REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITÉ SAAD DAHLAB BLIDA 1

Faculté des Sciences

Département : Informatique

Mémoire de Fin d'Étude pour l'Obtention du Diplôme de Master en Informatique

OPTION : Systèmes Informatiques et Réseaux

Thème :

Développement d'un Système de Gestion des Urgences Sismiques basé sur des Communications Opportunistes de Smartphones dans les Réseaux Centrés sur l'Information (Information Centric Network, ICN)

Réalisé par :

M^{elle} BOUDJEMA HASNA

M^{elle} DRIOUCH ASMA

Soutenu le 09/09/2020 devant le jury composé de :

- **M^{r}** OULD-KHAOUA Mohamed — **President**
- **M^{me}** ABED Hafida — **Examinatrice**
- **M^{me}** AROUSSI Sana — **Promotrice**
- **M^{me}** ARKAM Meriem — **Co-promotrice**

Année Universitaire : 2019-2020

Remerciement

Nous tenons tout d'abord à remercier Dieu le tout puissant et miséricordieux, qui nous a donné la force et la patience d'accomplir ce modeste travail.

Nous tenons à remercier Madame ARKAM Meriem et Madame AROUSSI Sana pour avoir accepté de nous encadrer, pour sa disponibilité tout au long de réalisation de ce mémoire, pour la qualité de ses conseils qui nous a permis de mener à bien ce travail et pour nous avoir fait bénéficier de son avoir.

Nos vifs remerciements vont également aux membres du jury pour l'intérêt accordé à notre travail en l'examinant minutieusement et de l'enrichir par leurs propositions.

Enfin, nous remerciements les plus sincères à toutes les personnes qui avaient contribué de près ou de loin à l'élaboration de ce mémoire ainsi qu'à la réussite de cette année universitaire.

Merci.

Dédicace

C'est avec profonde gratitude et sincères mots, que je dédie ce modeste travail de fin d'étude :

À la mémoire de mon grand-père qui aurait été si fier de moi.

À mes chers parents pour tous leurs sacrifices, leur amour, leur tendresse, leur soutien et leurs prières tout au long de nos études. Que Dieu leur protège et accorde une longue vie pleine de santé et de bonheur.

À mes frères et surtout ma sœur Fella pour avoir contribué à la réussite de ce travail d'une manière indirecte, et pour leur conseil et encouragement.

À toute ma famille pour leur soutien tout au long de notre parcours universitaire en particulier mes oncles, ma tante et ma chère cousine Hadjer.

À mes amies, pour leur soutien et encouragement.

À tous ceux qui me sont chers.

ASMA.

Dédicace

Je dédie ce modeste travail en signe de respect, reconnaissance et de remerciement :

A mes chers parents, qui ont sacrifie leur vie pour notre réussite et nous ont éclairé le chemin par leurs conseils judicieux.

J'espère qu'un jour, je pourrais leurs rendre un peu de ce qu'ils ont fait pour moi. Que Dieu leur prête bonheur et longue vie.

A mes chers sœurs Amina et Nassima ainsi qu'à mon frère Djalel, en reconnaissance de leur affection toujours constante.

A la personne qui m'a soutenu toute l'année, ma binôme Asma, un grand merci.

A tous mes ami(e)s qui m'ont toujours encouragé, et à qui je souhaite plus de succès.

Et à tous ceux qui me sont chers.

HASNA.

Résumé

Les réseaux centrés sur l'information (Information Centric Network, ICN), ont été proposées principalement pour faire face aux nouveaux besoins d'Internet depuis que son utilisation principale a changé d'un modèle de communication entre les hôtes à une distribution de contenus. L'objectif est de fournir un service d'infrastructure réseau mieux adapté à l'utilisation actuelle (en particulier, la distribution de contenu et la mobilité) et plus résistant aux perturbations et aux pannes.

Dans ce travail, nous avons proposé un système de gestion des urgences sismiques basé sur une communication opportuniste de smartphones offerte par le réseau mobile ad hoc dans la nouvelle architecture de réseau centré contenu (ICN).

Pour cela, nous avons conçu une application Android permettant la gestion des urgences sismiques où nous supposons que les données sont communiquées à travers le réseau nommé des données NDN (Named Data Networking) qui représente l'architecture la plus utilisée des ICNs. Nous avons aussi opté pour le principe du transfert EADE (Ecouter Avant Diffuser Ensuite) ou LFBL (Listen First Broadcast Later) du réseau mobile ad hoc MANET (Mobile Ad Hoc Network) pour offrir une communication opportuniste et garantir la mobilité.

Les résultats préliminaires obtenus sous simulateur ndnSIM montrent le bon fonctionnement de notre proposition en offrant des capacités de communication efficaces et résilientes en cas d'un séisme.

Mots clés : Systèmes de gestion des urgences et catastrophe (SGUC), séisme, réseaux centrés sur l'information (ICN), réseau de donné nommé (NDN), communication opportuniste, réseau mobile ad hoc MANET, stratégie de transfert LFBL, simulateur ndnSIM.

Abstract

Information Centric Network (ICN) has been proposed primarily to meet the new needs of the Internet since its primary use has changed from a model of communication between hosts to a distribution of content. The aim is to provide a network infrastructure service that is better suited to today's use (in particular, content distribution and mobility) and more resistant to disruption and failure.

In this work, we proposed a seismic emergency management system based on opportunistic smartphone communication offered by the ad hoc mobile network in the new information-centric network (ICN) architecture.

For this, we have designed an Android application allowing the management of seismic emergencies where we assume that the data is communicated through the network named NDN (Named Data Networking) which represents the most used architecture of ICNs. We have also opted for the principle of EADE (Listen Before Broadcast Next) or LFBL (Listen First Broadcast Later) transfer from the MANET (Mobile Ad Hoc Network) to offer opportunistic communication and guarantee mobility.

The preliminary results obtained under the ndnSIM simulator show how well our proposal works by offering effective and resilient communication capacities in the event of an earthquake.

Keywords: Emergency and disaster management systems (SGUC), earthquake, information-centric networks (ICN), named data network (NDN), opportunistic communication, MANET ad hoc mobile network, LFBL transfer strategy, ndnSIM simulator.

ملخص

تم اقتراح شبكة المعلومات المركزية (ICN) في المقام الأول لتلبية الاحتياجات الجديدة للإنترنت منذ أن تغير استخدامها الأساسي من نموذج الاتصال بين المضيفين إلى توزيع المحتوى. الهدف هو توفير خدمة بنية تحتية للشبكة أكثر ملاءمة للاستخدام اليوم (على وجه الخصوص، توزيع المحتوى والتنقل) وأكثر مقاومة للاضطراب والفشل.

في هذا العمل، اقترحنا نظامًا لإدارة الطوارئ الزلزالية يعتمد على الاتصالات الهاتفية الانتهازية التي تقدمها شبكة الهاتف المحمول المخصصة في بنية الشبكة الجديدة التي تركز على المحتوى (ICN).

لهذا، قمنا بتصميم تطبيق Android يسمح بإدارة حالات الطوارئ الزلزالية حيث نفترض أن البيانات يتم توصيلها من خلال الشبكة المسماة NDN (شبكات البيانات المسماة) والتي تمثل البنية الأكثر استخدامًا لشبكات ICN. لقد اخترنا أيضًا مبدأ EADE (استمع أولاً بث لاحقًا) أو نقل LFBL (استمع أولاً بث لاحقًا) من شبكة الهاتف المحمول المخصصة MANET لتقديم اتصالات مفيدة وضمان التنقل.

تظهر النتائج الأولية التي تم الحصول عليها في إطار محاكاة ndnSIM مدى جودة عمل اقتراحنا من خلال توفير قدرات اتصال فعالة ومرنة في حالة حدوث زلزال.

الكلمات الرئيسية: أنظمة إدارة الطوارئ والكوارث(SGUC) ، الزلازل، الشبكات التي تتمحور حول المعلومات(ICN) ، شبكة البيانات المسماة(NDN) ، الاتصال الانتهازي، شبكة المحمول المخصصةMANET ، استراتيجية نقلLFBL ، محاكي ndnSIM.

Table des Matières

Liste des Figures

Liste des Tableaux

Liste d'Acronymes

Acronymes	Signification
ACK	ACKnowledgement
API	Application Programming Interface
AS	Autonomous System
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
CA	Content Announcement
CCN	Content Centric Networking
CDN	Content Delivery Netrwork
COMET	COntent Mediator architecture for contentaware nETworks
CS	Content Store
DHCP	Dynamic Host Configuration Protocol
DINET	Deep Impact Network
DNS	Domain Name System
DONA	Data Oriented Network Architecture
DT	Distance Table
DTN	Delay Tolerant Network
EM	Exact Match
EMS	Emergency Medical Service
FIB	Forwarding Information Base
FIFO	First In First Out
FTP	File Transfer Protocol
GACF	Greedy Ant Colony Forwarding
GIS	Geographic Information System
GPS	Global Positioning System
HoBHIS	Hop-By-Hop Interest Shaping
HTTP	Hypertext Transfer Protocol

ICN	Information Centric Network
IP	Internet Protocol
IS-IS	Intermediate System to Intermediate System
ISP	Internet Service Provider
LFBL	Listen first broadcast later
LOMCF	Location-aware On-demand Multipath Caching and Forwarding
LPM	Longest Prefix Match
LRU	Least Recently Used
MANET	Mobile Ad Hoc Network
METERON	Multi-Purpose End-To-End Robotic Operation Network
NAIF	Neighbor Aware forwarding
NASA	National Aeronautics and Space Administration
NDN	Named Data Networking
NDO	Named Data Object
NFD	Named Data Networking Forwarding Daemon
NRS	Name Resolution System
OSPF	Open Shortest Path First
P2P	Peer-to-Peer
PAF	Provider Aware Forwrding
PDA	Personal Digital Assistant
PIT	Pending Interest Table
PSIRP	Publish Subscribe Internet Routing Paradigm
PURSUIT	Publish Subscribe Internet Technology
QoS	Quality of Service
REMIF	Robust and Efficient Multipath Interest Forwarding
REP	REsPonse
REQ	REQuest
RSU	Road Side Unit

SAIL	Scalable & Adaptive Internet soLutions
SGUC	Système de Gestion des Urgences et Catastrophes
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
TLV	Type-Length-Value
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VANET	Vehicule Ad Hoc Network
VoiIP	Voice Over Internet Protocol
WSN	Wireless Sensor Network

Introduction Générale

Le tremblement de terre est la catastrophe naturelle la plus meurtrière et la plus destructrice dans le Monde[1]. Bien qu'on ne puisse toujours rien face aux catastrophes, mais on peut minimiser leurs effets défavorables par un processus systématique fondé sur les principes essentiels de gestion présenté par un Système de Gestion des Urgences et Catastrophes (SGUC).

La communication est un facteur clé d'une meilleure performance offerte par les SGUC mais les catastrophes peuvent gravement endommager les infrastructures de communication, rendant difficile pour les personnes sinistrées de recevoir et d'envoyer des informations. Dans les heures qui suivent une catastrophe, des communications sont nécessaires pour diffuser des informations critiques aux personnes dans la zone sinistrée, ainsi que pour la communication des équipes de secours et pour réaliser conscience de la situation. Alors, il existe un besoin urgent d'une communication et d'une distribution de contenu fiables / efficaces, qui peuvent être prises en charge par les réseaux mobiles ad hoc. Ce type de réseau peut être très bénéfique pour collecter et diffuser les informations vitales d'urgences via les smartphones et les tablettes. Selon le rapport annuel de Cisco, le nombre totale d'abonnés mobiles dans le monde passera de 5,1 milliards (66% de la population) en 2018 à 5,7 milliards (71% de la population) d'ici 2023[2].

Cependant, lorsque le nombre de dispositifs impliqués dans la formation du réseau augmente, de grandes difficultés se posent dans la configuration, la maintenance, la mise à jour et la configuration automatiques des réseaux, en raison de la nature conversationnelle du paradigme TCP / IP. En effet, Internet a été initialement proposé dans le but d'interconnecter quelques hôtes distants mais son infrastructure ne gère pas d'autres aspects plus importants comme la mobilité et la sécurité.

Face à tout ceci, un nouveau paradigme a été proposée sous le nom de réseau centré sur l'information (Information Centric Network, ICN). Il a été exploré par de nombreux projets comme la Data-Oriented Network Architecture (DONA) [3], le Content-Centric Networking (CCN) [4] le Named Data Networking (NDN) [5] et le Convergence [4] pour faire face aux limites de l'Internet. Son idée principale est de considérer les contenus nommés comme l'élément central du réseau, contrairement aux adresses IP qui identifient les hôtes dans les réseaux actuels. Pour récupérer un contenu, un utilisateur ne se préoccupe plus de son emplacement mais il n'a besoin que de spécifier le nom de ce contenu. Le concept de ce nouveau réseau (ICN) s'appuie sur la mise en cache dans

le réseau, la communication multipartite par réplication. L'objectif est de fournir un service d'infrastructure réseau mieux adapté à l'utilisation actuelle (en particulier, la distribution de contenu et la mobilité) et plus résistant aux perturbations et aux pannes.

L'objectif principal de ce travail de master est de développer un système de gestion des urgences sismiques basé sur une communication opportuniste de smartphones offerte par le réseau mobile ad hoc dans la nouvelle architecture de réseau centré contenu (ICN) et d'étudier le potentiel et l'applicabilité de ce que cette nouvelle architecture peut offrir aux systèmes de gestion des urgences et catastrophes en général et aux systèmes de gestion des urgences sismiques en particulier.

Ce présent mémoire est organisé comme suit :

- **Chapitre I** : où nous présentons une étude bibliographique sur la gestion des urgences et catastrophes et les différents systèmes de communication en cas d'urgence.
- **Chapitre II** : où nous étudions les limites d'Internet et la notion de réseau centré sur l'information (ICN) ses fonctionnalités de base et une comparaison entre les principaux projets.
- **Chapitre III** : où nous décrivons le projet Named Data Network (NDN), son fonctionnement et nous discutons sur les différentes stratégies qui existent dans MANET sous NDN.
- **Chapitre IV :** où nous expliquons la conception de notre solution qui s'agit d'un SGUC basé sur la stratégie de transfert EADE du réseau MANET-NDN.
- **Chapitre V :** nous présentons l'interface graphique d'application, les résultats de simulation et leurs discussions.
- Nous terminerons par une conclusion générale et quelques perspectives pour des travaux futurs.

Chapitre I : Systèmes de Gestion des Urgences et des Catastrophes

I.1 Introduction

Les catastrophes ont affecté les humains depuis l'aube de notre existence. En réponse, les individus et les sociétés ont fait de nombreuses tentatives pour réduire leur exposition aux conséquences de ces catastrophes, en élaborant des mesures pour faire face à l'impact initial, ainsi qu'aux besoins d'intervention et de relèvement post-catastrophe. Quelle que soit l'approche adoptée, tous ces efforts ont le même objectif : la gestion des catastrophes.

Dans ce chapitre, nous commençons par un court historique des catastrophes et la gestion de ces dernières. Ensuite, nous définissons la gestion des catastrophes et des urgences et ses principales caractéristiques. Puis, nous présentons les différents systèmes de communication en cas d'urgence. Enfin, nous finissons avec la communication opportuniste.

I.2 Les catastrophes à travers l'histoire

Les catastrophes ne sont pas simplement des événements ornementaux ou intéressants qui ornent notre record historique collectif, ces perturbations ont servi à le guider et à le façonner. Les civilisations entières ont été décimées en un instant. Pour des milliers de fois, les épidémies et les pandémies ont entraîné des réductions importantes de la population mondiale - jusqu'à 50% en Europe au cours de la pandémie de peste bubonique (peste noire) du XIVe siècle. Les théoriciens ont même osé suggérer que de nombreuses grandes civilisations de l'histoire, y compris les Mayas, les Nordiques, les Minoens et le vieil Empire égyptien, ont finalement été mises à genoux non pas par leurs ennemis mais par les effets des inondations, des famines, des tremblements de terre, tsunamis, et autres catastrophes [6].

En 21 Mai 2003, le tremblement de terre de Boumerdes qui a frappé la région centrale de l'Algérie, a entraîné un très grand nombre de pertes humaines (plus de 2 300 morts et 10 000 blessés) et des dommages très importants à l'environnement bâti (plus de 100 000 logements ou constructions se sont effondrés ou plus ou moins gravement endommagés)[7]. Ses conséquences

semblent presque inconcevables mais ce n'est pas près de battre des records, ni même d'être unique, dans le contexte historique (voir tableau I.1).

Alors que la gestion des catastrophes au cours des derniers milliers d'années s'est limitée à des actes uniques ou à des programmes traitant des risques individuels ; la gestion moderne des catastrophes, organise les efforts pour répondre à des scénarios dynamiques en impliquant plusieurs autorités, intérêts et acteurs pour assurer la sécurité publique [6].

Catastrophes	Année	Nombre de victimes
Séisme méditerranéen (Egypte et Syrie)	1201	1,100,000
Séisme au Shaanxi (Chine)	1556	830,000
Volcan Tambora (Indonésie)	1815	80,000
Épidémie de grippe	1917	20,000,000
Inondation du fleuve Yangtze (Chine)	1931	3,000,000
Séisme de Tangshan (Chine)	1976	655,000
Séisme et tsunami l'océan Indien	2004	250 000
Séisme Haïti	2010	280000

***Tableau I.1** : Certaines catastrophes notables à travers l'histoire[6]*

I.3 La gestion des catastrophes et des urgences

Au fil du temps et par itération, un processus reconnu et systémique de réponse aux catastrophes internationales a commencé à émerger. Des normes de réponse ont été élaborées par de multiples sources et un groupe reconnu de participants a été identifié, comme les institutions financières nationales et internationales, les organisations et les associations régionales, les organisations à but non lucratif et les donateurs locaux et régionaux et d'autres.

I.3.1 Terminologie

La gestion des catastrophes et des urgences est décrite en utilisant un certain nombre de termes. Nous consacrons ce paragraphe à la définition de ces termes qui vont être utilisés tout au long de ce chapitre.

- Une **urgence** est une déviation par rapport à un comportement prévu ou attendu ou à un ensemble d'événements qui met en danger ou affecte négativement les personnes, les biens ou l'environnement[8].
- Une **catastrophe** est un événement naturel ou causé par l'homme, elle se caractérise par l'étendue d'une urgence. Une urgence devient une catastrophe lorsqu'elle dépasse la capacité des ressources locales à la gérer. Les catastrophes entraînent souvent d'importants dommages, pertes ou destructions[8].
- Le **risque** est la probabilité selon laquelle il y aura des pertes en conséquence d'un événement défavorable, vu le danger et la vulnérabilité[9].
- Le **danger** fait généralement référence aux caractéristiques physiques qui peuvent provoquer une urgence. Par exemple, les failles sismiques, les volcans actifs, les zones inondables et les champs de broussailles très inflammables sont tous des dangers[8].
- Le **séisme** est un mouvement vibrant et tremblant de la surface de la terre en conséquence des mouvements des plaques le long d'un plan de faille ou en conséquence d'activités volcaniques[9].
- Le **système de gestion des urgences et catastrophes** est un processus systématique fondé sur les principes essentiels de gestion : la *planification*, *l'organisation* qui couvre la *coordination et le contrôle.* Il vise à réduire l'effet négatif ou les conséquences d'évènements indésirables. Qu'on ne peut toujours rien face aux catastrophes, mais on peut minimiser les effets défavorables[9].

I.3.2 Le cycle de gestion des catastrophes

La gestion complète des catastrophes est basée sur quatre phases distinctes (figure I.1) : atténuation, préparation, réponse et récupération. Bien qu'une gamme de terminologie soit souvent utilisée pour les décrire, une gestion efficace des catastrophes utilise chaque phase de la manière suivante[6] :

- **Atténuation :** Cela implique de réduire ou d'éliminer la probabilité ou les conséquences d'un danger, ou les deux. L'atténuation vise à traiter le danger de manière à ce qu'il affecte la société à un moindre degré.
- **Préparation :** Cela implique d'équiper les personnes qui peuvent être touchées par une catastrophe ou qui peuvent être en mesure d'aider ceux qui sont touchés avec les outils pour augmenter leurs chances de survie et minimiser leurs pertes financières et autres.
- **Réponse :** Implique de prendre des mesures pour réduire ou éliminer l'impact des catastrophes qui se sont produites ou se produisent actuellement, afin d'éviter de nouvelles souffrances, des pertes financières ou une combinaison des deux. Les secours, un terme couramment utilisé dans la gestion internationale des catastrophes, sont un élément de la réponse.
- **Récupération :** Implique le retour de la vie des victimes dans un état normal suite à l'impact des conséquences d'une catastrophe. La phase de récupération commence généralement après la fin de la réponse immédiate et peut persister pendant des mois ou des années par la suite.

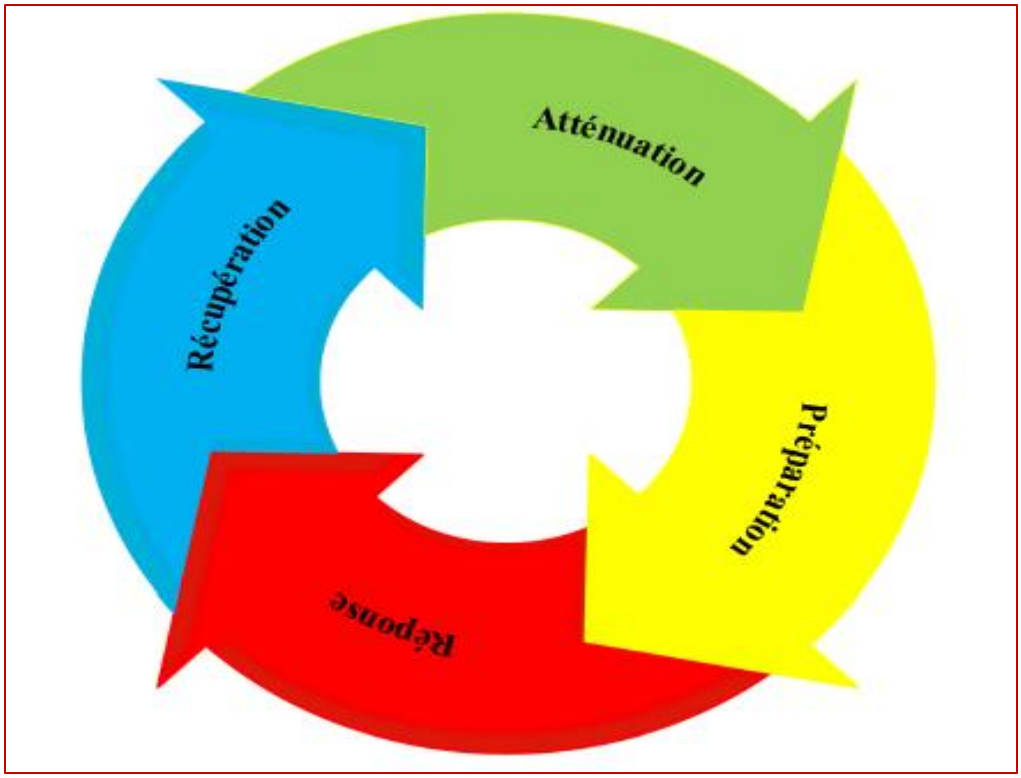


Figure I.1 : *Le cycle de gestion des catastrophes[6]*

La gestion des catastrophes est un processus cyclique ; même si une phase du cycle ne doit pas nécessairement s'achever pour laisser la place à une autre. Souvent, plusieurs phases ont lieu simultanément. La prise de décision au bon moment durant chaque phase entraîne une meilleure préparation, les meilleures alertes, une vulnérabilité réduite ou la prévention des catastrophes à venir.

I.3.3 Les composants des systèmes de gestion des urgences

Les systèmes et les outils dont disposent les gouvernements pour faire face aux risques de dangers dans leurs communautés sont relativement universels dans le monde. Bien que les organisations et les systèmes de gestion des urgences de chaque pays se soient développés indépendamment de diverses sources, un vaste partage institutionnel entre les pays a créé une normalisation globale des types d'organisations de gestion des urgences, notamment dans le domaine de la première intervention. De plus, la mondialisation a facilité la normalisation des pratiques, des protocoles et des équipements utilisés par les organisations de gestion des urgences.

La figure I.2 illustre un flux d'informations et d'actions déclenché par une catastrophe. Premièrement, les sinistrés appellent immédiatement les centres d'appels pour informer de la situation d'urgence ; certains sinistrés peuvent publier la situation d'urgence sur les réseaux sociaux. La situation de catastrophe peut également être détectée automatiquement par des dispositifs de surveillance sur site, tels que des capteurs d'alarme séisme. Ensuite, dès que l'information sur la situation est transmise au centre de commandement unifié, le plan de sauvetage et la décision sont pris immédiatement. En fonction de la gravité de catastrophe et de la capacité en ressources de chaque département (tels que le service de police, l'armée et autres) ces derniers procèdent enfin à l'exécution de leurs tâches pour atténuer la situation.

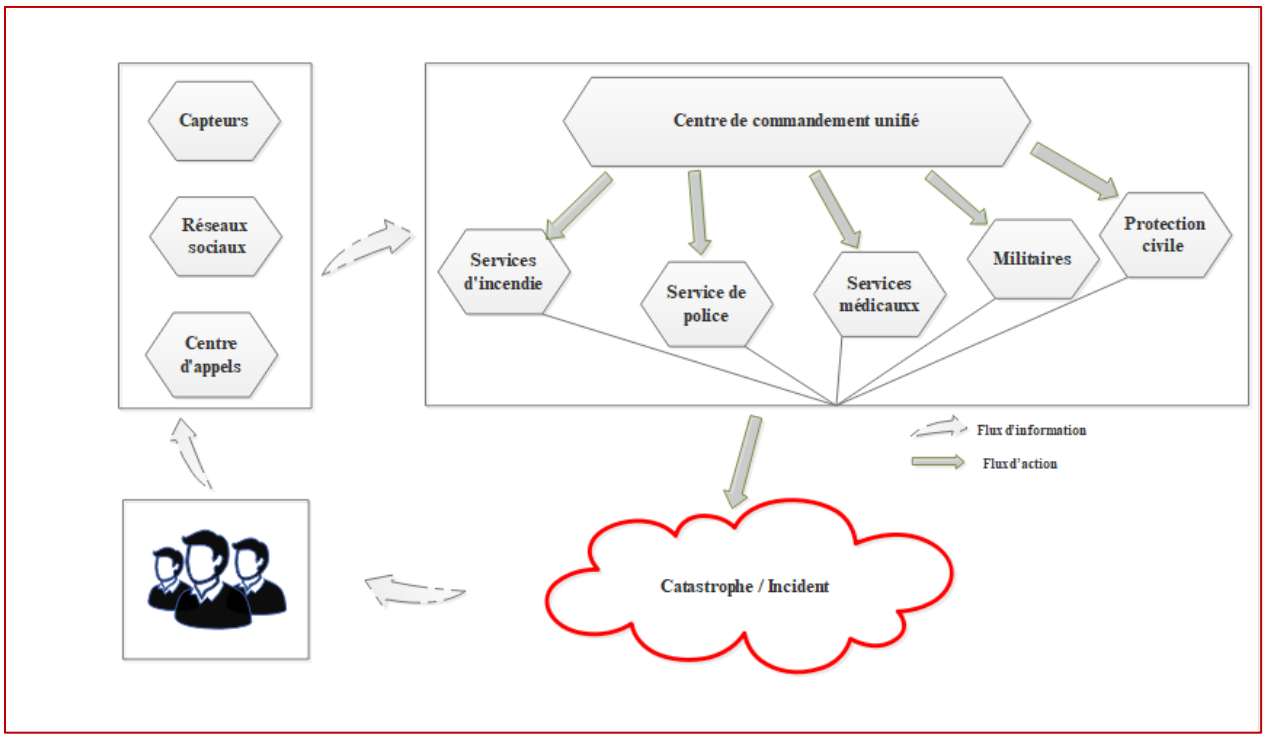


Figure I.2 : *Flux d'information et d'action en cas de catastrophe/incendie [10]*

Dans ce qui suit, nous définissons les différentes composantes des systèmes de gestion des urgences [6], [10] qui existent dans la plupart des pays du monde (Services d'incendie, Service de police, Protection civile, Services médicaux d'urgence, Militaires). Bien que certains facteurs, notamment la richesse, l'expertise technique, le type de gouvernement et le profil de risque spécifique, contribuent à définir la façon dont chaque agence est organisée et équipée, leurs missions fondamentales sont presque identiques.

- **Services d'incendie :**

Les services d'incendie également appelés « pompiers » sont la structure de gestion des urgences la plus courante dans les communautés locales du monde entier. Cela est parfaitement logique, car les incendies sont les dangers les plus courants auxquels les communautés sont confrontées quotidiennement.

Les services d'incendie peuvent être organisés au niveau local, régional ou national. La structure d'un service d'incendie dépend souvent de la rémunération du personnel des services

d'incendie et du type de gouvernement existant. Les trois types de niveaux organisationnels des services d'incendie et des exemples de pays employant chaque type sont fournis ci-dessous :

- ✓ Structure organisationnelle locale (Canada, Allemagne, États-Unis)
- ✓ Structure organisationnelle régionale (Algérie, Australie, Royaume-Uni)
- ✓ Structure organisationnelle nationale (Espagne, France, Hong Kong)

- **Service de police :**

Les services de police également appelés « forces de l'ordre » sont des entités gérées par le gouvernement chargé de maintenir la loi et l'ordre au sein de la communauté. La police et d'autres services chargés de l'application des lois font souvent partie de la fonction de gestion des urgences au niveau local. Bien que la lutte contre le crime soit la responsabilité première de la police, la responsabilité de gestion des urgences peut inclure :

- ✓ Sécurité des scènes de catastrophe.
- ✓ Emission d'avertissement.
- ✓ Sécurité dans les installations critiques.
- ✓ Recherche et sauvetage.
- ✓ Contrôle du trafic.

- **Protection civile :**

Le domaine de la gestion des urgences était pratiquement inexistant jusqu'aux jours de la protection civile des années 50, lorsque de nombreux gouvernements de pays industrialisés ont commencé à préparer officiellement la guerre nucléaire. Ces systèmes, souvent appelés protection civile, ont aidé à préparer les communautés en construisant des abris et en formant des premiers intervenants. Au fil du temps, les bureaux de la protection civile ont commencé à faire face à d'autres risques catastrophiques. Quelques agences ont même commencé à assumer des fonctions de coordination des interventions et du relèvement. Aujourd'hui, la plupart des pays maintiennent une certaine forme de bureau de protection civile ou de gestion des urgences au niveau du gouvernement central, qui s'occupe de l'atténuation et de la préparation aux catastrophes majeures.

- **Services médicaux d'urgence :**

Les services médicaux d'urgence, souvent appelés « EMS » ou « service d'ambulance », sont des soins médicaux spécialisés dispensés sur les lieux de la catastrophe ou de l'urgence ou les techniciens médicaux d'urgence sont des professionnels hautement qualifiés qui offrent une assistance médicale dépassant largement les premiers soins de base. Bien que de nombreux policiers et pompiers soient formés pour fournir les premiers soins et l'assistance médicale, les organisations EMS sont généralement formées et équipées pour aller au-delà des bases, et peuvent même être certifiées pour effectuer des procédures invasives ou pour administrer une gamme de médicaments.

- **Militaires :**

Presque tous les pays incluent les militaires dans leur processus global de planification et réponse de gestion des catastrophes. Ils ont des budgets sécurisés, un équipement spécialisé, une main-d'œuvre formée et rapidement déployable, et une structure hiérarchique hautement organisée. Le lien entre l'armée et la gestion des urgences va au-delà de la simple coïncidence ou de la commodité pour de nombreux pays de nombreuses structures modernes de gestion des urgences qui existent aujourd'hui ont leurs racines ou sont toujours enracinées dans la protection civile. La gestion des urgences est née d'un besoin défensif, et l'armé a été impliquée tout au long de ce processus évolutif. En tant que tel, leur statut de ressource précieuse est largement reconnu et souvent considéré comme l'ultime dernier recours.

I.3.4 Étude des systèmes de gestion des catastrophes existants

La gestion des catastrophes à grande échelle implique une diversité d'organisations et de produits.

Cette section a pour but d'étudier quelques systèmes de gestion des catastrophes existants, ainsi que leurs architectures.

I.3.4.1 Sahana

Sahana [11] , une application gratuite et open source, fournit une solution complète pour la gestion de l'information dans la récupération et la réhabilitation des opérations de secours. Une architecture en couches de Sahana est représentée sur la figure I.3. Cette dernière se compose de quatre couches : le cadre d'application Sahana se trouve au cœur, entouré d'un ensemble de bibliothèques et d'interfaces de programmation d'applications (API) telles que les API de localisation, GIS et de création de rapports, les modules de base sont ensuite construits au-dessus du cadre d'application Sahana et les API, avec les modules périphériques optionnels situés à la couche la plus externe, et sont installés à la demande des utilisateurs. En général, les modules de couche externe peuvent utiliser la fonctionnalité des modules internes.

Les fonctionnalités suivantes sont fournies dans le cadre de Sahana :

- ✓ Une architecture flexible et modulaire qui garantit que les tâches et les événements à l'échelle du système peuvent être facilement gérés et synchronisés.
- ✓ Sécurité au niveau modulaire et prise en charge de l'internationalisation et de la localisation de contenu.
- ✓ Un moyen facile d'installer et de configurer le Sahana et sa base de données.
- ✓ Prise en charge de la détection automatique de nouveaux modules, ainsi que de l'installation et de l'activation et de la configuration dynamiques de modules tiers grâce à son architecture flexible.
- ✓ Capacité de travailler avec une base de données commune pour accéder à ses données de schéma et celle de catastrophe.
- ✓ La fonctionnalité d'administration pour les autres modules du système.

