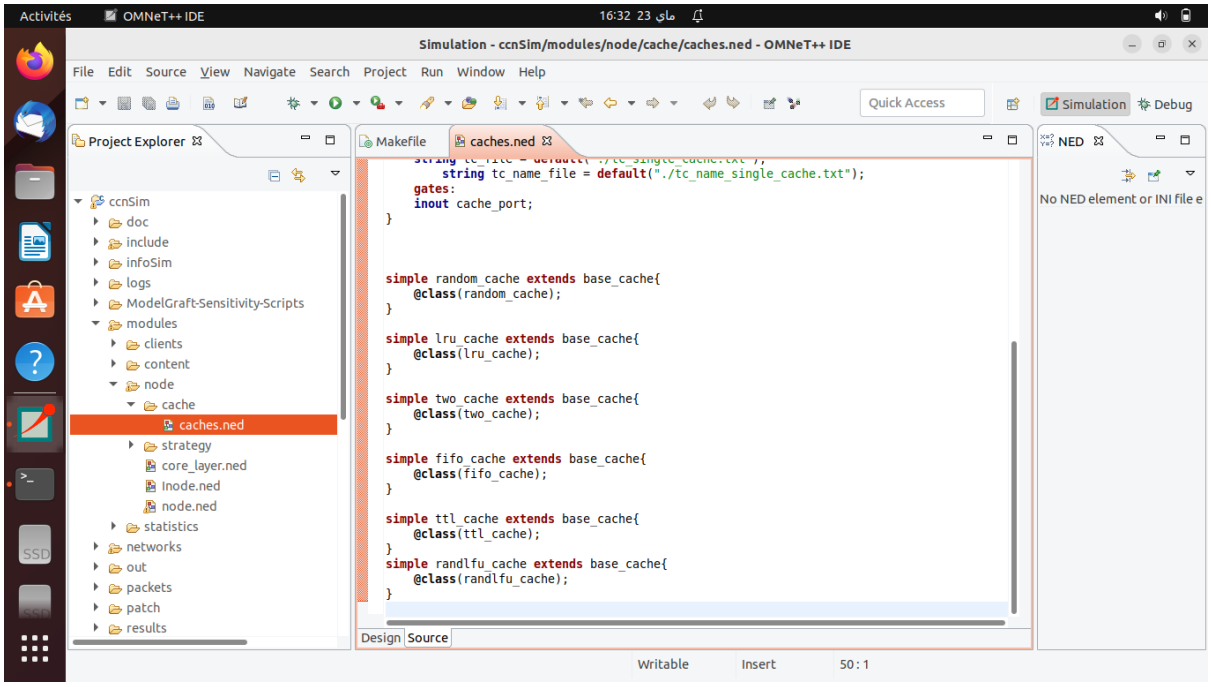


Figure 35 L'ajout de la stratégie dans la base de cache

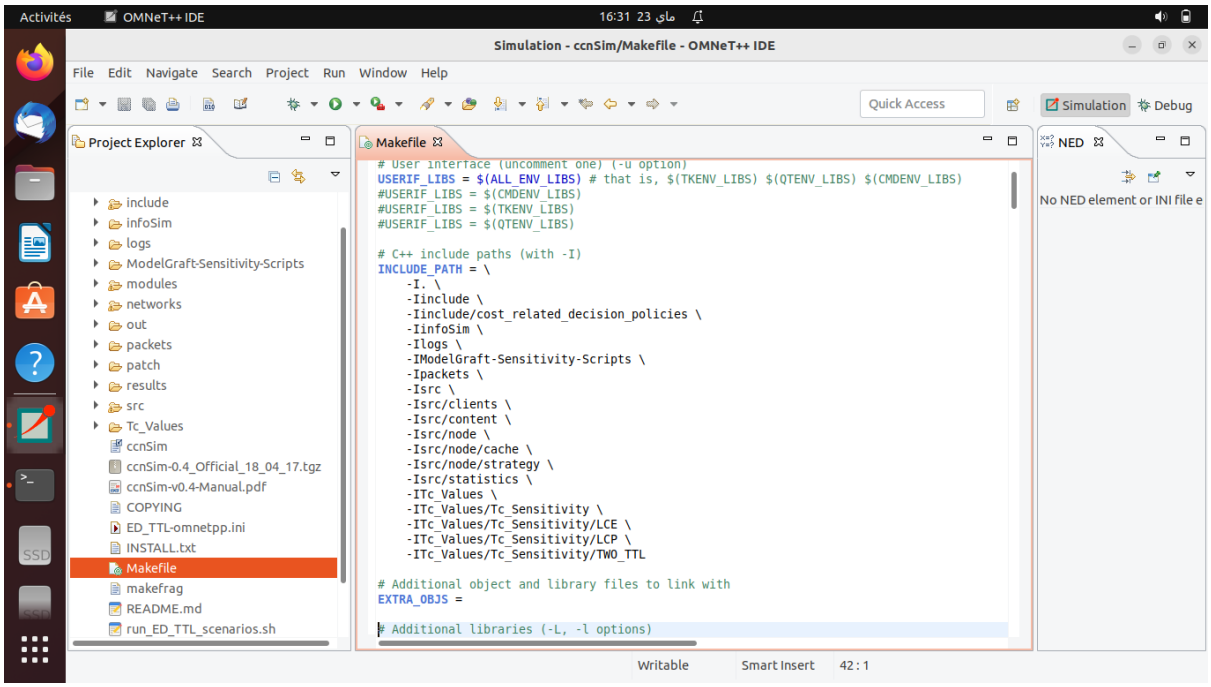


Figure 36 L'ajout d'un chemin menant à cette stratégie

3) Etude des topologies de la simulation :

Le simulateur ccnSim comprenant plusieurs topologies, nous avons utilisé deux d'entre elles pour la réalisation de notre simulation. Ces topologies sont : ***tree*** et ***ndntestbed_26***. Nous avons fait une comparaison des différentes stratégies dans ces deux topologies afin de connaitre les meilleures stratégies de placement et de remplacement de mise en cache dans les deux cas.

3.1) La topologie tree :

Dans la topologie tree, les clients sont agrégés en nœud de feuilles de et le nœud racine est la seule passerelle connectée à la source de contenu [68]. Voir figure :

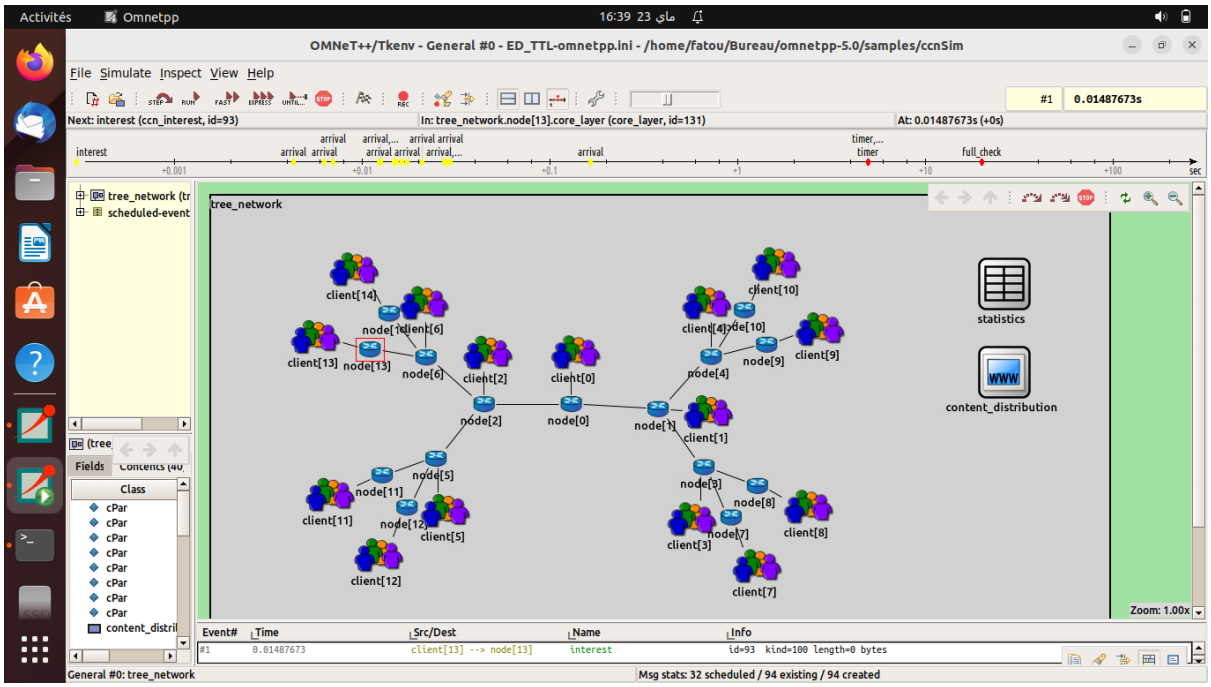


Figure 37 La topologie tree.

