République Algérienne Démocratique et Populaire
Ministère de l'enseignement supérieur et de la recherche scientifique
Université Larbi Tébessi - Tébessa
Faculté des Sciences Exactes et des Sciences de la Nature et de la Vie
Département : Mathématiques et Informatique

Mémoire de fin d'étude
Pour l'obtention du diplôme de MASTER
Domaine : Mathématiques et Informatique
Filière : Informatique
Option : Systèmes et Multimédia

Thème

Un système d'ingénierie de trafic adaptatif basé sur des topologies de routage virtuels.

Présenté Par :
CHABANE Issam

Devant le jury :

Mr Ahmim Ahmed	*MCA*	*Univérsité Larbi Tébessa*	*Président.*
Mr Tag Samir	*MAA*	*Univérsité Larbi Tébessa*	*Examinateur.*
Mr Derdour Makhlouf	*MCA*	*Univérsité Larbi Tébessa*	*Encadreur.*
Mr Sahraoui Abdelatif	*MAB*	*Univérsité Larbi Tébessa*	*Co-Encadreur.*

Date de soutenance : 23/06/2019

Résumé

Les recherches dans le domaine des réseaux se succèdent sans relâche, un tout nouveau champ productif vient juste d'apparaître et d'être martelé d'un poing de fer qui provoque un écho important puisqu'il touche divers axes de l'informatique, c'est le concept de **virtualisation** que nous pouvons rencontrer dans presque tous les domaines de l'informatique : systèmes d'exploitation, environnement de développement, émulateurs, réseaux et le Cloud.

Parler des réseaux de point de vue flux, répartition de charge, bande passante provoque toujours la prise en compte du problème de **congestion**. La congestion est une situation critique dans le Traffic dans laquelle les données sont bloquées dans un nœud ou plus et où le destinataire attend quelque chose qui peut ne pas arriver.

Nous avons rencontré de nombreux sujets et modèles sur la décomposition de la structure des réseaux avec des points intéressants à plusieurs égards. Notre contribution commence par le trafic conçu et son mode de mesure. Ensuite, la manière d'adapter le trafic en se basant sur des technologies de virtualisation et des systèmes d'ingénierie du trafic basés sur le routage virtuel. Dans ce mémoire, nous suggérons une technique pour gérer le trafic de manière dynamique en utilisant deux étapes : la surveillance du réseau et l'adaptation des réseaux.

Abstract

The research in the field of networks succeeds one after the other, a brand-new productive field has just appeared and hammered with an iron fist which provokes an important echo since it touches various axes of the computer science. the concept of virtualization that we can encounter in almost all areas of computing: operating systems, development environment, emulators, networks and the cloud. Speaking networks from a point of view: flow, load balance, bandwidth always causes the problem of congestion to be taken into account. Congestion is a critical situation in traffic where data is stuck in one or more nodes and the receiver is waiting for something that may not happen. We have come across many topics and models on the decomposition of the network structure with points of interest in several aspects. Our contribution begins with the designed traffic and its mode of measurement. Then, how to adapt the traffic based on virtualization technologies and traffic engineering systems based on virtual routing. In this thesis, we suggest a technique of managing traffic dynamically using two steps: network monitoring and network adaptation.

ملخص

تعمل الأبحاث في مجال الشبكات على مدار الساعة دون توقف دائمًا ، وهو حقل خصب جديد ومتكامل برزحديثا مسببا قفزة كبيرًة حيث يلامس مختلف محاور الكمبيوتر. هو مفهوم المحاكاة الافتراضية التي يمكن أن نجدها في جميع مجالات الحوسبة تقريبًا: أنظمة التشغيل ، بيئة التطوير ، المحاكيات ، الشبكات والسحابة.