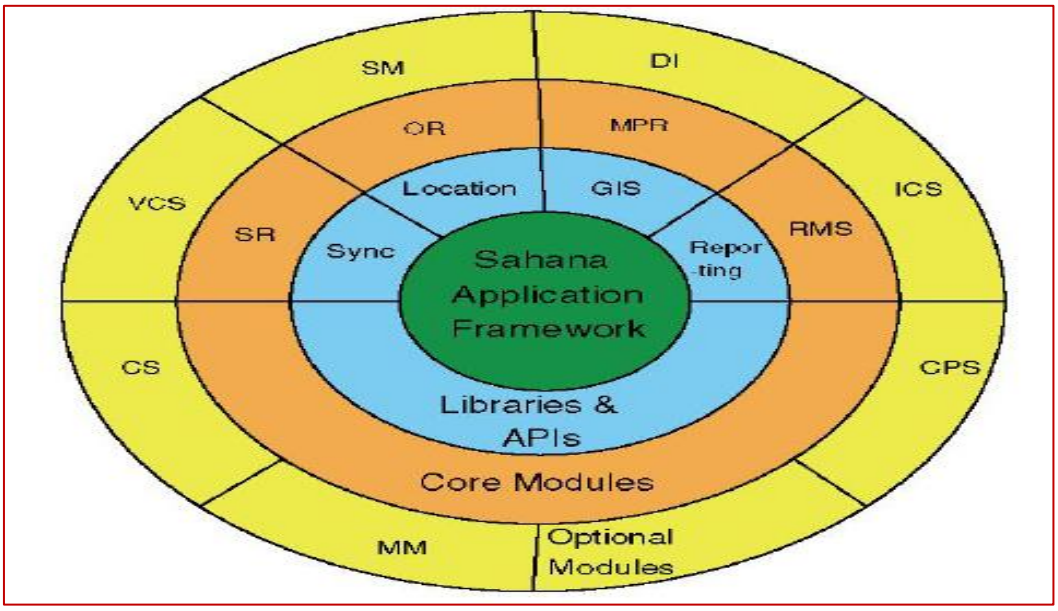


Figure I.3 : *Vue d'ensemble de l'architecture Sahana [11]*

L'architecture basée sur les composants d'un système typique construit sur le framework Sahana est illustrée à la figure I.4. Un tel système est composé d'un système d'exploitation, au-dessus duquel une base de données et un serveur Web peuvent être déployés pour prendre en charge le cadre Sahana. Ce système peut tirer parti d'autres bibliothèques, telles que XAJAX, NuSoap et MapServer, pour faciliter ses opérations et s'attaquer à des tâches plus difficiles dans la gestion des catastrophes.

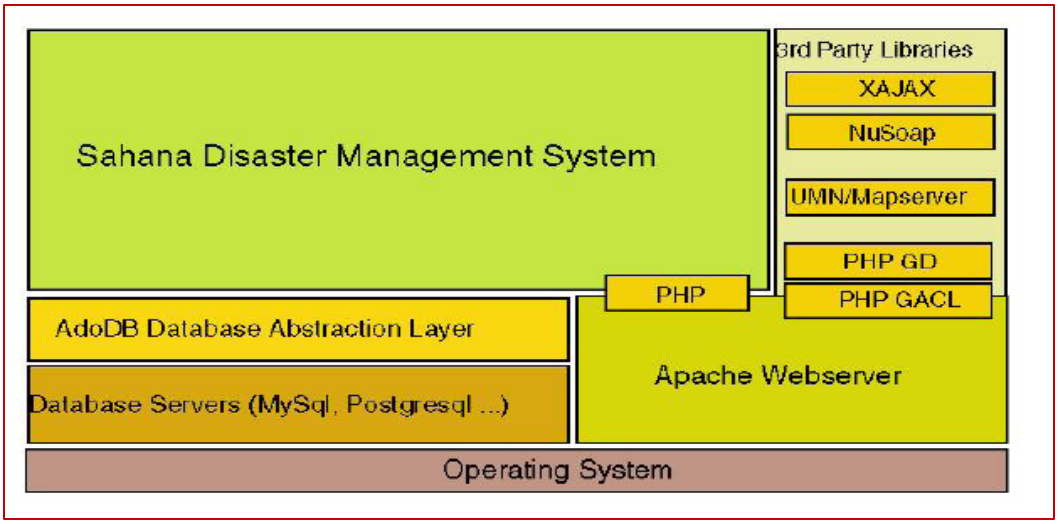


Figure I.4 : *Architecture des composants [11]*

I.3.4.2 WebEOC

Un système de gestion des crises et des catastrophes appelé WebEOC [10] a été développé pour gérer les événements et les catastrophes à grande échelle, soutenir le partage d'informations sur la sécurité publique et fournir une connaissance de la situation en temps réel. Le système est géré par la Division de la sécurité intérieure et de la gestion des urgences ainsi que par l'État du New Hampshire et le Département de la sécurité.

L'un des principaux objectifs de WebEOC est de :

- ✓ Fournir aux commandants des incidents, aux chefs de communauté et au personnel de niveau de commandement une image opérationnelle commune des opérations de sécurité publique, des informations sensibles et des perturbations de l'infrastructure, sur laquelle des décisions éclairées et efficaces peuvent être prises concernant les efforts de rétablissement et d'atténuation.
- ✓ Utiliser comme une passerelle pour partager des informations entre les centres des opérations d'urgence de l'État et les entités de sécurité.

L'architecture système de WebEOC est illustrée à la figure I.5, ce système peut être divisé en trois niveaux par les limites Internet. Le niveau le plus à gauche est la couche utilisateur, où les utilisateurs peuvent accéder à WebEOC par navigateur ou API de service. Tous logiques métiers sont implémentés sur le serveur Web au niveau intermédiaire. Au niveau le plus à droite, les informations sur les catastrophes et les données GIS sont stockées dans la base de données. Pour éviter la perte de données due à une catastrophe, le serveur Web et le serveur de base de données sont sauvegardés avec des serveurs de réplication.

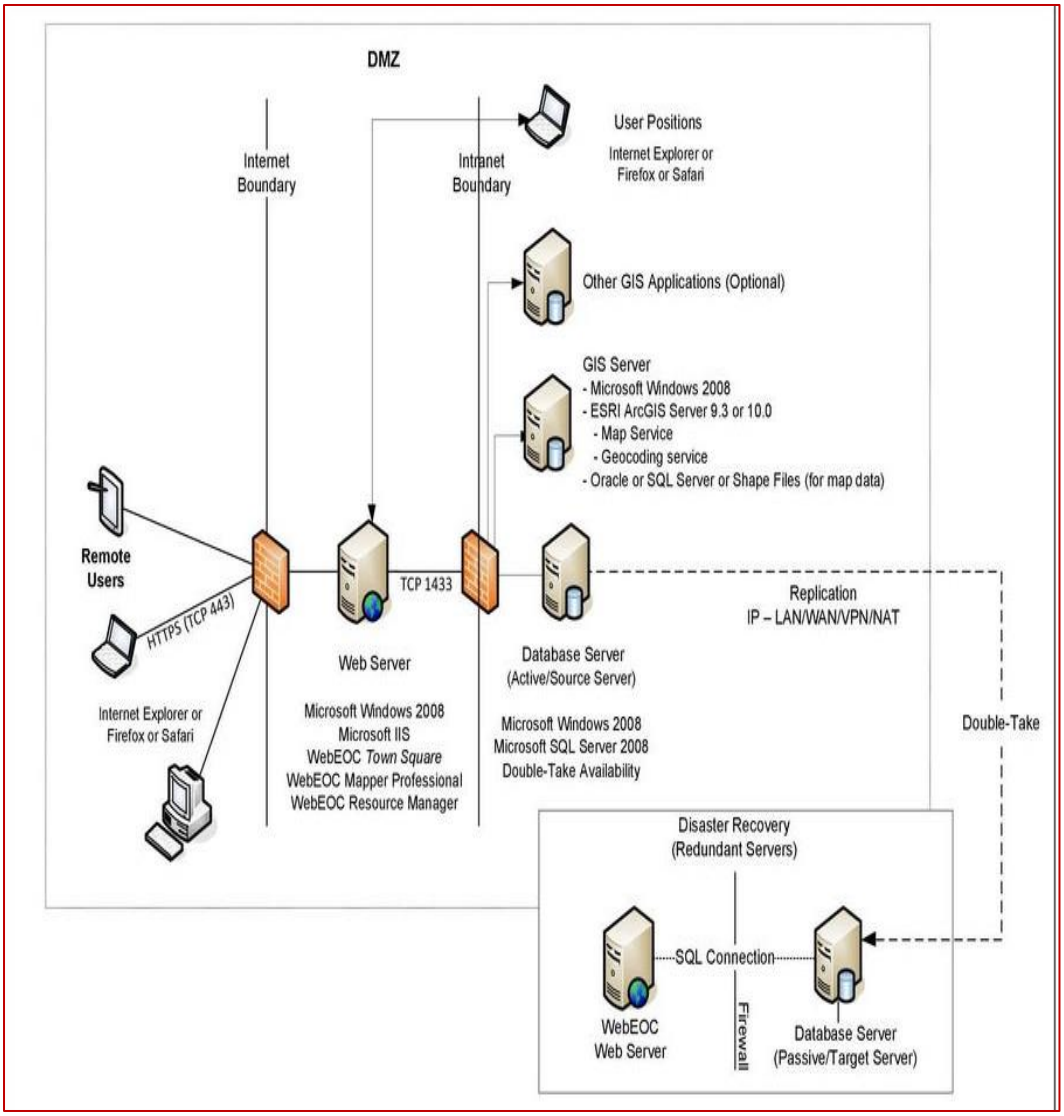


Figure I.5: *L'architecture système de WebEOC [10]*

I.3.4.3 ADSB

Le système ADSB (All-Hazard Disaster Situation Browser)[12], qui fonctionne sur des appareils mobiles afin de partager efficacement les informations sur les catastrophes (figure I.6), prend en charge les fonctionnalités suivantes :

- ✓ Fournit aux utilisateurs une liste personnalisée des rapports qui sont les plus importants par rapport aux utilisateurs.

- ✓ Présente une vue complète de chaque rapport individuel, dans laquelle toutes les informations connexes sont affichées.
- ✓ Permet aux utilisateurs d'obtenir des informations résumées par des recherches par mots clés.
- ✓ Fournit un partage instantané des informations sur les catastrophes grâce à la gestion de la communauté, qui offre aux utilisateurs un canal d'échange informations liées aux catastrophes et suivre l'évolution de la situation d'un événement spécifique.

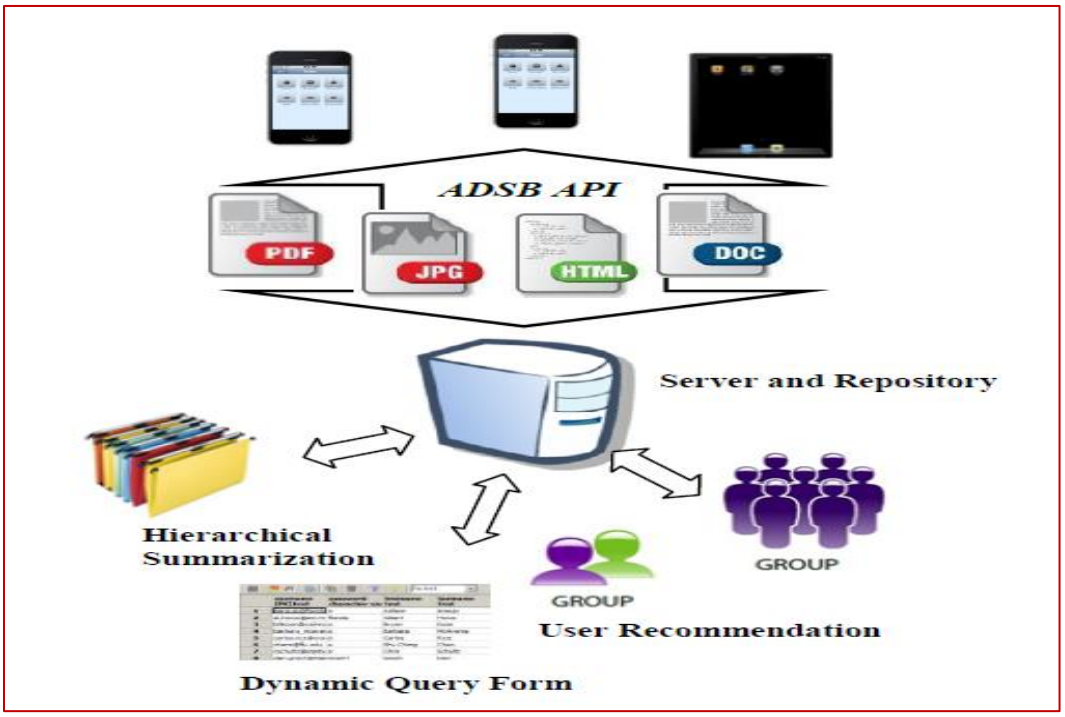


Figure I.6 : *L'architecture du système ADSB [12]*

I.3.4.4 BCIN

Les chercheurs de la Florida International Université ont travaillé en collaboration avec le gouvernement et des partenaires de l'industrie pour développer un service Web BCIN (Business Continuity Information Network) disponible toute l'année grâce auquel les bureaux de gestion des urgences, les entreprises locales et les organisations peuvent partager des informations essentielles et soutenir les efforts pendant tous les cycles de gestion des catastrophes. Le BCIN [13] est un réseau communautaire interentreprises qui permet aux membres de suivre leurs ressources clés et de localiser les fournitures, l'équipement et les services de reprise après sinistre requis. En particulier, le système facilite les organisations professionnelles telles que les chambres de

commerce pour aider leurs membres dans les secours en cas de catastrophe et accélère les agences gouvernementales pour évaluer les dommages afin de prioriser les efforts de sauvetage. Le site Web du projet Figure I.7 est un instantané du prototype actuel, qui affiche les informations recueillies auprès de diverses sources de manière intuitive et conviviale. Le panneau supérieur est le tableau de bord de situation, dans lequel chaque ligne représente une juridiction et chaque colonne représente une installation. Un symbole de couleur représente le statut d'une installation dans une juridiction. Par exemple, un cycle vert (resp., rouge) indique que l'installation est ouverte (resp., fermée). Les panneaux en bas à gauche offrent aux utilisateurs des vues plus riches (telles que des images, des images, des vidéos) des menaces et des impacts actuels, tandis que le panneau en bas à droite affiche une liste de rapports récents soumis par des utilisateurs autorisés et fiables. Plusieurs options de filtrage sont fournies qui permettent aux utilisateurs d'extraire rapidement des informations précieuses du système.

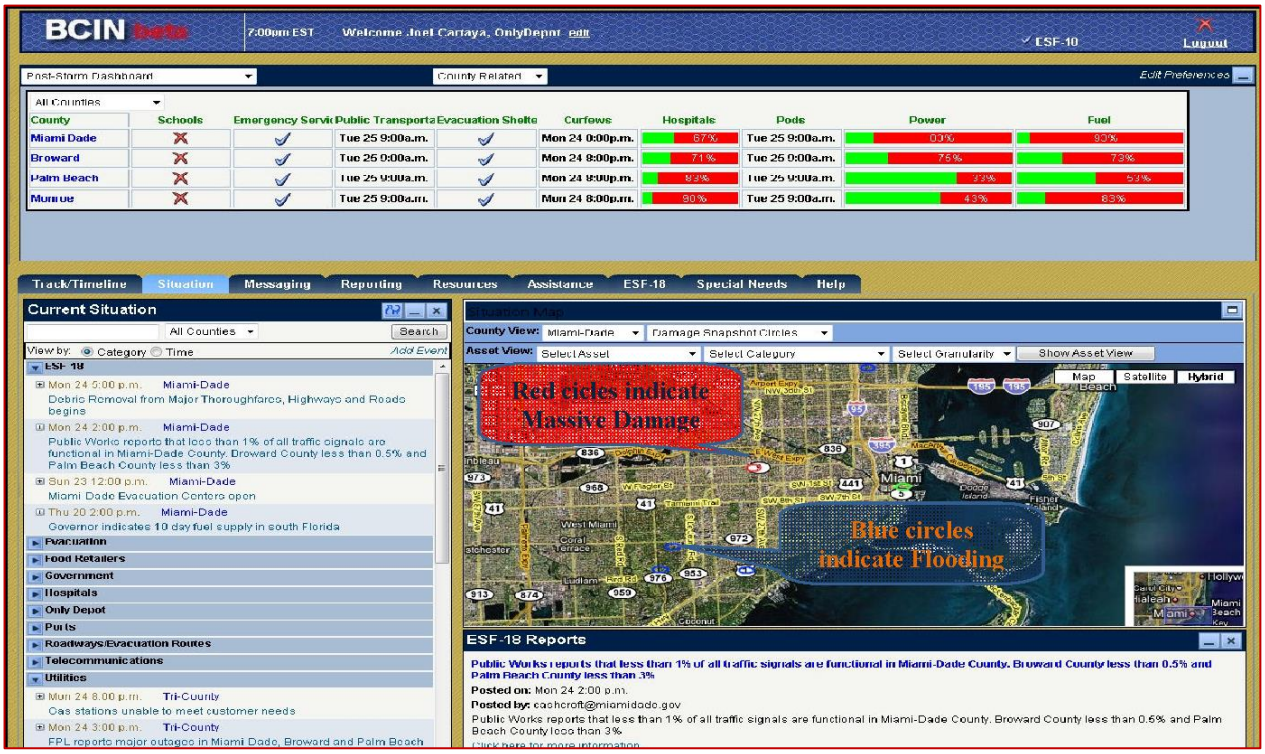


Figure I.7 *: L'interface de BCIN [13]*

I.3.4.5 Comparaison

Les systèmes de gestion des catastrophes sont passés par plusieurs étapes de la dernière décennie. Au cours de la première étape, un système agit uniquement comme un système de gestion des informations traditionnel qui stocke les informations sur les catastrophes dans un schéma spécifique pour prendre en charge un traitement efficace des requêtes. Dans la deuxième étape, une quantité croissante d'informations sur les catastrophes provenant de sources hétérogènes nécessite des techniques plus avancées de collecte, de gestion, d'analyse et de découverte d'informations. Ces techniques avancées découlent souvent de résultats de recherche de pointe dans des domaines tels que l'extraction d'informations, le filtrage d'informations, la récupération d'informations, l'exploration de données et les plates-formes informatiques distribuées. Dans la troisième étape, avec l'essor des médias sociaux et la prévalence des appareils mobiles, les gens sont capables de partager des informations sur les catastrophes avec peu de contraintes spatiales ou temporelles. En conséquence, les systèmes de gestion des catastrophes sont requis pour fournir une solution complète qui intègre des techniques d'information, médias sociaux et appareils mobiles[6], [10].

Le tableau I.2 résume les systèmes de gestion des catastrophes examinés au-dessus. Comme constat, les systèmes WebEOC et BCIN gèrent complètement les catastrophes en se basant sur les quatre phases de cycle de vie contrairement au système Sahana qui traite deux phases seulement (préparation et réponse) ou au système ADSB qui ne traite pas la phase d’atténuation. De plus, certains systèmes sont gratuits, voire open source (Sahana), et d’autres commerciales. Enfin, dire quel est le meilleur système est quasiment impossible car chaque système possède des avantages et des inconvénients selon son domaine d’application.

Systèmes	Phases de cycle de vie	Type de solution	Avantages	Inconvénients
Sahana	-Préparation -Réponse	Gratuit Open source	+Fournir un ensemble d'applications modulaires de gestion des catastrophes sur le Web. +Sélection et stockage de la hiérarchie des emplacements. +Protéger les données des victimes et réduire les risques d'abus de données. +Fournir une solution gratuite de bout en bout accessible à tous.	-Non prise de variété d'environnements où l'infrastructure de communication de base peut être détruite. -Manque des réponses en temps réel pour certains modules tels que la messagerie mobile et le contrôle de situation.
WebEOC	-Préparation -Réponse -Récupération -Atténuation	Solution commerciale	+Gestion des événements et des catastrophes à grande échelle. +Soutenir le partage d'informations sur la sécurité publique.	-La version propriétaire du logiciel pose des défis dans certains cas, elle ne peut pas communiquer avec d'autres agences comme cela serait nécessaire lors d'un événement à grande échelle.
ADSB	-Préparation -Réponse -Récupération	Gratuit	+Partager les informations de manière instantanée sur les catastrophes avec d'autres personnes par le biais d'appareils mobiles. + Fournir des Rapports personnalisés.	- Lecture et assimilation des informations situationnelles prend beaucoup de temps avec une forte probabilité d'exposition à des informations redondantes.

BCIN	-Préparation -Réponse -Récupération -Atténuation	Gratuit	+Fournir un service Web de partage et d'échange d'informations à utiliser pendant et après une période de récupération après une catastrophe. + Créer une vue résumée des documents. +Identifier les ressources de préparation et de reprise après catastrophes. +Extraire les informations à partir de données textuelles.	-Absence d'incorporation et d'utilisation des éléments de données multimédias tels que des vidéos, des audios.

***Tableau I.2**: Résumé des systèmes de gestion des catastrophes et urgences.*

I.4 Les réseaux de communications des systèmes de gestion des urgences et catastrophes

Les réseaux de communication sont un outil essentiel pour les services d'urgence. De nos jours, ils sont utilisés pour la coordination, la collecte d'informations, l'alerte de la population et plus encore, et cela via les appareils mobiles, les téléphones et les assistants numériques portables (PDA) qui sont devenus les outils que chacun a son accès au quotidien. Presque tout le monde détient une telle sorte de dispositif portable en raison de laquelle l'application de bureau est allée trop loin derrière.

Une étude au Bangladesh a établi que les technologies sans fil mobiles peuvent être utilisées dans la gestion des informations sur les catastrophes. Les résultats ont montré que la technologie mobile peut être utilisé pour diffuser des alertes et des annonces post-catastrophe, pour recevoir des informations sur les besoins de secours, et d'échanger des informations sur danger pour la santé [14]. Aussi, dans la gestion des catastrophes, la situation géographique des personnes dans le besoin est importante. En utilisant leurs téléphones portables, leurs emplacements peuvent soit être déterminé en utilisant le système de réseau mobile ou grâce à l'utilisation d'un positionnement global intégré dans leur portable GPS. Pour cette raison, les réseaux mobiles sont une alternative intéressante, non seulement pour les secours en cas de catastrophe, mais aussi pour le fonctionnement quotidien des services d'urgence. Pour cela, dans notre travail, nous nous intéressons aux réseaux mobiles comme moyen de communication entre les différents composants (sinistré, centre de commandement unifié) du système de gestion des urgences et des catastrophes.

I.4.1 Les réseaux mobiles

Les réseaux mobiles sont des réseaux qui utilisent des ondes radio pour connecter des appareils, sans avoir besoin d'utiliser des câbles, permet ces réseaux nous trouvons les réseaux mobiles Ad Hoc, les réseaux Ad Hoc Véhiculaires, les réseaux à tolérance de retard et les réseaux de capteurs sans fil, qui sont décrits dans la section suivante.

I.4.1.1 MANET

Un réseau mobile Ad Hoc (Mobile Ad Hoc Network, MANET) est une sorte de réseau ad hoc sans fil. C'est un réseau constitué d’un ensemble d’unités mobiles connectés par des liaisons sans fil sans point d'accès et auto organisée. Chaque appareil mobile dans le réseau est autonome.

Les appareils mobiles sont libres de se déplacer au hasard et de s'organiser arbitrairement. En d'autres termes, le réseau ad hoc ne repose sur aucune infrastructure fixe. La communication dans MANET s'effectue en utilisant des chemins à sauts multiples. Les nœuds du MANET partagent le support sans fil et la topologie du réseau change de façon irrégulière et dynamiquement. Dans MANET, la rupture de la liaison de communication est très fréquente, car les nœuds sont libres de se déplacer n'importe où. La densité des nœuds et le nombre de nœuds dépendent des applications dans lesquelles MANET est utilisé [15].

Les caractéristiques de MANET sont les suivantes [16], [17]:

- **Topologie dynamique :** les raisons principales des changements de topologie dans ces réseaux sont liées à des facteurs non contrôlables tels que la mobilité des nœuds, les interférences et le bruit, à des facteurs contrôlables tels que la puissance de transmission et la direction de l'antenne et au mécanisme de mise en veille des nœuds pour la préservation de l'énergie. Ainsi, la topologie du réseau peut changer fréquemment d'une manière non prévisible.
- **Contrainte d'énergie :** les nœuds dans un réseau ad hoc sont alimentés typiquement par des batteries dont la capacité en puissance est souvent limitée. Par conséquent, une batterie ne peut satisfaire les demandes d'énergie d'un nœud pour un fonctionnement normal durant une période de temps raisonnable.
- **Capacité des liens limités et variables** : celle-ci est limitée, par rapport à la capacité des réseaux filaires, et peuvent varier au cours du temps pour au moins deux raisons principales : le changement des conditions de propagation et variation des distances entre les nœuds.
- **Sécurité limitée** : les réseaux ad hoc mobiles sont plus vulnérables par rapport aux autres réseaux filaires et cellulaires. Cette vulnérabilité est due essentiellement à la nature du médium de propagation sans fil qui rend possibles certaines attaques malicieuses allant de l'écoute clandestine passive aux interférences actives.
- **Liens avec perte :** les nœuds du MANET sont de nature mobile, de sorte que tout nœud peut sortir de la portée du réseau à tout moment. Cela entraîne fréquemment des pertes de liens entre les nœuds.
- **Évolutivité du réseau :** les nœuds du MANET peuvent accéder au réseau à tout moment. En d'autres termes, le réseau peut grandir à n'importe quelle mesure.

- **Contraintes de bande passante** : les nœuds du MANET utilisent des liaisons sans fil pour communiquer. Ces liens sont à faible bande passante par rapport aux réseaux câblés.
- **Périphérique hétérogène :** Les périphériques ou nœuds dans MANET sont de nature hétérogène. Les nœuds mobiles peuvent être des téléphones, des ordinateurs portables ou des tablettes, etc. avec différentes configurations.
- **Auto-organisé :** MANET peut être déployé sans aucun point central ou point d'accès. Les nœuds du MANET sont intelligents pour gérer toutes les fonctions du réseau, y compris leur propre transmission de données, et sont donc auto-organisés.

Les principaux domaines d'applications de MANET sont[16]:

- **Applications de collaborations :** Les utilisateurs professionnels ont besoin d'applications particulières lors d'échanges entre collaborateurs. Au cours de réunions ou de conférences pour s'échanger des informations, ou faire une vidéo conférence entre bureaux voisins. Les réseaux ad hoc sont bien concernés à ces besoins.
- **Urgences :** Lors de catastrophes d'origine naturelle (comme les tremblements de terre, les tsunamis, les feux de forêt ou d'habitations…) ou non, les infrastructures préexistantes peuvent ne pas être opérationnels compliquant l'importance plus les besoins de communications des moyens de secours. Les réseaux sans fil, par leur compacité et leur rapidité de déploiement, permettre aux différentes équipes de secours d'obtenir rapidement des liaisons et d'échanger des informations.
- **Militaires :** Lors d'interventions en milieu hostile, il peut être difficile ou trop encombrant utilisé un réseau à infrastructure. Les réseaux sans fil sont parfaitement bien adaptés à ce type d'environnement où les déplacements restent peu rapides et peu soutenus.
- **Extension des réseaux :** Un problème majeur des réseaux avec infrastructure est la couverture limitée, pour cela les réseaux ad hoc sont sollicités afin d'étendre la couverture des réseaux cellulaire par exemple.

I.4.1.2 VANET

Un réseau Ad Hoc véhiculaires (Vehicule Ad Hoc Network, VANET) est une sorte de réseau qui a vu le jour avec l'idée de créer un réseau de véhicules dans le même but et la même situation d'utilisation. Les VANET sont considérés comme l'un des réseaux les plus fiables utilisés pour connecter les véhicules dans un environnement tel que les autoroutes et les zones urbaines.

L'objectif principal d'un VANET est d'établir une communication réseau entre un certain nombre de véhicules indépendamment de tout contrôleur ou station de base [18].

Les caractéristiques de MANET sont les suivantes[19] :

- **Topologie dynamique :** La topologie de l'environnement VANET évolue en permanence vers la grande mobilité des véhicules. La connexion entre deux véhicules circulant dans des directions opposées à une vitesse moyenne reste pour une courte durée. Ce temps de connexion est encore plus court dans un environnement où les vitesses des véhicules sont plus élevées.
- **Modèles de mobilité prévisibles :** des itinéraires prédéfinis sont disponibles dans l'environnement VANET à travers lequel un véhicule se déplace. Ainsi, les concepteurs de réseaux peuvent prédire les modèles de mobilité dans le réseau.
- **Tailles de réseau illimitées :** les VANET peuvent varier en taille d'une ville ou de plusieurs villes à un ou plusieurs pays.
- **Protection des nœuds :** les nœuds VANET sont physiquement mieux protégés que les autres et peuvent réduire l'effet des attaques d'infrastructure.
- **Faible consommation d'énergie :** les VANET n'ont aucun problème avec la consommation d'énergie, ils utilisent très peu d'énergie.

Les domaines d'applications de VANET sont nombreux, et nous pouvons citer les applications suivantes[19]:

- **Trafic en temps réel :** les données peuvent être stockées dans une unité routière (RSU) afin de pouvoir être utilisées à tout moment.
- **Transfert de messages coopératifs :** les véhicules lents / arrêtés partagent des messages et coopèrent entre eux.
- **Avertissement de collision coopérative** : VANET permet d'avertir les conducteurs de tout danger à venir, afin qu'ils puissent corriger leur itinéraire.
- **Amélioration de la vision :** par mauvais temps, VANET guide les conducteurs avec des informations claires sur les véhicules et les obstacles.

I.4.1.3 DTN

Le réseau à tolérance de retard ou réseaux tolérants aux perturbations (Delay Tolerant Network, DTN) est une technique de configuration de l'environnement réseau dans le but de localiser les problèmes techniques dans divers réseaux. Ces problèmes techniques peuvent

entraîner un manque de connexion réseau permanente. Des exemples de tels réseaux sont ceux fonctionnant dans des réseaux mobiles ou des environnements terrestres extrêmes[20], [21].

Les réseaux à tolérance de retard sont des réseaux mobiles qui peuvent ne jamais avoir un chemin contemporain de bout en bout. Les caractéristiques de DTN sont différentes de celles des réseaux ad hoc traditionnels. Les protocoles de routage de DTN suivent le mécanisme de store-carry-forward [1]pour minimiser la probabilité de perte de paquets, tolérer les retards et améliorer les performances de livraison en termes de taux de livraison et de latence de livraison[22].

Les caractéristiques des réseaux à tolérance de retard sont les suivantes[23] :

- **Connexion intermittente :** le réseau tolérant aux retards fait face à des déconnexions fréquentes en raison de la mobilité dans le réseau. L'état de la connexion et la topologie ne cessent de changer, c'est pourquoi il n'existe aucune garantie d'atteindre le chemin de communication de bout en bout.
- **Retard élevé :** la communication directe de bout en bout ne se produit pas dans les réseaux tolérants au retard. Le retard de bout en bout peut être calculé en additionnant le retard total sur l'itinéraire causé par chaque saut. Le délai comprend le temps d'attente, de mise en file d'attente et de transmission. Le retard dépend de la période de temps pendant laquelle les connexions sont inaccessibles.
- **Topologie dynamique :** la topologie continue de changer avec le mouvement des nœuds d'un emplacement à un autre, ce qui entraîne la partition réseau et les déconnexions. Les réseaux tolérants aux retards traitent ce réseau partitionné et déconnecté afin de délivrer le message avec succès.
- **Interconnexions hétérogènes :** le DTN est un réseau de superposition pour transmettre le message asynchrone. La couche bundle permet aux réseaux tolérants au retard de fonctionner sur des réseaux hétérogènes.

[1] Le mécanisme store-carry-forward est comme un système de messagerie électronique. Le long du trajet entre le nœud source et la destination, le nœud intermédiaire conserve les paquets en stockage pendant un certain temps jusqu'à ce que le nœud suivant devienne disponible.

- **Transmission fiable :** les réseaux tolérants au retard utilisent l'approche de stockage différé pour transmettre le message vers la destination. Il réduit les retransmissions et augmente la probabilité de livraison réussie d'un message à destination.

Nous pouvons citer les applications suivantes[23] :

- **Application de réseau en haute mer** : Le réseau à impact profond (Deep Impact Network, DINET) est une application de DTN dans la mise en réseau en haute mer qui est testée par la NASA[2]. Une autre application en haute mer du DTN comprend le réseau d'opérations robotisées de bout en bout (METERON[3]). Il se concentre sur la simulation de scénarios spécifiques comme la télécommande immersive pour le robot en orbite par l'astronaute autour de l'objet cible (comme la Lune et Mars).
- **Suivi de la faune :** Le DTN est utilisé pour surveiller la faune. Le « zebranet » est un système de communication très populaire et efficace pour les réseaux tolérants aux retards. Il est utilisé pour garder une trace des activités liées au zèbre. Un autre réseau de communication comme zebranet est « SWIM » qui surveille les baleines dans la mer en utilisant la communication DTN sous-marine.
- **Réseau de communication villageois** : la communication dans les villages éloignés est peu pratique et coûteuse en raison de la non-disponibilité des infrastructures fixes. À ces endroits, le DTN peut desservir une communication à faible coût. Le « Darknet » est un réseau de communication DTN largement utilisé pour les villages.
- **Application de réseaux sous-marins ou acoustiques** : Les réseaux sous-marins sont généralement construits par des capteurs océaniques à liaison acoustique, des véhicules sous-marins autonomes et des stations de surface qui utilisent les liaisons avec le point de contrôle à terre. Ces réseaux sont en pleine expansion en raison des avantages de la prévention des catastrophes, de la robotique sous-marine, de la surveillance tactique océanique, du portail

[2] L'Administration Nationale de l'aéronautique et de l'espace (National Aeronautics and Space Administration NASA), est l'agence gouvernementale responsable de la majeure partie du programme spatial civil des Etats-Unis.