3.2) La topologie ndntestbed :

Cette topologie permet la liaison de plusieurs routeurs provenant de plusieurs institutions participantes, des nœuds d'hébergement d'application et d'autres appareils. Voir figure :

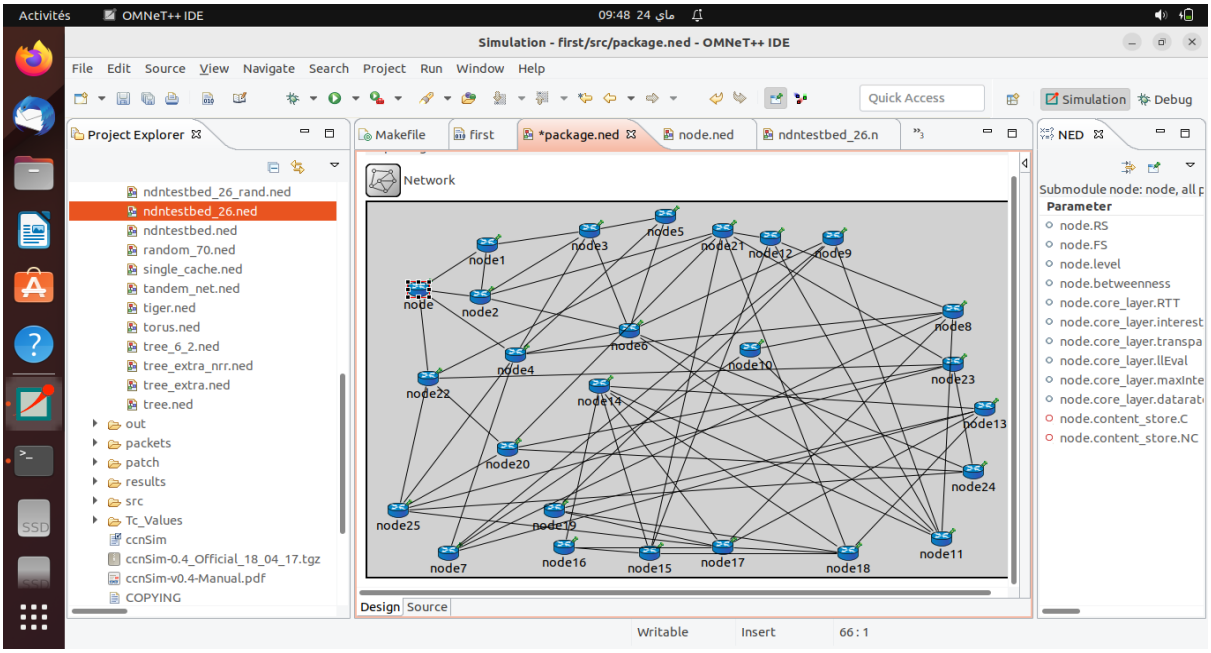


Figure 38 La topologie NDNtestbed.

4) L'analyse et l'interprétation des résultats :

Dans cette sous-section nous ferons une comparaison des différentes stratégies de mise en cache sélectionnées pour connaitre les meilleures parmi elles. Cette comparaison reposera sur la métrique du taux de réussite qui est le hit ratio.

4.1) Les paramètres de simulation :

- Topologie (nœuds) : Tree (15), NDNTestbed (26)
- Taille du Catalogue : contenus (objets) différents.
- Taille du contenu : 1 chunk.
- Nombre de Sources (Producer) : 1.
- Nombre de Clients (Consumer) : 15 (Tree), 26 (NDNTestbed).
- Taille du cache : 1000 contenus.
- Facteur de Popularité : α=1 (de la distribution Mandelbrot MZipf)
- Débit de requêtes Interests : 10 Interests/s.
- Stratégie de placement du cache : LCE, LCD, ProbCache.
- Politique de remplacement du cache : LFU, LRU, LRFU, RANDLFU, RANDLRU, RANDLRFU, FIFO, RANDOM.
- Stratégie d'Acheminement : Plus court chemin (Best Route / Short Path Route).
- Métrique de performance : Taux de réussite du Cache (Cache Hit Ratio : CHR).
- Durée de Simulation : 50000 s (14,5 Heures). Métriques

La distribution Mzipf : est la meilleure fonction permettant de modéliser et représenter les contenus des requêtes Web générés par les clients (Users). Ainsi, le contenu d'une requête Interest (c.à.d. le nom du contenu demandé par un client) est sélectionné à partir des différents contenus du catalogue suivant la distribution de contenus Mzipf.

p_hit : Le taux d'accès au cache mesure le nombre de requêtes de contenu servies par rapport au nombre de requêtes qu'il reçoit [69].

Le hit ratio a pour formule :

$$\frac{\text{Number of cache hits}}{(\text{Number of cache hits} + \text{Number of cache misses})} = \text{Cache hit ratio}$$

Figure 39 La formule du cache hit ratio.

Où :

Number of cache hits : représente le nombre de requêtes satisfaites à partir de la cache.

Number of cache hits + Number of cache misses : représente le nombre total de requêtes.

4.2) Les résultats de la simulation :

Les tableaux ci-dessous contiennent les résultats de la mise en cache avec les différentes stratégies de placement avec les différentes topologies utilisées:

1. La topologie tree :

- Les résultats obtenus avec la stratégie LCE dans la topologie tree :

Table 2 Les résultats avec la stratégie de placement LCE dans la topologie tree

Stratégie de placement / Stratégie de remplacement	lce
lfu	36,56%
lrfu	34,71%
randlfu	30,20%
randlrfu	29,93%
lru	28,58%
randlru	28,41%
random	26,79%
fifo	26,65%

- Interprétation des résultats du tableau :

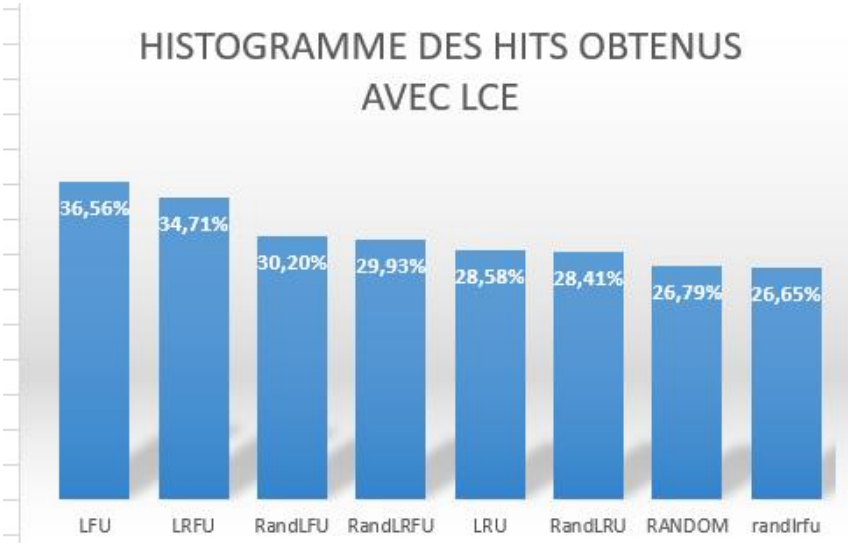


Figure 40 L'histogramme des résultats avec LCE dans la topologie tree.

Dans la stratégie de placement LCE, la stratégie de remplacement LFU représente la meilleure parmi les autres stratégies de remplacement car elle a le taux de réussite le plus élevé. LRFU est à la deuxième position. RANDLFU vient à la troisième position ensuite, RANDLRFU, LRU, RANDLRU, RANDOM, et FIFO vient à la dernière position.

- Stratégie de placement LCD dans la topologie tree:

Table 3 Les résultats obtenus avec la stratégie lcd dans la topologie tree.

Stratégie de placement / Stratégie de remplacement	lcd
lrfu	36,57%
lru	35,30%
randlru	36,11%
randlfu	36,08%
randlrfu	35,88%
lfu	35,62%
fifo	35,32%
randlrfu	35,27%

- Interprétation des résultats du tableau :

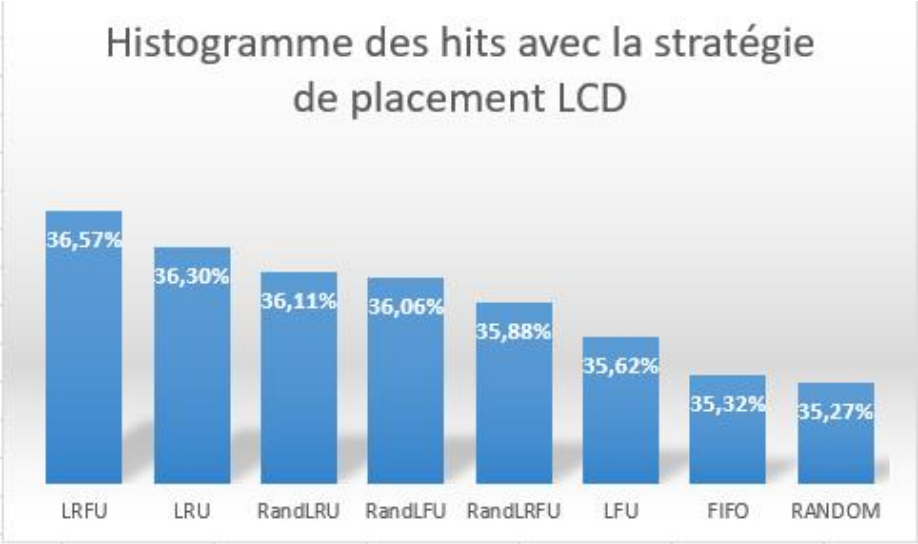


Figure 41 L'histogramme des résultats avec LCD dans la topologie tree

Dans la stratégie de placement LCD, la stratégie de remplacement LRFU vient à la première position. LRU est à la deuxième position. RANDLFU vient à la troisième position ensuite, RANDLRU, RANDLRFU, LFU, FIFO et Random vient à la dernière position.

- Résultats obtenus avec la stratégie de placement probcache :

Table 4 Les résultats obtenus avec la stratégie de placement probcache dans la topologie tree.