التحدث عن الشبكات من وجهة نظر التدفق ، توزيع الحمل ، وعرض النطاق الترددي يحتم دائما الأخذ بعين الإعتبارمشكلة الازدحام التي يتعين مراعاتها. الازدحام هو موقف حرج في حركة مرور وتبادل المعلومات حيث يتم تعليق البيانات في عقدة واحد أو أكثر و إنتظار شيئًا قد لا يحدث.

لقد واجهنا العديد من الموضوعات والنماذج حول تحليل بنية الشبكة مع وجود نقاط اهتمام من عدة جوانب. تبدأ مساهمتنا مع حركة المرور المصممة وطريقة القياس. ثم ، كيفية تكييف حركة المرور بناءً على تقنيات المحاكاة الافتراضية وأنظمة هندسة المرور المعتمدة على التوجيه الظاهري. في هذه الرسالة ، نقترح تقنية لإدارة حركة المرور بشكل حيوي باستخدام خطوتين: مراقبة الشبكة والتكيف مع الشبكة.

Remerciements

Avant tout, je remercie Dieu le tout puissant de m'avoir donné le courage et la patience de terminer ce travail.

Je tiens à exprimer mes sincères remerciements et ma reconnaissance à mes encadreurs de mémoire monsieur le Docteur Makhlouf Dardour et monsieur le Docteur Sahraoui Abdelatif qui m'ont encadré et soutenu tout au long de ce travail de mémoire. Leurs grandes qualités humaines, leurs conseils scientifiques, et leurs critiques constructives ont rendu ce travail particulièrement enrichissant. Je tiens à les remercier pour m'avoir communiqué leurs passions pour la recherche scientifique.

Je tiens à remercier mon frère FATHI qui a fait preuve de patience à mon égard. Il a supporté mon indisponibilité et mes sautes d'humeur en m'écoutant et en me conseillant. Cette aide morale fut d'un grand réconfort. Merci d'être à mes côtés chaque jour et de m'apporter ton courage et ta gaieté.

Mes sincères remerciements s'adressent à mes parents, mes frères, mes sœurs ainsi qu'à toute la famille pour leur soutien moral, leur encouragement inconditionnel et leurs aisés financiers. Sans oublier de remercier tous les enseignants et enseignantes qui, pendant mon cursus universitaire, ont veillé pour ma formation et ma réussite.

Je remercie également mon maitre de stage, Mr B.Houcine, pour son accueil, le temps consacré et le partage de son expertise au quotidien.

Tous les mots restent faibles pour exprimer ma profonde reconnaissance à tous ceux qui m'ont aidé de près ou de loin pour la réalisation de ce travail, en particulier tous mes ami(e)s pour leur soutien moral et leur présence à mes côtés.

Dédicaces

Je rends grâce au mon Dieu de m'avoir donné la force, la volonté et la sagesse afin de parvenir à cette conclusion de mon cycle.
Dans cet espace je souhaiterai dédier ce travail à mes très chers parents
En premier lieu mes dédicaces vont droit à ma chère mère. Tes encouragements et tes prières ont été d'un grand soutien pour moi je te remercie infiniment.
Je remercie également mon cher père pour sa présence dans ma vie, de son soutien et tous ses sacrifices et ses précieux conseils, j'espère avoir réussi à te rendre fière chose que je tâcherai de continuer à faire.
Je le dédie aussi à tous mes oncles et tantes. À mes adorables frères : ramzy, fouad, khalil, mes sœurs pour leur patience.
A la personne qui m'a toujours soutenu et a été présent à mes côtés, Hadjer.
À chaque cousins speclialement salim et cousines.
Enfin je le dédie à tous mes amis : Ayemen, Saif, Ali, Ishak, Badida, Thabet, Aziz, Bilal, et mes amies : Sakina, Ahlem et à toute personne qui ma aider et encourager de prêt ou de loin toute au long de mes étude.