[3] METERON (Multi-Purpose End-To-End Robotic Operation Network) est une suite d'expériences portant sur la validation des technologies nécessaires au fonctionnement d'actifs robotiques à la surface de la Lune ou de Mars à partir d'une station orbitale lunaire / martienne.

portuaire, de la surveillance des gazoducs et des oléoducs, du moniteur de pollution sous-marine, etc. d'une sorte de réseau de communication sous-marine. Le DTN est le réseau de communication bien adapté à la mise en œuvre de tels réseaux.

I.4.1.4 WSN

Un réseau de capteurs sans fil (Wireless Sensor Network, WSN) est le résultat collaboratif de centaines ou de milliers de nœuds de capteurs. Chaque nœud de capteur contient quatre parties essentielles, telles qu'une unité de détection, une unité de traitement, une unité radio et une unité d'alimentation. Ensemble, les unités peuvent tenir dans un espace aussi petit qu'une boîte d'allumettes ou même un module plus petit. Comme les nœuds de capteur ont des capacités de détection et de calcul limitées, ils ne peuvent se déplacer que sur de courtes distances. Ces nœuds s'étalent et s'organisent pour accomplir une tâche commune[24].

Les WSN sont les réseaux qui sont répartis dans l'espace sur la plage et rassemblent des informations du monde physique. Ils sont utilisés pour observer les facteurs environnementaux tels que la pression, la température, l'humidité, etc., et envoyer ces données à l'évier ou au nœud de destination[25].

Les caractéristiques de WSN sont les suivantes[26]:

- **Déploiement, topologie et couverture :** selon l'environnement opérationnel, les nœuds constitutifs d'un réseau de capteurs peuvent être déployés de manière planifiée (choix de positions spécifiques pour chaque nœud) ou de façon aléatoire. Le déploiement peut être un processus itératif, c'est-à-dire que des capteurs peuvent être ajoutés périodiquement dans l'environnement ou peuvent être une activité ponctuelle. Le déploiement affecte des paramètres importants tels que la densité des nœuds, la couverture, la résolution de détection, la fiabilité, l'allocation des tâches et les communications.
- **Ressources limitées :** Les réseaux de capteurs traitent avec une bande passante, un traitement et une énergie limités.
- **Communication et routage :** parce que les réseaux de capteurs traitent avec une bande passante, un traitement et une énergie limités, fonctionnent dans des environnements très incertains et hostiles (par exemple, les champs de bataille), changent constamment de topologie et de couverture, manquent d'adressage global et ont des nœuds qui sont bruyants et sujets aux

pannes, les protocoles de communication Internet traditionnels tels que les protocoles Internet (IP), y compris l'IP mobile peut ne pas être adéquate.

Nous pouvons citer les applications suivantes[19] :

- **Détection et poursuite des intrusions :** des capteurs sont transportés le long de la frange d'un champ de bataille pour détecter, classer et suivre le personnel et les véhicules intrus.
- **Surveillance météorologique :** La surveillance météorologique est un aspect important, des nœuds dédiés sont utilisés qui peuvent prédire des paramètres météorologiques tels que la température, la vitesse du vent, la pression, la quantité de précipitations, l'humidité, etc.
- **Surveillance à l'intérieur :** elles sont utilisées pour assurer la sécurité dans les galeries d'art, les hôpitaux, les centres commerciaux et autres installations.
- **Analyse du trafic :** elles peuvent surveiller le trafic ou une partie congestionnée d'une ville pour aider les gens à atteindre facilement leur destination.

I.4.2 Choix du Meilleur Réseau Mobile pour les SGUC

La réalisation et le déploiement d'infrastructures de réseaux capables de garantir la connectivité à des zones géographiques caractérisées par des conditions d'accès dangereuses (comme les champs de bataille, cas de catastrophe) a une grande importance. Le tableau I.3 ci-dessous montre les différentes caractéristiques des réseaux précédemment présentés.

	MANET	DTN	WSN	VANET
Topologie dynamique	✓	✓		✓
Connectivité intermittente		✓		
Long délai		✓		
Ressources limitées	✓	✓	✓	
Taux de perte élevé	✓		✓	✓
Hétérogénéité	✓	✓	✓	

Tableau I.3 : *Classification des réseaux de communication*

En procédant par élimination, MANET semble le plus judicieux pour garantir la communication entre les différents composants de SGUC, En fait :

- WSN ne supporte pas la mobilité, car les nœuds sont placés dans des zones géographiques bien précises pour collecter l'information, et ce n'est pas le cas des composants du SGUC qui nécessite un changement constamment de topologie et de couverture.
- VANET comme son nom l'indique, est un réseau qui utilise des nœuds véhiculaires pour communiquer entre eux alors que les véhicules ne font pas parties des composants du SGUC.
- DTN repose sur le principe de store_carry and forward pour minimiser la probabilité de perte de paquet et ainsi garantir l'arrivé des messages aux destinataires. Il est caractérisé par un délai de transmission (latence) élevé et une grande capacité de stockage dans les nœuds car un nœud stocke des messages dans son tampon pendant de longues périodes jusqu'à ce qu'il trouve un autre nœud entré dans la même plage réseau. Ce qui peut provoquer un débordement de la mémoire tampon et entrainer des pertes fréquentes des messages. Alors que les réseaux de réponse aux catastrophes doivent garantir que les messages peuvent atteindre leur destination le plutôt possible (latence courte) pour sauver des vies.

Par ailleurs, MANET tente d'établir un chemin de bout en bout entre nœuds source et destination de nature symétrique avec délai de livraison inférieur à celui de DTN[19] ce qui est très importante dans les scénarios de catastrophe.

I.5 Communication Opportuniste

Le réseau opportuniste est une évolution des réseaux mobiles ad hoc (MANET), les nœuds de ce type de réseau peuvent interagir les uns avec les autres, même en l'absence de route entre eux. Les informations sur la topologie du réseau ne sont pas prédéterminées au nœud qui transmettra les données. Dans une communication opportuniste pendant que les messages sont envoyés, les routes sont construites dynamiquement. Lorsque les données sont transférées de la source à la destination, les sauts sont créés de manière opportuniste en fonction de la plus proche par rapport à la destination. Dans ce type de réseau, le chemin de bout en bout peut exister ou beaucoup n'existe pas, donc trouver le chemin sera une partie délicate. La fonction principale lors du transfert des données est la fiabilité et les contrôles de congestion sont inefficaces dans les réseaux opportunistes. Les nœuds intermédiaires se chargent de la maintenance des données et démarrent le transfert une fois la connectivité rétablie[27].

I.6 Conclusion

Dans ce premier chapitre introductif, nous avons présenté le système de gestion de catastrophe, ensuite nous avons cité les principaux systèmes de gestion d'urgences existant et nous avons fini avec une description des réseaux de communication. Dans notre travail, nous avons opté pour le réseau MANET comme moyen de communication opportuniste entre les composants du système de gestion des urgences et de catastrophe.

Dans le chapitre suivant nous allons décrire la raison de passage de paradigme TCP/IP vers les réseaux centrés sur l'information ICN.

Chapitre II : Réseaux Centrés sur l'Information (ICN)

II.1 Introduction

Internet est apparu, au début des années 70, dans le simple but de connecter deux ordinateurs. Quelques années plus tard, l'utilisation d'Internet a évolué avec la création de nouveaux services, notamment le World Wide Web (1991), YouTube (2005), Dropbox (2008).

Parallèlement, de nombreuses nouvelles technologies ont vu le jour, telles que les technologies sans fil (1999). De plus, le nombre d'utilisateurs qui accèdent au Web a augmenté, et cette communication mondiale augmente considérablement le trafic réseau. Considérant cette évolution, tout le concept d'Internet évolue également. Aujourd'hui, il s'agit de connecter les données, les objets et les environnements. Dans ce processus de communication, la machine elle-même perd de plus en plus son importance pour faire place aux données.

Dans ce chapitre, nous commençons par introduire l'architecture d'Internet courante, ses limites et les solutions courantes. Ensuite, nous définissons le paradigme ICN et ses principales caractéristiques. Après cela, nous fournissons des motivations pour soutenir le paradigme ICN comme une solution pour les systèmes de gestion des urgences sismiques. Comme de nombreuses architectures ICN ont été introduites depuis 2007, nous nous concentrons, dans ce chapitre, sur laquelle de ces architectures est plus adaptée aux catastrophes.

II.2 L'architecture d'Internet courante

Avant de pouvoir discuter des limites d'architecture Internet actuelle, nous devons brièvement examiner le fonctionnement d'Internet actuel.

II.2.1 Le fonctionnement d'Internet

Les objectifs de conception qui sous-tendent l'architecture Internet actuelle par ordre d'importance sont les suivants[28] :

(1) Pour connecter des réseaux existants.

(2) Pour la survivre.

(3) Pour prendre en charge plusieurs types de services.

(4) Pour accueillir une variété de réseaux physiques.

(5) Pour permettre une gestion distribuée.

(6) Pour être rentable.

(7) Pour permettre l'attachement de l'hôte avec un faible niveau d'effort.

(8) Pour permettre la responsabilisation des ressources.

Pour atteindre ces objectifs, les **principes de conception** suivants ont été utilisés [28]:

a) La superposition (Layering).

b) La commutation des paquets (Packet switching).

c) Un réseau de réseaux collaborateurs.

d) Les systèmes terminaux intelligents.

e) L'argument de bout en bout.

Les principes de conception d'origine d'Internet garantissent qu'Internet remplit la plupart des objectifs de conception d'Internet d'origine (1-6). Les autres objectifs de conception ont été atteints par des béquilles telles que DHCP[4] (septième objectif de conception) ou le protocole de gestion de réseau simple SNMP[5] et NetFlow[6] (huitième objectif de conception).

Par la suite, nous examinons comment ces principes de conception permettent à Internet d'aujourd'hui de remplir la plupart des objectifs de conception énoncés ci-dessus.

II.2.1.1 Superposition

L'utilisation de couches réseau conduit à une pile réseau et offre une réduction de la complexité, l'isolement des fonctionnalités, et un moyen de structurer leurs conceptions de protocoles réseaux. Chaque couche de la pile réseau offre un service à la couche suivante. Il implémente ce service en utilisant les services offerts par la couche ci-dessous, ce qui se traduit par une situation où la communication logique se produit au sein de chaque couche. Pourtant, pendant la communication réelle, les données passent la pile du réseau à l'expéditeur de haut en bas et au récepteur de bas en haut.

---

[4]DHCP est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station ou d'une machine.

[5] SNMP est protocole qui permet aux administrateurs réseau de gérer les équipements du réseau et de diagnostiquer les problèmes de réseau.

[6] NetFlow est un protocole utilisé pour les statistiques de données de flux, il a été développé par Cisco pour surveiller et enregistrer tout le trafic lorsqu'il entre ou sort d'une interface.

Internet comporte les cinq couches suivantes (de haut en bas) : application, transport, réseau, liaison et physique (voir la figure II.1).

- La couche physique est responsable du codage des données et de leur transport sur le fil.
- La couche liaison permet une communication de voisin à voisin.
- La couche réseau, souvent appelée couche IP, permet la communication d'hôte à hôte et fournit un moyen d'habiller les hôtes via les adresses IP, envoyer des données (via les paquets IP), ainsi que la détermination des itinéraires.
- La couche transport permet la communication vers l'application soit en tant que flux binaire via TCP ou en tant que service de messagerie via UDP. TCP offre un transfert de données fiable, avec contrôle du débit et de la congestion, tandis que le protocole UDP offre la possibilité l'enregistrement et / ou la réception de messages.
- La couche application implémente l'échange de protocole spécifique à l'application comme HTTP ou FTP. L'interface entre l'application et la couche de transport est l'API Socket.

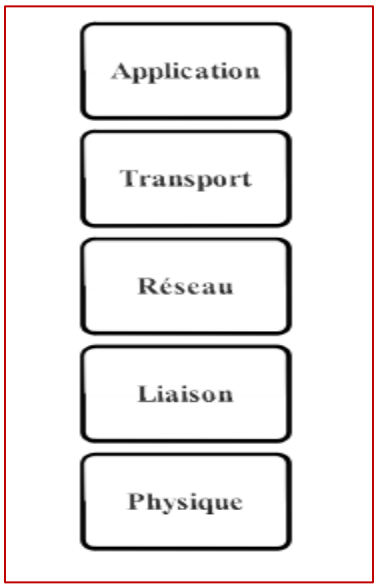


Figure II.1 *: Pile des Protocole d'Internet [28]*

L'utilisation des couches de communication permet l'interconnexion simple des réseaux existants (objectif de conception 1) et permet l'hébergement d'une variété de réseaux (quatrième objectif de conception). Dès qu'un réseau offre le service requis par une couche spécifique, il peut être considéré comme implémentant cette couche.

II.2.1.2 Commutation des paquets

La décision d'utiliser la commutation de paquets implique que les données doivent être divisées en paquets. Chaque paquet porte l'adresse de sa destination et traverse le réseau indépendamment des autres paquets. N'importe quel paquet peut utiliser la bande passante complète du lien sur n'importe quel lien, mais peut devoir attendre dans une file d'attente si d'autres paquets utilisent déjà le lien. Si un paquet rencontre une file d'attente complète, il est simplement supprimé, ce qui correspond au principe du meilleur service possible. Cela signifie qu'il est possible d'utiliser un système de routage sans état au niveau de la couche réseau, ce qui ne nécessite pas état de connexion. Cela garantit l'évolutivité et contribue à la rentabilité (sixième objectif de conception).

II.2.1.3 Réseau de réseaux collaborateurs

Sur Internet, les décisions de routage sont prises sur une base de réseau IP (un ensemble d'adresses IP associées) basé sur la table de routage de chaque routeur, qui est calculée de manière distribuée. En effet, Internet est divisé en une collection de systèmes autonomes (Autonomous System, AS).

Chaque AS est géré par un fournisseur de services Internet (Internet Service Provider, ISP) qui exploite un réseau fédérateur qui se connecte aux clients et autres fournisseurs de services. Au sein d'un AS, le routage est déterminé par des protocoles de passerelle intérieure tels que OSPF[7] et IS-IS[8] et le routage entre les AS est contrôlé par le BGP[9].

II.2.1.4 Systèmes d'extrémité intelligents / l'argument de bout en bout

Le fait que la couche réseau puisse simplement supprimer des paquets est un résultat de garder le réseau débile et de placer l'intelligence au système final. Si l'application nécessite un transfert de données fiable, il est de la responsabilité du système final de fournir le service, comme dans la

[7] OSPF est un protocole de routage à états de liens a été développé par l'IETF pour répondre au besoin d'un protocole de routage intérieur (IGP, "Internal Gateway Protocol") dans la pile des protocoles TCP/IP.

[8] IS-IS est un protocole IGP (Interior Gateway Protocol) normalisé par IETF et couramment utilisé dans les grands réseaux de fournisseurs de services. C'est un protocole de routage à état de liaison, offrant une convergence rapide et une excellente évolutivité.

[9] BGP est un protocole de routage de politique, qui distribue des informations de routage entre des routeurs appartenant à différents systèmes autonomes.

couche transport via le protocole TCP. En effet, l'argument de bout en bout peut être utilisé comme un moyen de placer une fonctionnalité. Il y a deux raisons de placer la fonctionnalité à l'intérieur du réseau plutôt qu'au niveau des systèmes finaux : si toutes les applications en ont besoin, ou si un grand nombre d'applications bénéficient d'une augmentation des performances. Ce n'est pas le cas pour la fiabilité. Toutes les applications ne l'exigent pas exemple VoIP[10] et les applications doivent souvent implémenter la fiabilité de bout en bout de toute façon, par exemple DNS[11]. Par conséquent, la commutation de paquets et l'argument de bout en bout contribuent à garantir la survie (deuxième objectif de conception) et la rentabilité (sixième objectif de conception).

II.2.2 Les limites de l'architecture d'internet actuelle

Malgré ces principes de conception, l'architecture d'Internet courante possède plusieurs lacunes, les plus importantes [28], [29]:

a. La sécurité :

La sécurité repose sur l'utilisation de protocoles de système final (exemple, sécurité de la couche transport) ou de dispositifs de réseau supplémentaires (exemple, pare-feu ou systèmes de détection d'intrusion). Il n'y a pas de soutien inhérent à la sécurité, car les adresses IP ne fournissent pas de renseignements personnels sur les identités (elles peuvent être usurpées facilement).

b. La mobilité :

Actuellement, la plupart des appareils sont équipés d'interfaces sans fil. Selon Cisco Visual Networking Index d'ici 2022, 70 % du trafic Internet mondial sera généré par des appareils sans fil. Contrairement aux dispositifs d'extrémité conventionnels, ces dispositifs doivent changer leur point d'accès lorsqu'ils sont transportés, ce qui les oblige à changer leur adresse IP. La modification de l'adresse IP interrompt la session de communication et nécessite le rétablissement d'une nouvelle session. Pire encore, lorsque le point final qui retient les données est mobile, le changement de son adresse le rend inaccessible par d'autres hôtes car il n'y a pas de mécanisme pour indiquer leur adresse actuelle. En effet, ces approches sont superposées à l'architecture réseau

[10] VoiIP est une technologie qui permet de délivrer des communications vocales ou multimédia via le réseau Internet (IP).
[11] DNS (Domain Name System) est une base de données distribuée dans laquelle vous pouvez mapper des noms d'hôtes à des adresses IP via le protocole DNS à partir d'un serveur DNS.

actuelle. Avec une croissance aussi rapide du contenu et des utilisateurs simultanément, les modifications ou solutions incrémentielles de l'architecture Internet actuelle résisteront difficilement à l'évolution d'Internet.

c. La qualité de service :

Bien que les mécanismes de fourniture de la qualité de service (Quality of Service, QoS) sur Internet ainsi que les réseaux en mode de transfert asynchrone (Asynchronous Transfer Mode, ATM) aient été très bien étudiés, les problèmes d'interaction entre les couches du réseau (principe de conception a) ne sont toujours pas résolus et la gestion de ces services, y compris la configuration, la configuration des politiques, la mise en charge, les configurations inter-fournisseurs, etc… est toujours ouverte (principes de conception b et c).

II.2.3 Solutions courantes

La croissance rapide du trafic et les attentes des utilisateurs ont fait naître le besoin d'un nouveau modèle de communication. Ce problème a inspiré à la fois la communauté de la recherche et l'industrie. Quelques solutions pour correspondre au nouveau modèle de trafic ont été proposées telles que les réseaux pairs à pair (Peer-to-Peer, P2P) et les réseaux de distribution de contenu (Content Delivery Netrwork, CDN), pour alléger la pression sur les réseaux actuels.

II.2.3.1 Les réseaux pairs à pair (Peer-to-Peer, P2P)

Les réseaux pair-à-pair (P2P) sont des systèmes naturellement distribués superposés sur les réseaux IP. Elles permettent à plusieurs ordinateurs de communiquer sur un réseau. La particularité de leurs architectures réside dans le fait que les données peuvent être transférées directement entre deux stations connectées au réseau sans passer par un serveur central. L'absence d'organisation hiérarchique et de contrôle centralisé leur permet d'aller au-delà des fonctionnalités et des services offerts par les architectures serveur-client traditionnelles. En ayant des rôles symétriques où chaque pair peut être un client et en même temps un serveur.

Les réseaux P2P offrent une tolérance aux pannes, un partage de ressources massivement évolutif et auto-organisé. Cependant, ils ont plus de difficultés que les systèmes client-serveur à diffuser des informations et à coordonner l'interconnexion des nœuds, garantissant ainsi de faibles retards dans les demandes[30].

II.2.3.2 Les réseaux de distribution de contenu (Content Delivery Network, CDN)

Un réseau de distribution de contenu (CDN), représente un groupe de serveurs géographiquement dispersés sur lesquels le contenu est reproduit afin de faciliter la diffusion de l'information générée par les éditeurs Web de manière opportune et efficace. Les CDN sont complètement transparents pour les utilisateurs finaux. Cette transparence est obtenue en utilisant des mécanismes spéciaux de routage, à la charge et des mécanismes de cartographie de l'internet afin de rediriger les recherches DNS vers les sites proches (du client)[31].

La distribution de plusieurs copies du même contenu sur Internet élimine la nécessité pour un consommateur de passer par un grand nombre de routeurs pour accéder au contenu. Les CDN étaient la solution la plus sollicitée[32]. Ils fournissent des fonctionnalités de distribution de contenu construites au niveau de la couche application sur le dessus de l'infrastructure Internet actuelle. Quelques déductions extraites du dernier Cisco, l'indice de réseautage visuel (VNI), qui analyse la composition du trafic, affirme que le Internet évolue vers un Internet mobile efficace. En effet, les données mobiles représenteront 86% du trafic total d'ici 2021. Selon Cisco, les CDN sont identifiés comme les approches les plus appropriées pour la diffusion de données mobiles. Ils s'attendent à ce que 71% de tous les mobiles le trafic traversera les CDN d'ici 2021[33].

Malgré leur importance, les CDN ont montré quelques limites. Les principaux inconvénients sont liés au coût. En réalité, les CDN sont des solutions très coûteuses, surtout s'ils sont déployés à grande échelle. De plus, ils engendrent un coût élevé en termes de ressources (bande passante, stockage, distribution des nœuds). Le déploiement des serveurs et le choix de leurs emplacements ne sont pas bien contrôlés en raison à un manque de collaboration entre les différents opérateurs d'accès à Internet. En plus, les CDN actuels sont mono-spécialisés. Ils distribuent le contenu conformément aux accords avec les fournisseurs de données d'origine. Enfin, il n'y a pas de collaboration entre les différents fournisseurs CDN et chacun opèrent individuellement.

II.3 Réseaux Centrés sur l'Information

Malgré leurs avantages, les réseaux cités précédemment ne donnent pas de solution radicale pour faire face aux problèmes fondamentaux causés par l'architecture Internet actuelle. Par conséquent, de nombreux efforts ont été donnés ces dernières années pour développer des solutions

"Clean Slate"[12] pour l'architecture du futur Internet[28] [34]. Dans ce contexte, on trouve les réseaux centrés sur l'information (Information Centric Network, ICN), qui ont été proposées principalement pour faire face aux nouveaux besoins d'Internet depuis que son utilisation principale a changé d'un modèle de communication entre les hôtes à une distribution de contenus. L'idée principale d'un ICN est de considérer les contenus nommés comme l'élément central du réseau, contrairement aux adresses IP qui sont l'identifiant principal des hôtes dans les réseaux Internet. Pour récupérer un contenu, un utilisateur ne se préoccupe plus de son emplacement mais il n'a besoin que de spécifier le nom de son contenu. Le réseau se charge ensuite de router sa demande vers la meilleure source possédant une copie et de retourner ce contenu au demandeur en suivant le chemin inverse[34].

II.3.1 La terminologie

Les réseaux centrés sur l'information sont décrits en utilisant une certaine terminologie. Nous consacrons ce paragraphe à la définition de ces termes qui vont être utilisés tout au long de ce chapitre[34], [35].

- Un **NDO** est un objet de données nommé (Named Data Object, NDO) représente l'unité de données adressable dans un réseau ICN. Il peut être une page Web, un document texte, ...etc. En d'autres termes, les fichiers sont divisés en segments similaires aux réseaux actuels et ces segments sont identifiés de façon unique. Par conséquent, un NDO peut être de tout type que nous pouvons identifier, stocker et accéder de manière unique via le réseau. Il est indépendant de l'emplacement, de la méthode de stockage, des programmes d'application et de la méthode de transport.
- Un **demandeur/consommateur** correspond à une entité qui envoie une demande de contenu NDO.
- Un **producteur** correspond à une entité responsable d'informer le réseau de sa possession d'un contenu NDO en publiant son nom dans le réseau, de sorte qu'une demande pour ce

[12] Le système est entièrement repensé pour offrir des abstractions et / ou des performances améliorées, tout en offrant des fonctionnalités similaires basées sur de nouveaux principes de base.

contenu peut lui être acheminée. Le producteur correspond généralement au créateur ou au propriétaire du contenu.

- Une **source de contenu** correspond à un nœud de réseau stockant le contenu.
- Un **nœud** correspond à tout routeur ou hôte capable de prendre des décisions de routage et de mise en cache.

II.3.2 Les fonctions de base des ICNs

Les ICN proposent de changer l'Internet, qui est actuellement basé sur les localisations des serveurs avec des adresses bien définies, vers une architecture basée sur le nom des contenus (voir la Figure II.2), avec des fonctionnalités nativement intégrées comme le nommage indépendant de la localisation, la faculté de cacher des continus dans les réseaux, le routage basé sur les noms de contenu, la sécurisation des contenus et la mobilité. Le tableau II.1 compare ces fonctionnalités à ceux de l'Internet actuel et montre que les ICNs sont plus efficaces pour délivrer des contenus aux utilisateurs avec une meilleure qualité et permettent aussi d'améliorer la gestion des capacités réseaux fournisseurs des réseaux[36].

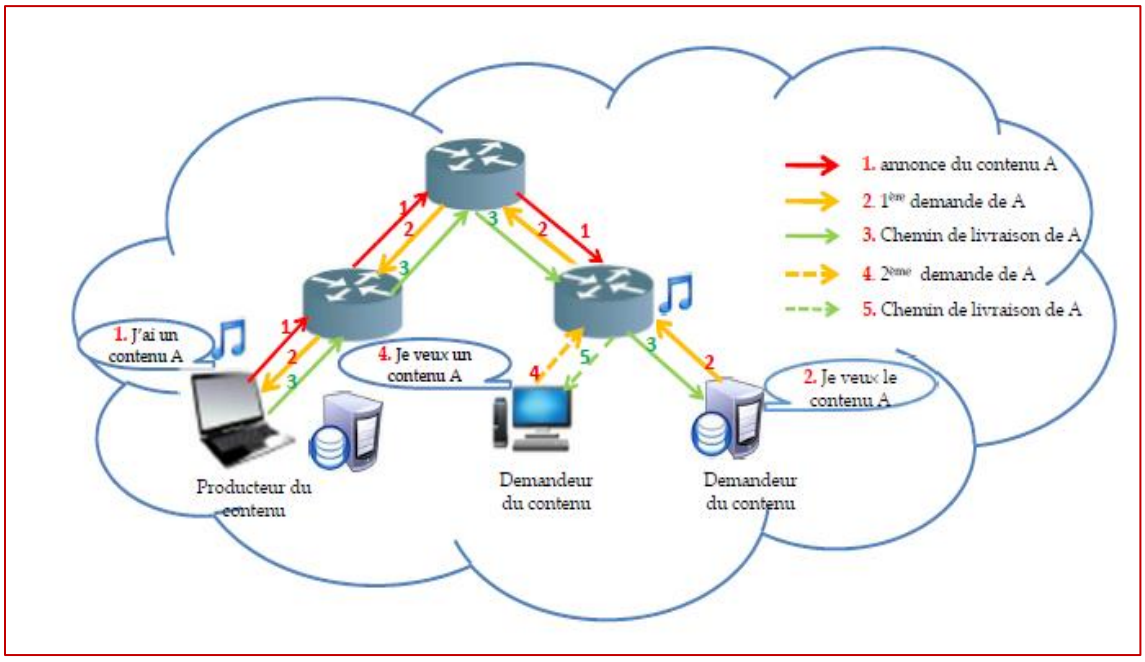


Figure II.2 *: L'architecture des réseaux ICN [37]*

	Internet	ICN
Nommage	Relatif à l'emplacement d'hôte	Relatif au contenu, indépendant de son emplacement
Mise en cache	Dans des serveurs spécifiques	Dans n'importe quel nœud du réseau
Routage	Entre les hôtes en utilisant des adresses IP	Entre un demandeur et n'importe quel nœud du réseau détenant une copie du contenu, en utilisant son nom du contenu
Sécurité	Des canaux de communication entre les hôtes	Du contenu lui-même
Mobilité	Des hôtes interrompent la session de communication et les rend inaccessible par d'autres hôtes	Des consommateurs permettent de reconfigurer l'emplacement de leur réseau sans interrompre la connectivité, tandis que la mobilité des producteurs permet aux sources de se déplacer sans perturber la disponibilité du contenu.

Tableau II.1: *Comparaison entre Internet et ICN [36]*

Par la suite. Nous écrivons les principales fonctionnalités intégrées dans un ICN.

II.3.2.1 Le nommage

Nommer des objets de données est un pilier aussi important pour ICN que l'adressage d'hôtes l'est pour Internet d'aujourd'hui. Selon ce nouveau paradigme, le consommateur demande un contenu par son nom au lieu d'utiliser sa localisation réseau. Cela étant dit, chaque contenu doit être identifié à l'aide d'un nom unique, persistant et indépendant de l'emplacement. Selon l'architecture, les noms peuvent être plats ou hiérarchiques et peuvent ou non être lisibles par l'homme[4]. L'espace de noms hiérarchique à une structure similaire aux URL[13]. Les noms sont une séquence de chaînes séparées par "/". Par exemple, *parc.com/animal/video.mp3*. L'avantage des noms hiérarchiques est qu'ils peuvent contenir d'autres informations comme la version et le

[13] URL (Uniform Resource Locator) est un format de nommage universel pour désigner une ressource sur Internet.

numéro de bloc. Un nom plat est représenté par une chaîne comme *0x9lp653llalla*. Comme nous pouvons le voir, les noms peuvent être lisibles par l'homme, ce qui facilite aux consommateurs qui demandent le contenu souhaité. D'un autre côté, les consommateurs ne peuvent pas comprendre un nom non lisible par l'homme. Cependant, ces noms sont auto-certifiés. En réalité, les noms peuvent être chiffrés avec les données elles-mêmes et leur producteur, ce qui les rend non lisible par l'homme. Ce groupe d'espace de noms présente l'avantage de sécurité. Étant donné que les demandes peuvent être satisfaites par des nœuds autres que les producteurs d'origine de confiance, les consommateurs devraient pouvoir vérifier l'intégrité et la provenance des données reçues au moyen d'informations de "sécurité" inclus dans l'objet de données.

Pour récapituler, il existe trois catégories d'espaces de noms (plats vs hiérarchiques vs combinaison de ces deux) qui peuvent êtres auto-certifiés ou lisibles par l'homme. Le choix dépend des applications et des attentes des consommateurs. La décision d'utiliser une classe des noms affecte principalement l'évolutivité du plan de routage ICN.

II.3.2.2 La mise en cache

Le modèle de communication repose sur la demande et la distribution des contenus NDO. Un producteur annonce au réseau la disponibilité d'un contenu nommé, et ceci sans connaissance préalable des consommateurs qui peuvent être intéressés par ce contenu. Un consommateur déclare ensuite son intérêt pour ce contenu en spécifiant son nom, sans la connaissance des producteurs potentiels. Pour satisfaire cette demande, le réseau se base sur le nom de contenu demandé pour le consommateur. Il lance un chemin de distribution vers le demandeur[37].

Comme les contenus peuvent être nommés indépendamment de l'emplacement des producteurs respectifs, ils peuvent être stockés partout sur le réseau. Par conséquent, des copies du même contenu stocké à différents endroits du réseau, sont considérés comme un contenu unique. Il s'agit de la mise en cache dans le réseau, qui est un élément constitutif majeur de l'ICN. Il représente la caractéristique la plus courante et la plus importante des architectures ICN. Il a été introduit pour alléger la pression sur la bande passante du réseau et par conséquent améliorer l'efficacité de transmission dans la diffusion de contenu[38].

Comme le montre la figure II.3, le consommateur 2 envoie une requête pour récupérer le contenu nommé *X*. Lors de l'envoi de la réponse, le nœud 2 et le nœud 6 stocke une copie du

contenu. Ensuite, lorsque le consommateur 1 ou 3 demandes le même contenu X, la requête est satisfaite par le nœud 2 ou 6.

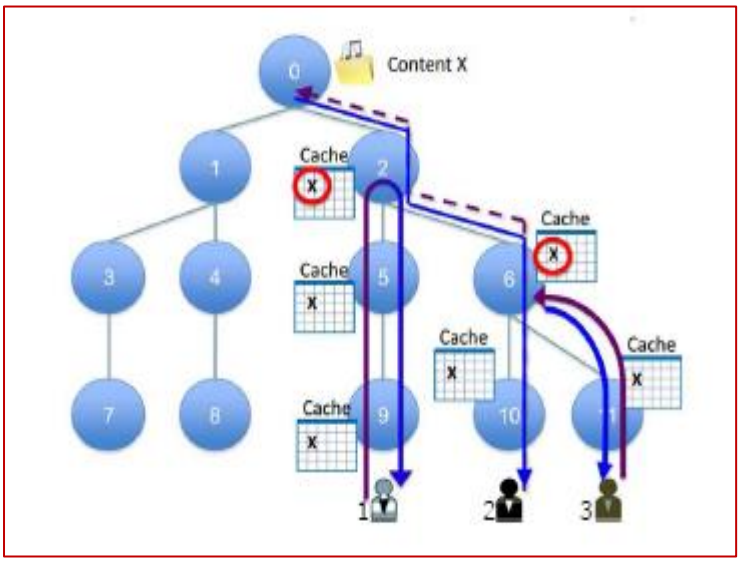


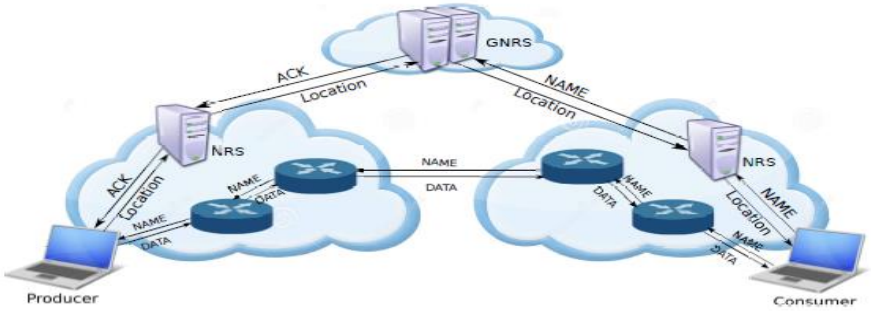
***Figure II.3** : La mise en cache en ICN [39]*

Le concept de mise en cache, qui n'est pas un terme révolutionnaire, a été largement utilisé sur le Web, les systèmes P2P et les CDN. Cependant, dans ICN, la mise en cache dans le réseau est plus importante et plus difficile que dans les systèmes de mise en cache déjà existants. Tout d'abord, il est transparent et ne nécessite aucune application spécifique pour mettre en cache le contenu. Deuxièmement, il est omniprésent puisque tous les nœuds ICN peuvent être un cache[38].