Stratégie de placement / Stratégie de remplacement	probcache
lfu	36,55%
lrfu	35,33%
lru	32.54%
randlru	32,08%
randlfu	32,04%
randlrfu	31,69%
random	28,34%
randlrfu	28,33%

- Interprétation des résultats du tableau :

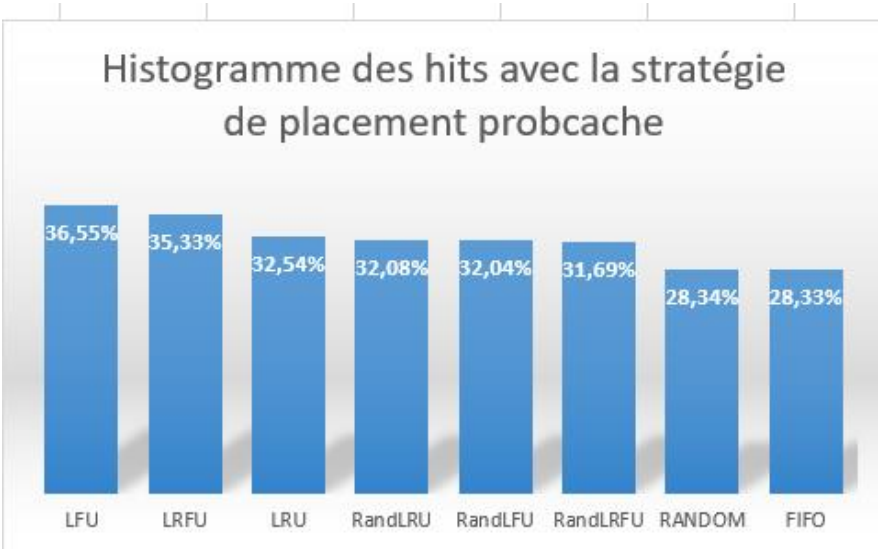


Figure 42 L'histogramme des résultats probcache dans la topologie tree

Dans la stratégie de placement probcache, la stratégie de remplacement LFU a le plus grand taux de réussite donc est la meilleure. LRFU est à la deuxième position. LRU vient à la troisième position ensuite, RANDLRU, RANDLFU, RANDLRFU, RANDOM, et FIFO vient à la dernière position.

2. Topologie ndntestbed :

- Résultats obtenus avec la stratégie de placement lce :

Table 5 Les résultats obtenus avec lce dans la topologie ndntestbed.

Stratégie de placement / Stratégie de remplacement	lce
lfu	36,48%
lrfu	34,93%
randlfu	30,44%
randlrfu	30,16%
lru	28,80%
randlru	28,65%
random	26,98%
fifo	26,83%

- Interprétation des résultats du tableau :

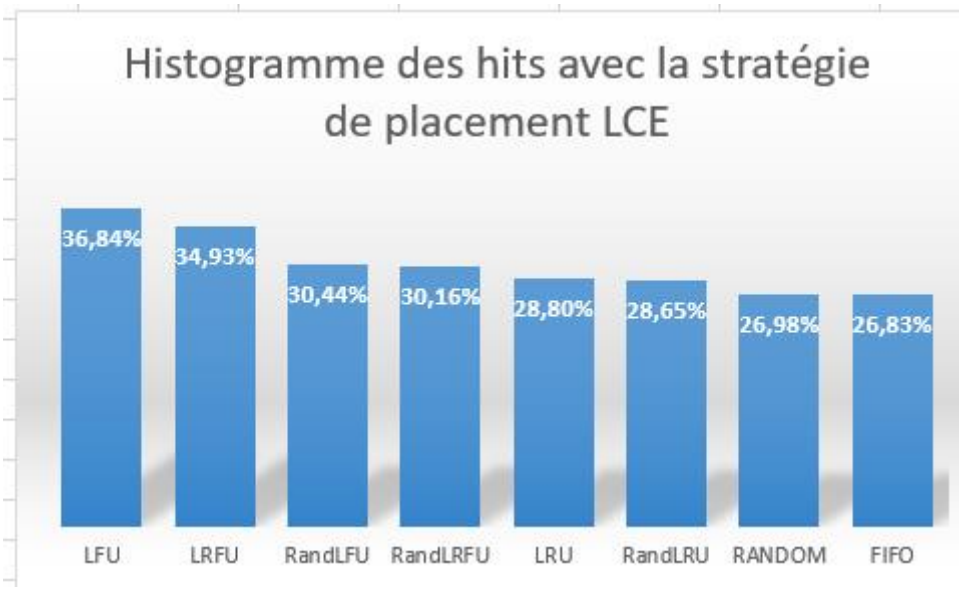


Figure 43 L'histogramme des résultats du tableau 5

Dans la stratégie de placement LCE de la topologie ndntestbed, la stratégie de remplacement LFU représente la meilleure parmi les autres stratégies de remplacement car elle a le taux de réussite le plus élevé. LRFU est à la deuxième position. RANDLFU vient à la troisième position ensuite, RANDLRFU, LRU, RANDLRU, RANDOM, et FIFO vient à la dernière position.

- Résultats obtenus avec la stratégie de placement lcd :

Table 6 Les résultats obtenus avec la stratégie lcd dans la topologie ndntestbed.

Stratégie de placement / Stratégie de remplacement	lcd
lrfu	36,91%
lru	36,78%
randlru	36,56%
randlfu	36,49%
randlrfu	36,33%
lfu	35,97%
fifo	35,74%
random	35,68%

- Interprétation du tableau :

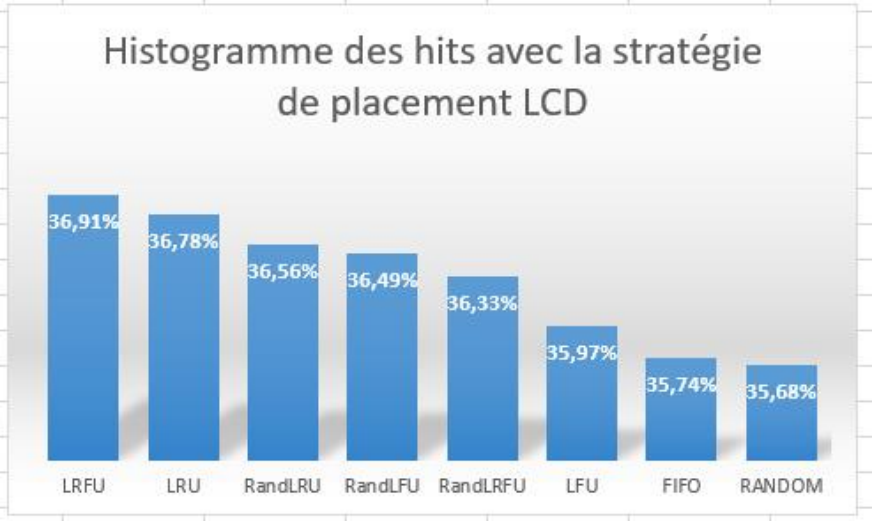


Figure 44 L'histogramme des résultats avec lcd dans la topologie ndntestbed

Dans la stratégie de placement LCD, la stratégie de remplacement LRFU vient à la première position. LRU est à la deuxième position. RANDLRU vient à la troisième position ensuite, RANDLFU, RANDLRFU, LFU, FIFO et Random vient à la dernière position.

- Résultats obtenus avec la stratégie de placement probcache :

Table 7 Les résultats obtenus avec probcache dans la topologie ndntestbed

Stratégie de placement / Stratégie de remplacement	probcache
lfu	36,90%
lrfu	35,59%
lru	32,79%
randlru	32,34%
randlfu	32,30%
randlrfu	31,94%
random	28,54%
randlrfu	28,52%

- Interprétation du tableau :

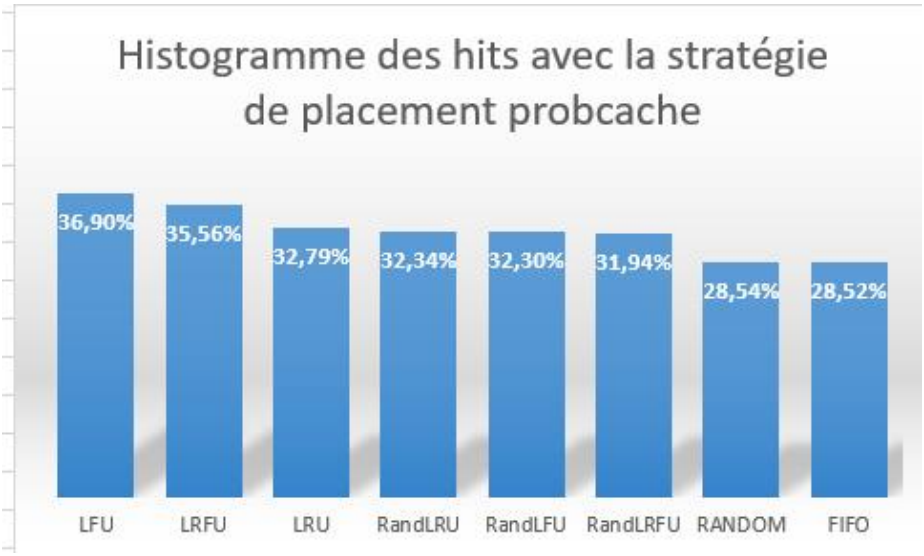


Figure 45 L'histogramme des résultats avec probcache dans la topologie ndntestbed

Dans la topologie ndntestbed, avec la stratégie de placement probcache, la stratégie de remplacement LFU a le plus grand taux de réussite donc elle est la meilleure. LRFU est à la deuxième position. LRU vient à la troisième position ensuite, RANDLRU, RANDLFU, RANDLRFU, RANDOM, et FIFOMY vient à la dernière position.

3. Les résultats :

D'après les résultats de simulation dans les topologies "Tree" et "NDNtestbed" pour les stratégies de placement LCE, LCD et probcache, Il est intéressant de constater que :

1) Dans la plupart des cas, la stratégie de remplacement LFU obtient les meilleurs résultats en termes de taux de réussite. Cela signifie que cette stratégie est efficace pour conserver les données les plus fréquemment utilisées dans le cache, ce qui permet de réduire les temps de recherche et d'améliorer les performances globales du système.

2) La stratégie de remplacement LRFU se classe généralement en deuxième position dans la plupart des cas. Cela indique que cette stratégie, qui combine des éléments de LFU et de LRU, est également efficace pour maintenir les données fréquemment utilisées dans le cache, mais avec une pondération supplémentaire pour l'aspect temporel de l'utilisation des données.

3) La stratégie de remplacement LRU se classe souvent à la deuxième ou à la troisième position. Bien qu'elle ne soit pas aussi performante que LFU ou LRFU, elle reste une méthode populaire pour le remplacement des données en se basant sur l'historique récent de leur utilisation

4) Les stratégies de remplacement aléatoires, telles que RANDOM et FIFO, obtiennent généralement les moins bons résultats en termes de taux de réussite. Cela suggère que l'utilisation purement aléatoire ou basée sur l'ordre d'arrivée des données ne permet pas d'optimiser efficacement l'utilisation du cache.