Table des matières

Table des matières

Table des matières

Liste des figures

Liste des figures

Introduction générale

Les protocoles de communication constituent de plusieurs règles pour un type de communication particulier afin de transmettre des informations échangées entre des hôtes via un réseau ou un autre intermédiaire, chaque protocole doit maîtriser des règles d'émission et de réception des données. Un protocole internet, (Internet Protocol abrégé en IP) a été utilisé pour permettre la communication entre deux hôtes. IP est un protocole hors ligne fournit des fragments de grandes quantités de données en paquets de petite taille transmissible. On dit qu'un réseau IP est congestionné lorsque la demande d'une ressource dépasse sa capacité. Il s'agit de la situation dans laquelle une augmentation des transmissions de données entraîne une réduction proportionnelle de débit ou une réduction de débit, cela entraîne une faible qualité de service (QoS), des connexions VoIP instables, une expérience de navigation Internet médiocre et une frustration des performances de médias en streaming.

Le transfert de données à beaucoup participer à l'explosion d'un grand trafic sur L'internet, d'où il a besoin d'une fonction du trafic qui le gère et l'organise. Le routage du trafic est considéré comme la plus importante fonction remplie par Internet. Par conséquent, l'importance du contrôle et de l'optimisation de la fonction de routage peut être une fonction distinctive dans l'ingénierie du trafic sur Internet. Afin d'organiser le trafic réseau de façon plus efficace, le routage doit chercher des routes efficaces pour atteindre les performances réseau souhaitées.

Les fournisseurs de réseau Internet sont intéressés par le mécanisme d'ingénierie du trafic, qui cherche à optimiser les performances du réseau et la distribution du trafic. En outre, certains problèmes d'ingénierie du trafic importants, notamment la robustesse, les interactions entre opérateurs et terminaux et l'interopérabilité avec le routage auto-hiérarchique par superposition [WHPH08]. Ainsi, Le succès des services de l'Internet a engendré une explosion du trafic ; ce qui a mené les opérateurs à utiliser de nouvelles technologies dans le cœur des réseaux telles que l'IP sur ATM et l'IP sur le MPLS.

D'autre part, le terme de réseaux virtuels a attiré une attention croissante dans la communauté de la recherche qui permet de virtualiser des ressources réseau au-dessus de la même infrastructure réseau physique, d'où ces ressources incluent des éléments physiques tels que des routeurs ou des liens, ainsi que des autres ressources logicielles telles que des topologies de réseau logiques via des configurations leur permettant de coexister de manière élégante. Dans le même contexte les réseaux virtuels peuvent être instanciés avec leurs propres noms, topologie, routage et gestion des ressources spécifiques à l'application. Comme la congestion du trafic est un problème majeur et croissant dans tous les réseaux traditionnels, et aussi dans les réseaux virtuels. La congestion ralentit le trafic dans les réseaux virtuels en plusieurs raisons comme le partage des périphériques (exemple : les cartes réseaux physiques, switches …) ce qui provoque un retard ou une perte de paquet et ce qui signifie presque une

corruption des données. En outre, s'il y a une congestion de trafic, les paquets mettent plus de temps pour traverser le réseau, ce qui cause la plénitude des mémoire tampon (Les buffers), alors des paquets seront abandonnés. Si la congestion continue d'augmenter, il peut en résulte la perte totale du réseau. Il est donc nécessaire de l'identifier le plus rapidement possible afin de le résoudre.

Dans ce contexte l'objectif de notre recherche est de proposer une méthode pour la gestion dynamique du trafic dans les réseaux de capteurs virtuels qui exécute un contrôle adaptatif du trafic en utilisant plusieurs topologies de routage virtualisées.

Le structure de notre mémoire est organiser en quatre chapitres fondamentaux. Tous d'abord, nous allons introduire dans le premier chapitre le concept d'ingénierie du trafic et leur gestion et taxonomie. Nous allons également mentionner ces principes. Ensuite, nous allons présenter leur mesure et discuter notamment la dynamique d'ingénierie du trafic en introduisant le système MPLS après la description de la congestion du trafic. Puis, nous allons aborder la stratégie DLB (Dynamic Load-Balancing) et certaines d'autres techniques d'adaptation du trafic, telles que MATE et DATE.