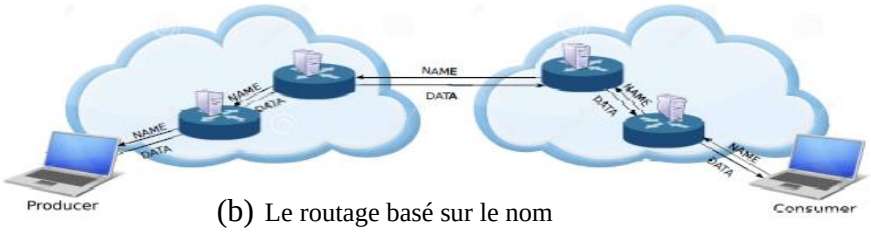
En revanche, il convient de noter que la taille du cache est limitée et une fois le cache plein, une éviction du cache est effectuée pour permettre la mise en cache de nouveaux éléments. Par conséquent, la mise en cache dans le réseau impose l'établissement d'une politique de remplacement de cache. Selon la politique de remplacement, l'un des contenus mis en cache est sélectionné et supprimé.

II.3.2.3 Le routage

Le routage est une question de savoir comment les demandes sont acheminées vers le producteur via le réseau, puis comment les données sont acheminées vers le consommateur. Il existe deux approches générales dans les ICN pour gérer les demandes de routage, toutes deux fortement dépendantes des propriétés de l'espace de noms d'objets [34].ICN implémente le routage de résolution de nom (name resolution routing) et le routage basé sur le nom (name-based routing) décrit respectivement dans la figureII.4 (a) et la figure II.4 (b).



(a) Le routage de résolution de nom



(b) Le routage basé sur le nom

***Figure II.4** : Les approches de routage[39]*

Avec la méthode de résolution de noms, la récupération des données est effectuée en deux étapes comme indiqué sur la figureII.4 (a). Tout d'abord, le nom du contenu est traduit dans un ou plusieurs localisateurs s'il existe. Ces derniers sont les localisateurs topologiques actuels du contenu demandé dans le réseau, il peut s'agir de l'adresse du producteur ou d'un nœud de cache qui conserve une copie du contenu souhaité. L'entité qui stocke ces informations d'emplacement s'appelle « système de résolution du nom » (Name Resolution System, NRS). Le NRS stocke une liaison entre les noms de contenu et leurs localisateurs actuels. Les NRS sont organisés de manière hiérarchique et chacun couvre une zone spécifique du réseau, par conséquent, le consommateur

doit rediriger la demande vers son NRS dédié pour récupérer les informations de localisation. Si le NRS ne dispose pas des informations de localisation, il redirige la demande vers le NRS global du niveau supérieur. Une fois ces informations sont obtenues, le consommateur peut ensuite transmettre directement les demandes vers la destination optimale en fonction des protocoles de routage. Différents NRS de la topologie sont peuplés grâce aux messages de signalisation provenant des producteurs pour annoncer une disponibilité de contenu. Il est à noter que chaque producteur ne notifie que son NRS dédié.

Contrairement au routage à résolution nommée, la méthode de routage basée sur le nom, présentée dans la figure II.4 (b), repose sur une seule étape pour récupérer un contenu. Cette approche est basée sur la hiérarchie des noms pour acheminer les demandes et les transmettre directement aux producteurs sans avoir à résoudre les noms aux localisateurs lors d'une étape précédente. À chaque nœud vers le producteur, la demande est envoyée à la prochaine interface qui correspond au préfixe le plus long. Cela signifie que chaque nœud doit connaître une partie des informations de routage. Une fois que le producteur a reçu la demande, les données sont redirigées vers le consommateur via le chemin inverse de la demande[39].

II.3.2.4 La sécurité

Dans l'architecture ICN, l'utilisateur peut utiliser n'importe quelle copie disponible, la sécurité ne peut pas être liée aux points de terminaison ou à l'emplacement de stockage comme une architecture centrée sur l'hôte. Puisque le contenu dans ICN est désigné par son nom, la vérification de la liaison entre le nom et le contenu est essentielle pour s'assurer que le destinataire a reçu le contenu correct et complet (intégrité et authenticité du contenu). Dans la communication centrée sur le contenu, chaque paquet est livré avec une signature numérique qui permet aux destinataires autorisés de vérifier l'authenticité du contenu par le déchiffrement des contenus, et non pas via des connexions de communication sécurisées comme IP.[40]

Dans ICN, les attaques, telles que le déni de service, nécessitent des approches différentes par rapport aux attaques similaires dans la communication IP. Dans ICN, le contenu est distribué sur les nœuds du réseau et non sur un nœud spécifique. Par conséquent, un déni de service ne peut pas être simplement lancé en envoyant un grand nombre de requêtes aux mêmes données. Au lieu de cela, il faut faire des efforts pour arrêter les services de plusieurs nœuds du réseau

II.3.2.5 La mobilité

La mobilité en ICN peut être classée en mobilité des producteurs et mobilité des consommateurs [41]. D'une part, même si un producteur (le contenu) change d'emplacement, il sera toujours accessible car son nom est indépendant de l'emplacement. D'autre part, lorsqu'un consommateur se déplace, il lui suffit de réexprimer son intérêt pour un objet de données à partir du nouvel emplacement. Que ce soit avec le routage basé sur le nom ou le routage NRS, la mobilité du producteur peut entraîner la perte de paquets de demande lorsque la demande n'est pas satisfaite par un nœud de cache. Dans le cas d'un routage basé sur le nom, la demande sera redirigée saut par saut en fonction des informations de routage dans chaque nœud. Lorsqu'une mobilité se produit, les informations de routage doivent être mises à jour dans tous les nœuds appartenant au chemin de demande. Dans l'autre cas, le routage est basé sur l'emplacement récupéré à partir du NRS correspondant. Après un transfert, les systèmes NRS doivent être mis à jour pour faire correspondre les noms aux nouveaux emplacements.

II.3.3 Avantages des ICNs dans les situations de catastrophes et urgences

Les avantages potentiels que l'ICN pourrait apporter aux situations de catastrophe sont[42]:

- **Résilience de l'information :**

  Le concept de résilience dans un ICN est révolutionné lorsqu'on le compare aux réseaux centrés sur l'hôte (Internet), parce que le maintien de la résilience dans un ICN n'implique pas nécessairement le maintien de la connectivité entre les dispositifs (ex., hôtes finaux, routeurs). Il s'agit plutôt de maintenir la connectivité entre les consommateurs et l'information qu'ils désirent (possiblement disponible dans de nombreux endroits). Dans le cas le plus simple, les parties déconnectées d'un réseau peuvent toujours être en mesure d'atteindre des répliques de données mises en cache, même si l'origine des données n'est plus accessible. Cela est possible en offrant la découverte locale de sources de contenu, ainsi que la vérification de l'information basée sur le hachage qui ne repose pas sur une infrastructure à clé publique. En plus les ICN ne font aucune distinction entre le réseau et les ressources de stockage. Par exemple, on pourrait imaginer que les intervenants d'urgence transportent des sacs à dos avec des dispositifs de stockage portatifs permettant aux îles déconnectées d'accéder plus facilement aux informations du monde entier. De telles installations seraient presque

impossibles sur Internet sans des application d'intelligence sophistiquée, mais seraient parfaitement intégrées dans un ICN.

- **Interactions sans connexion :**

Les ICN proposent un paradigme d'interaction requête / réponse piloté par le récepteur, où il n'est pas nécessaire d'établir des connexions à long terme (contrairement à TCP). Cela signifie que les problèmes TCP courants (par exemple les délais d'expiration, l'élimination des paquets en panne) sont supprimés. Cela évite également de gaspiller des allers-retours inutiles pour établir des connexions, temps qui pourrait être mieux utilisé en utilisant une connectivité éphémère.

- **Communications déployées à la hâte :**

Souvent, les situations d'urgence entraînent l'utilisation de communications de secours, par ex. Wifi ad hoc. Les ICN peuvent facilement créer des îlots de connectivité ad hoc, offrant une accessibilité aux informations d'intérêt sans aucune modification complexe des hôtes demandeurs.

- **Collaboration résiliente :**

Actuellement, lorsque deux hôtes interagissent pour échanger des données, le réseau considère cela comme un flux de paquets. La seule facilité offerte par le réseau est de s'assurer que les paquets atteignent leur destination (même la différenciation de la qualité de service est mal prise en charge). En intégrant des connaissances centrées sur l'information dans le réseau, les opérateurs de réseau peuvent commencer à jouer un rôle beaucoup plus proactif dans le processus de livraison. Par exemple, ils peuvent reconfigurer le placement du cache, ainsi que conserver de manière proactive des informations importantes dans leurs domaines pour améliorer la résilience. Ces décisions pourraient être éclairées par des informations collaboratives provenant d'autres parties prenantes, s'informant mutuellement de l'importance respective des différentes NDO et de la manière dont elles devraient être traitées (par exemple, le contenu en direct devrait être traité différemment des pages Web). Surtout, en rendant ces opérations de réseau explicites, cela pourrait être effectué automatiquement sans négociation humaine. L'importance de cela est peut-être mieux mise en évidence par le tremblement de terre de Taiwan, qui s'est produit pendant les vacances de Noël alors que la plupart du personnel était en vacances.

- **Tolérance supérieure aux perturbations :**

La tolérance aux perturbations est généralement obtenue à l'aide d'un mécanisme de cache et de transfert par lequel les routeurs conservent temporairement les paquets jusqu'à ce qu'ils puissent être transférés. Cela permet de gérer les périodes de perturbation (par exemple, défaillance de la liaison) sans supprimer les données. C'est particulièrement le cas pour le contenu statique et immuable que les utilisateurs peuvent attendre de recevoir. Surtout, les routeurs ICN sont déjà équipés des caches nécessaires pour fournir un stockage tolérant aux retards. Alors que la mise en cache est généralement utilisée pour des raisons de performances (stockage des objets les plus populaires), les scénarios d'urgence peuvent déclencher des stratégies alternatives qui conservent les informations les plus critiques.

II.4 Les projets ICN

Les ICNs ont été explorée par de nombreux projets comme le montre le tableau II.2 [4]. Ce dernier compare les différents projets ICN disponibles dans les référentiels open source publics. La comparaison est basée sur la disponibilité de la littérature académique telle que le dernier article publié, le nombre de citations dans Google Scholar et la disponibilité de site web officiel.

Projet	Date	Cité en Google Schollar	Dernier article	Site Web
DONA	2007	1246	2007	ND[14]
AsiaFI	2007	3	2007	http://www.asiafi.net/
COMET	Jan 2010-Dec2012	10	2013	http://www.comet-project.org/
ANR Connect	Jan2011-Dec 2012	ND	ND	http://www.anr-connect.org/
Convergence	Jun 2010-Fev 2013	105	2013	http://www.ict-convergence.eu/
CCN	2009	2665	2016	http://www.ccnx.org/
NDN	Sep2010-Aoû2013	2519	2017	http://www.named-data.net/
NetInf	2010	ND	ND	https://sail-project.eu/about-sail/netinf/
PSIRP	Jan2008-Jun2010	ND	ND	http://www.psirp.org/
PURSUIT	Sep2010-Fev 2013	ND	2011	http://www.fp7-pursuit.eu/
4WARD	Jan 2008-Jun 2010	35	2010	http://www.4ward-project.eu/

[14] Non Défini

SAIL	Aoû2010-Jan 2013	ND	2013	http://www.sail-project.eu/
MobilityFirst	Sep2010-Sep 2013	60	2015	http://mobilityfirst.winlab.rutgers.edu/

Tableau II.2 : *Les projets ICNs*

Comme le montre le tableau II.2, les projets les plus cités et les plus documentés sont DONA (Data Oriented Network Architecture), CCN (Content Centric Networking), NDN (Named Data Networking) et Convergence, tandis que les autres projets sont moins activement cités dans la littérature. C'est pourquoi, nous allons étudier et comparer dans les paragraphes suivants que ces quatre projets.

II.4.1 Comparaison

Dans le tableau II.3, nous comparons ces quatre projets selon les fonctions de base d'ICN.

- **Le nommage des données** dans ICN est classé en trois catégories : le nommage hiérarchique, le nommage plat, et une combinaison de ces deux derniers. L'architecture DONA utilise le nommage plat, chaque donnée est directement identifiée par un nom ou par le résultat d'une fonction de hachage qui renvoie un identifiant unique du contenu. Le nommage hiérarchique quant à lui est utilisé par les architectures CCN et NDN. Ce type de nommage est séparé en plusieurs parties permettant de localiser l'objet dans une organisation de noms. Enfin, l'architecture de Convergence utilise une combinaison de ces deux types de nommage : un nommage plat à l'intérieur des domaines, et hiérarchique entre différents domaines mais la plupart des travaux Convergence sont basés sur le nommage hiérarchique.[4], [43]
- **La mise en cache** est une caractéristique fondamentale des architectures ICN, car la détection des informations permet au réseau d'identifier les informations mises en cache sans recourir à la couche application, comme dans la mise en cache Web. Les architectures ICN permettent aux nœuds de stocker localement les données ; deux cas sont alors possibles : La mise en cache sur le chemin (In-path) permet la récupération du contenu à partir des nœuds se trouvant seulement sur le chemin de transmission alors que la mise en cache hors chemin (Out-path) permet de bénéficier de n'importe quelle copie disponible dans le réseau.L'architecture DONA et Convergence récupèrent les données uniquement dans un cache situe sur le chemin de transmission (in-path). Les architectures CCN et NDN vont pouvoir récupérer les données à partir des nœuds se trouvant sur le chemin de transmission ou pas (in-path et out-path).[4], [43]
- **Le routage** dans DONA utilise une transmission saut à saut en se basant sur des résolveurs hiérarchises. Le résolveur racine du réseau connait l'ensemble des données à disposition

ainsi que le prochain saut pour y accéder. Ainsi, l'acheminement des requêtes se fait en remontant vers la racine lorsque le nœud ne connait pas le prochain saut pour accéder au contenu. Ensuite, le contenu est transmis à l'utilisateur en utilisant le routage IP sur lequel repose DONA.Concernant les architectures CCN et NDN, ils effectuent un transfert saut à saut et lors l'absence de règles pour transmettre une requête, le nœud émet la requête sur l'ensemble de ses autres interfaces et inonde le réseau. Alors que le routage en Convergence se base sur entité qui effectue la résolution des noms, cette entité va calculer la route entre le demandeur et le producteur possédant la donnée. Ainsi, le chemin est mis en place pour la requête.[4], [43]

- **La sécurité** dans le but est de garantir la confidentialité et l'intégrité des informations dans ICNs, contrairement à la confidentialité des canaux et à l'intégrité des solutions IP. Dans l'architecture DONA pour les données mutables, un demandeur recevra la donnée et également comme métadonnées la clé publique du principal et une signature pour l'objet de données lui-même, et pour les données immuables, le demandeur peut vérifiez simplement que l'étiquette est bien le hachage cryptographique de l'objet d'information. En NDN et CCN chaque message contient une signature sur le nom et les informations incluses dans le message, ainsi que des informations sur la clé utilisée pour produire la signature, par exemple, la clé publique du signataire, un certificat pour cette clé publique ou un pointeur vers eux. Cela permet à n'importe quel nœud de vérifier la liaison entre le nom du paquet et les informations qui l'accompagnent. Ce mécanisme de sécurité est adopté aussi au Convergence.[4], [43]
- **La mobilité.** Au niveau de DONA, les demandeurs mobiles peuvent simplement émettre de nouveaux messages à partir de leur emplacement actuel, pour les producteurs mobiles peuvent également désenregistrer et réenregistrer leurs informations lorsqu'ils changent d'emplacement réseau. Lorsqu'un demandeur change son emplacement dans les architectures CCN et NDN, il peut simplement émettre de nouveaux messages à partir de leur emplacement actuel, et pour la mobilité de producteur ça nécessite de publier à nouveau les préfixes de nom des informations qu'il héberge via le protocole de routage. L'approche de mobilité en Convergence est la même que celui de NDN.[4]

Par ailleurs, pour déployer, tester et mettre en place ces architectures, plusieurs simulateurs ont été développés. Contrairement aux projets DONA et convergence où nous n'avons pas trouvé des simulateurs disponibles sur le Net, les autres projets offrent un ensemble de simulateurs propriétaires (comme CCN) ou gratuits (comme NDN). En effet, NDN offre un ensemble d'outils open source dont les codes source des logiciels sont libres, gratuits, accessibles au public par l'intermédiaire du site Web NDN et fondés sur des langages populaires (C++, Python). C'est pour cette raison que NDN est utilisé par un grand nombre de chercheurs et de nombreux projets qui font vivre sa communauté aussi bien de chercheurs académiques que d'industriels.

	DONA	Convergence	CCN	NDN
Nommage	Plat	Plat/Hiérarchique	Hiérarchique	Hiérarchique
Mise en Cache	Sur le chemin	Sur le chemin	Sur le chemin et hors chemin	Sur le chemin et hors chemin
Routage	-Basé sur le nom	-Basé la résolution des noms	-Basé sur le nom.	-Basé sur le nom.
Sécurité	- Le principal est le hachage de la clé publique. L'étiquette peut être un hachage de contenu immuable.	- Signatures incluses dans les paquets.	- Signatures incluses dans les paquets. La chaîne de certification peut suivre la hiérarchie des noms.	- Signatures incluses dans les paquets. La chaîne de certification peut suivre la hiérarchie des noms.
Mobilité	-Mobilité des demandeurs via de nouvelles demandes. -La mobilité des producteurs nécessite des inscriptions supplémentaires.	- Mobilité des demandeurs via de nouvelles demandes. -La mobilité des producteurs repose sur un système de résolution de noms non spécifié.	-Mobilité des demandeurs via de nouvelles demandes. -Protocole d'inondation d'intérêt pour la mobilité des producteurs.	- Mobilité des demandeurs via de nouvelles demandes. -Protocole d'inondation d'intérêt pour la mobilité des producteurs.

Simulation	ND	ND	-CCN-lite -SCoNet -CCNSim -CCNPL-Sim -Mini-CCNx	- NdnSim -Omnet++

Tableau II.3 *: Comparaison entre les principaux projets ICNs.*

D'autre part, nous montrons dans le tableau II.4 les avantages apportés par les quatre projets ICNs dans les situations de catastrophes et urgences (comme décrit dans la section II.3.3) et leur adéquation pour une mise en œuvre du réseau ad hoc MANET. Comme nous pouvons le constater, les projets CCN et NDN sont les plus intéressants pour mettre en place les SGUC. Néanmoins, NDN offre plus de soutien technique et de littérature académique que CCN, NDN a été sélectionné comme particulièrement adapté aux MANET.

Projets	**DONA**	**Convergence**	**CCN**	**NDN**
Résilience de l'information	✓	✓	✓	✓
Interactions sans connexion			✓	✓
Communications déployées à la hâte			✓	✓
Collaboration résiliente	✓	✓	✓	✓
Tolérance supérieure aux perturbations	✓	✓	✓	✓
Mise en œuvre du MANET			✓	✓

***Tableau II.4** : Les projets ICNs et les SGUC*

En conclusion, sur la base des principales fonctions d'ICN, et des avantages apportés dans les situations de catastrophes et urgences, le NDN semble être le plus applicable dans les SGUC et les MANET. Ainsi, NDN a été adopté comme base de notre solution.

II.5 Conclusion

Dans ce chapitre, nous avons discuté de certaines solutions déjà déployées dans l'architecture TCP / IP pour surmonter ses limites fondamentales.

Ensuite, nous avons défini les concepts généraux de ce mémoire, notamment le paradigme ICN avec ses principaux projets. Nous avons également montré, dans ce chapitre, que l'ICN peut être un réseau efficace pour les scénarios de catastrophes qui peuvent améliorer la diffusion des données et faire face aux limitations actuelles du réseau. Nous avons enfin démontré que NDN est l'architecture ICN la plus appropriée pour SGUC et MANET. Dans le chapitre suivant, nous allons étudier en détail le déploiement du réseau MANET sur NDN.

Chapitre III : MANET dans NDN

III.1 Introduction

Avec la croissance rapide de volume de trafic réseau en termes de contenu et de données mobiles, la mise en réseau centrée sur l'information (ICN) via son projet Named Data Networking (NDN) offre de nouvelles perspectives sur la communication mobile ad hoc qui vise à atteindre une distribution de contenu très efficace car le routage est basé sur des noms mais pas sur des identifiants de point final.

Dans ce chapitre, nous concentrons sur l'architecture NDN avec leurs différentes caractéristiques, ensuite nous allons discuter sur des différentes stratégies qui existent dans MANET sous NDN.

III.2 L'architecture NDN

Un réseau de donnée nommé (Named Data Networking, NDN) est une nouvelle architecture d'Internet qui change le modèle de communication réseau de la livraison de paquets point à point à la récupération de données nommée, où les consommateurs envoient des intérêts pour récupérer des données.

En termes de participants au NDN, il existe trois entités, à savoir le producteur, le consommateur et le routeur de contenu. Le producteur est le fournisseur de contenu, publiant son contenu sur NDN, tandis que le consommateur est l'abonné de ces contenus publiés, demandant le contenu souhaité à NDN. Les paquets de données sont indépendants des producteurs et de l'endroit où ils sont stockés, car chaque paquet de données porte le nom et la signature des données plutôt que la source et la destination IP dans l'architecture IP. Étant donné que chaque objet de contenu a un nom unique, le contenu authentique peut être stocké et mis en cache par n'importe quel nœud. Si la connectivité à une source de contenu est interrompue, il n'est pas nécessaire de créer un nouveau chemin vers la même source, mais le contenu peut également être récupéré à partir d'un nœud plus proche qui fournit la même copie de contenu. La communication a lieu par échange deux types de paquets qui sont l'intérêt et les données (figure III.1). Les consommateurs de données envoient des paquets d'intérêt sous forme de noms. Les routeurs transmettent le paquet d'intérêt en fonction du nom des données et conservent également les informations d'état des intérêts en attente

qui permettent aux routeurs NDN de détecter les boucles, de mesurer les performances d'un chemin différent, de détecter rapidement les échecs et de réessayer le chemin alternatif. Le producteur répond avec un paquet de données qui prend le chemin inverse des intérêts[5], [44].

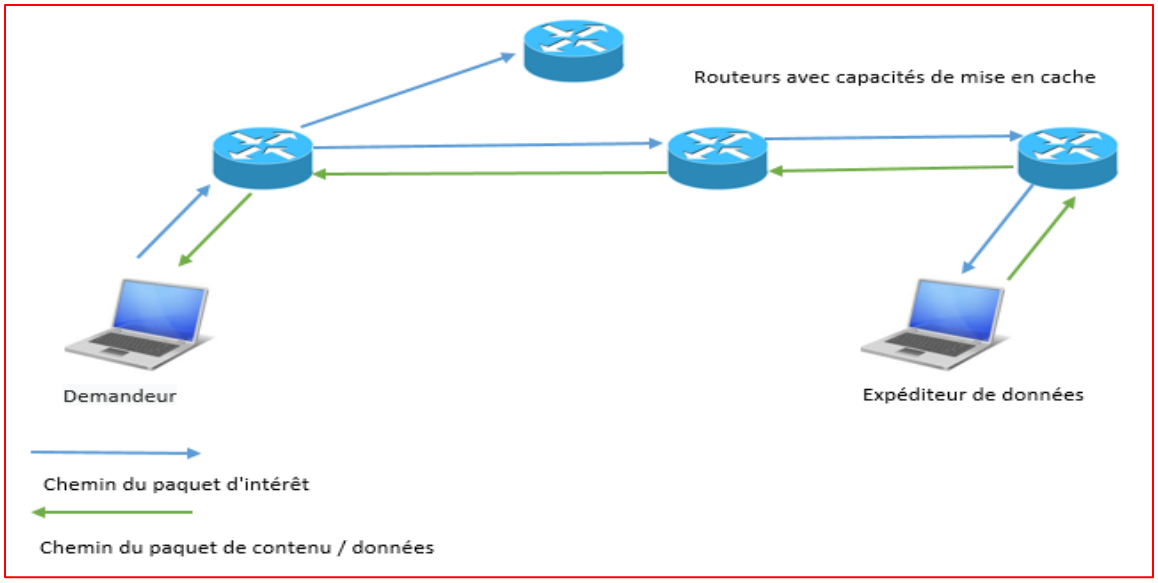


Figure III.1 : *Présentation d'architecture NDN [44]*

III.2.1 Les paquets NDN

Pour transmettre des données, le NDN se base sur deux types de paquets (figure III.2) : les paquets d'intérêt et les paquets de données. Ces paquets peuvent avoir une taille maximale de 8800 octets et sont encodés selon le format TLV (Type-Length-Value)[15]. Ainsi un paquet NDN n'a pas de forme définitive et pourra évoluer dans le temps.

[15] TLV est un schéma de codage utilisé pour un élément d'information facultatif dans un certain protocole, ou le Type un code binaire, souvent simplement alphanumérique, qui indique le type de champ que représente cette partie du message. Longueur c'est la taille du champ de valeur et en dernier la Valeur qui est une série d'octets de taille variable qui contient des données pour cette partie du message.

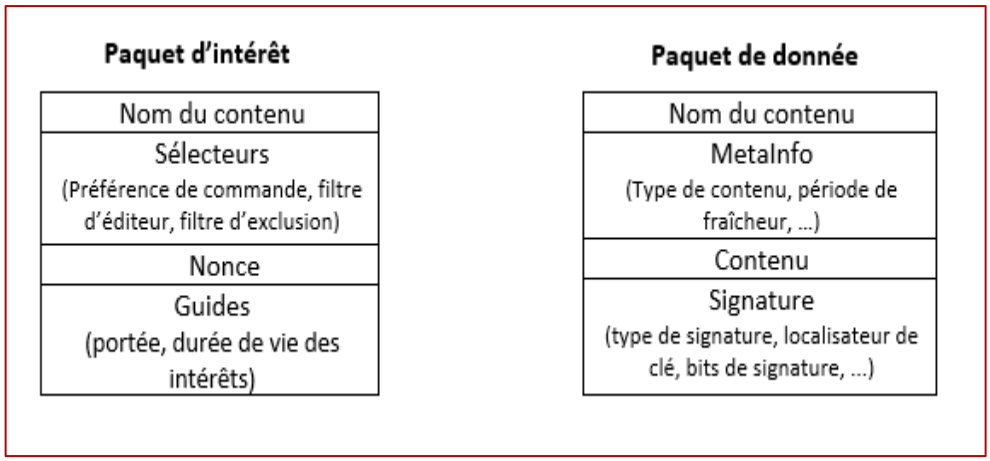


Figure III.2 : *Spécification des paquets NDN [41]*

Les paquets d'intérêt [45], qui permettent d'effectuer une requête, doivent être au minimum composé d'un nom NDN et d'un nonce. Le nonce est un entier de 32 bits qui permet pour un nom donné d'avoir un paquet d'intérêt théoriquement unique. Le principal avantage de cette propriété est d'éviter aux paquets d'intérêt d'effectuer des boucles dans le réseau. Il existe aussi, en plus du nom et du nonce, deux types de champs supplémentaires optionnels : les sélecteurs et les guides. Les sélecteurs permettent de préciser la requête, il en existe six comme illustré dans le tableau III.1, les guides servent à spécifier le comportement des routeurs avec ces paquets ; combien de temps le routeur va garder l'entrée de ce paquet avant de la supprimer.

Nom de sélecteurs	Rôle
MinSuffixComponents	Définir le nombre minimum de nom des composants qui doivent suivre le nom utilisé dans le paquet d'intérêt
MaxSuffixComponents	Définir le nombre maximum de nom des composants qui doivent suivre le nom utilisé dans le paquet d'intérêt
PublisherPublicKeyLocator	Spécifier le nom de la clé qui devra être utilisée pour signer le paquet data, ce qui permet d'une certaine façon de sélectionner le producteur de contenus
Exclude	Exclure une liste de nom des composants qui pourrait suivre le nom du paquet envoyé, ce qui permet d'explorer ou d'éviter certains contenus en particulier ceux partageant un même préfixe
ChildSelector	Spécifier le membre le plus à gauche ou le plus à droite lorsque le nom des composants suivant serait un numéro de version
MustBeFresh	Préciser dans le cas où la réponse à cette requête a déjà été envoyée et est encore présente dans le cache des routeurs si l'on accepte un contenu expiré ou non

Tableau III.1 *: Les types des sélecteurs*

Pour répondre aux paquets d'intérêt, le NDN prévoit un autre type de paquet nommé paquet de données. Celui-ci reprend le même champ de nom NDN pour permettre le routage inverse du contenu au client, les autres champs lui étant propres. Le champ MetaInfo regroupe actuellement trois variables permettant de décrire le contenu comme illustré dans le tableau III.2. Le champ contenu contient les données du contenu et en dernier le champ Signature contient la signature, ainsi que les informations associées à cette signature comme le nom de la clé publique utilisée.

Nom de variables	Rôle
Content Type	Décrit le type de contenus avec quatre valeurs possibles BLOB, LINK, KEY, NACK
Freshness Period	Indique combien de temps, en ms, la donnée et considérée comme valide après réception
Final BlockId	Permet aux utilisateurs de savoir quel est le dernier segment du contenu lorsque le contenu ne peut pas être envoyé en un seul paquet

Tableau III.2 : *Les variables de champs MetaInfo*

III.2.2 Les nœuds NDN

Pour implémenter les fonctions de transfert de l'intérêt et des données, chaque routeur NDN préserve trois structures de données principales qui sont (figure III.3). Magasin de contenu (Content Store, CS), tableau des intérêts en attente (Pending Interest Table, PIT) et transfert de la base d'informations (Forwarding Information Base, FIB), ainsi que de deux règles de recherche : Correspondance de préfixe la plus longue (Longest Prefix Match, LPM) et correspondance exacte (Exact Match, EM)[46].

- FIB : est similaire à la table de transfert conventionnelle en ce qu'elle contient une collection de préfixes et leurs interfaces de saut suivant, mais la différence est que les préfixes sont des préfixes de nom et la recherche est basée sur le nom plutôt que sur l'adresse. Il stocke des informations sur les interfaces du paquet d'intérêt et les transmet en amont au saut suivant en utilisant LPM.
- PIT : garde une trace de tous les paquets d'intérêt jusqu'à ce qu'ils soient satisfaits ou que leur durée de vie soit expirée. Il utilise la méthode de correspondance exacte (EM) pour rechercher les entrées PIT et peut transmettre plusieurs paquets d'intérêt. Lorsqu'un contenu spécifique a plusieurs paquets d'intérêt, le premier paquet d'intérêt est transmis, tandis que tous les autres sont en attente dans PIT et attendent le paquet de données correspondant. Les d'interface entrants des demandes sont également conservés dans PIT de sorte que lorsque les données reviennent, le routeur peut transmettre les données plus en aval aux demandeurs via ces interfaces.
- CS : consiste à optimiser le temps de récupération du contenu, la latence de livraison et à économiser la bande passante. Il est utilisé comme cache temporaire pour les paquets de données car plusieurs utilisateurs peuvent demander le même contenu en conséquence. Par exemple, plusieurs utilisateurs peuvent regarder la même vidéo. CS utilise également la méthode EM pour rechercher des entrées CS.