Ces résultats peuvent aider à guider le choix de la stratégie de remplacement appropriée. En utilisant la stratégie la plus performante on peut maximiser les performances du cache, cela permet de réduire le temps de recherche et d'améliorer la satisfaction des requêtes, ce qui est crucial dans les réseaux NDN où l'accès aux données est basé sur leur nom plutôt que sur leur emplacement physique.

Les classements des stratégies de remplacement peuvent varier d'une topologie à une autre. Cela peut être dû aux différences dans la distribution des données, aux schémas de trafic ou aux caractéristiques spécifiques de chaque topologie. Il est donc important de prendre en compte la topologie du réseau lors du choix de la stratégie de remplacement adaptée.

CONCLUSION :

Dans ce chapitre, nous avons abordé les étapes d'installation des outils de simulation nécessaires et nous avons expliqué les différentes étapes pour lancer le simulateur. Ensuite, nous avons présenté les résultats obtenus lors des simulations en utilisant des paramètres spécifiés.

Nous avons évalué et comparé les performances des différentes stratégies de remplacement dans les topologies "***Tree***" et "***NDNtestbed***", en fonction de la stratégie de placement choisie. Notre principal critère d'évaluation était le taux de réussite.

Les stratégies de remplacement étudiées étaient LFU, LRFU, LRU, RANDLRU, RANDLFU, RANDLRFU, RANDOM et FIFO. Chacune de ces stratégies a été testée dans les deux topologies mentionnées.

Les résultats obtenus mettent en évidence l'importance de choisir une stratégie de remplacement adaptée pour optimiser les performances du cache dans les réseaux NDN. En analysant les taux de réussite, nous avons pu identifier les stratégies les plus efficaces dans chaque cas.

Il est important de noter que les résultats peuvent varier en fonction des caractéristiques spécifiques du réseau et des charges de trafic. Il est donc recommandé de mener des simulations et des évaluations approfondies pour choisir la stratégie de remplacement la plus appropriée dans un contexte donnée.

CONCLUSION GENERALE

Le NDN est une architecture de réseau qui vise à améliorer plusieurs aspects de l'Internet actuel. Son objectif principal est de remplacer le modèle basé sur les adresses IP et les connexions point à point par un modèle centré sur les données, en réduisant la charge de trafic sur le réseau, en améliorant la sécurité et la confidentialité des données et en permettant une meilleure utilisation des ressources réseau. Il peut également être plus résistant aux pannes et aux attaques, car les nœuds NDN peuvent récupérer les données demandées à partir de caches locaux, plutôt que de dépendre de serveurs centraux.

Cependant, malgré ses avantages potentiels, NDN est toujours en phase de développement et son adoption à grande échelle par l'industrie n'a pas encore eu lieu. La transition vers une infrastructure de réseau entièrement basée sur NDN nécessiterait une refonte majeure de l'Internet existant et une coordination entre de nombreux acteurs. Des recherches supplémentaires sont nécessaires pour évaluer la faisabilité technique, les défis potentiels et les implications économiques d'une telle transition.

Notre travail avait pour objectif d'étudier le réseau NDN en le simulant et en l'interprétant. Pour atteindre cet objectif, nous avons d'abord présenté le projet NDN et souligné les limites de l'architecture traditionnelle actuelle, le TCP/IP. Nous avons examiné les concepts d'ICN et de CCN, puis nous nous sommes penchés sur le réseau NDN en détaillant son architecture, son fonctionnement en matière de communication, de nommage, de routage et de sécurité.

Ensuite, nous avons abordé la question de la mise en cache dans le NDN en décrivant les différentes stratégies utilisées et en fournissant des exemples d'algorithmes associés à chaque stratégie. Nous avons constaté que la mise en cache pouvait être à l'origine d'attaques dans le réseau.

Nous avons ensuite réalisé une étude sur l'attaque DDoS, en mettant particulièrement l'accent sur l'attaque IFA (Interest Flooding Attack, IFA). Nous avons également évoqué le mécanisme LSTM (Long Short Term Memory) comme une méthode permettant de contrer les attaques dans les réseaux NDN.

Enfin, nous avons procédé à la simulation et à l'interprétation de la mise en cache dans le réseau NDN en évaluant le taux de réussite des différentes stratégies. Les résultats ont été présentés sous forme de tableau, et l'interprétation a été visualisée à l'aide d'un histogramme afin de déterminer les meilleures stratégies en termes de mise en cache.

REFERENCES

[1] J. Roberts, «The clean-slate approach to future internet design: a survey of research initiatives,» *Annals of telecommunications,* vol. 64, n° %15, pp. 271-276, 2009.

[2] C. N. V. V. A. S. N. F. C. T. X. V. K. V. K. e. G. C. P. G. Xylomenos, «A survey of information-centric networking research,» *Communications Surveys & Tutorials, IEEE,* vol. 16, n° %12, pp. 1024-1049, 2014.

[3] I. M. J. B. e. a. A. Afanasyev, «NDN naming conventions,» *Technical Report NDN-0005, NDN,* 2013.

[4] M. M. D. S. a. J. G.-L.-A. V. Jacobson, «Content-centric networking,» *Whitepaper (Palo Alto Research Center).,* pp. 2-4, 2007.

[5] J. B. L. Z. B. Z. K. C. C. P. T. A. L. W. J. A. H. a. P. C. V. Jacobson, «Named Data Networking Next Phase (NDN-NP) Project May 2014-April 2015 Annual Report,» *UCLA, NDN Technical Report NDN-0011.,* 2015.

[6] M. C. B.-G. C. A. E. K. H. K. S. S. a. I. S. T. Koponen, «A data-oriented (and beyond) network architecture,» *ACM SIGCOMM Computer Communication Review,* vol. 37, n° %14, pp. 181-192, 2007.

[7] D. K. B. O. S. F. B. A. a. H. K. C. Dannewitz, «Network of information (netinf) - an information-centric networking architecture,» *Computer Communications,* vol. 36, n° %17, pp. 721-735, 2013.

[8] «From content delivery today to information centric networking,» *Computer Networks,* vol. 57, n° %116, pp. 3116 - 3127, 2013.

[9] V. N. I. Cisco, «Forecast and methodology, 2014-2019 white paper,» *Technical report Cisco, Tech. Rep.,,* 2015.

[10] A.-M. K. Pathan and R. Buyya, « A taxonomy and survey of content delivery networks,» *Grid Computing and Distributed Systems Laboratory, University of Melbourne, Technical Report,* p. 7, 2007.

[11] J. C. M. P. R. S. a. S. L. E. K. Lua, «A survey and comparison of peer-to-peer overlay network schemes,» *Communications Surveys & Tutorials, IEEE,,* vol. 7, n° %12, pp. 72 - 93, 2005.

[12] G. P. a. A. Vakali, «Insight and perspectives for content delivery networks,» *Communications of the ACM,* vol. 49, n° %11, pp. 101 - 106, 2006.

[13] D. K. B. O. S. F. B. A. a. H. K. C. Dannewitz, *Computer Communications,* vol. 36, n° %17, pp. 721 - 735, 2013.

[14] J. Seedorf et al., *Internet Engineering Task Force, RFC 5693,* October 2009.

[15] N. Z. Y. Y. a. R. A. H. Song, «Decoupled application data enroute (decade) problem statement,,» *Internet Engineering Task Force, Tech. Rep.,,* July 2012.

[16] D. Lagutin, «Securing the internet with digital signatures,,» *Ph.D. dissertation,Aalto University, Department of Computer Science and Engineering,* 2010.

[17] T. Dierks, «The transport layer security (tls) protocol version 1.2,,» *Internet Engineering Task Force, RFC 5246,* 2008.

[18] S. Frankel and S. Krishnan, «Ip security (ipsec) and internet key exchange (ike) document roadmap,,» *Internet Engineering Task Force, RFC 6071,* February 2011..

[19] S. P. a. R. J. J. Pan, «A survey of the research on future internet architectures,» *Communications Magazine, IEEE,,* vol. 49, n° %17, pp. 26 - 36, 2011.

[20] S. H. A. S. H. B. a. D. K. M. A. Yaqub, «Information-centric networks (icn),» *in Content-Centric Networks,* pp. 19 - 33, 2016.

[21] D. K. Smetters and V. Jacobson, «Securing network content,,» *PARC Tech Report TR-2009-1, Xerox Palo Alto Research Center-PARC,,* 2009.

[22] A. Feldmann, «Internet clean-slate design : what and why ?,» *ACM SIGCOMM Computer Communication Review,* vol. 37, n° %13, pp. 59 - 64, 2007.

[23] T. U. e. a. Qureshi, «Mobile Internet Connectivity: An Empirical Study of What Improves the Quality of Service in Developing Countries,» *IEEE Communications Magazine,* vol. 56, n° %19, pp. 96-101., 2018.

[24] V. S. D. K. T. J. D. P. M. F. B. N. H. &. B. R. L. Jacobson, «Networking named content,» *Proceedings of the 5th International Conference on Emerging Networking Experiments and Technologies,* pp. 1 - 12, 2009.

[25] V. &. S. D. K. Jacobson, « Future Internet architecture: Named data networking,» *Proceedings of the 2009 Workshop on Re-Architecting the Internet (ReArch),* pp. 1 - 7, 2012.

[26] A. M. I. Z. L. &. Z. B. Afanasyev, «CCNx 1.0 implementation: high-performance named-object networking,» *IEEE Communications Magazine,* vol. 52, n° %11, pp. 118-124, 2014.

[27] A. A. J. B. e. V. J. Lixia Zhang, «Named data networking (NDN) project,» *ACM SIGCOMM Computer Communication Review,* 2014.

[28] A. A. e. a. Lixia Zhang, «Named Data Networking,» *IEEE Communications Magazine ,* 2014.