Dans le deuxième chapitre, nous expliquerons le concept de virtualisation et leur classification, et nous décrirons la virtualisation du réseau avec des techniques telles que VLAN et VPN, après ça nous ferons référence au terme de routage qui peut être statique ou dynamique, et nous discuterons la classification de ses protocoles (protocoles IGP ou BGP), puis d'une enquête sur l'ingénierie du trafic basée sur la topologie IGP multi-adaptative, le dernier titre abordant les systèmes les plus essentiels basés sur les topologies de routage virtuel.

Le troisième chapitre est consacré à la description de notre méthode proposée pour la gestion dynamique du trafic dans les réseaux de capteurs virtuels qui exécute un contrôle adaptatif du trafic en utilisant plusieurs topologies de routage virtualisées.

Le quatrième chapitre, nous allons présenter un cas d'étude sous OMNeT++, ainsi qu'une implémentation de la méthode proposée en essayant de montrer certaines de nos idées, telles que détecter la congestion du trafic et la distribution du trafic via des trajets multiples virtuels dans des réseaux de capteurs sans fil.

Chapitre 01 : L'ingénierie du trafic

Chapitre 01 : L'ingénierie du trafic

Introduction

La société de l'information en émergence exige des services de communication permettant une utilisation intégrée des données multimédia tels que l'audio, image, vidéo et texte dans un environnement de télécommunication unique. Les fournisseurs de services réseau doivent donc exploiter leurs réseaux pour fournir ces services aux utilisateurs finaux. Le processus de gestion de l'allocation des ressources réseau pour acheminer le trafic sujet à des contraintes de qualité de service spécifiées par l'utilisateur est appelé ***ingénierie de trafic***. Cette ingénierie a pour objectif d'accroître l'efficacité de l'utilisation des ressources du réseau, tout en assurant les contraintes de qualité de service.

Les activités d'ingénierie du trafic Internet traditionnelles étaient réalisées avec une intervention humaine directe. Cependant, ces activités deviennent de plus en plus exigeantes et utilisent beaucoup de données. Il a été remarqué dans les réseaux IP publics à grande échelle, Étant donné de la taille, de la complexité et du fonctionnement multiserveur croissants du réseau. Sur ce scénario, le défi fondamental que l'ingénierie du trafic pose à l'intelligence artificielle est la réalisation de capacités de contrôle automatisé qui s'adaptent rapidement et à moindre coût aux changements importants de l'état du réseau, tout en maintenant la stabilité. Ceci serait idéalement accompli de manière proactive en utilisant des techniques de prévision pour anticiper les tendances futures et en appliquant des actions pour éviter les états futurs indésirables prédits.

1. Ingénierie du trafic

L'ingénierie du trafic (Traffic Engineering ou TE en anglais) est définie par l'IETF (Internet Engineering Task Force) comme étant l'aspect de l'ingénierie de réseau traitant du problème de l'évaluation et de l'optimisation des performances des réseaux IP [ACE01]. L'ingénierie du trafic doit mapper efficacement les demandes de trafic sur la topologie du réseau et configurer le mappage de manière adaptative aux conditions changeantes du réseau. L'ingénierie du trafic englobe l'application de principes technologiques et scientifiques à la mesure, à la caractérisation, à la modélisation et au contrôle du trafic Internet [AWD2].

L'application systématique des concepts d'ingénierie du trafic aux réseaux opérationnels présente un avantage subtil mais pratique : elle permet d'identifier et de structurer les objectifs et les priorités en termes d'amélioration de la qualité du service fourni aux utilisateurs finals des services réseau. L'application de concepts d'ingénierie de trafic facilite également la mesure et l'analyse de la réalisation des objectifs. Les aspects d'optimisation de l'ingénierie du trafic peuvent être atteints grâce à la gestion de la capacité et à la gestion du trafic.