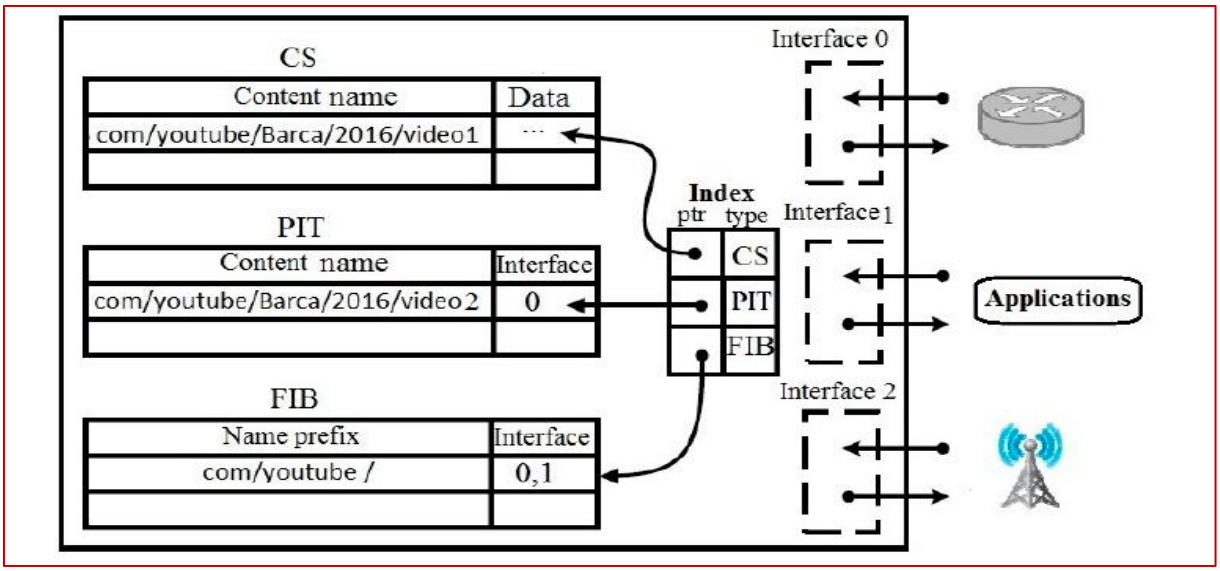


Figure III.3 : *Routeur NDN et ses composants [46]*

III.2.3 Le nommage

Chaque paquet dans NDN est identifié par un nom unique au monde. Le nom du paquet est opaque pour le réseau et dépend de l'application. L'application peut implémenter une méthode de dénomination basée sur ses besoins car elle est indépendante du réseau[47]. Les noms dans NDN sont hiérarchiques (figure III.4) et peuvent être similaires aux URL, par exemple, un nom NDN peut être /aueb.gr/ai/main.html. Cependant, les noms NDN ne sont pas nécessairement des URL : leur première partie n'est pas un nom DNS ou une adresse IP et il n'est pas nécessaire qu'ils soient lisibles par l'homme. Dans NDN, une demande de nom est considérée comme correspondant à toute information dont le nom a le nom demandé comme préfixe, par exemple, /aueb.gr/ai/main.html peut être mis en correspondance par un objet d'information nommé /aueb.gr /ai/main.html/_v1/_s1, ce qui pourrait signifier le premier segment de la première version des données demandées. Alors que la manière dont les objets d'information sont segmentés devrait être connue de l'application de l'abonné, la règle de correspondance de préfixe permet à une application de découvrir ce qui est disponible. En outre, il permet à l'abonné de demander des données qui n'ont pas encore été produites : un producteur peut annoncer qu'il peut répondre aux demandes d'un préfixe spécifique, puis renvoyer des objets d'information avec des noms NDN complets. Cela peut être utilisé pour implémenter diverses applications dans lesquelles les objets d'information sont

générés dynamiquement, par conséquent leurs noms complets ne peuvent pas être connus à l'avance, comme la conférence vocale[4].

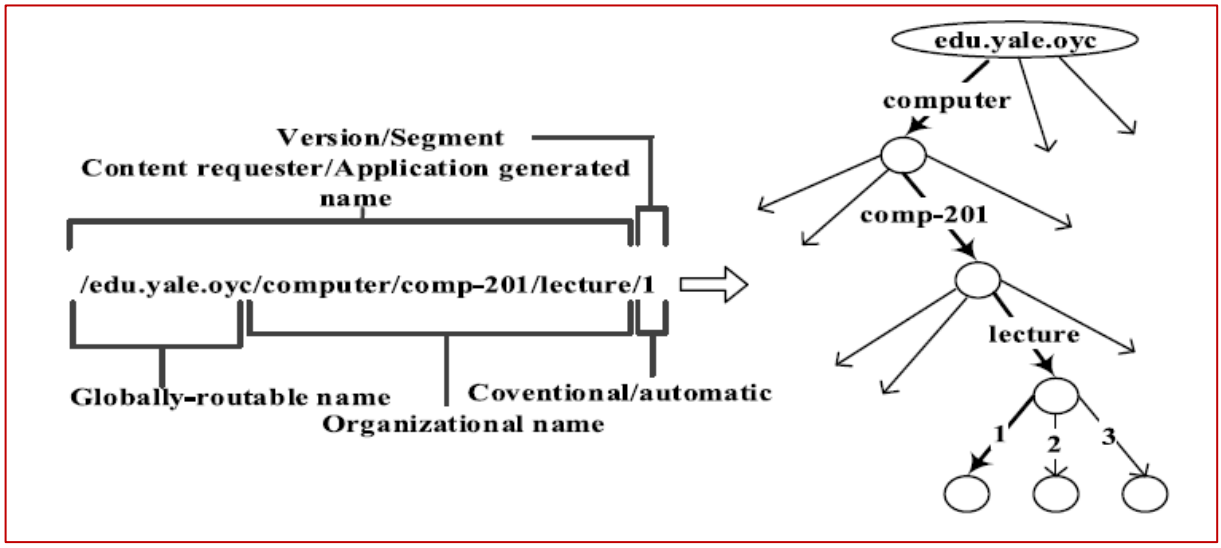


Figure III.4 *: Exemple de nom lisible par l'homme et sa représentation hiérarchique [45]*

III.2.4 La mise en cache

Dans les réseaux NDN [48], un routeur peut stocker les paquets de données reçus dans son CS et les utiliser pour satisfaire les demandes futures. Lors de la réception d'un nouvel intérêt, le routeur vérifie d'abord le CS pour les données correspondantes ; s'il existe, le routeur renvoie les données sur l'interface d'où provient l'intérêt.

La mise en cache du contenu dans CS est analogue à la mémoire tampon des routeurs IP, la différence est que les routeurs IP ne peuvent pas réutiliser les données après leur transmission, tandis que les routeurs NDN peuvent réutiliser les données car elles sont stockées dans les CS et identifiées par des noms persistants. NDN réalise une livraison de données presque optimale pour les fichiers statiques. Même le contenu dynamique peut bénéficier de la mise en cache en cas de multidiffusion, comme la téléconférence en temps réel ou la retransmission après une perte de

paquet. Le CS ne peut pas stocker de paquets de données pendant longtemps, il utilise donc différentes politiques de remplacement telles que LRU[16], FIFO[17], etc.

III.2.5 Le processus de communication

Le processus de communication NDN peut être divisé en deux phases : routage et transfert. Dans la phase de routage, l'accessibilité du contenu est propagée et maintenue via des protocoles de routage. La phase de transfert exploite les différentes tables pour livrer des paquets à partir de consommateur au producteur.

III.2.5.1 Le routage

Dans NDN, le routage est utilisé pour définir la topologie et les politiques et gérer leurs modifications à long terme, ainsi que pour mettre à jour la table de transfert. Le protocole de routage NDN se coordonne avec le plan de transmission NDN pour le classement et le sondage de l'interface[49], [50]. Dans NDN, la seule différence entre le routage et le transfert est que, tandis que le routage décide de la disponibilité des itinéraires, le transfert décide des préférences et de l'utilisation des itinéraires en fonction de leurs performances et état. Les algorithmes de routage d'état de liaison et de vecteur de distance peuvent être utilisé pour le NDN en modifiant les types de messages (intérêt / donnée) et en ajoutant le transfert par trajets multiples[51]. NDN utilise le FIB pour stocker les informations relatives au routage. Il recherche le préfixe de nom dans la FIB pour trouver le ou les sauts suivants et récupère les données, pas nécessairement la copie la plus proche.

III.2.5.2 Le transfert

La stratégie de transfert essaie de choisir la ou les meilleures interfaces pour transférer les paquets en fonction des informations FIB. Les routeurs NDN transfèrent les intérêts en fonction des noms et conservent l'état de transmission pour chaque intérêt en attente. Lorsque les paquets de données arrivent, les routeurs utilisent des noms pour les faire correspondre aux intérêts en

[16] LRU (Least Recently Used) est un algorithme de remplacement de lignes de cache qui remplace la ligne de mémoire cache qui ne sera pas utilisée pour la plus grande période de temps.

[17] FIFO (First In First Out) est un algorithme de remplacement de lignes de cache dont les lignes de la mémoire cache sont effacées dans l'ordre où elles sont arrivées.

attente correspondants et les transferts en conséquence. Par la suite, nous examinons brièvement le processus de transfert de NDN et la façon dont il gère les échecs de liaison.

Dans NDN, seuls les paquets d'intérêt sont routés. Le processus de transmission est résumé comme suit[46] :

Une fois qu'un paquet d'intérêt arrive à une interface du routeur NDN, comme le montre la figure III.5, la procédure suivante est exécutée :

1. Le routeur consulte son CS si le paquet de données souhaité est déjà mis en cache. Si une entrée correspondante est disponible, le paquet de données est envoyé en suivant le chemin inverse du paquet d'intérêt.
2. Si le CS n'a pas d'entrée disponible pour le paquet de données souhaité, alors le routeur recherche le PIT pour trouver une entrée pour le paquet d'intérêt correspondant. Si une entrée correspondante est disponible, l'entrée donnée est agrégée dans la liste des interfaces entrantes dans le PIT.
3. Si aucune entrée ne correspond dans le PIT, le routeur insère une nouvelle entrée pour le paquet d'intérêt dans le PIT et recherche dans la FIB sur la base de LPM pour sélectionner le saut suivant.
4. Si une entrée FIB correspondante est trouvée, l'intérêt est transmis par le module de stratégie de transfert. Sinon, le routeur ne peut pas satisfaire l'intérêt et peut renvoyer un NACK à l'interface entrante de l’intérêt.

Lorsqu'un paquet de données arrive sur le routeur NDN, le routeur exécute la procédure suivante :

1. Le routeur recherche toutes les entrées PIT. S'il existe une entrée correspondante, le routeur transfère le paquet de données aux interfaces liées au PIT et supprime son entrée correspondante dans le PIT. Le paquet de données peut être mis en cache selon la politique de mise en cache du routeur, ce qui peut conduire à la mise à jour du CS.
2. Si aucune entrée correspondante n'existe dans le PIT (pour des raisons de durée de vie ou pour d'autres raisons), le paquet de données est supprimé.

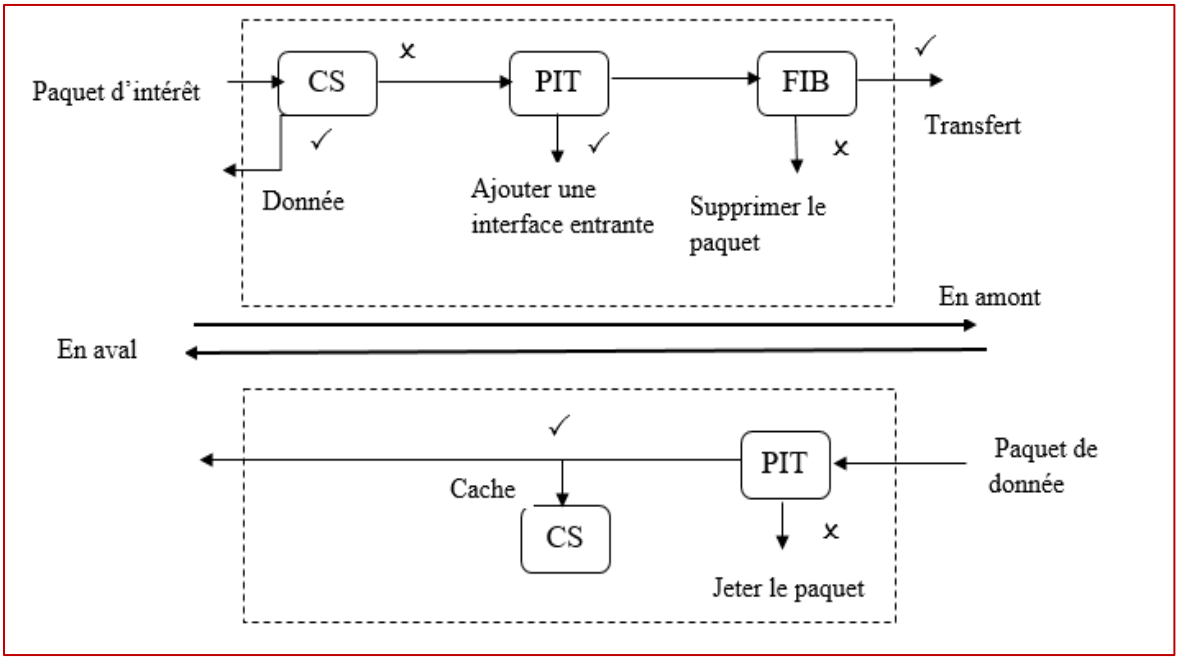


Figure III.5 : *Processus de transfert sur le routeur NDN [45]*

III.2.6 La sécurité

Le NDN sécurise les données elles-mêmes, c'est-à-dire que le contenu est sécurisé au lieu du canal et de la connexion (comme dans l'architecture IP), de sorte que les producteurs sécurisent le contenu en signant cryptographiquement avec sa clé secrète chaque élément de données, ce qui garantit l'intégrité des données et l'authenticité. Par conséquent, les consommateurs peuvent déterminer facilement la provenance des données, ce qui leur permet d'être indépendants de l'endroit et de la façon dont les données sont obtenues [48].

III.2.7 La mobilité

La nature centrée sur les données du NDN fait passer le problème de mobilité de la livraison de paquets à un Nœud Mobile NM à la récupération des données produites par un NM. Étant donné le flux bidirectionnel d'intérêt / de paquets de données dans le NDN, la mobilité du NDN peut être divisée en deux sous-problèmes : comment les données demandées peuvent être retournées à un consommateur en mouvement (mobilité du consommateur) et comment les consommateurs peuvent atteindre les données générées par les producteurs en mouvement (mobilité des producteurs).

III.2.7.1 La mobilité des consommateurs

Pour récupérer les données souhaitées, les consommateurs NDN expriment leur intérêt pour le réseau NDN. Étant donné que les paquets de données sont renvoyés en traçant le chemin d'intérêt vers le consommateur, l'architecture NDN fournit la prise en charge intégrée de la mobilité des consommateurs. Lorsque le consommateur se déplace pendant que le réseau récupère les données demandées, le consommateur peut réexprimer ses intérêts en attente ou expirés pour mettre à jour ou recréer le chemin inverse vers son emplacement actuel. Si l'ancien et le nouveau chemin se croisent, les intérêts réexprimés récupèrent les données précédemment demandées à partir du cache d'un routeur ou sont combinés avec l'intérêt précédent sans se propager davantage[52].

III.2.7.2 La mobilité des producteurs

Le problème de mobilité du producteur NDN peut sembler similaire à la mobilité IP. Il y a cependant une différence conceptuelle : le NDN concerne la récupération de données et non la livraison de paquets à un nœud mobile. Par conséquent, l'accompagnement de la mobilité des producteurs consiste à faire des rendez-vous d'intérêts avec les données générées par un Producteur Mobile (PM).

Dans le tableau ci-dessous, nous passons les solutions de mobilité des producteurs proposées ces dernières années. Il existe deux approches de PM-poursuite (cartographie et traçage) et deux approches de rendez-vous de données (dépôt de données et point de données)[52].

Poursuite des producteurs mobiles (PM)	
Cartographie	Avec l'utilisation de rendez-vous (RV) stables pour suivre les PM. Le PM rapporte au RV le mappage du nom de donnée à son Point d'Attache actuel (PoA) par lequel ses données peuvent être récupérées
Tracé	Le PM crée un « fil d'Ariane » du RV vers lui-même, que les intérêts peuvent suivre
Données de rendez-vous	
Dépôt de données	Le PM déplace ses données vers un dépôt stationnaire connu
Spot de données	Les données sont produites dans une région stationnaire par n'importe quel PM de cette région

Tableau III.3 : Les approches de mobilité des producteurs NDN [52]

III.3 Les stratégies de transfert des données nommées dans les réseaux ad hoc sans fil

Les réseaux mobiles ad hoc (MANET) sont des réseaux multi-saut auto-organisés qui prennent en charge l'échange d'informations sans s'appuyer sur une infrastructure réseau préexistante. La recherche sur les stratégies de transmission MANET en est à leurs débuts. Les MANET présentent de nombreux défis qui n'existent pas dans les réseaux câblés. Les stratégies de transmission doivent prendre en compte la nature du canal sans fil et la transmission des paquets en évitant les collisions et en gérant la topologie dynamique.

La stratégie de transfert dans NDN décide comment utiliser efficacement plusieurs options de transfert et choisir la meilleure interface pour transférer le paquet d'intérêt. La conception d'une stratégie de transfert dépend de l'environnement et du contexte du réseau. Cette section traite des stratégies de transfert qui sont (ou pourraient être) mise en place sur NDN et que nous appelons tout simplement « *stratégies de transfert MANET-NDN* » illustrée dans la figure suivante :

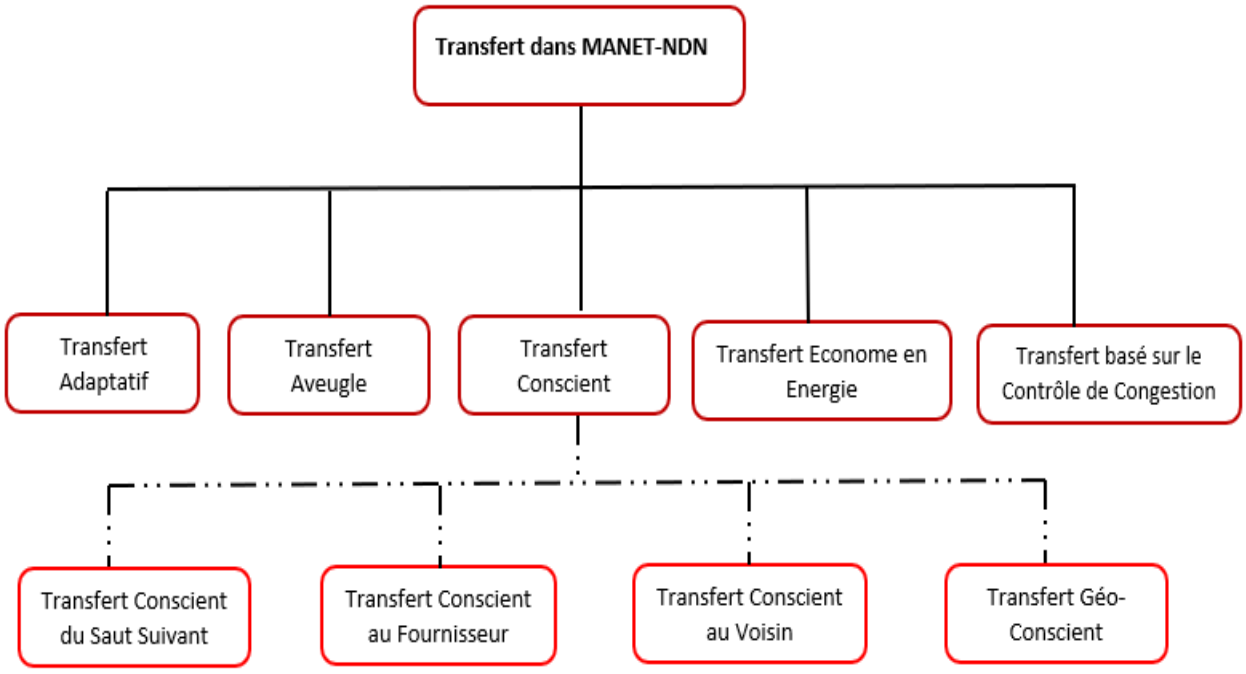


Figure III.6 : *Stratégies de transfert dans les MANET-NDN [53]*

Les stratégies de transfert pour les MANET-NDN sont classées en cinq catégories[53] :

- Transfert adaptatif (Adaptive Forwarding)
- Transfert aveugle (Blind Forwarding)
- Transfert conscient (Aware Forwarding)
- Transfert économe en énergie (Energy Efficient Forwarding)
- Transfert basé sur le contrôle de congestion (Congestion Control Forwarding)

III.3.1 Le transfert adaptatif

Le transfert adaptatif garantit la récupération des paquets de données via le meilleur chemin possible et met également l'accent sur les performances. Il détecte tout problème possible, comme la congestion, pendant le processus de transfert. Un champ NACK est introduit dans cette stratégie. NACK retournera aux nœuds en aval en cas de problème de transmission avec le même nom que celui du paquet d'intérêt, avec un code d'erreur expliquant la raison de la génération de NACK (congestion, pas de donnée, dupliquer). PIT maintient un état de transmission de datagrammes et crée une entrée pour chaque nom avec des interfaces entrantes. L'entrée FIB contient une liste classée de plusieurs interfaces et des informations de routage des décisions de transfert adaptatif. Un schéma de coloration simple est utilisé dans ce transfert adaptatif. Lorsqu'une nouvelle entrée FIB est créée, l'état de l'interface devient jaune, il devient vert si les données reviennent actuellement à partir de cette interface, si le temps RTT expire avec intérêt en attente, il devient jaune ; et il devient rouge si NACK est reçu en cas d'échec. L'entrée FIB est classée pour sélectionner la stratégie de transfert en fonction de la situation. En cas d'absence d'entrée PIT pour un intérêt nouvellement arrivé, le routeur crée une nouvelle entrée PIT et transfère l'intérêt en utilisant l'interface verte disponible la mieux classée pour le préfixe de nom, sinon l'interface jaune est utilisée. Dans d'autres cas, si l'intérêt correspond à PIT mais que nonce ne correspond pas, alors l'intérêt est considéré comme une retransmission. Le routeur de transfert explore d'autres interfaces chaque fois qu'un NACK est reçu jusqu'à ce qu'il réussisse ou jusqu'à l'expiration du temporisateur, ce qui se met ensuite à explorer une voie alternative.

Un exemple de cette stratégie est Probability aware forwarding (PAF) [54] qui utilise l'optimisation de colonies des fourmis (Ant Colony) dans le contexte de NDN. Une interface est sélectionnée de manière probabiliste pour transmettre le paquet intérêt et donnée utilisés pour

sonder les performances des interfaces (par exemple, retard). Cette méthode permet de minimiser les retards et d'équilibrer automatiquement la charge. Un modèle statistique est utilisé pour la transmission de paquets qui a changé de manière adaptative en fonction des conditions du réseau.

III.3.2 Le transfert aveugle

L'inondation est le moyen le plus simple et le plus facile d'envoyer le paquet intérêt dans un schéma sans fil. Les inondations aident à partager le contenu du réseau. En cas d'inondation, un nœud peut inspecter les données d'un paquet d'intérêt entrant à partir de n'importe quel nœud sans aucune demande explicite, ce qui entraîne un nombre moindre de transmissions. Pour se débarrasser de la tempête diffusée, les inondations doivent être gérées très soigneusement. Des mécanismes et des techniques de développement de paquets distribués sont présents dans la littérature pour contrôler les collisions de paquets et la redondance.

Nous citons la stratégie timer-based packet suppression [55] pour l'amélioration des performances de livraison de paquets. L'idée de cette technique est de supprimer le même paquet entendu dans le canal.

L'inondation aveugle n'a pas confirmé qu'il n'y avait pas de collision de paquets ou de redondance de paquets. Ce type de transfert crée un problème de tempête de diffusion (Broadcast Storm) sous contrôle. Cependant, la collision de paquets est toujours un problème qui ne peut pas être traité dans le transfert aveugle. Des techniques de transfert conscientes sont utilisées pour éviter ces problèmes[53].

III.3.3 Le transfert conscient

La transmission consciente peut être classée de différentes manières. La catégorisation suivante dépend du prochain saut, du voisin, de l'emplacement et de la distance [53] :

- Transfert conscient du saut suivant.
- Transfert conscient au fournisseur.
- Transfert conscient au voisin.
- Transfert géo-conscient.

III.3.3.1 Transfert conscient du saut suivant

Le consommateur diffuse l'intérêt dans la transmission sélective en direction de ses voisins d'un saut[56], et le nœud le plus éloigné est sélectionné comme nœud relais dans chaque quadrant. Deux paquets additifs (CMD, ACK) sont échangés saut par saut entre l'expéditeur et les nœuds qui sont des redirecteurs intermédiaires et leurs voisins.

L'algorithme Greedy Ant Colony Forwarding (GACF) [57] utilise deux types de fourmis pour progresser dans l'optimisation du routage et du transfert. Les fourmis d'intérêts et de données sont les paquets utilisés. Deux types de paquets sont utilisés pour collecter les informations de transfert et de routage à la réception des données : les paquets normaux, produits par le consommateur, et paquets Hello, produits par le routeur. Les paquets Hello sont responsables de l'optimisation et du routage du chemin pour les paquets normaux. La sélection du prochain saut est effectuée par les fourmis, en utilisant l'approche gourmande. Le saut suivant est sélectionné de manière probabiliste par une fourmi Hello, ce qui signifie que l'état actuel du réseau est mis à jour et que de nouveaux chemins peuvent être trouvés. GACF est un algorithme de transfert prenant en charge la qualité de service qui réduit l'influence de l'encombrement du réseau et de la défaillance de la liaison.

III.3.3.2 Transfert conscient au fournisseur

Le transfert conscient au fournisseur est principalement basé sur les techniques de transmission sensibles à la distance. Si un consommateur obtient du contenu à partir de plusieurs sources, la sélection est basée sur le meilleur fournisseur de performances. Le mécanisme consiste à envoyer une commande d'autorisation à un fournisseur au cas où il y aurait plus d'un fournisseur. Après réception de l'autorisation commande, le fournisseur envoie une réponse au consommateur. Le consommateur répondre à un meilleur fournisseur, si les réponses proviennent de plus d'une source.

Listen first broadcast later (LFBL) [58] est une stratégie de transfert qui a été conçue à l'origine pour les réseaux sans fil multi hop avec adressage centré sur les données, il est indépendant de la topologie, les changements fréquents cette dernière n'affectent pas les performances car il support la mobilité physique des nœuds et logique des données au niveau de l'application. Le fonctionnement de base de LFBL est simple. À chaque saut, la responsabilité des décisions de transfert est placée carrément entre les mains du destinataire plutôt que de l'expéditeur.

Après avoir reçu un paquet, un redirecteur potentiel s'arrête pour écouter le canal, attendant de voir si un nœud plus optimal transfère le paquet en premier. S'il n'entend pas une telle transmission, il transfère le paquet lui-même. La seule structure de données requise par cette stratégie est DT (Table de distance) qui conserve les informations de distance entre les nœuds terminaux et chaque nœud participant à la communication. Trois types de paquets, REQ, REP et ACK sont exploités par le LFBL. La demande de contenu (REQ) est utilisée comme paquet d'intérêt tandis que la réponse de contenu (REP) est utilisée comme paquet de données. La sélection du fournisseur est confirmée par le champ d'accusé de réception (ACK). Dans LFBL un nœud demandeur inonde REQ, tous les nœuds qui contiennent ces données demandées envoient le REP qui transmit au demandeur à l'aide des informations collectées par les nœuds intermédiaires pendant le transfert. Enfin, le demandeur envoie ACK en tant que rétroaction pour encourager ou décourager ces réponses.

III.3.3.3 Transfert conscient au voisin

Le Transfert conscient au voisin [59] est un mécanisme de propagation adaptatif qui maintient la robustesse et réduit les frais généraux des inondations. Toutes les transmissions sont diffusées. Les problèmes de congestion et de collision peuvent être créés si les expéditeurs sont masqués les uns des autres et envoient des paquets identiques. Le transfert contrôle la transmission et contrôle également le taux de transfert. Si un nœud entend les nœuds voisins envoyer des paquets de données correspondant aux paquets d'intérêt qu'il a abandonnés, il réduira son débit de transmission. Il y a une augmentation du taux de transmission si un nœud détecte qu'il a perdu trop de paquets intérêt. De cette façon, les collisions et les encombrements peuvent être traités.

TOP-CCN[60] est une stratégie de transfert consciente du voisin du voisin qui est conçue pour faire face au problème de la tempête de diffusion (Broadcast Storm) et pour améliorer la stabilité de la livraison de contenu dans MANET. Un paquet d'annonce de contenu (CA) est périodiquement diffusé par chaque nœud dans TOP-CCN qui contient les informations de préfixe du voisin et de l'expéditeur. Pour améliorer la précision des informations d'interface, chaque nœud met occasionnellement à jour sa table FIB, y compris les informations de voisinage à 1 et 2 sauts. Il existe trois champs étendus dans les paquets intérêts et données de TOP-CCN. Un champ ID qui représente l'ID unique du consommateur et de l'expéditeur ainsi que la distance entre le consommateur et le fournisseur est stocké dans le saut attendu, et le nombre de sauts conserve le

nombre de sauts parcourus par les paquets. Le saut attendu est également mis à jour par le nœud de relais et l'expéditeur pour réduire la plage d'inondation. Deux tables sont définies dans TOP-CCN, voisin à 1 saut et voisin à 2 sauts pour garantir livraison et découverte de contenu stables. Les paquets sont inondés pour la livraison de contenu et les demandes à l'aide de FIB et PIT. Grâce à l'inondation limitée des paquets d'intérêts et des paquets de contenu, les performances de TOP-CCN sont réduites à l'aide de l'algorithme de contrôle de la plage d'inondation. TOP-CCN offre l'avantage de disponibilité du contenu la plus élevée.

III.3.3.4 Transfert géo-conscient

Un schéma de transfert sélectif de la direction[56] proposé pour le transfert de paquets, dans lequel un expéditeur décide de la stratégie de transfert. Le nœud émetteur divise le plan en quatre quadrants égaux, puis transmet l'intérêt à l'un des nœuds voisins. Avant d'envoyer un ACK, les nœuds voisins vérifient toutes les demandes en double et lors de l'envoi de l'ACK, faites le compte de duplication et renvoyez la donnée ACK à l'expéditeur de la même manière.

Location-aware On-demand Multipath Caching and Forwarding (LOMCF)[61] est une stratégie de transfert proposée pour MANET basés sur NDN. Le LOMCF est un mécanisme de transmission réactive qui tient compte de l'emplacement du nœud dans le processus de transfert de paquets. Le temps de récupération du contenu est atténué et la fiabilité des paquets augmentés par le LOMCF en utilisant les techniques de transfert par trajets multiples. Une politique de mise en cache est également incluse dans ce schéma qui réduit la duplication des paquets en utilisant matrices de distance. Le nœud transmettra le paquet vers le producteur ou le consommateur uniquement s'il se trouve à une distance inférieure d'eux. Cela réduira l'impact d'inondation des paquets inutiles. L'énergie restante du nœud est également considérée pour améliorer les performances de l'ensemble du réseau. La transmission basée sur la minuterie dans LOMCF réduit la probabilité de collision de paquets.

III.3.4 Transfert économie en énergie

Dans MANET, les entités participant à la communication sont contraintes en énergie comme les ordinateurs portables et les téléphones portables. Dans les stratégies de transmission éco énergétiques, il existe des mécanismes pour réduire la consommation d'énergie des nœuds participants qui améliorent l'efficacité du réseau.

Robust and Efficient Multipath Interest Forwarding REMIF[62] est un nouveau schéma proposé pour MANET basés sur NDN. REMIF, en réduisant l'inondation des paquets d'intérêt, augmente l'efficacité du réseau. L'énergie résiduelle des nœuds NDN actifs est également prise en compte dans ce schéma et le mécanisme de retransmission des messages intérêt repose sur l'état énergétique des nœuds. Selon le mécanisme de REMIF, un expéditeur envoie un paquet intérêt avec le nom du contenu. Après avoir reçu l'intérêt, le nœud récepteur identifie d'abord si le paquet est expiré ou répliqué. Le paquet est abandonné s'il s'agit d'un paquet intérêt expiré ou répliqué. Si ce n'est pas le cas, il inspecte en outre le CS pour la disponibilité des données et le délai du nœud pour reporter le temps si les données sont trouvées. Il supprimera la transmission s'il reçoit les mêmes données en retour dans ce délai. Sinon, il renvoie le paquet donné au nœud consommateur. Après vérification des entrées CS et PIT, si aucune entrée n'est trouvée dans ces dernières tables, le nœud NDN relais examine l'énergie du message avec un seuil de 13%. Une énergie inférieure à cette valeur entraîne une mise à jour du PIT la structure des données et la fin de la transmission, tandis que l'énergie au-dessus du seuil conduit le nœud à écouter le canal pendant un temps de retard.

III.3.5 Transfert basé sur le contrôle de congestion

Dans NDN, le contrôle de l'encombrement peut être géré par des nœuds intermédiaires, car chaque nœud intermédiaire maintient une table de paquets avec accusé de réception. Ainsi, le nœud contrôle lui-même le problème de congestion[63]. Dans le mécanisme de contrôle d'encombrement basé sur le récepteur, l'encombrement peut être contrôlé par le contrôle du débit de donnée à l'extrémité du récepteur en limitant le débit d'envoi. Le mode récepteur de NDN permet d'obtenir ce contrôle.

Le mécanisme HOp-By-Hop Interest Shaping HoBHIS[64] est un schéma de contrôle de la congestion ou nœud intermédiaire maintient le taux de transfert et détecte la congestion en limitant et en contrôlant le taux de transfert. HoBHIS contrôle le taux de transfert en fonction de la longueur de file d'attente des blocs. Le contrôle d'encombrement bond par bond a fait une direction de recherche très prometteuse, car elle s'adapte aux fonctionnalités multi-sources et sans connexion du transport du réseau NDN.

III.3.6 Comparaison et discussion

Le tableau suivant résume les différents algorithmes des stratégies MANET-NDN ainsi que leurs points forts et faibles :

- Le transfert adaptatif malgré ses points fort mais il se base sur une communication bout en bout qui ne garantit pas la communication dans une zone catastrophique.
- Le transfert économe en énergie, comme son nom indique, économise l'énergie des nœuds qui est très bénéfique pour les smartphones, néanmoins la latence est très élevée alors la réponse aux catastrophes nécessite une latence courte pour sauver les vies.
- Le transfert basé sur le contrôle de congestion est une solution non évolutive limité ce qui n'est pas bien pour notre réseau.
- En revanche, le transfert aveugle garantit la communication opportuniste par le principe de diffusion sauf que ce dernier hérite tous les problèmes de diffusion qui sont résolu par le transfert conscient via ses différents algorithmes. Le principe LFBL (Ecouter Avant et Diffuser Ensuite) semble être la meilleure solution pour assurer la communication opportuniste et garantir les différents types de mobilité (physique et logique). C'est pour cela, nous avons opté pour le principe de LFBL dans notre solution.