[29] A. A. J. B. V. J. k. c. P. C. C. P. L. W. a. B. O. Lixia Zhang, «Named data networking,» *ACM SIGCOMM Computer Communication Review 44,* pp. 66-73, 3 July 2014.

[30] A. A. Z. Z. e. L. Z. Y. Yu, «Ndn technical memo: Naming conventions,» *Technical report, UCLA, Tech. Rep,* 2014.

[31] A. A. J. B. e. L. Z. Yu Zhang, «A Survey of Mobility Support in Named Data Networking,» *IEEE,* 2016.

[32] S. O. A. A. A. B. Z. L. Z. a. L. W. A K M Mahmudul Hoque, «NLSR: Named-data Link State Routing Protocol,» *Rapport technique, NDN.,* August 2013.

[33] B. Z. L. Z. A. A. C. Y. Lan Wang, «Scaling NDN Routing: Old Tale, New Design,» n° %19, July 2013.

[34] M. J. K. e. V. Jacobson, «Congestion avoidance and control,» *Proceedings of the SIGCOMM '88 Symposium on Communications Architectures and Protocols,* pp. 7 - 9, November 1988.

[35] A. A. J. B. V. J. k. c. P. C. C. P. L. W. a. B. Z. Lixia Zhang, «NDN Security: Threat Model and Ten Security Mechanisms,» *IEEE Communications Magazine,* p. 62, 2014.

[36] J. B. D. E. L. Z. B. Z. G. T. K. C. D. K. D. M. C. P. e. a. V. Jacobson, « Named Data Networking (NDN) Project 2012-2013 Annual Report,» *N/A (rapport annuel),* p. N/A (rapport annuel), 2014.

[37] D. K. S. a. V. Jacobson, «Securing network content,» *PARC Tech Report TR-2009-1, Xerox Palo Alto Research Center-PARC,* p. N/A (Tech Report), 2009.

[38] B. HAMDANE, Réseaux du futur : sécurité et nommage, Tunis: ÉCOLE SUPERIEURE DES COMMUNICATIONS DE TUNIS, 2016.

[39] F. N. E. Houda, Mesures de performance d'une architecture NDN avec comme objectif la, oran: Université des Sciences et de la Technologie d'Oran -MED BOUDIAf, 2022.

[40] D. K. A. S. J. S. C. Mirothali Chand.C, A COMPARATIVE SURVEY ON DIFFERENT CACHING MECHANISMS IN NAMED DATA NETWORKING (NDN) ARCHITECTURE, Pondicherry : Pondicherry University, 2019.

[41] N. S. S. A. A. Mohammad Alkhazaleh, «A COMPREHENSIVE SURVEY OF INFORMATION- CENTRIC NETWORK: CONTENT CACHING STRATEGIES PERSPECTIVE,» vol. 7, n° %1ISSN- 2394-5125 , 2020.

[42] J. M. H. d. M. A. L. D. C. Elídio Tomás da Silva, «NDN Content Store and Caching Policies: Performance Evaluation,» 2022.

[43] Mounir, «Mécanisme de mise en cache dans le réseau Ad hoc,» Université Béjaia, Bejaia.

[44] S. .. .. A. .. W. .. a. F. .. .. Abrams .M, «Caching Proxies: Limitations and Potentials,» chez *Proceedings Of the 4th International WWW Conference*, Boston, Décembre 1995.

[45] I. .. a. B. .. Menaud .J .M, «Improving effectiveness of Web caching. In Recent Advances in Distributed Systems,» *Lecture Notes in Computer Science Springer-Verlag,,* vol. 1752, p. 375–401, 2000.

[46] C. .. D. .. F. .. .. a. J. .. .. Arlitt .M .F, «Evaluating content management techniques for Web proxy caches,» *ACM SIGMETRICS Performance Evaluation Review,* vol. 27, n° %14, pp. 3-11, Mars 2000.

[47] A. .. S. .. .. A. .. a. F. .. .. Williams .S, «Removal policies in network caches for World Wide Web documents,» *In Proceedings of ACM SIGCOMM. ACM Press,* pp. 293-305, 1996.

[48] S. H. ,. M. A. P. Syambas Nana Rachmana, «Least Recently Frequently Used Replacement Policy in Named Data Network,» chez *IEEE 5th International Conference on Wireless and Telematics (ICWT)*, Badung, Juillet 2019.

[49] Z. .. .. a. Z. .. T. s. p. Yang .Q, «A cache replacement policy based on second-order trend analysis,» chez *In Proceedings of the 34th Hawaii International Conference on Systems Sciences*, IEEE Computer Society, Piscataway, New Jersey, USA, 2001.

[50] T. K. B. R. e. S. S. S. Arianfar, «"On preserving privacy in content-oriented networks",» *Proc. ACM SIGCOMM Workshop on Information-Centric Networking,* pp. 19 - 24, 2011.

[51] G. T. e. E. U. C. Ghali, «"Network-layer trust in named-data networking",» *ACM SIGCOMM Computer Communication Review,* vol. 44, n° %15, pp. 12 - 19, 2014.

[52] T. S. a. M. V. M. Wahlisch, «Lessons from the past: Why data-driven states harm future information-centric networking,» *IFIP Networking Conference,* n° %11 - 9, 2013.

[53] K. K. S. K. e. B. R. S. Choi, « "Threat of DoS by interest flooding attack in content-centric networking",» *Proc. IEEE International Conference on Information Networking (ICOIN),* n° %1315-319, 2013.

[54] «Courtesy of Cisco Systems, Inc.Unauthorized use not permitted. Technical report, Cisco, March 2020.,» *Cisco. Annual Internet Report,* 2018 - 2023.

[55] D. Menscher., «Exponential growth in DDoS attack volumes.,» *google Cloud Blog,,* 2020.

[56] S. Kottler., «February 28th DDoS Incident Report,» *GitHub blog ,* 2018.

[57] G. K. A. S. a. J. V. Constantinos Kolias, «DDoS in the IoT: Mirai and other botnets.,» *Computer,,* vol. 50, n° %17, pp. 80 - 84, 2017.

[58] G. T. E. U. e. L. Z. P. Gasti, «DoS and DDoS in named data networking,» *Proc. 22nd IEEE International Conference on,* pp. 1 - 17, 2013.

[59] M. C. P. G. a. G. T. A. Compagno, «“Poseidon: Mitigating interest flooding DDoS attacks in named data networking,”,» *Proc. 38th IEEE Conf. on Local Computer Networks (LCN),* pp. 630 - 638, 2013.

[60] S. Hochreiter and J. Schmidhuber, « “Long short-term memory,”,» *Neural Computation,,* vol. 9, n° %18, pp. 1735–1780,, 1997.

[61] A. M. a. L. P. A. Basu, «Hypothesis testing for two discrete populations based on the Hellinger distance,» *Statistics & Probability Letters,* vol. 80, n° %13-4, pp. 206-214, 2010.

[62] B. V. M. C. G. e. a. K. Cho, «Learning phrase representations using RNN encoder-decoder for statistical machine translation,» 2014.

[63] J. Schmidhuber, «Deep learning in neural networks: an overview,,» *Neural Networks,* vol. 61, p. 85–117, 2015.

[64] K. C. e. Y. B. D. Bahdanau, «Neural machine translation by jointly learning to align and translate,» 2014.

[65] V. D. A. S.-M. Y. Z. e. A. E. G. Zhang, «Classification of hand movements from EEG using a deep attention-based LSTM network,» *IEEE Sensors Journal,* pp. 3113-3122, 2020.

[66] Y. Z. J. F. P. Z. e. Z. C. Y. Ding, «Interpretable spatio-temporal attention LSTM model for flood forecasting,» *Neurocomputing,,* vol. 403, p. 348–359, 2020.

[67] [En ligne]. Available: https://omnetpp.org/omnetpp. [Accès le 15 Mai 2023].

[68] «usermanual.wiki,» [En ligne]. Available: http://www.usermanual.wiki. [Accès le 15 Mai 2023].

[69] «cloudfare,» [En ligne]. Available: http://www.cloudfare.com. [Accès le 17 Mai 2023].

Un projet pour obtenir le certificat d'une institution émergente dans le cadre de la résolution ministérielle 1275

Sommaire

Le quatrième axe : le plan de production et d'organisation

- Objectifs de production.
- Ressources nécessaires.
- Plan de travail.
- Gestion des risques.
- Contrôle de la qualité.
- Budget.

Le cinquième axe : le plan financier

- Budget initial.
- Plan de trésorerie (mensuel).
- Sources de financement.
- Prévisions financières (sur un an).
- Ajustements réguliers

Le sixième axe : le prototype expérimental

- Identification des dispositifs connectés.
- Configuration des routeurs NDN.
- Intégration des dispositifs connectés.
- Diffusion des données.
- Accès aux données.
- Sécurité et gestion de la mise en cache.

Titre du projet : Etude et simulation d'un réseau NDN

Le premier axe : Présentation du projet

1. Idée de projet (solution proposée):

Notre projet de startup vise à développer et commercialiser un réseau basé sur l'architecture NDN. Nous proposons une solution complète de mise en œuvre du réseau NDN, offrant des fonctionnalités avancées pour la gestion et la sécurisation des données, ainsi qu'une meilleure utilisation de la bande passante. Notre objectif est de permettre aux entreprises de tirer parti de cette technologie révolutionnaire et d'améliorer leurs performances en matière de communication et de partage de données.

2. Valeurs proposées:

- Performance optimisée : Notre projet de réseau NDN permettra une transmission de données plus rapide et plus efficace, réduisant la latence et améliorant l'expérience d'utilisateur.

- Sécurité renforcée : En se basant sur la gestion des noms de données plutôt que sur les adresses IP, notre solution NDN offrira une sécurité avancée, rendant les attaques basées sur l'adresse IP plus difficiles et garantissant la confidentialité et l'intégrité des données.