Stratégie de transfert		Exemple des Algorithmes	Points forts	Points faibles
Transfert adaptatif		PAF [54]	-Augmenter la disponibilité des données. -Minimiser les retards.	-Echec de liaison. -Détournement de préfixe (Hijacking).
Transfert aveugle		Timer-Based Packet Suppression [55]	-Le moyen le plus simple et le plus facile d'envoyer des intérêts.	-Broadcast Storm. -La collision de paquets. -La redondance des paquets.
Transfert conscient	**Du saut suivant.**	GACF [57]	-Réduire la congestion et l'échec de liaison. -Optimiser la QoS.	-Surcharge du réseau est augmentée en raison de l'utilisation des messages supplémentaires.
	Au fournisseur.	LFBL [58]	-Offrir une mobilité fluide.	-Ne prend pas en compte l'énergie restante des nœuds pendant la communication.
	Au voisin.	TOP-CCN [60]	-Absence de Broadcast Storm, contrôle de la congestion.	-Ne prend pas en compte l'énergie restante des nœuds pendant la communication.
	Géo-conscient.	LOMCF [61]	-Réduire les collisions de paquets.	-La récupération des données échoue si le fournisseur potentiel est inaccessible.
Transfert économe en énergie		REMIF [62]	-Prise en charge l'état énergétique des nœuds.	-Mauvaise latence
Transfert basé sur le contrôle de congestion		HoBHIS [64]	-Éviter la congestion	-Shema non scalable.

Tableau III.4 : *Tableau comparative des stratégies MANET-NDN*

III.4 Conclusion

Dans ce chapitre, nous avons décrit les différents concepts de base de NDN, ensuite nous avons fourni une taxonomie des stratégies de transfert NDN basé sur MANET existantes dans la littérature avec des exemples de chaque stratégie dont nous avons choisi le principe de LFBL pour notre solution.

Dans le chapitre suivant, nous présenterons la conception détaillée de notre solution.

Chapitre IV : Conception de la Solution Proposée

IV.1 Introduction

Avant mise en place de notre solution, une conception de système proposé s'impose. Nous commençons par une description générale de notre solution. Ensuite, nous expliquons le processus de communication basé sur le principe LFBL sous MANET-NDN. Enfin, nous détaillons par une étude conceptuelle de notre application.

IV.2 Description de la solution proposée

La figure IV.1 décrit l'architecture de système proposé (que nous appelons « SOS Application ») ainsi que les interactions entre ses différentes entités.

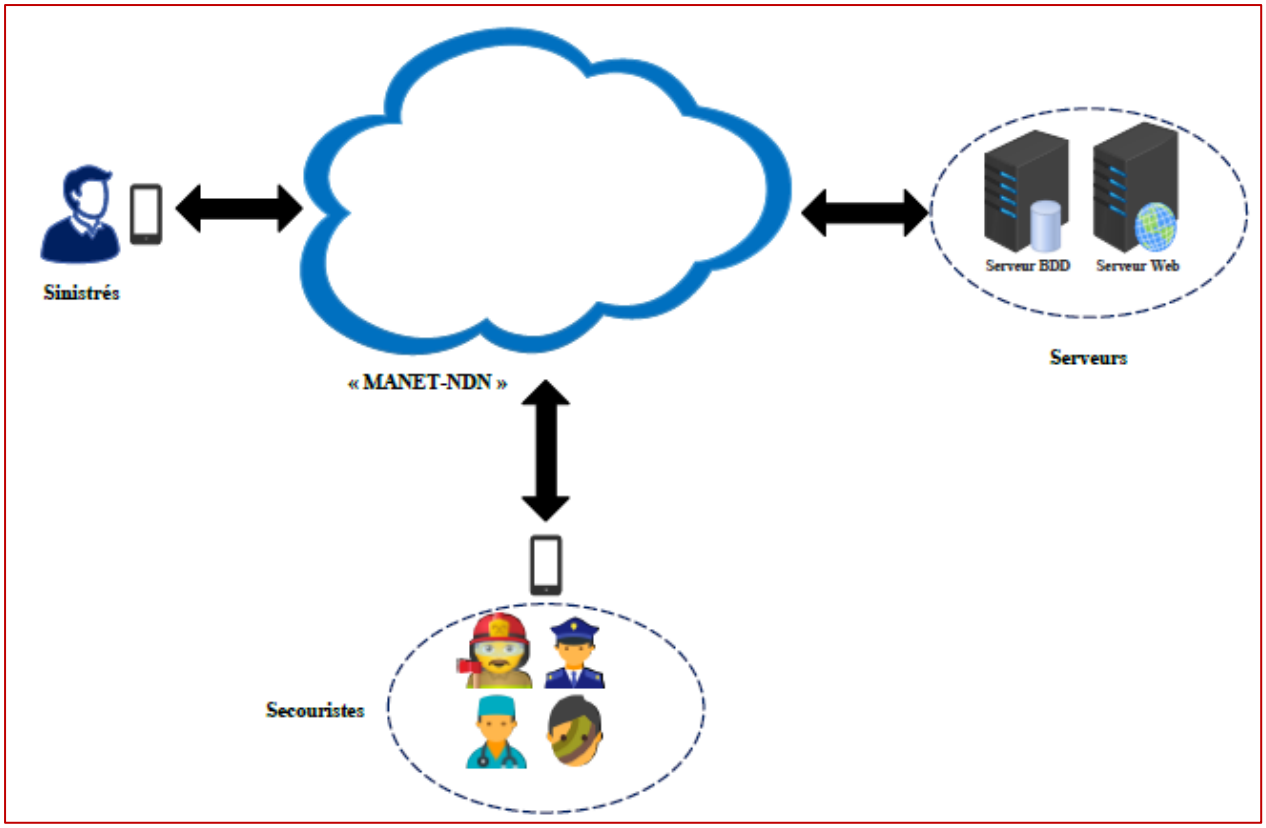


Figure IV.1 : *Architecture de système proposé*

Le système est constitué des entités suivantes :

- Un ensemble d'utilisateurs (sinistrés, secouristes).
- Des appareils mobiles qui héberge l'application mobile.
- Un serveur base de données qui fournit un service de stockage des données.
- Un serveur web qui fournit le service GPS et les données en temps réels.
- Un réseau ad hoc de communication nommé donné ou tout simplement MANET-NDN.

Lors d'un séisme, le sinistré accède à « SOS Application » afin d'envoyer un message de secours et de bénéficier des autres services offerts. Les secouristes inscrits peuvent répondre aux appels de secours et se déplacer pour aider le sinistré. La communication se fait à l'aide d'un réseau ad hoc mobile MANET sur NDN via le biais de la stratégie de transfert EADE-NDN expliqué en détails au niveau de la section suivante.

IV.3 Processus de communication

Dans le contexte de ce projet, nous proposons une stratégie de transfert pour les réseaux sans fil MANET sous le réseau NDN, que nous appelons EADE-NDN « Ecouter Avant et Diffuser Ensuite » basé sur le principe de stratégie LFBL (décrite dans la section III.3.3.2).

La communication dans EADE-NDN se compose de deux phases : une phase de demande et une phase de données.

La phase de demande où le consommateur (sinistré) envoie un paquet d'intérêt qui est diffusé à travers le réseau. Une fois qu'un paquet d'intérêt arrive à un nœud, comme le montre la figure IV.2, la procédure suivante est exécutée :

a. Le nœud consulte son CS pour savoir si le paquet de données souhaité est déjà mis en cache. Si « oui » (i.e. une entrée correspondante dans CS est disponible), le paquet de données est envoyé en suivant le chemin inverse du paquet d'intérêt.

b. Si « non » (i.e. le CS n'a pas d'entrée disponible pour le paquet de données souhaité), alors le paquet d'intérêt sera inséré dans une file d'attente des intérêts et le nœud passe par une étape d'attente en écoutant le canal pour voir si un autre nœud transfère le paquet lui-même.

Si un des nœuds voisins transmet le même paquet d'intérêt alors ce paquet sera supprimé pour réduire le phénomène de tempête de diffusion (Broadcast Storm).

c. Dans le cas contraire, où le temps d'écoute s'écoule sans que d'autres nœuds voisins transmet le même paquet d'intérêt, alors le nœud recherche dans le PIT le paquet d'intérêt correspondant. Si une entrée correspondante est disponible, l'entrée donnée est agrégée dans la liste des interfaces entrantes dans le PIT.

d. Si aucune entrée ne correspond dans le PIT, le nœud insère une nouvelle entrée pour le paquet d'intérêt dans le PIT et diffuse ce paquet.

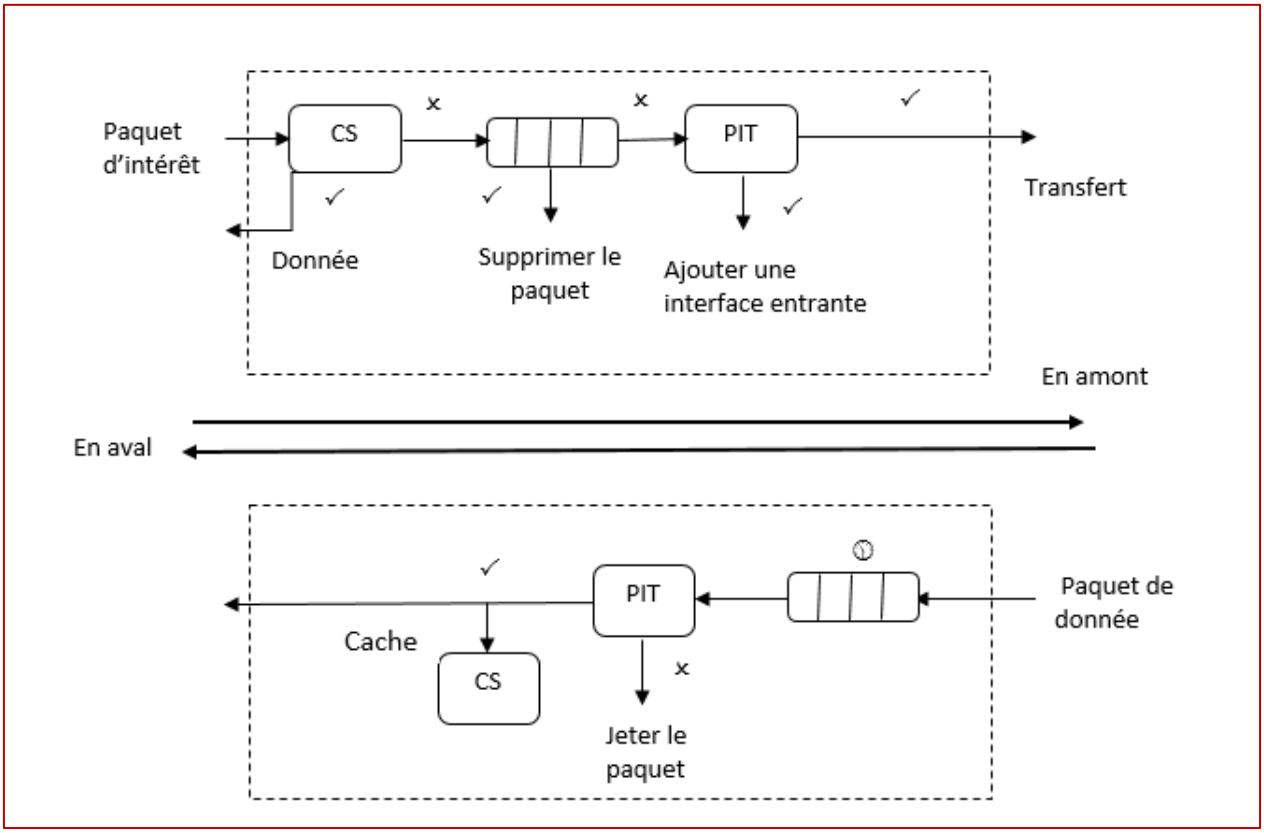


Figure IV.2 : *Processus de transfert dans EADE-NDN*

La phase de données commence lorsqu'une source potentielle pour les données demandées reçoit un intérêt. Dans cette phase, le nœud exécute la procédure suivante :

a. Le nœud insère la donnée dans la file d'attente de données et passe à l'étape d'attente en écoutant le canal pour éviter la collision si un des nœuds voisins transmet un paquet de données.

b. Après l'expiration de temps d'attente, le nœud recherche toutes les entrées PIT. S'il existe une entrée correspondante, le nœud transfère le paquet de donnée aux interfaces liées au PIT et supprime son entrée correspondante dans le PIT. Le paquet de donnée peut être mis en cache selon la politique de mise en cache du nœud, ce qui peut conduire à la mise à jour du CS.

c. Si aucune entrée correspondante n'existe dans le PIT (pour des raisons de durée de vie ou pour d'autres raisons), le paquet de donnée est supprimé.

La phase de données se poursuit jusqu'à ce que le consommateur cesse d'envoyer des intérêts ou ne reçoive plus de réponses à ses intérêts. Dans ce dernier cas, le demandeur revient à la phase de demande.

La diffusion avec un temps d'écoute est la pyramide de notre stratégie, puisqu'il y aura généralement plus d'un fournisseur de donné pour chaque transmission. Avant le transfert, chaque nœud choisit un certain temps aléatoire pour attendre et écouter le canal dans le but de voir si d'autres nœuds effectuent la tâche de transfert. Cette durée est appelée période d'écoute du nœud. Elle permet de réaliser le principe « d'Ecouter Avant et Diffuser Ensuite ou Listen First Broadcast Later » qui sert à minimiser les collisions et le Broadcast Storm en réduisant les chances que deux nœuds transmettent simultanément et provoquent une collision.

IV.4 Etude Conceptuelle de notre application mobile

La réalisation de notre application de gestion des urgences doit être précédée d'une conception dans le but de formaliser les étapes de son développement. Pour cela, nous allons utiliser le langage UML afin de présenter l'ensemble des besoins et des exigences.

IV.4.1 Diagramme de cas d'utilisation

Un diagramme de cas d'utilisation permet de décrire et illustrer l'interaction et les liens entre les acteurs et les différents cas d'utilisations.

- **Un acteur** : est une entité ayant un comportement comme une personne, une entreprise ou un système, qui interagit avec les cas d'utilisations de système.
- **Cas d'utilisation** : représente un ensemble d'actions à réaliser par le système du point de vue d'utilisateur.

Dans le cas de notre système, nous pouvons distinguer les acteurs suivants :

- **Administrateur :** qui administre l'application.
- **Sinistré :** qui demande l'aide.
- **Secouriste :** qui fournit l'aide.

Le diagramme global suivant (figure IV.3) regroupe toutes les fonctionnalités établies par les utilisateurs de l'application mobile. Il est suivi d'une description détaillée des chacune d'elle (tableau IV.1).

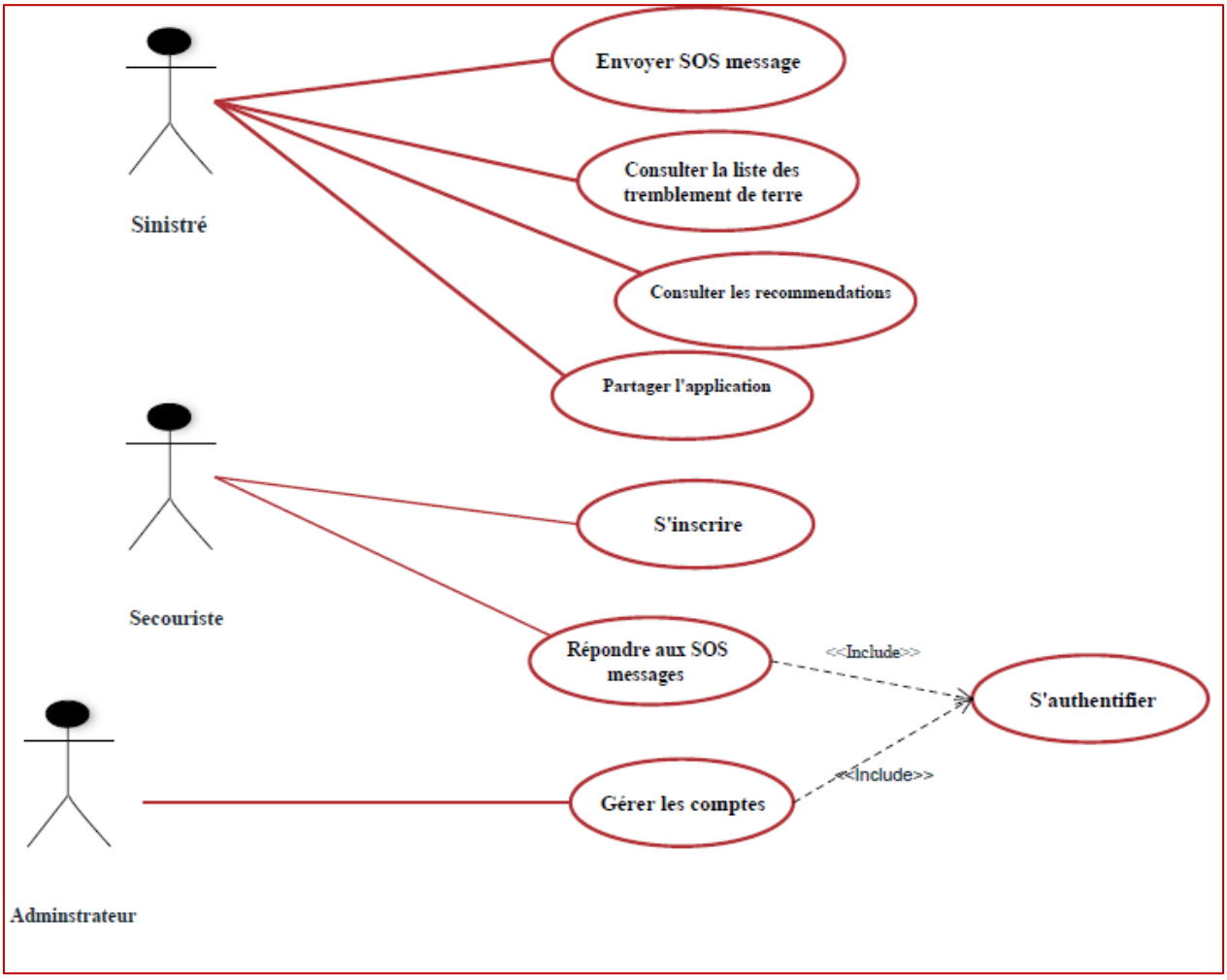


Figure IV.3 : Diagramme de cas d'utilisation globale

Cas d'utilisation	Acteur	Description du cas d'utilisation
Envoyer un message SOS	Sinistré	Chaque utilisateur peut envoyer un message SOS.
Consulter la liste des tremblements de terres	Sinistré	Permet de voir les derniers séismes selon leurs degrés, la date et la localisation.
Consulter des recommandations	Sinistré	Permet de savoir quoi faire avant, pendant et après un tremblement de terre.
Partager d'application	Sinistré	Permet de partager l'applications avec l'entourage.
S'inscrire	Secouriste	Permet au secouriste de s'inscrire au système à partir d'un formulaire.
Répondre aux messages SOS	Secouriste	Permet au secouriste de répondre aux messages SOS.
S'authentifier	Secouriste Administrateur	Authentification est obligatoire pour accéder aux messages SOS et les gérer.
Gérer les comptes	Administrateur	Permet d'ajouter, supprimer un compte.

***Tableau IV.1** : Description des cas d'utilisation du diagramme globale*

IV.4.2 Diagramme de séquence

Nous allons décrire le fonctionnement de notre système à l'aide du diagramme de séquence qui permet de représenter la succession chronologique des opérations réalisées par un acteur et qui font passer d'un objet à un autre pour représenter un scénario.

Dans ce qui suit nous allons décrire les principaux scénarios ainsi que leurs représentations par les diagrammes de séquences.

Le diagramme de séquence suivant représente les interactions qui permettre à un sinistré d'envoyer un message SOS.

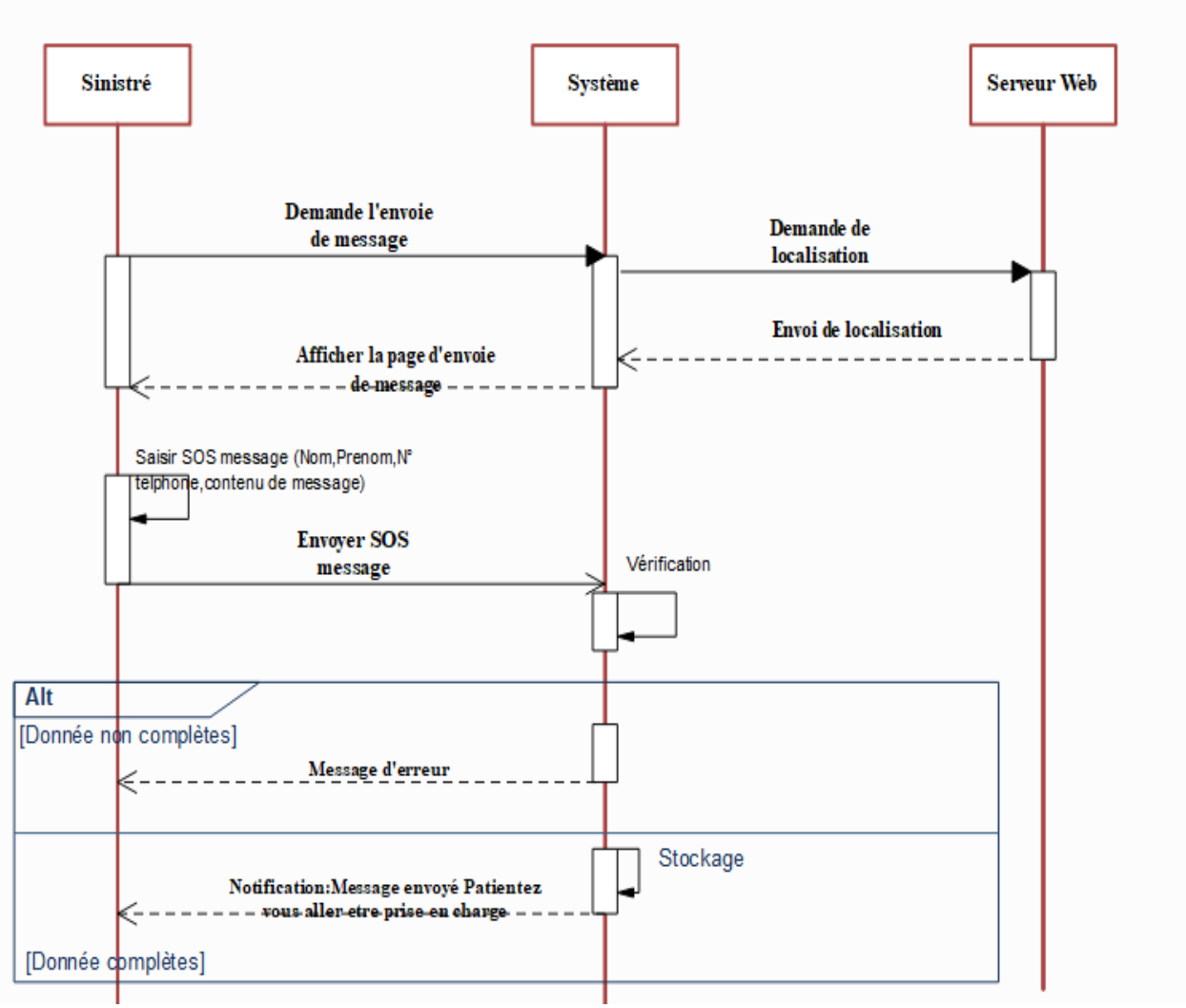


Figure IV.4 : Diagramme de séquence « Envoyer SOS message »

Le diagramme de séquence suivant représente les interactions qui permettre à un secouriste de répondre aux messages SOS.

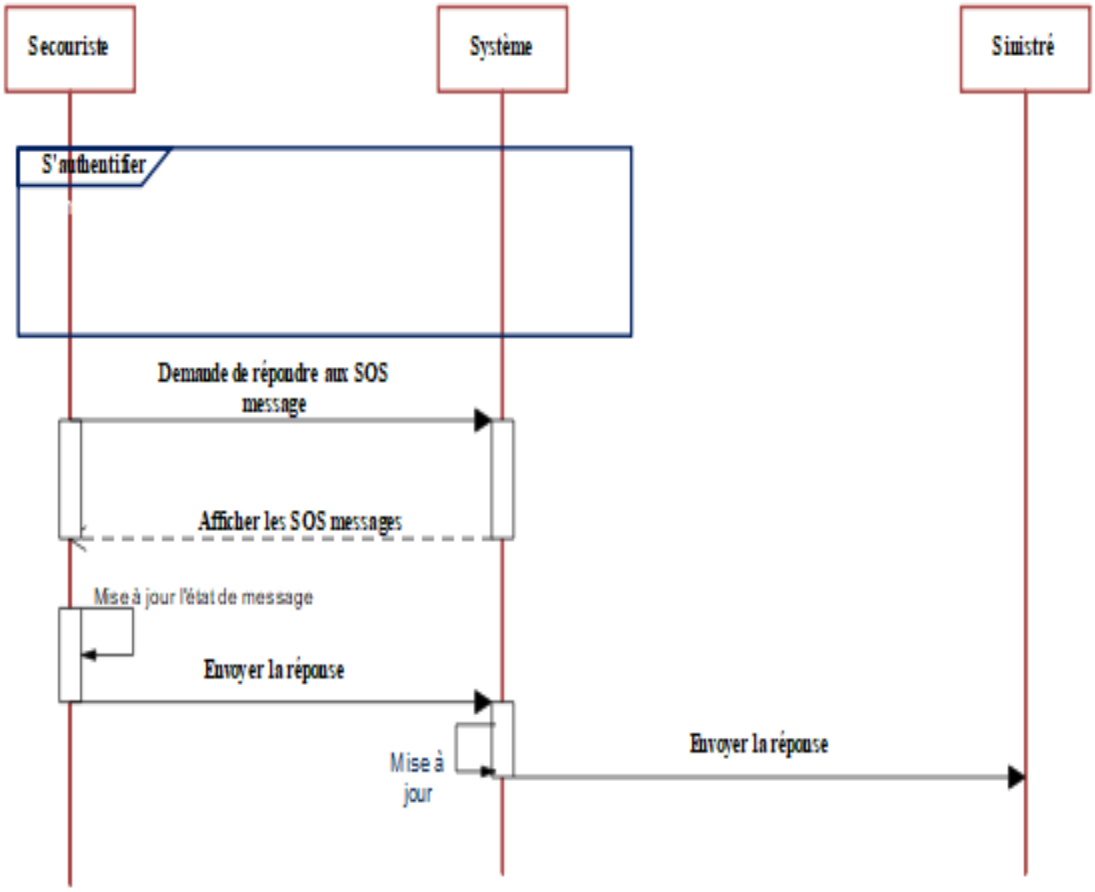


Figure IV.5 : Diagramme de séquence « Répondre aux SOS message »

IV.4.3 Diagramme de classe

Le diagramme de classe est un schéma utilisé pour présenter les classes et les interfaces des systèmes ainsi que les différentes relations entre celle-ci. Notre diagramme de classe et sa description sont illustrés respectivement dans la figure IV.6 et le tableau IV.2.

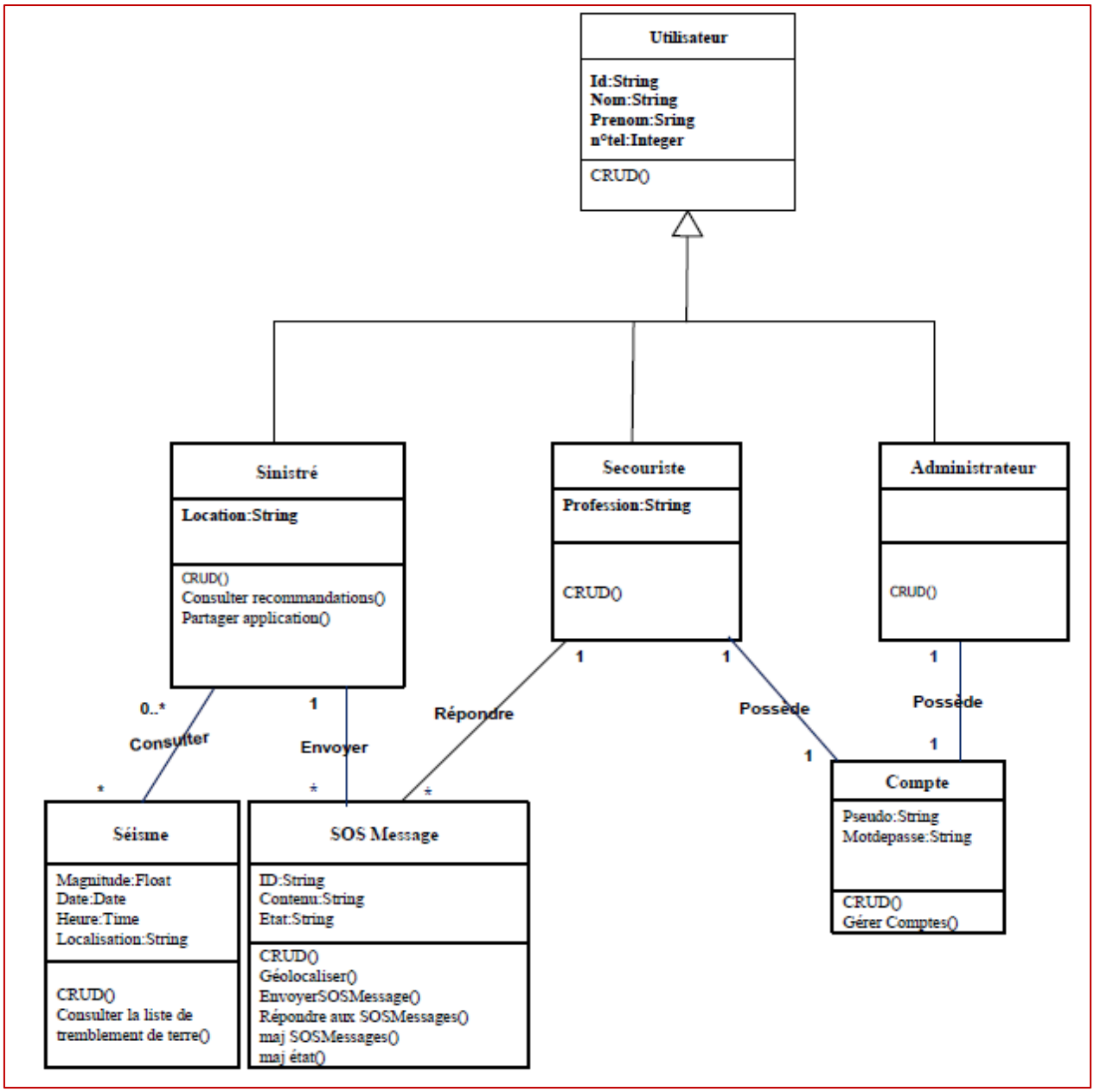


Figure IV.6 : *Diagramme de classe*

Classe	Attribut	Type	Désignation	Méthode
Utilisateur	Id	String	Identifiant d'utilisateur	CRUD ()
	Nom	String	Nom d'utilisateur	
	Prénom	String	Prénom d'utilisateur	
	N° tel	Integer	Numéro de téléphone d'utilisateur	
Sinistré	Location	String	Localisation de sinistré	CRUD () Consulter recommandations () Partager application ()
Secouriste	Profession	String	Profession de secouriste	CRUD ()
Administrateur				CRUD ()
Séisme	Magnitude	Float	Magnitude de séisme	CRUD () Consulter la liste de tremblement de terre ()
	Date	Date	Date de séisme	
	Heure	Time	Heure de séisme	
	Localisation	String	Laïcalisation de séisme	
SOS message	Id	String	Identifiant de SOS message	CRUD () Géolocaliser () Envoyer SOS Message () Répondre aux SOS Messages () Maj SOS messages ()
	Contenu	String	Contenu de SOS message	
	Etat	String	Etat de SOS message	
Compte	Pseudo	String	Email	CRUD () Gérer des comptes
	Mot de passe	String	Mot de passe	

Tableau IV.2 : *Tableau descriptif des classes*

IV.5 Conclusion

Ce chapitre était consacré à la conception détaillée de la solution proposé en décrivant le processus de communication du réseau ainsi que notre application SOS.

Dans le chapitre suivant, nous présentons les étapes suivis dans l'implémentation et la réalisation de cette solution.

Chapitre V : Implémentation, Test et Résultat

V.1 Introduction

Nous allons présenter dans ce chapitre deux parties. La première partie représente la réalisation de notre application qui a pour objectif de mettre en œuvre le système de gestion des urgences sismiques. Quant à la deuxième partie, elle présente les résultats obtenus lors de la simulation de notre stratégie EADE-NDN.

V.2 Outils de développement

La figure V.1 montre les principaux logiciels pour mettre en œuvre notre travail, la description des logiciels de développement utilisés (Android Studio, Firebase, le simulateur ndnSIM) est présentée dans les sections suivantes.