- Utilisation efficace de la bande passante : Grâce à la mise en cache des données populaires et à la gestion intelligente du trafic, notre architecture NDN permettra une utilisation plus efficiente de la bande passante, réduisant les coûts et améliorant les performances.

- Scalabilité et flexibilité : Notre solution sera conçue pour s'adapter aux besoins évolutifs des entreprises, offrant une architecture évolutive et modulaire.

3. Travail d'équipe:

Notre équipe est composée comme suit :

- Etudiante 01 : BELGOUMENE Sara, Spécialité : Master en réseau et télécommunication.
- Etudiante 02 : SACKO Fatoumata, Spécialité : Master en réseau et télécommunication.

Titre du projet : Etude et simulation d'un réseau NDN

Nous avons une solide expertise dans le domaine du réseau NDN et une passion commune pour l'innovation technologique. Notre équipe est hautement collaborative, créative et motivée à faire de ce projet une réussite.

4. Les objectifs du projet:

- Développer un réseau NDN fonctionnel et évolutif répondant aux besoins des entreprises.

- Assurer l'interopérabilité avec d'autres infrastructures de réseau existantes.

- Établir des partenariats stratégiques avec des entreprises et des fournisseurs de services pour promouvoir l'adoption de la technologie NDN.

- Acquérir une part de marché significative et devenir un acteur majeur dans le domaine des réseaux basés sur NDN.

5. Un échéancier pour la réalisation du projet:

1) Phase de recherche et d'étude (3 mois) :

- Étude approfondie des concepts et des principes fondamentaux du réseau NDN.

- Analyse des travaux de recherche existants et des publications pertinentes.

- Identification des défis et des opportunités spécifiques liés à la mise en œuvre du réseau NDN.

2) Phase de conception et de spécification (2 mois) :

- Conception détaillée de l'architecture du réseau NDN, en définissant les composants, les protocoles et les interfaces nécessaires.

- Élaboration des spécifications techniques pour les mécanismes de résolution de noms, de routage, de gestion de cache et de sécurité.

- Définition des cas d'utilisation et des exigences fonctionnelles spécifiques à intégrer dans le réseau NDN.

3) Phase de développement (6 mois) :

- Implémentation du protocole NDN et des fonctionnalités clés dans les logiciels correspondants.

- Développement des modules de routage, de résolution de noms, de gestion de cache et de sécurité.

- Intégration des composants matériels nécessaires pour les routeurs NDN.

4) Phase de tests et de validation (2 mois) :

- Réalisation de tests approfondis pour évaluer les performances, la sécurité et la compatibilité du réseau NDN.

- Validation des fonctionnalités en utilisant des scénarios réels et des cas d'utilisation spécifiques.

- Identification et résolution des problèmes et des bogues rencontrés lors des tests.

5) Phase de déploiement pilote (3 mois) :

- Déploiement d'une version pilote du réseau NDN dans un environnement contrôlé.

- Collecte de données de performance et d'utilisabilité pour évaluer l'efficacité du réseau NDN dans des conditions réelles.

- Rétroaction des utilisateurs et ajustements basés sur les résultats de la phase pilote.

Le deuxième axe : les aspects innovants

Notre projet se distingue par les aspects innovants suivants :

- Adoption du réseau NDN : En tant que l'une des premières entreprises à se concentrer exclusivement sur la mise en œuvre du réseau NDN, nous sommes à la pointe de l'innovation technologique et de l'adoption de cette nouvelle architecture de communication.

- Approche centrée sur les données : Notre solution met l'accent sur la gestion des noms de données, offrant une approche innovante qui améliore les performances, la sécurité et l'efficacité de la communication et du partage de données.

- Utilisation intelligente de la mise en cache : Nous développons des mécanismes avancés de mise en cache pour optimiser l'utilisation de la bande passante et réduire les temps de latence, offrant ainsi une expérience utilisateur améliorée.

Le troisième axe : analyse stratégique du marché

1. Le marché potentiel :

Le marché potentiel pour la technologie NDN est évalué en fonction du nombre d'utilisateurs d'Internet et de l'adoption croissante des technologies de l'information et de la communication. Selon les statistiques, le taux de pénétration d'Internet en Algérie a considérablement augmenté ces dernières années, atteignant environ 63% de la population en 2021. Cela indique un marché potentiellement intéressant pour les solutions basées sur NDN.

2. Segmentation du marché :

Algérie Télécom est l'un des principaux acteurs du secteur des télécommunications en Algérie, offrant une gamme de services de communication aux particuliers, aux entreprises et aux organismes publics. En tant qu'opérateur national, Algérie Télécom cherche en permanence à améliorer l'efficacité de son infrastructure réseau pour répondre aux besoins croissants de connectivité et de services de communication.

En ciblant Algérie Télécom, notre solution NDN peut offrir des avantages significatifs en termes d'optimisation de l'infrastructure réseau, de sécurité renforcée et d'amélioration de la distribution de contenu. En tant qu'opérateur de télécommunications, Algérie Télécom peut bénéficier de l'adoption de NDN pour gérer plus efficacement les flux de données, améliorer la qualité de service pour les utilisateurs finaux et réduire les coûts opérationnels liés au réseau.

De plus, notre solution NDN peut être adaptée aux objectifs stratégiques d'Algérie Télécom, notamment dans le cadre de la modernisation de son infrastructure et de sa transformation numérique. En aidant Algérie Télécom à fournir des services innovants, à améliorer l'expérience utilisateur et à rester compétitif sur le marché en constante évolution des

télécommunications en Algérie, notre solution NDN peut jouer un rôle clé dans la réalisation de ces objectifs.

3. Analyse de concurrence :

Algérie Télécom : Cette entreprise de télécommunication bien établie en Algérie propose une gamme complète de services de communication, y compris des solutions de réseau. Ils ont une large base de clients et une solide présence sur le marché. Leurs forces résident dans leur infrastructure réseau étendue et leur capacité à offrir des services fiables et de haute qualité. Cependant, leur approche traditionnelle basée sur les adresses IP pourrait les rendre moins flexibles pour gérer la croissance exponentielle du trafic de données et les nouvelles exigences de sécurité.

4. Marché cible :

En Algérie, le nombre d'utilisateurs d'Internet connaît une croissance rapide, témoignant de l'importance croissante d'Internet dans la vie quotidienne des Algériens. Cette augmentation du nombre d'utilisateurs crée une demande croissante de services de communication et de connectivité de qualité.

Les Algériens utilisent de plus en plus Internet pour des activités telles que la recherche d'informations, les réseaux sociaux, le commerce électronique, les services bancaires en ligne et le divertissement. Ils ont des attentes élevées en termes de vitesse, de fiabilité et de sécurité de leur connexion Internet.

En tant que fournisseurs de solutions NDN, nous pouvons répondre à cette demande croissante en proposant une modernisation de l'infrastructure de réseau qui offre une meilleure gestion des données, une évolutivité améliorée et une sécurité accrue. Notre solution peut aider à relever ces défis et à fournir des services de communication de qualité aux utilisateurs d'Internet en Algérie.

5. Analyse des tendances du marché :

L'analyse des tendances du marché en Algérie révèle plusieurs facteurs qui peuvent avoir un impact sur l'adoption et les opportunités commerciales de notre solution NDN. Voici quelques tendances émergentes à prendre en compte :

a) Croissance de la connectivité Internet : L'Algérie connaît une croissance rapide du nombre d'utilisateurs d'Internet, avec une augmentation significative de la pénétration d'Internet au cours des dernières années. Cette tendance se poursuivra probablement à mesure que de plus en plus de personnes auront accès à Internet via des appareils mobiles et fixes. Cette augmentation de la connectivité Internet crée une demande croissante de solutions qui peuvent offrir une connectivité fiable, une vitesse élevée et une expérience utilisateur optimale, ce qui représente une opportunité pour notre solution NDN.
b) Besoin de gestion efficace des données : Avec la prolifération des services en ligne, des applications et des appareils connectés, les opérateurs de télécommunications en Algérie sont confrontés à un volume croissant de données à gérer. Une tendance émergente est la nécessité de disposer de solutions qui permettent une gestion efficace des données, y compris la transmission, le stockage et l'accès aux données de manière sécurisée. Le réseau NDN est une réponse à ce besoin en offrant une architecture de basée sur le contenu, qui permet une distribution et une gestion efficaces des données.
c) Prise de conscience croissante de la sécurité des données : Avec l'augmentation des cyberattaques et des incidents de sécurité, la sécurité des données est devenue une préoccupation majeure pour les entreprises et les utilisateurs en Algérie. Les réglementations en matière de protection des données personnelles se renforcent également. Les opérateurs de télécommunications cherchent des solutions qui offrent des niveaux de sécurité élevés pour protéger les informations sensibles. NDN peut répondre à cette tendance en offrant des mécanismes de sécurité intégrés, tels que le chiffrement des données et l'authentification robuste, garantissant ainsi la confidentialité et l'intégrité des données.

d) Transition vers des infrastructures plus flexibles : Les opérateurs de télécommunications cherchent à moderniser leurs infrastructures pour les rendre plus agiles et flexibles, afin de faire face aux évolutions rapides du marché et aux besoins changeants des utilisateurs. Les tendances telles que la virtualisation du réseau, le Cloud Computing et la mise en œuvre de technologies de réseau définies par logiciel (SDN) gagnent en popularité. Donc NDN peut être alignée sur cette tendance en offrant une architecture de réseau flexible et évolutive, permettant aux opérateurs de télécommunications de s'adapter rapidement aux demandes du marché.

6. Les stratégies de marketing :

a) Campagnes de sensibilisation : Nous allons créer du contenu éducatif tel que des articles de blog, des vidéos et des infographies mettant en évidence les avantages de NDN pour améliorer l'efficacité de leur infrastructure réseau. Nous allons utiliser les médias sociaux, la publicité en ligne et les partenariats avec des influenceurs du secteur pour maximiser la portée de notre campagne.

b) Développement de relations avec les acteurs clés : Nous allons identifier les principaux acteurs du marché des télécommunications en Algérie, tels que Algérie Télécom, et établir des relations solides avec eux par une organisation des réunions individuelles pour présenter notre implémentation NDN et discuter des avantages potentiels pour leur entreprise.

c) Participation à des événements sectoriels : Nous allons identifier les salons professionnels et les conférences du secteur des télécommunications en Algérie, tels que les forums technologiques et les rencontres des opérateurs de télécommunications. Nous allons participer en tant qu'exposant et présentez le réseau NDN lors de conférences ou de tables rondes. Nous allons bien profiter de ces événements pour établir des contacts avec les décideurs de l'industrie et renforcer notre visibilité.

Le quatrième axe : le plan de production et d'organisation

1. Objectifs de production :

L'objectif principal de notre projet NDN est de développer et de mettre en œuvre un réseau de communication basé sur le modèle Named Data Networking. Nous visons à créer un prototype fonctionnel qui démontre les avantages de cette architecture par rapport au modèle traditionnel basé sur les adresses IP.

2. Ressources nécessaires :

Pour la réalisation de ce projet, nous aurons besoin des ressources suivantes :

- Une équipe de développement comprenant des ingénieurs réseau, des développeurs logiciels et des experts en sécurité.

- Un environnement de test avec du matériel réseau approprié.

- Des logiciels de simulation et de modélisation pour évaluer les performances du réseau NDN.

- Un financement adéquat pour couvrir les coûts de développement, de matériel et de licences logicielles.

3. Plan de travail :

Notre plan de travail comprendra les étapes suivantes :

- Phase 1 : Analyse des besoins et spécifications du projet.

- Phase 2 : Conception de l'architecture réseau NDN et développement des protocoles correspondants.

- Phase 3 : Mise en place de l'infrastructure réseau NDN dans un environnement de test.

- Phase 4 : Développement d'applications NDN pour démontrer les avantages de cette technologie.

- Phase 5 : Tests approfondis, optimisation des performances et résolution des problèmes identifiés.

- Phase 6 : Documentation complète du projet et préparation pour le déploiement.

5. Gestion des risques :

Nous identifions les risques potentiels suivants et proposons des stratégies d'atténuation :

- Risque technique : Possibilité de problèmes de compatibilité matérielle ou logicielle. Solution : Effectuer des tests approfondis avant l'implémentation.

- Risque de délais : Risque que certaines étapes prennent plus de temps que prévu. Solution : Suivi régulier de l'avancement et réaffectation des ressources si nécessaire.

- Risque de sécurité : Possibilité de vulnérabilités dans le réseau NDN. Solution : Effectuer des audits de sécurité réguliers et appliquer les correctifs nécessaires.

6. Contrôle de la qualité :

Nous mettrons en place les mesures suivantes pour garantir la qualité :

- Effectuer des tests unitaires et des tests d'intégration tout au long du processus de développement.

- Mettre en place des scénarios de test pour évaluer les performances, la fiabilité et la scalabilité du réseau NDN.

- Effectuer des audits de code réguliers pour garantir la conformité aux normes de codage et la qualité du logiciel développé.

7. Budget :

Notre budget prévisionnel inclura les coûts estimés pour les ressources humaines, les équipements, les licences logicielles, les tests et les frais de communication. Nous suivrons les dépenses réelles par rapport au budget prévu et ajusterons en conséquence.

Le cinquième axe : le plan financier.

1. Budget initial :

- Matériel informatique : 10 273 034 DZD

(Ils peuvent inclure :

1) Routeurs : Les routeurs NDN sont spécifiquement conçus pour prendre en charge le routage basé sur le nom. Ils acheminent les paquets de données en fonction des noms de contenu plutôt que des adresses IP.
2) Commutateurs : Les commutateurs réseau permettent de connecter différents dispositifs au sein d'un réseau NDN. Ils facilitent la communication entre les serveurs, les routeurs et les autres périphériques du réseau.
3) Cartes réseau : Les cartes réseau sont nécessaires pour connecter les dispositifs au réseau NDN. Elles permettent aux ordinateurs et aux serveurs de communiquer entre eux en utilisant les protocoles NDN.
4) Disques de stockage : Des disques de stockage sont nécessaires pour stocker les données et les caches dans un réseau NDN. Cela peut inclure des disques durs internes ou externes, des disques SSD (Solid-State Drive) ou d'autres formes de stockage.
5) Équipements de sécurité : Les équipements de sécurité, tels que les pare-feu et les systèmes de détection d'intrusion, sont importants pour protéger le réseau NDN contre les menaces potentielles et garantir la confidentialité et l'intégrité des données.
6) Équipements de surveillance : Les outils de surveillance du réseau, tels que les sondes de trafic et les logiciels de gestion du réseau, peuvent être utilisés pour surveiller les performances du réseau NDN, détecter les problèmes et optimiser les opérations.)

- Logiciels et licences : 500 000 DZD

- Frais de développement : 150 000 DZD

Titre du projet : Etude et simulation d'un réseau NDN

(Ils peuvent inclure :

1) Développement logiciel : Cela comprend les dépenses liées à la programmation et à la création du code source pour mettre en œuvre les fonctionnalités spécifiques de notre projet NDN.
2) Tests et débogage : Les coûts liés à la phase de test et de débogage pour s'assurer que notre projet NDN fonctionne correctement, qu'il est stable et qu'il répond aux exigences de performance et de sécurité.
3) Infrastructure technique : Il peut y avoir des frais associés à l'acquisition ou à la mise à niveau de l'infrastructure matérielle et logicielle nécessaire pour prendre en charge notre projet NDN. Cela peut inclure des serveurs, des équipements réseau, des licences de logiciels, etc.
4) Intégration de systèmes : notre projet NDN nécessite l'intégration avec d'autres systèmes ou technologies existants, des frais de développement sont engagés pour assurer une intégration fluide et harmonieuse.
5) Conception et expérience utilisateur : nous voulons offrir une interface utilisateur conviviale et attrayante, alors nous devons engager des frais pour la conception graphique, l'ergonomie, l'expérience utilisateur, etc.
6) Documentation et support : Il est important de fournir une documentation adéquate et un support technique à nos utilisateurs. Les coûts associés à la rédaction de guides d'utilisation, de manuels, de tutoriels, ainsi qu'au support client peuvent être inclus dans les frais de développement.)

- Marketing et publicité : 100 000 DZD

- Frais généraux (loyer, services publics, etc.) : 80 000 DZD

- Total des dépenses initiales : 3 530 000 DZD

Tableau 1 Les dépenses initiales

Matériel informatique	10 273 034 DA
Logiciels et licences	500 000 DA
Frais de développement	150 000 DA
Marketing et publicité	100 000 DA
Frais généraux (Loyer…)	80 000 DA/mois
Total des dépenses initiales	**11 103 034 DA**

Tableau2 Les dépenses et coûts fixes du projet

Assurances	**Assurances : 364 000 DA.**
Téléphone, internet	**Téléphone : 28 800 DA.** **Internet : 36 000 DA.**
Autres abonnements	/
Carburant, transports	**Carburant : 480 000 DA.** **Transports : 384 000 DA.**
Frais de déplacement et hébergement	**Frais de déplacement et hébergement : 100 000 DA.**
Eau, électricité, gaz	**Eau, électricité, gaz : 36 000 DA.**
Mutuelle	**Mutuelle : 58 750 DA.**
Fournitures diverses	**Fournitures diverses : 50 000 DA.**
Entretien matériel et vêtements	**Entretien matériel et vêtements : 100 000 DA.**
Nettoyage des locaux	**Nettoyage des locaux : 20 000 DA.**
Budget publicité et communication	**Budget publicité et communication : 500 000 DA.**
Total	**2 157 550 DA**

2. Plan de trésorerie (mensuel) :

- Janvier : Revenus - 70 000 DZD / Dépenses - 60 000 DZD

- Février : Revenus - 80 000 DZD / Dépenses - 55 000 DZD

Taux d'évolution = ((80 000 – 70 000)/70 000) *100

Taux d'évolution = 14,28%

- Mars : Revenus - 90 000 DZD / Dépenses - 70 000 DZD

Taux d'évolution = 12,50%

- Avril : Revenus - 100 500 DZD / Dépenses - 65 000 DZD

Taux d'évolution = 11,66%

- Mai : Revenus - 120 000 DZD / Dépenses - 75 000 DZD

Taux d'évolution = 19,40%

- Juin : Revenus - 140 000 DZD / Dépenses - 80 000 DZD

Taux d'évolution = 16,28%

- Juillet : Revenus - 150 000 DZD / Dépenses - 85 000 DZD

Taux d'évolution = 7,14%

- Août : Revenus - 160 000 DZD / Dépenses - 90 000 DZD

Taux d'évolution = 6,66%

- Septembre : Revenus - 180 000 DZD / Dépenses - 95 000 DZD

Taux d'évolution = 12,50%

- Octobre : Revenus - 200 000 DZD / Dépenses - 100 000 DZD

Taux d'évolution = 11,11%

- Novembre : Revenus - 210 000 DZD / Dépenses - 105 000 DZD

Taux d'évolution = 5,00%

- Décembre : Revenus - 230 000 DZD / Dépenses - 110 000 DZD

Taux d'évolution = 9,52%

Tableau 3 Le plan de trésorerie (mensuel)

Mois	Revenus prévus (en DZ)	Dépenses prévus (en DZ)	Taux d'évolution
Janvier	70 000	60 000	-
Février	80 000	55 000	14,80 %
Mars	90 000	70 000	12,50 %
Avril	100 500	65 000	11,66 %
Mai	120 000	75 000	19,40 %
Juin	140 000	80 000	16,28 %
Juillet	150 000	85 000	7,14 %
Aout	160 000	90 000	6,66 %
Septembre	180 000	95 000	12,50 %
Octobre	200 000	100 000	11,11 %
Novembre	210 000	105 000	5,00 %
Décembre	230 000	110 000	9,52 %
Total	**1 730 500**	**990 000**	-