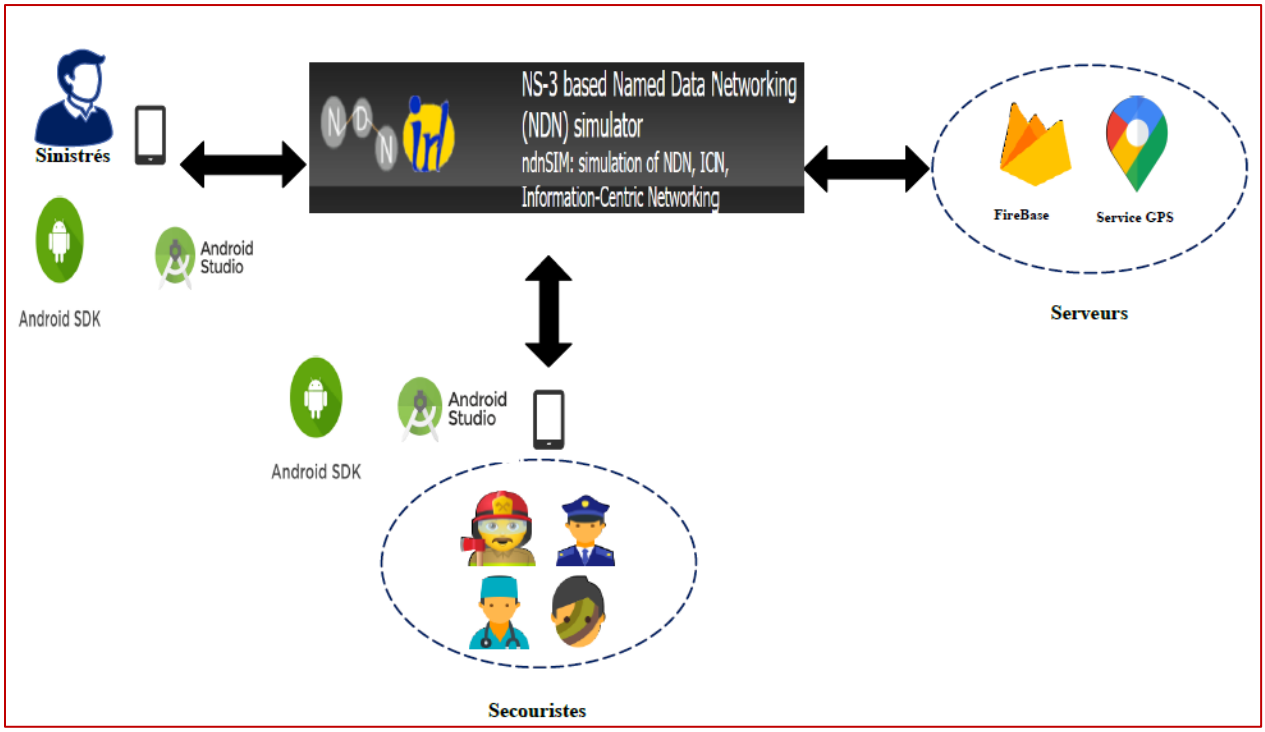


Figure V.1 : *Logiciels de développement*

V.2.1 Android Studio

Android Studio est l'environnement de développement intégré (IDE) officiel pour le développement d'applications Android avec le langage Java, basé sur IntelliJ IDEA[18]. Il offre beaucoup de fonctionnalités qui améliorent la création d'applications Android, telles que : un environnement unifié pour tous les appareils Android. Il s'adapte à beaucoup de structures différentes talque les smartphones, les tablettes. Il offre un émulateur rapide et riche en fonctionnalités avec une visualisation des écrans rapide avec des résolutions variées[65].

V.2.2 SDK Android

Les applications Android sont développées en Java, mais un appareil sous Android ne comprend pas le Java tel quel, il comprend une variante du Java adaptée pour Android. Un kit de développement logiciel (Software Development Kit, *SDK***)** est un ensemble d'outils que met à disposition un éditeur afin de permettre de développer des applications pour un environnement précis. Le SDK Android permet, donc, de développer des applications pour Android et uniquement pour Android[65].

V.2.3 Firebase

Firebase est une plate-forme de développement d'applications mobiles et web qui fournit aux développeurs une pléthore d'outils et de services pour les aider à développer des applications de haute qualité. Parmi ces services offerts nous avons utilisé deux services : le premier est Firebase RealTime Database est une base de données NoSql hébergée dans le cloud qui nous permettre de stocker et de synchroniser des données en temps réel. Le deuxième service est Firebase Authentification qui fournit des services backend, des SDK faciles à utiliser et des bibliothèques d'interface utilisateur pour la création de système d'authentification sécurisé, tout en améliorant l'expérience de connexion et d'intégration pour les utilisateurs de notre application[66] [67].

[18] https://www.jetbrains.com/idea/

V.3 Présentation de l'application

Au lancement de l'application, la première interface de notre application est présentée comme suit :

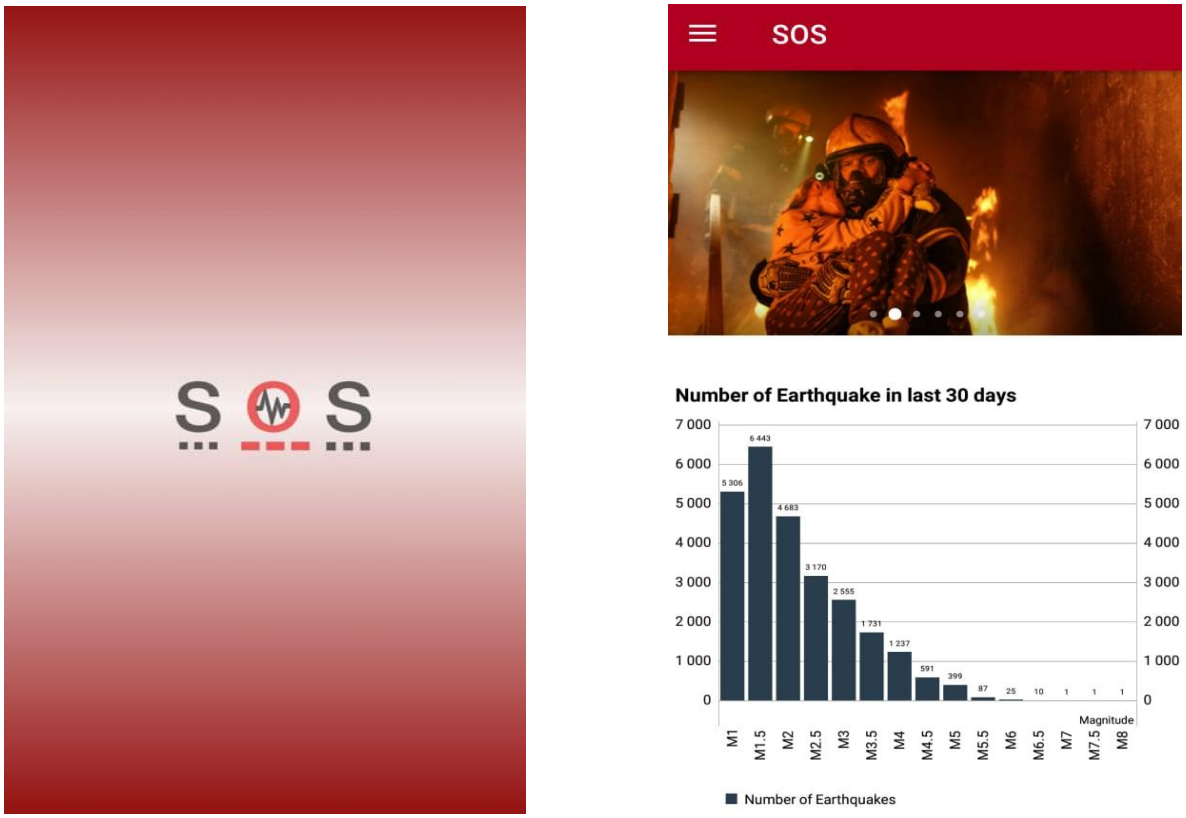


Figure V.2 : *Interface Principale*

Le sinistré accède au menu de l'application (figure V.3) pour bénéficier de toutes les fonctionnalités offertes qui sont présentés dans les figures suivantes :

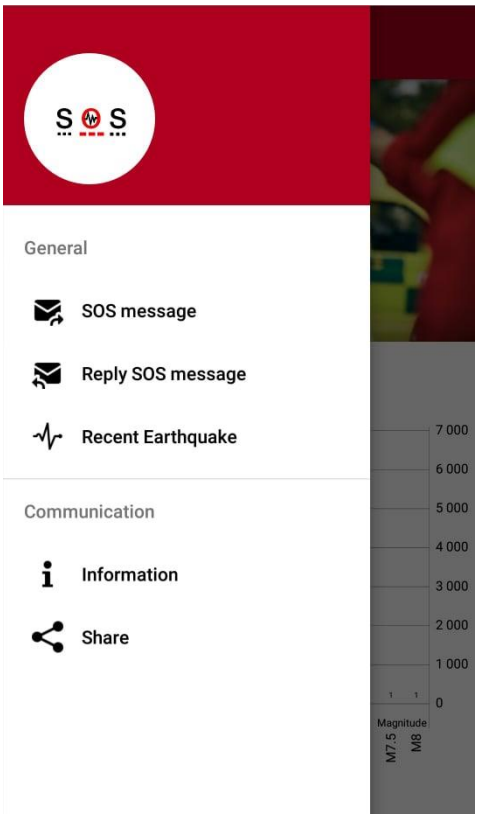


Figure V.3 : *Menu de l'application*

1. SOS message

Cet espace (figure V.4) permet au sinistré d'introduire les informations nécessaires envoyée à l'équipe des secouristes :

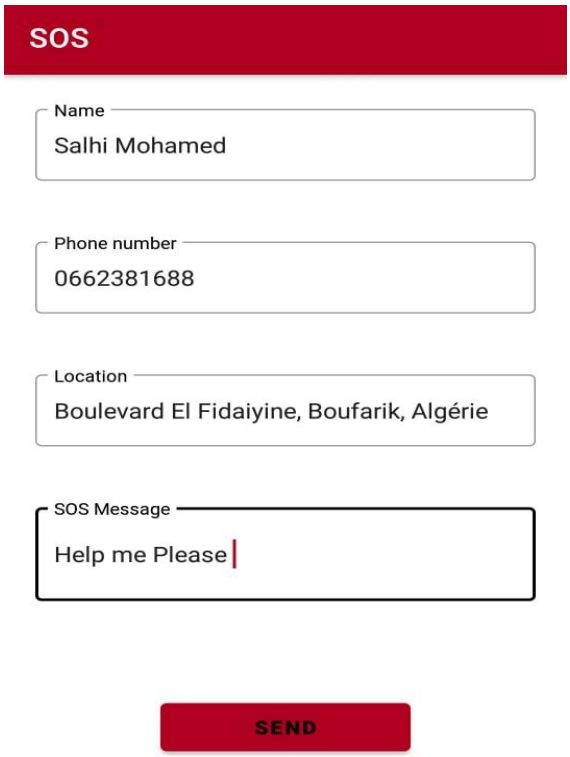


Figure V.4: *Envoyer un message SOS*

2. Consulter la liste des derniers tremblements de terres (Recent Earthquakes)

Le sinistré peut consulter les derniers tremblements de terres dans le monde en temps réels comme le montre la figure V.5.

Figure V.5: *La liste des derniers tremblements de terres*

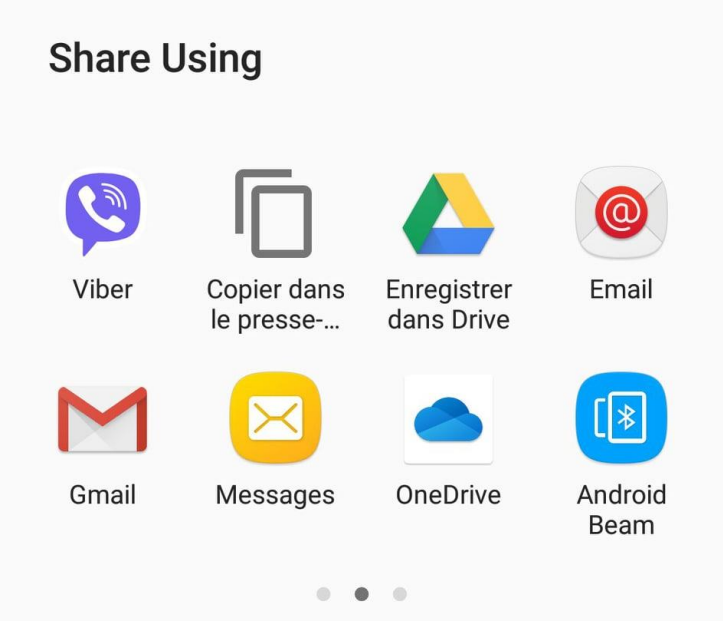
3. Consulter des recommandations

Cette espace permet de rappeler au sinistré quoi faire correctement avant, pendant et après un tremblement de terre (V.6).

Figure V.6 : *Les recommandations à suivre*

4. Partager l'application

Cet espace permet au sinistré de partager l'application avec son entourage.



5. Répondre aux messages SOS

Quant au secouriste, il s'inscrit s'il ne possède pas déjà un compte, sinon de se connecter en introduisant son email et mot de passe (V.7)

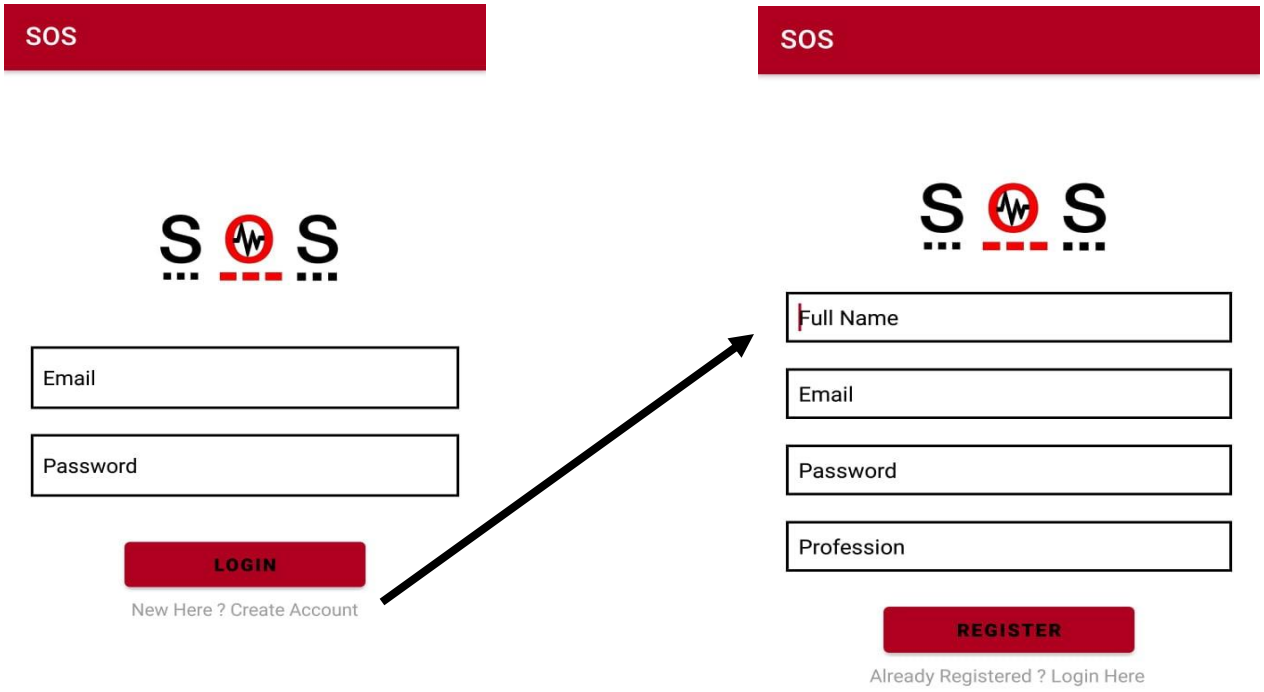
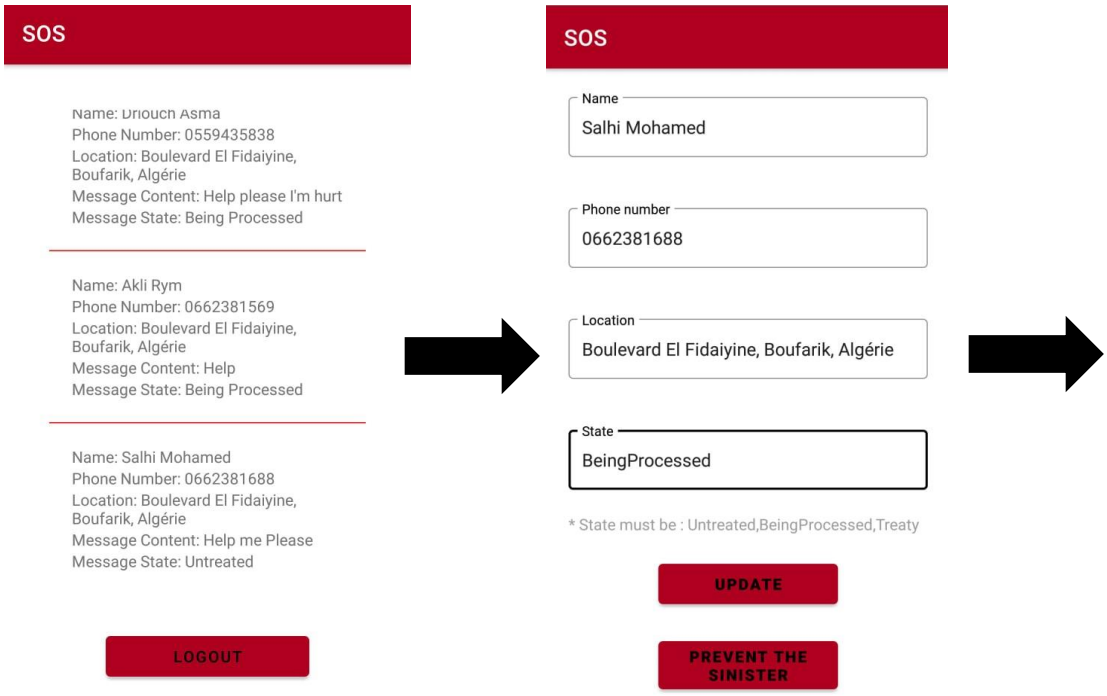
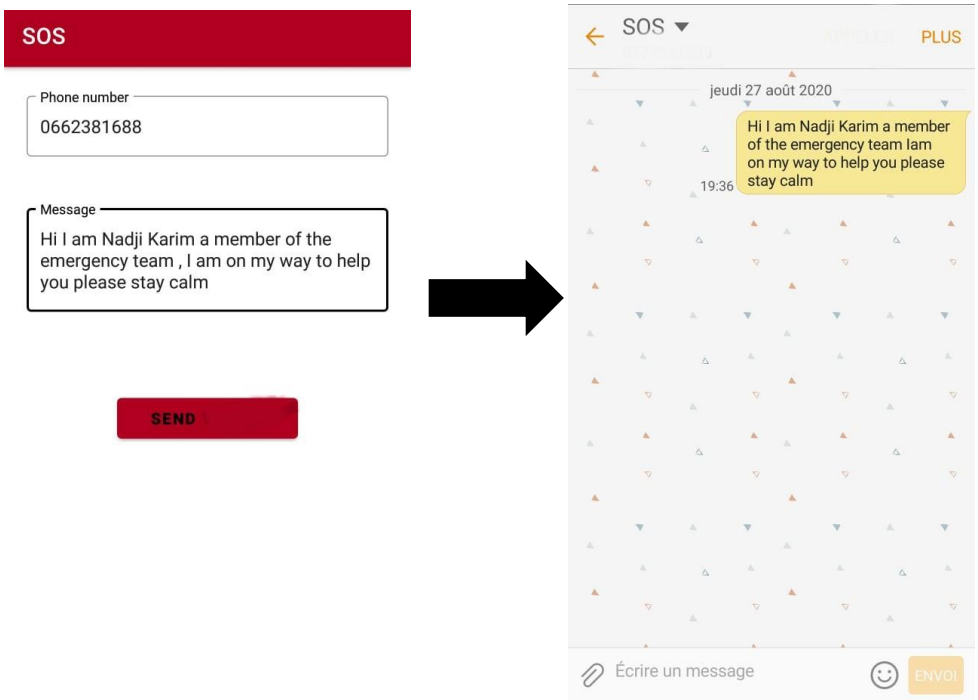


Figure V.7 : *Connexion / inscription d'un secouriste*

Une fois le secouriste est connecté, il a l'accès à tous les messages SOS envoyés. Pour répondre à un des messages, il suit la procédure suivante :


SOS
Name: Driouch Asma
Phone Number: 0559435838
Location: Boulevard El Fidaiyine, Boufarik, Algérie
Message Content: Help please I'm hurt
Message State: Being Processed
Name: Akli Rym
Phone Number: 0662381569
Location: Boulevard El Fidaiyine, Boufarik, Algérie
Message Content: Help
Message State: Being Processed
Name: Salhi Mohamed
Phone Number: 0662381688
Location: Boulevard El Fidaiyine, Boufarik, Algérie
Message Content: Help me Please
Message State: Untreated
LOGOUT
SOS
Name
Salhi Mohamed
Phone number
0662381688
Location
Boulevard El Fidaiyine, Boufarik, Algérie
State
BeingProcessed
* State must be : Untreated,BeingProcessed,Treaty
UPDATE
PREVENT THE SINISTER


SOS
Phone number
0662381688
Message
Hi I am Nadji Karim a member of the emergency team , I am on my way to help you please stay calm
SEND
SOS
PLUS
jeudi 27 août 2020
Hi I am Nadji Karim a member of the emergency team Iam on my way to help you please stay calm
19:36
Écrire un message
ENVOI

V.4 Simulation

Afin de tester notre processus de communication et la stratégie EADA-NDN proposée, il fallait utiliser un simulateur vu qu'il n'existe pas un émulateur ou un déploiement réel du réseau ICN, voire NDN. Pour cela, nous avons choisi le simulateur ndnSim le plus utilisé et documenté.

V.4.1 Simulateur ndnSIM

NdnSIM [68]est un simulateur open source basé sur NS-3[19] qui implémentait fidèlement les composants de base d'un réseau NDN de manière modulaire. La conception de ndnSIM a les objectifs suivants :

- Être un package open source pour permettre à la communauté de recherche d'exécuter des expérimentations sur une plate-forme de simulation commune.
- Être capable de simuler fidèlement toutes les opérations de base du protocole NDN.
- Être capable de supporter des expériences de simulation à grande échelle.
- Faciliter les expérimentations de la couche réseau avec le routage, la mise en cache des données, le transfert de paquets et la gestion de la congestion.
- Explorer différents environnements de réseau (véhicule, sans fil ad hoc, mobile et IoT).

La figure V.8 présente la structure globale de l'environnement ndnSIM [68], [69] composé d'un ensemble de plateforme, bibliothèques et des applications expliqués en détails au niveau de tableau V.1.

[19] https://www.nsnam.org/releases/ns-3-31/documentation/

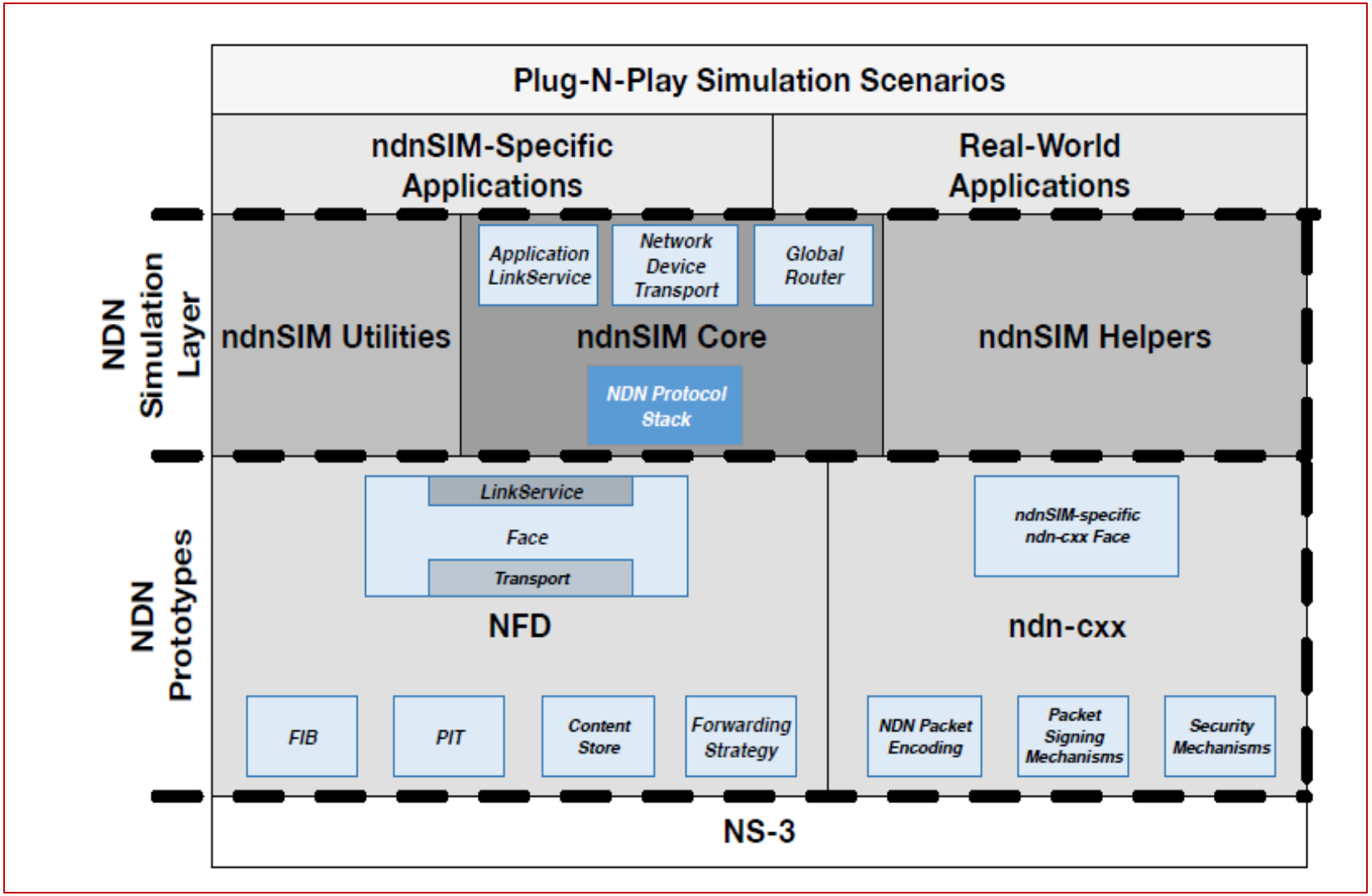


Figure V.8 : *Structure de simulateur ndnSIM [68]*

Les composants	L'explication
NS-3	Une plate-forme de simulation de réseau open-source basée sur la planification d'événements discrets. Il est écrit en C ++ et répond aux besoins de la recherche moderne sur les réseaux.
NFD	Un redirecteur de réseau qui implémente et évolue avec le protocole NDN. Sa fonctionnalité principale est de transmettre des paquets d'intérêt et de données.
Ndn-cxx	Une bibliothèque qui implémente les principales primitives NDN qui peuvent être utilisées pour implémenter diverses expériences d'application réelles.
ndnSIM Core	C'est la pile de protocoles NDN, la réalisation de NFD's Transport pour fournir une communication au-dessus des NS3 et NetDevice, la réalisation de LinkService de NFD pour faciliter la communication directe entre les applications spécifiques à ndnSIM.
ndnSIM Utilities	C'est un certain nombre de traceurs de paquets pour obtenir des résultats de simulation (traçage au niveau des liens, du réseau et de l'application) et des lecteurs de topologie pour simplifier la définition des topologies de simulation.
ndnSIM Helpers	C'est un ensemble d'assistants pour installer et configurer la pile NDN et les applications simulées sur les nœuds, pour gérer les stratégies de transfert et les politiques de remplacement de cache, pour simplifier la modification des états des liens dans les topologies simulées.
ndnSIM-Specific Applications	Sont un moyen pratique de générer des flux de paquets d'intérêt / données pour diverses évaluations au niveau du réseau, y compris le comportement des stratégies de transfert, des politiques de cache, etc
Real-World Applications	Exprime des intérêts et envoyer les données récupérées aux rappels fournis, détecter les délais d'expiration des intérêts, enregistrer les préfixes avec le NFD local, utiliser les API de signature et de vérification des paquets.
Plug-N-Play Simulation Scenarios	Une collection de scénarios de simulation qui fournissent des exemples de fonctionnalités ndnSIM.

Tableau V.1 : *Les détails des composants de simulateur ndnSIM*

V.4.2 Environnement de simulation

Nous allons décrire l'environnement matériel ainsi que la configuration du scénario du simulation utilisés pour réaliser notre simulation.

V.4.2.1 Environnement matériel

La simulation a été réalisée sur deux machines dont leurs caractéristiques sont les suivantes :

Caractéristiques	**Machine 1**	**Machine 2**
Systèmes d'exploitation	Ubuntu 16.04 (Virtuelle Machine)	Ubuntu 16.04
Processeur	Intel® Core™ i7-7500U CPU @ 2.70 GHZ @2.90 GHZ	Intel® Core™ i3-5005U CPU @ 2.00GHz
RAM	8 GO	4,00 Go
Disque Dur	1 TB	500 Go

Tableau V.2 : *Caractéristiques des machines utilisées*

V.4.2.2 Scénario de simulation

Pour tester le comportement général de la stratégie EADE-NDN, plusieurs simulations ont été exécutées sous le simulateur ndnSIM. Ces simulations testent les communications mobiles sans fils dans un réseau où un ensemble des nœuds est déployé aléatoirement. Parmi ces nœuds, ils y en un qui sont des consommateurs et il y a des autres producteurs qui tente d'envoyer des paquets de données à ce dernier à l'aide des nœuds intermédiaire comme illustré dans la figure V.9.

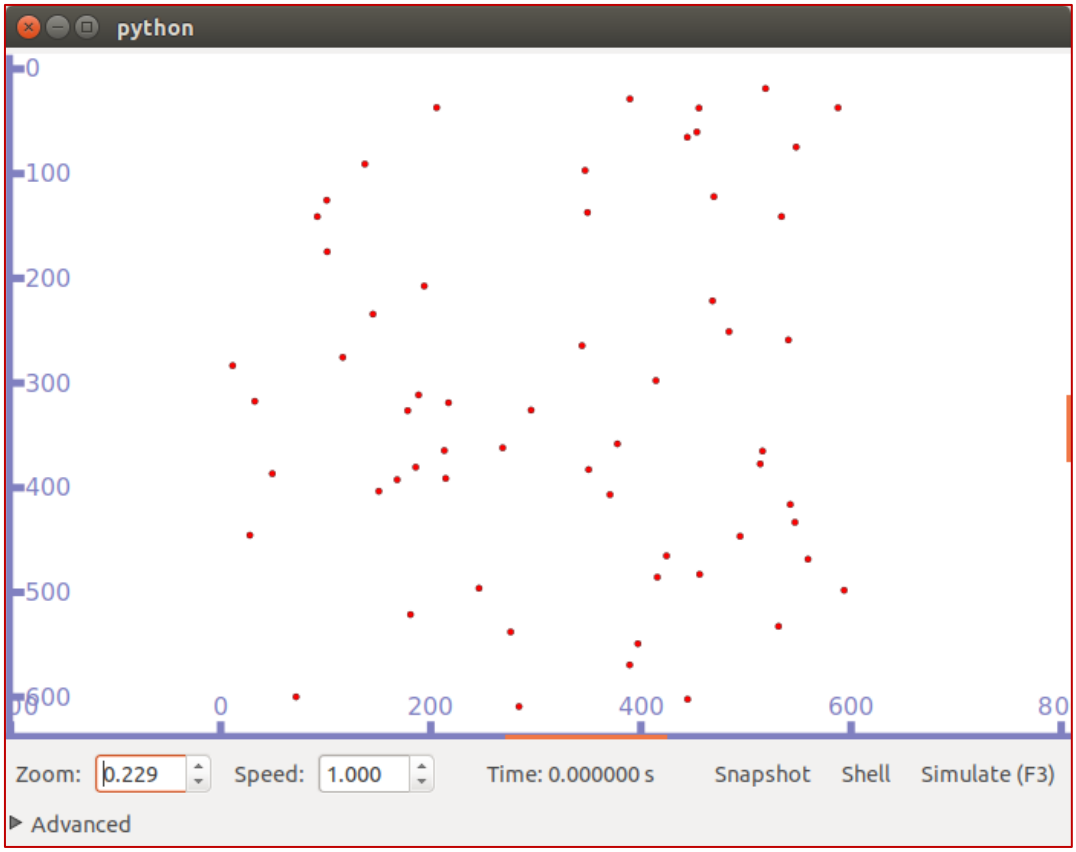


Figure V.9 : *Topologie aléatoire des nœuds*

Pour nos simulations, nous avons utilisé BonnMotion[20] comme outil de génération de topologie mobile. Le modèle utilisé est Random Waypoint[21] qui est un modèle aléatoire pour le mouvement des utilisateurs mobiles. Dans notre scénario, nous modifions à chaque fois le nombre total de nœuds implique dans simulations avec 12 consommateurs et 4 producteurs placés aléatoirement dans le réseau sur une surface de 1200 m^2 et nous voyons comment cela peut affecter les performances. Chaque simulation a été menée pendant 900 secondes. Les paramètres de simulation utilisés dans toutes les simulations sont présentés dans le tableau V.3

[20] http://sys.cs.uos.de/bonnmotion/

[21] Dans ce modèle de simulation de mobilité à base aléatoire, les nœuds mobiles se déplacent de manière aléatoire et librement sans restriction.

Paramètre	Valeur
Simulateur	ndnSIM 2.6
Nombre de nœud	20, 30, 40, 50,60
Fréquences des paquets d'intérêt	10 paquets/seconde
Simulation area	600 m * 600 m
Vitesse du Nœud	20 m/s
Nombre de consommateurs	12
Nombre de producteur	4
Temps de simulation	900 s
Modèle de mobilité	Random Waypoint
Spécification WIFI	802.11a
Transmission Range	100

Tableau V.3 : *Paramètres de simulation*

V.4.3 Métriques de performance

Différentes métriques sont définies pour évaluer les performances EADE selon le scénario mis en jeu. Ces métriques sont :

- **Délai moyen**. Le délai est défini comme la différence entre le moment de l'expression du premier intérêt d'un nom spécifique et le moment de la réception des données correspondantes. Le délai moyen est défini dans l'équation V.1. Un délai moyen plus faible indique que la stratégie de réexpédition peut garantir une meilleure qualité de service en termes de retard.

$$\text{Délai moyen} = \frac{1}{N} \sum T_R - T_E \qquad (V.1)$$

  - ✓ **N :** nombre totale de données reçues
  - ✓ $\mathbf{T_R}$ **:** temps d'arrivé de la donnée
  - ✓ $\mathbf{T_E}$ **:** temps d'envoi d'intérêt

- **Retransmission des intérêts**. Après l'émission d'un intérêt, un délai d'expiration est défini. Si le délai est dépassé sans réception des données, cet intérêt sera retransmis. Nous définissons la retransmission des intérêts comme le nombre moyen de retransmissions

d'intérêts pour tous les intérêts avant de recevoir les données correspondantes (l'équation V.2). Les décisions judicieuses d'une stratégie de transfert induisent une retransmission à faible intérêt, fournissant une livraison rapide des données demandées.

$$\text{Taux de retransmission} = \frac{\text{nombre d'interets retransmis}}{\text{nombre de donnée reçu}} \qquad (V.2)$$

- **Satisfaction des intérêts.** Elle représente le nombre moyen des paquets de données qui répond aux intérêts de consommateur (l'équation V.3). La valeur de satisfaction élevée indique que la stratégie est bonne.

$$\text{Taux de satisfaction} = \frac{\text{nombre de donnée reçu}}{\text{nombre d'interet envoyés}} \qquad (V.3)$$

V.4.4 Résultats obtenus

Nous avons effectué nos simulations pour vérifier si EADE est performant en termes de délai, retransmission et satisfaction des intérêts. La figure V.10 montre les différents liens de diffusion inondée par chaque nœud.

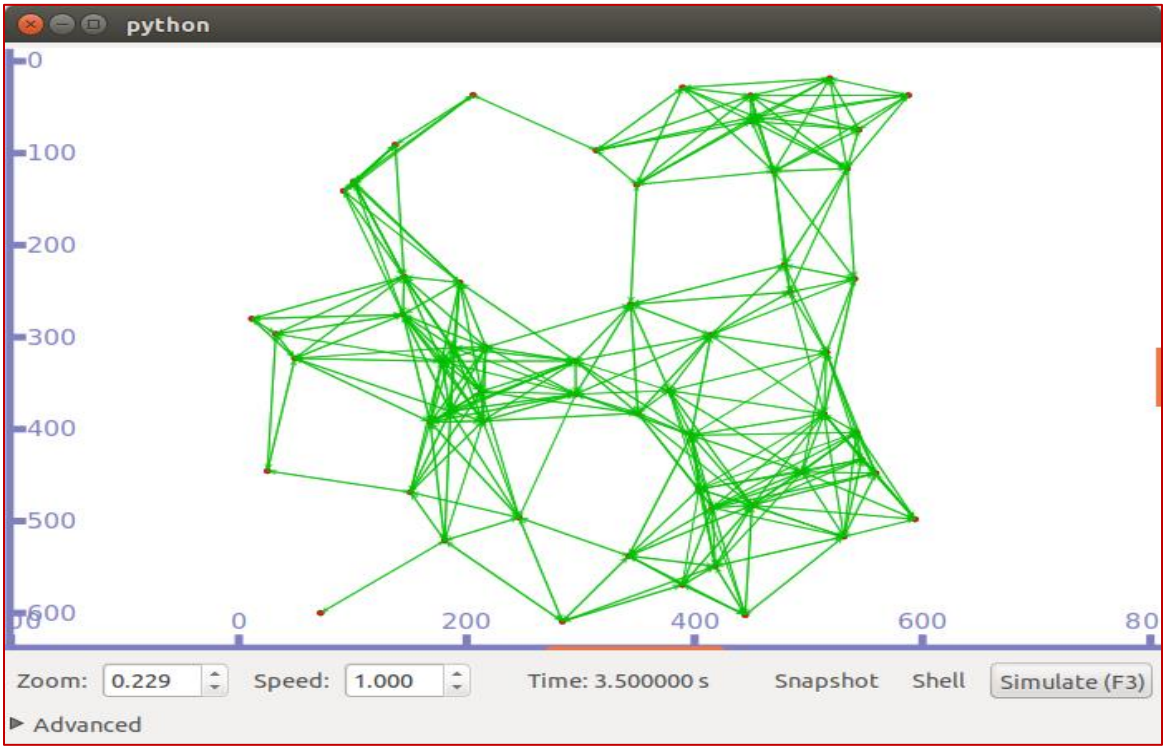


Figure V.10 : *Les chemins d'EADE*

La figure V.11 montre les entrées de la table PIT dans un nœud qui utilise la stratégie EADE. La table contient les paquets d'intérêt demandée par l'utilisateur et les informations correspondant comme durée de vie et nonce.

Prefix	Info
/secouriste/prefix_help/%FE%B4	/secouriste/prefix_help/%FE%B4?ndn.InterestLifetime=2000&ndn.Nonce=2266790580
/secouriste1/prefix_help/%FE%86	/secouriste1/prefix_help/%FE%86?ndn.InterestLifetime=2000&ndn.Nonce=3019466766
/tsecouriste1/prefix_help/%FE%CF	/tsecouriste1/prefix_help/%FE%CF?ndn.InterestLifetime=2000&ndn.Nonce=2634574137
/tsecouriste1/prefix_help/%FE%D3	/tsecouriste1/prefix_help/%FE%D3?ndn.InterestLifetime=2000&ndn.Nonce=3957224267
/tsecouriste1/prefix_help/%FE%D6	/tsecouriste1/prefix_help/%FE%D6?ndn.InterestLifetime=2000&ndn.Nonce=1918777372
/secouriste/prefix_help/%FE%BC	/secouriste/prefix_help/%FE%BC?ndn.InterestLifetime=2000&ndn.Nonce=2336187709
/tsecouriste1/prefix_help/%FE%DF	/tsecouriste1/prefix_help/%FE%DF?ndn.InterestLifetime=2000&ndn.Nonce=1270563091
/tsecouriste1/prefix_help/%FE%D9	/tsecouriste1/prefix_help/%FE%D9?ndn.InterestLifetime=2000&ndn.Nonce=2069993980
/secouriste/prefix_help/%FE%BA	/secouriste/prefix_help/%FE%BA?ndn.InterestLifetime=2000&ndn.Nonce=2581090005

Figure V.11 : *Les entrées de la table PIT*

Dans un premier test de simulation, nous déterminons le délai moyen de transfert par second en fonction du nombre de nœuds (Figure V.12).

Nous pouvons voir clairement que le délai moyen d'EADE augmente avec la croissance de nombre des nœuds de la topologie mais il reste faible quand même dans un réseau de 20 nœuds le délai est estimé à 0.01 seconde et 0.11 secondes pour une topologie de 60 nœuds due au mécanisme de transfert d'EADE.

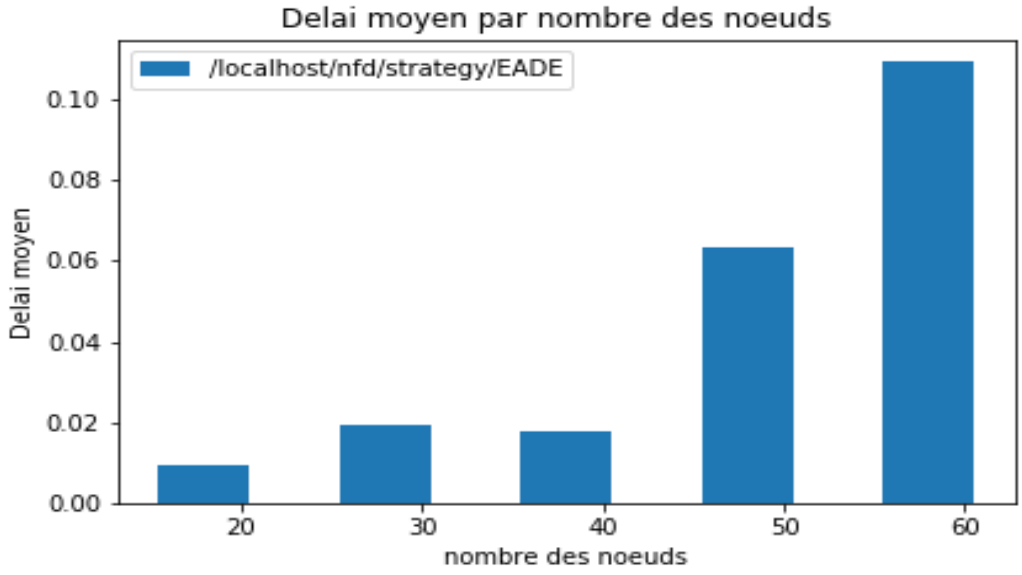


Figure V.12 : *Délai d'EADE*

Dans le deuxième test de simulation, nous déterminons la retransmission des intérêts en fonction de nombres de nœuds (figure V.13).

Nous remarquons que le taux de retransmission se diminue avec l'augmentation de nombre des nœuds. Le meilleur taux est marqué avec 50 nœuds, et stabilisé dans 60 car les nœuds sont satisfaits et ils n'ont pas besoin de retransmettre les intérêts.

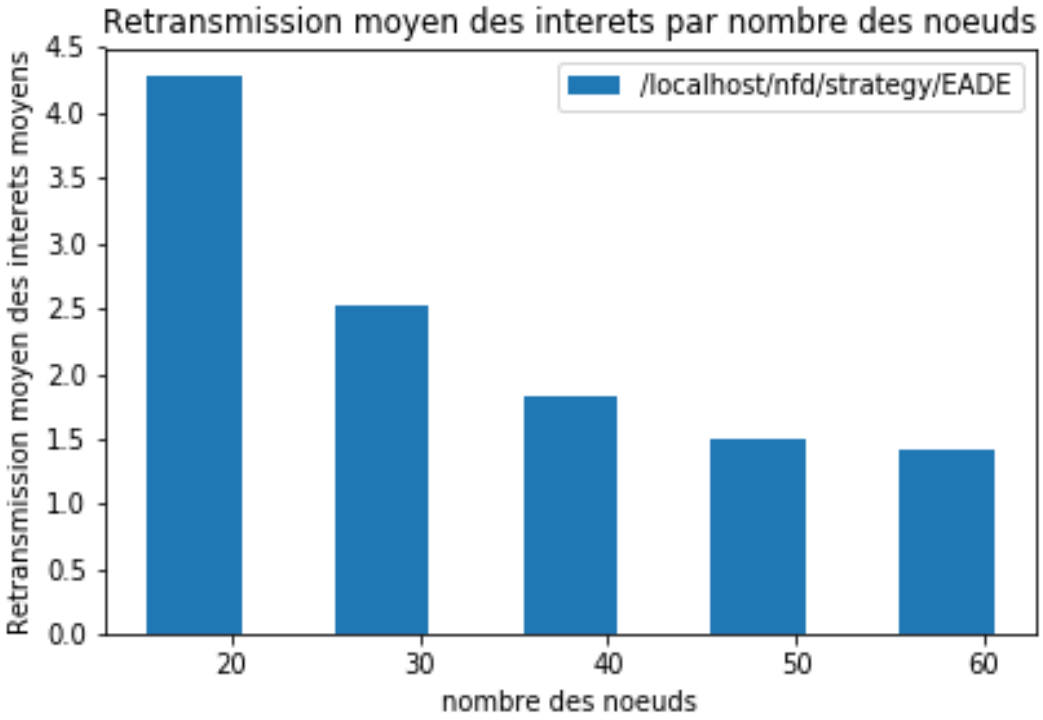


Figure V.13 : *Retransmission des intérêts EADE*

Dans le troisième test de simulation, nous déterminons la satisfaction des intérêts en fonction du nombre de nœuds (Figure V.14).

Nous remarquons que le taux de satisfaction d'intérêt augmente proportionnellement avec le nombre des nœuds, plus le nombre de nœuds augmente plus les intérêts sont satisfaits. C'est le résultat de la diffusion qui permet de trouver plusieurs chemins, par conséquent trouver le producteur (qui satisfait plusieurs consommateurs) à temps réduit.

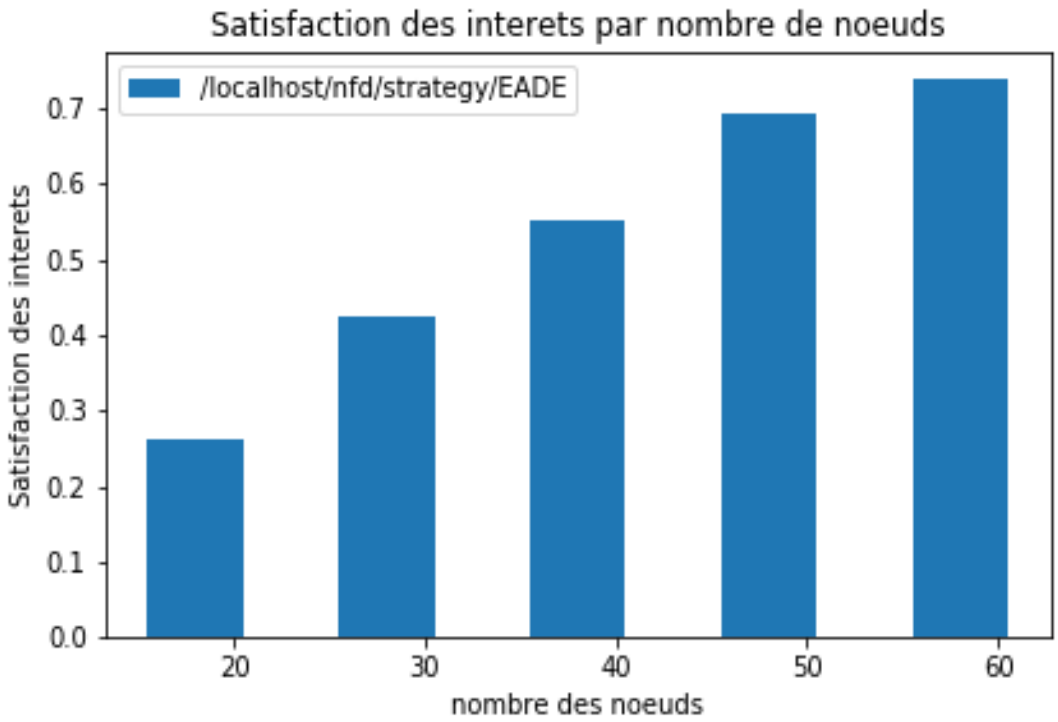


Figure V.14 : *Satisfaction des intérêts EADE*

À travers ces différents résultats, nous pouvons dire qu'EADE a eu des bons résultats en termes de délai, taux de satisfaction et retransmission d'intérêt ce qui a montré le bon fonctionnement de la solution proposée.

V.5 Conclusion

Dans ce chapitre, nous avons présenté en premier lieu les outils d'environnement utilisés Android studio et ndnSIM. Ensuite, nous avons présenté les différentes interfaces graphiques de notre SOS application et leur utilisation. Enfin, nous avons montré les différents résultats de simulation obtenus après avoir implémenté notre protocole EADE sous ndnSIM.

Conclusion Générale et Perspectives

Une meilleure performance d'un Système de Gestion des Urgences et Catastrophes (SGUC) dépend totalement de la communication en temps de catastrophe. Les premiers intervenants en cas de catastrophe comptent sur la capacité de communiquer. La communication est un facteur clé d'une conscience situationnelle adéquate et de la justesse des décisions. Les grands réseaux opportunistes sans-fil Ad-hoc peuvent être très bénéfiques pour collecter et diffuser les informations vitales d'urgence, sauf que la nature conversationnelle du paradigme TCP / IP pose énormes défis, notamment une absence de communication résilientes en cas d'une catastrophe. C'est pourquoi, un certain nombre d'efforts de recherche visant à concevoir de nouvelles architectures Internet ont pris leur essor au cours des dernières années. L'un de ses efforts est les réseaux centrés sur l'information (ICN) qui représentent un nouveau paradigme de mise en réseau basé sur la dénomination indépendante de localisation, de la mise en cache dans le réseau, du routage basé sur les noms et la mobilité des nœuds.

Dans la littérature, il existe de nombreuses propositions pour les architectures ICN comme DONA, CCN, NDN et Convergence. Après une comparaison de ces architectures, nous nous sommes orientés vers l'architecture du NDN car elle est le mieux adaptée à la communication opportuniste de smartphones offerte par le réseau mobile ad hoc MANET. Ensuite, nous nous sommes intéressées aux différentes

Stratégies de transfert des données nommées dans les réseaux ad hoc sans fil que nous avons nommé tout simplement « *stratégies de transfert MANET-NDN* », notamment le concept de LFBL (Listen first broadcast later) ou EADE (Ecouter Avant Diffuser Aprés). Nous avons opté pour la stratégie EADE-NDN afin d'assurer une communication opportuniste, de prendre en charge la mobilité (physique et logique) et ainsi de fournir des capacités de communication résilientes en cas d'un séisme.

De ce fait, nous avons proposé et développé une simple application Android qui représente notre SGUC en permettant aux sinistrés d'envoyer des messages SOS, ces messages sont transférés dans le réseau en se basant sur la stratégie EADE-NDN proposée. Afin de valider notre proposition, nous avons implémenté EADE-NDN sous le simulateur ndnSIM (v2.6). Les résultats de simulation

ont montré le bon fonctionnement de EADE en termes de délai, retransmission et satisfaction des intérêts.

Faute au temps, nous n'avons pas pu faire une étude de performance entre d'autres stratégies de transfert : version LFBL proposé dans [58]. Aussi, nous n'avons pas pu faire le lien entre l'environnement Android Studio et le simulateur ndnSIM, c'est-à-dire la conversation des messages et réponses SOS (paquets IP) à des paquets d'intérêts /données.

Ainsi, le travail réalisé dans le cadre de ce projet peut être étendu de plusieurs façons. Nous pouvons citer à titre d'exemple :

- Comparer les résultats de notre proposition avec d'autres stratégies MANET dans IP.
- Intégrer les autres stratégies de transfert conscient et les comparer avec les performances de notre stratégie EADE-NDN.
- Ajouter le lien entre Android Studio et le simulateur ndnSIM.
- Inclure d'autres métriques de mesure de performance comme l'énergie consommée, nombre de paquets supprimer, débit …
- Implémenter la stratégie EADE dans d'autres projets ICNs.

Bibliographie

[1] « Les catastrophes naturelles les plus meurtrières Monde 1980-2018 », *Statista*. https://fr.statista.com/statistiques/658314/catastrophes-naturelles-le-plus-de-morts/ (consulté le 12 août, 2020).

[2] « Cisco Annual Internet Report - Cisco Annual Internet Report (2018–2023) White Paper », *Cisco*. https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html (consulté le juill. 23, 2020).

[3] T. Koponen *et al.*, « A Data-Oriented (and Beyond) Network Architecture », p. 12.

[4] G. Xylomenos *et al.*, « A Survey of Information-Centric Networking Research », *IEEE Commun. Surv. Tutor.*, vol. 16, nº 2, p. 1024-1049, 2014, doi: 10.1109/SURV.2013.070813.00063.

[5] M. M. S. Soniya et K. Kumar, « A survey on named data networking », in *2015 2nd International Conference on Electronics and Communication Systems (ICECS)*, Coimbatore, India, févr. 2015, p. 1515-1519, doi: 10.1109/ECS.2015.7124841.

[6] D. P. Coppola, *Introduction to International Disaster Management*. 30 Corporate Drive, Suite 400, Burlington, MA 01803, USA: Butterworth–Heinemann.

[7] M. Belazougui, « BOUMERDES ALGERIA EARTHQUAKE OF MAY 21, 2003: DAMAGE ANALYSIS AND BEHAVIOR OF BEAM-COLUMN REINFORCED CONCRETE STRUCTURES », p. 8, 2008.

[8] R. Johnson, « GIS Technology for Disasters and Emergency Management », ESRI 380 New York St., Redlands, CA 92373-8100, USA •, mai 2000.

[9] G. Carrillo, T. Maama, et E. Kaputu, « Introduction à la gestion des catastrophes ». Virtual University for the Small States of the Commonwealth (VUSSC) Commonwealth of Learning (COL).

[10] T. Li *et al.*, « Data-Driven Techniques in Disaster Information Management », *ACM Comput. Surv.*, vol. 50, nº 1, p. 1-45, avr. 2017, doi: 10.1145/3017678.

[11] M. Careem, C. De Silva, R. De Silva, L. Raschid, et S. Weerawarana, « Sahana: Overview of a Disaster Management System », in *2006 International Conference on Information and Automation*, Colombo, Sri Lanka, déc. 2006, p. 361-366, doi: 10.1109/ICINFA.2006.374152.

[12] L. Zheng, C. Shen, L. Tang, T. Li, S. Luis, et S.-C. Chen, « Applying data mining techniques to address disaster information management challenges on mobile devices », in *Proceedings of the 17th ACM SIGKDD international conference on Knowledge discovery and data mining - KDD '11*, San Diego, California, USA, 2011, p. 283, doi: 10.1145/2020408.2020457.

[13] K. Saleem, S. Luis, Y. Deng, S.-C. Chen, V. Hristidis, et T. Li, « Towards a Business Continuity Information Network for Rapid Disaster Recovery », p. 10.

[14] J. T. B. Fajardo et C. M. Oppus, « A Mobile Disaster Management System Using the Android Technology », vol. 9, nº 6, p. 11, 2010.

[15] M. Kumar et R. Mishra, « An Overview of MANET: History, Challenges and Applications », vol. 3, nº 1, p. 5, 2012.

[16] M. Tahar Abbes, « Proposition d'un protocole à économie d'énergie dans un réseau hybride GSM et AD HOC », Universite d'Oran. Algerie, 2011.

[17] R. Sobti, « A Study on Challenges and Issues on MANET », vol. 4, nº 9, p. 8.

[18] « Vehicular Ad-Hoc Networks (VANETs) - An Overview and Challenges », p. 11.

[19] K. Ahmad, N. I. Udzir, et G. C. Deka, *Opportunistic Networks: Mobility Models, Protocols, Security, and Privacy*, 1re éd. Boca Raton : Taylor & Francis, a CRC title, part of the Taylor & Francis imprint, a member of the Taylor & Francis Group, the academic division of T&F Informa, plc, 2018.: Chapman and Hall/CRC, 2018.

[20] S. Ali, J. Qadir, et A. Baig, « Routing protocols in Delay Tolerant Networks - a survey », in *2010 6th International Conference on Emerging Technologies (ICET)*, Islamabad, Pakistan, oct. 2010, p. 70-75, doi: 10.1109/ICET.2010.5638377.

[21] K. K. Ahmed, M. H. Omar, et S. Hassan, « A Comprehensive Survey on Delay Tolerant Networks », p. 7.

[22] F. Z. Benhamida, A. Bouabdellah, et Y. Challal, « Using delay tolerant network for the Internet of Things: Opportunities and challenges », in *2017 8th International Conference on Information and Communication Systems (ICICS)*, Irbid, Jordan, avr. 2017, p. 252-257, doi: 10.1109/IACS.2017.7921980.

[23] P. Rathee, « Semantics for Delay-Tolerant Network (DTN) », in *Emerging Wireless Communication and Network Technologies*, K. V. Arya, R. S. Bhadoria, et N. S. Chaudhari, Éd. Singapore: Springer Singapore, 2018, p. 101-123.

[24] I. F. Akyildiz, Weilian Su, Y. Sankarasubramaniam, et E. Cayirci, « A survey on sensor networks », *IEEE Commun. Mag.*, vol. 40, nº 8, p. 102-114, août 2002, doi: 10.1109/MCOM.2002.1024422.

[25] P. Jadhav et R. Satao, « A Survey on Opportunistic Routing Protocols for Wireless Sensor Networks », *Procedia Comput. Sci.*, vol. 79, p. 603-609, 2016, doi: 10.1016/j.procs.2016.03.076.

[26] R. R. Selmic, V. V. Phoha, et A. Serwadda, *Wireless Sensor Networks Security, Coverage, and Localization*. Cham: Springer International Publishing, 2016.

[27] J. Divyateja et R.Vijay Prakash, « Opportunistic Networks: An Evolution in Mobile Ad-Hoc Networks », *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*

[28] A. Feldmann, « Internet clean-slate design: what and why? », *ACM SIGCOMM Comput. Commun. Rev.*, vol. 37, nº 3, p. 59-64, juill. 2007, doi: 10.1145/1273445.1273453.

[29] R. Jain, « Internet 3.0: Ten Problems with Current Internet Architecture and Solutions for the Next Generation », in *MILCOM 2006*, Washington, DC, USA, oct. 2006, p. 1-9, doi: 10.1109/MILCOM.2006.301995.

[30] D. Ó. Coileáin et D. O'mahony, « Accounting and Accountability in Content Distribution Architectures: A Survey », *ACM Comput. Surv.*, vol. 47, nº 4, p. 1-35, juill. 2015, doi: 10.1145/2723701.

[31] A. Vakali et G. Pallis, « Content delivery networks: Status and trends », *IEEE Internet Comput.*, vol. 7, nº 6, p. 68-74, nov. 2003, doi: 10.1109/MIC.2003.1250586.

[32] A.-M. K. Pathan et R. Buyya, « A Taxonomy and Survey of Content Delivery Networks », p. 44.

[33] « Cisco Visual Networking Index: Forecast and Methodology, 2016–2021 June 6, 2017 - Recherche Google ». https://www.reinvention.be/webhdfs/v1/docs/complete-white-paper-c11-481360.pdf (consulté le 15 juin, 2020).

[34] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, et B. Ohlman, « A survey of information-centric networking », *IEEE Commun. Mag.*, vol. 50, nº 7, p. 26-36, juill. 2012, doi: 10.1109/MCOM.2012.6231276.

[35] M. Waehlisch *et al.*, « Information-Centric Networking (ICN) Research Challenges ». https://tools.ietf.org/html/draft-irtf-icnrg-challenges-06 (consulté le juin 15, 2020).
[36] Wei You, « A Content-Centric Networking Node for a Realistic Efficient Implementation and Deployment », Télécom Bretagne, Université de Rennes, 2014.
[37] B. Hamdane, « Réseaux du futur : sécurité et nommage », p. 156.
[38] G. Zhang, Y. Li, et T. Lin, « Caching in information centric networking: A survey », *Comput. Netw.*, vol. 57, nº 16, p. 3128-3141, nov. 2013, doi: 10.1016/j.comnet.2013.07.007.
[39] M. Meddeb, « Information-Centric Networking, A natural design for IoT applications? », Ecole Nationale des Sciences de l'Informatique, Toulouse, 2017.
[40] E. G. AbdAllah, H. S. Hassanein, et M. Zulkernine, « A Survey of Security Attacks in Information-Centric Networking », *IEEE Commun. Surv. Tutor.*, vol. 17, nº 3, p. 1441-1454, 2015, doi: 10.1109/COMST.2015.2392629.
[41] Z. Zhou, X. Tan, H. Li, Z. Zhao, et D. Ma, « MobiNDN: A mobility support architecture for NDN », in *Proceedings of the 33rd Chinese Control Conference*, Nanjing, China, juill. 2014, p. 5515-5520, doi: 10.1109/ChiCC.2014.6895882.
[42] « Beyond content delivery: can ICNs help emergency scenarios? », *IEEE Netw.*, vol. 28, nº 3, p. 44-49, mai 2014, doi: 10.1109/MNET.2014.6843231.
[43] E. Aubry, « Protocole de routage pour l'architecture NDN », p. 135.
[44] M. A. Yaqub, S. H. Ahmed, S. H. Bouk, et D. Kim, « Information-Centric Networks (ICN) », p. 15.
[45] M. Xavier, « Architectures et fonctions avancées pour le déploiement progressif de réseaux orientés contenus », Université de Lorraine, 2019.
[46] A. Majed, X. Wang, et B. Yi, « Name Lookup in Named Data Networking: A Review », *Information*, vol. 10, nº 3, p. 85, févr. 2019, doi: 10.3390/info10030085.
[47] D. Saxena et V. Raychoudhury, « Radient: Scalable, memory efficient name lookup algorithm for named data networking », *J. Netw. Comput. Appl.*, vol. 63, p. 1-13, mars 2016, doi: 10.1016/j.jnca.2015.12.009.
[48] Abdelali Kerrouche, « Routing Named Data in Information-Centric Networks », Université Paris-Est, 2017.
[49] C. Yi, A. Afanasyev, I. Moiseenko, L. Wang, B. Zhang, et L. Zhang, « A case for stateful forwarding plane », *Comput. Commun.*, vol. 36, nº 7, p. 779-791, avr. 2013, doi: 10.1016/j.comcom.2013.01.005.
[50] C. Yi, J. Abraham, A. Afanasyev, L. Wang, B. Zhang, et L. Zhang, « On the role of routing in named data networking », in *Proceedings of the 1st international conference on Information-centric networking - INC '14*, Paris, France, 2014, p. 27-36, doi: 10.1145/2660129.2660140.
[51] L. Zhang *et al.*, « Named Data Networking (NDN) Project », p. 26.
[52] Y. Zhang, A. Afanasyev, J. Burke, et L. Zhang, « A survey of mobility support in Named Data Networking », in *2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, San Francisco, CA, USA, avr. 2016, p. 83-88, doi: 10.1109/INFCOMW.2016.7562050.
[53] A. Tariq, R. A. Rehman, et B.-S. Kim, « Forwarding Strategies in NDN-Based Wireless Networks: A Survey », *IEEE Commun. Surv. Tutor.*, vol. 22, nº 1, p. 68-95, 2020, doi: 10.1109/COMST.2019.2935795.
[54] H. Qian, R. Ravindran, G.-Q. Wang, et D. Medhi, « Probability-Based Adaptive Forwarding Strategy in Named Data Networking », p. 8.

[55] M. Varvello, I. Rimac, U. Lee, L. Greenwald, et V. Hilt, « On the Design of Content-Centric MANETs », p. 8.

[56] Y. Lu, B. Zhou, L.-C. Tung, M. Gerla, A. Ramesh, et L. Nagaraja, « Energy-efficient content retrieval in mobile cloud », in *Proceedings of the second ACM SIGCOMM workshop on Mobile cloud computing - MCC '13*, Hong Kong, China, 2013, p. 21, doi: 10.1145/2491266.2491271.

[57] C. Li, W. Liu, et K. Okamura, « A greedy ant colony forwarding algorithm for Named Data Networking », *Proc. Asia-Pac. Adv. Netw.*, vol. 34, nº 0, p. 17, mai 2013, doi: 10.7125/APAN.34.3.

[58] M. Meisel, V. L. Pappas, et L. Zhang, « Listen First , Broadcast Later : Topology-Agnostic Forwarding under High Dynamics », 2010.

[59] Yu-Ting Yu, R. B. Dilmaghani, S. Calo, M. Y. Sanadidi, et M. Gerla, « Interest propagation in named data manets », in *2013 International Conference on Computing, Networking and Communications (ICNC)*, San Diego, CA, janv. 2013, p. 1118-1122, doi: 10.1109/ICCNC.2013.6504249.

[60] Jaebeom Kim, Daewook Shin, et Young-Bae Ko, « TOP-CCN: Topology aware Content Centric Networking for Mobile Ad Hoc Networks », in *2013 19th IEEE International Conference on Networks (ICON)*, Singapore, Singapore, déc. 2013, p. 1-6, doi: 10.1109/ICON.2013.6781983.

[61] R. A. Rehman et B.-S. Kim, « LOMCF: Forwarding and Caching in Named Data Networking Based MANETs », *IEEE Trans. Veh. Technol.*, vol. 66, nº 10, p. 9350-9364, oct. 2017, doi: 10.1109/TVT.2017.2700335.

[62] R. A. Rehman, T. D. Hieu, Hong-Min Bae, Sung-Hoon Mah, et B.-S. Kim, « Robust and efficient multipath Interest forwarding for NDN-based MANETs », in *2016 9th IFIP Wireless and Mobile Networking Conference (WMNC)*, Colmar, France, juill. 2016, p. 187-192, doi: 10.1109/WMNC.2016.7543988.

[63] Y. Ren, J. Li, S. Shi, L. Li, G. Wang, et B. Zhang, « Congestion control in named data networking – A survey », *Comput. Commun.*, vol. 86, p. 1-11, juill. 2016, doi: 10.1016/j.comcom.2016.04.017.

[64] N. Rozhnova et S. Fdida, « An effective hop-by-hop Interest shaping mechanism for CCN communications », in *2012 Proceedings IEEE INFOCOM Workshops*, Orlando, FL, USA, mars 2012, p. 322-327, doi: 10.1109/INFCOMW.2012.6193514.

[65] « Meet Android Studio | Développeurs Android », *Android Developers*. https://developer.android.com/studio/intro?hl=fr (consulté le juill. 22, 2020).

[66] « Firebase ». https://firebase.google.com/ (consulté le juill. 22, 2020).

[67] « Introduction à Firebase 🔥 », *Les veilleurs de nuit*, avr. 26, 2018. https://lesveilleursdenuit.fr/introduction-a-firebase/ (consulté le juill. 22, 2020).

[68] S. Mastorakis, A. Afanasyev, et L. Zhang, « On the Evolution of ndnSIM: an Open-Source Simulator for NDN Experimentation », *ACM SIGCOMM Comput. Commun. Rev.*, vol. 47, nº 3, p. 19-33, sept. 2017, doi: 10.1145/3138808.3138812.

[69] S. Mastorakis, A. Afanasyev, I. Moiseenko, et L. Zhang, « ndnSIM 2.0: A new version of the NDN simulator for NS-3 », p. 8.