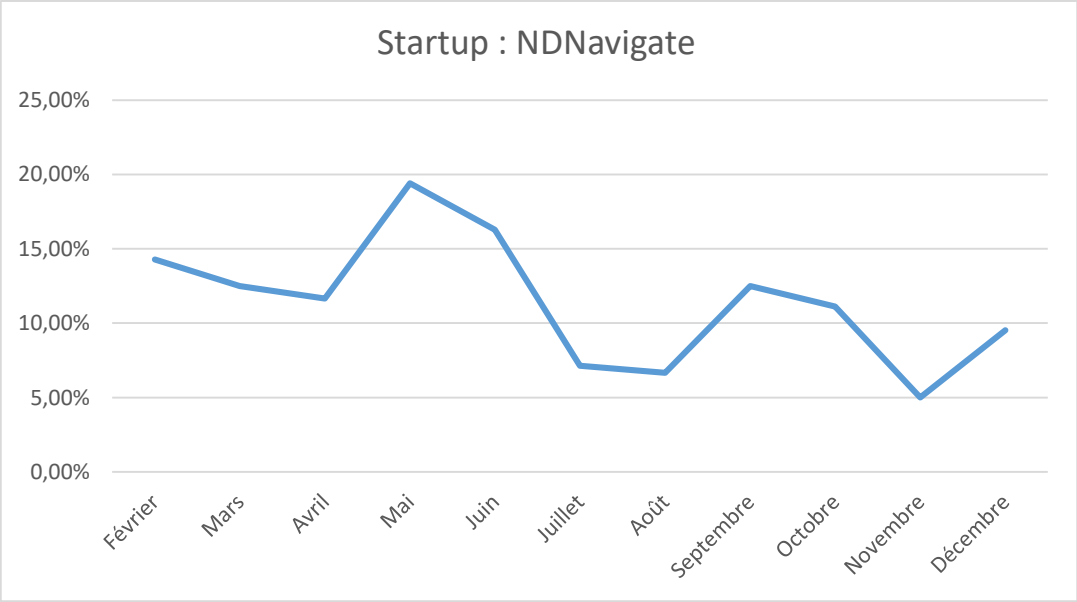


Figure 46 Le taux d'évolution pour un an

Titre du projet : Etude et simulation d'un réseau NDN

3. Sources de financement :

- Prêt bancaire : 13 000 000 DZD

- Apport personnel : 260 584 DZD

4. Prévisions financières :

Sur un an :

- Revenus totaux : 1 730 500 DZD

- Dépenses totales : 1 290 000 DZD

- Bénéfice net : 440 500 DZD

Sur deux ans :

- Revenus totaux : 1 800 000 DZD

- Dépenses totales : 1 200 000 DZD

- Bénéfice net : 600 000 DZD

Sur trois ans :

- Revenus totaux : 1 950 000 DZD

- Dépenses totales : 1 100 000 DZD

- Bénéfice net : 1 150 000DZD

Tableau 4 Les prévisions sur les trois premieres années.

	PREVISION		
	Sur un an	**Sur deux ans**	**Sur trois ans**
Revenus totaux	1 730 500	1 290 000	440 500
Dépenses totales	1 800 000	1 200 000	600 000
Bénéfice net	1 950 000	1 100 000	850 000

5. Ajustements réguliers :

- Surveillance régulièrement nos résultats financiers réels et les comparer à nos prévisions mensuelles. Effectuation des ajustements si nécessaire pour maintenir nos objectifs financiers et notre rentabilité.

(Ils peuvent inclure :

1. Suivi des résultats financiers réels : Comparez régulièrement les résultats financiers réels de notre projet NDN avec les prévisions que nous avons établies. Cela nous permettra de voir si nos revenus, nos dépenses et notre rentabilité correspondent à ce qui était prévu.

2. Analyse des écarts : Identification des écarts entre les résultats réels et les prévisions. Observation des raisons de ces écarts et évaluez leur impact sur nos finances. Par exemple, si nos dépenses sont plus élevées que prévu, nous chercherons les domaines spécifiques où nous pouvons réduire les coûts.

3. Révision des prévisions : Sur la base des écarts identifiés, nous ajustons nos prévisions financières pour les mois ou les trimestres à venir. Nous tenons compte des leçons apprises et des nouvelles informations pour affiner nos estimations de revenus, de dépenses et de rentabilité.

4. Adaptation des stratégies : Si les résultats réels diffèrent significativement de nos prévisions, il peut être nécessaire de revoir nos stratégies financières. Cela peut inclure des ajustements dans nos efforts de marketing, de vente, de réduction des coûts ou d'autres domaines afin d'aligner nos objectifs financiers avec la réalité.

5. Gestion de la trésorerie : Sur la base de nos résultats financiers réels et de nos ajustements prévus, nous assurons de gérer efficacement notre trésorerie. Nous allons identifier les périodes de déficit de trésorerie potentielles et nous prenons des mesures pour y remédier, comme la recherche de financements supplémentaires, la renégociation des délais de paiement avec les fournisseurs, ou l'optimisation de nos politiques de recouvrement des paiements des clients.

6. Surveillance continue : Nous allons garder une surveillance constante de nos résultats financiers et de l'évolution du marché. Nous allons identifier les tendances, les opportunités et les risques potentiels qui pourraient affecter nos prévisions financières. Cela nous permettra d'adapter rapidement nos stratégies et nos décisions en fonction des changements survenant dans notre environnement commercial.)

Le sixième axe : le prototype expérimental

Nous proposons un déploiement d'un réseau NDN pour prendre en charge les communications entre les dispositifs connectés dans un quartier résidentiel :

1. Identification des dispositifs connectés :

Nous allons identifier les dispositifs connectés présents dans le quartier résidentiel, tels que les compteurs d'électricité intelligents, les systèmes de surveillance domestique, les thermostats connectés, etc. Et déterminer les types de données qu'ils génèrent et les besoins de communication associés.

2. Configuration des routeurs NDN :

Nous allons déployer des routeurs NDN dans différentes zones du quartier résidentiel et les configurer pour permettre la découverte et la diffusion de données basées sur les noms en assurant que les routeurs sont correctement connectés entre eux pour former un réseau NDN cohérent.

3. Intégration des dispositifs connectés :

Nous allons également configurer les dispositifs connectés pour utiliser le protocole NDN. Cela peut nécessiter l'installation d'un logiciel client NDN sur les appareils ou l'utilisation de passerelles NDN pour les appareils qui ne prennent pas en charge directement NDN en assurant que chaque appareil possède un nom unique pour permettre l'adressage et la résolution des données.

4. Diffusion des données :

Les dispositifs connectés commencent à générer des données qui sont diffusées dans le réseau NDN. Par exemple, les compteurs d'électricité intelligents envoient des informations sur la consommation d'énergie, les systèmes de surveillance domestique diffusent des flux vidéo,

etc. Les données sont encapsulées dans des paquets NDN et diffusées dans le réseau en utilisant des noms de données.

5. Accès aux données :

Les applications et les utilisateurs peuvent accéder aux données en utilisant les noms associés. Par exemple, une application de suivi de la consommation d'énergie peut envoyer une requête pour obtenir les données du compteur d'électricité spécifique en utilisant le nom du compteur. Le routeur NDN achemine la requête vers le compteur approprié et renvoie les données correspondantes à l'application.

6. Sécurité et gestion de la mise en cache :

Le réseau NDN offre des mécanismes intégrés de sécurité et de gestion de la mise en cache. Les données peuvent être signées numériquement pour assurer leur intégrité et leur authenticité. De plus, les routeurs NDN peuvent mettre en cache les données populaires localement, ce qui réduit la latence et la charge sur le réseau.

En déployant un réseau NDN dans un quartier résidentiel, les dispositifs connectés peuvent communiquer de manière efficace et sécurisée en utilisant des noms de données. Les avantages de NDN, tels que la réduction de la congestion du réseau et la capacité de gérer de grandes quantités de données, peuvent améliorer les fonctionnalités et les performances des applications IoT dans le quartier résidentiel.

Annexe n°01 : Business Model

Partenaires :	**Activités clés :**	**Proposition de valeur :**	**Relation clients :**	**Le segment de marché :**
-Fournisseurs locaux d'équipements réseau. -Universités et instituts de recherche en Algérie (Université Ibn Khaldoun Tiaret). -Fournisseurs de services Internet.	-Recherche et développement continus pour améliorer la technologie NDN et la personnaliser pour les besoins du marché algérien. -Déploiement pilote de NDN dans les réseaux des clients pour démontrer les avantages et évaluer les performances. -Formation et support technique pour aider les clients à adopter et à utiliser efficacement NDN.	-Performance optimisée. -Sécurité renforcée. -Utilisation efficace de la bande. -Scalabilité et flexibilité.	-Collaboration étroite avec les clients. -Fourniture de support technique et de formation. - Notre site web. -Les réseaux sociaux.	-Fournisseurs de services Internet en Algérie (Algérie Télécom, Mobilis...).

	Ressources clés : -Une équipe multidisciplinaire d'experts en réseaux de communication et en technologie NDN. -Des laboratoires et des équipements de test pour le développement et la validation de solutions NDN. -Un solide réseau de partenaires, y compris des fabricants d'équipements réseau et des développeurs de logiciels spécialisés.		**Distribution :** -Vente directe aux fournisseurs de services Internet. -Participation à des conférences et à des événements du secteur en Algérie. -Marketing en ligne pour promouvoir la technologie NDN en Algérie.	

Titre du projet : Etude et simulation d'un réseau NDN

Structure de coûts :	**Source de revenue et modèle de pricing :**
-Coûts de recherche et développement pour améliorer la technologie NDN et l'adapter au marché algérien. -Coûts de marketing et de promotion pour atteindre les acteurs clés du marché et sensibiliser à la technologie NDN. -Coûts de maintenance, de support et de formation pour assurer une expérience client optimale.	-Vente de licences de la technologie NDN aux fournisseurs de services Internet en Algérie. -Contrats de déploiement et de consultation pour l'implémentation de NDN dans les réseaux existants en Algérie. -Revenus issus de services de maintenance, de support et de formation associés à NDN.