A. La gestion de la capacité

Cette gestion inclut la planification de la capacité, le contrôle de routage et la gestion des ressources. Les ressources réseau présentant un intérêt particulier incluent la bande passante de liaison, l'espace tampon et les ressources de calcul [ACE01].

B. La gestion du trafic

Notamment, la gestion du trafic contient plusieurs des fonctions qui ont spécialisée de contrôle du trafic nodal telles que le conditionnement du trafic, la gestion des files d'attente, la planification, et d'autres fonctions qui régulent le flux de trafic sur le réseau ou arbitrent l'accès aux ressources du réseau paquets ou entre différents flux de trafic.

C. Les objectifs d'optimisation de l'ingénierie du trafic Internet

L'ingénierie de trafic exige également le développement continu de nouvelles technologies pour l'amélioration des performances du réseau aussi elle exige de nouvelles méthodologies [ACE01]. Aussi ça peut changer avec le temps, que de nouvelles technologies apparaissent ou que de nouvelles connaissances sont apportées pour résoudre les problèmes sous-jacents. De plus, différents réseaux peuvent avoir différents objectifs d'optimisation, en fonction de leurs modèles commerciaux, de leurs capacités et de leurs contraintes d'exploitation. Les aspects d'optimisation de l'ingénierie du trafic concernent en définitive le contrôle du réseau, quels que soient les objectifs d'optimisation spécifiques dans un environnement particulier. Ce contrôle peut être proactif et / ou réactif [ACE02] dans le domaine de l'ingénierie du trafic Internet. Le système de contrôle d'ingénierie de trafic cherche à éviter les conditions défavorables futures du réseau, en prenant des mesures préventives dans le cas proactif, Il peut également être nécessaire de prendre des mesures pour créer un état plus souhaitable à l'avenir. Dans le cas réactif, le système de contrôle répond de manière correcte et éventuellement adaptative aux événements déjà survenus dans le réseau.

D. La dimension de contrôle de l'ingénierie du trafic Internet

De résolution temporelle aux événements réseau en étant répondu à plusieurs niveaux par la dimension de contrôle de l'ingénierie du trafic Internet. Certains aspects de la gestion de la capacité, tels que la planification de la capacité, répondent à des niveaux temporels très grossiers, allant de quelques jours à éventuellement plusieurs années. L'introduction de réseaux de transport optique à commutation automatique (basés sur les concepts de commutation lambda à protocoles multiples, par exemple) pourrait réduire considérablement le cycle de vie de la planification de la capacité en accélérant l'approvisionnement en bande passante optique. Les fonctions de contrôle de routage fonctionnent à des niveaux intermédiaires de résolution temporelle, allant de quelques millisecondes à plusieurs jours. Les entrées dans le système de contrôle d'ingénierie du trafic incluent des variables d'état du réseau, des variables de politique et des variables de décision. L'un des principaux défis de l'ingénierie du trafic Internet est la réalisation de capacités de contrôle automatisé qui s'adaptent rapidement et à moindre coût aux changements importants de l'état du réseau, tout en maintenant la stabilité [SLCWT01].

Une autre dimension critique de l'ingénierie du trafic Internet notée l'évaluation des performances du réseau. Elle est essentielle pour évaluer l'efficacité des méthodes d'ingénierie du trafic, ainsi que pour la surveillance et la vérification de la conformité aux objectifs de performance du réseau. Les résultats de l'évaluation des performances peuvent être utilisés pour identifier les problèmes existants, orienter la ré-optimisation du réseau et aider à prévoir les éventuels problèmes futurs. L'évaluation de la performance peut être réalisée de différentes manières [ACE01]. Les techniques les plus remarquables comprennent les méthodes

analytiques, la simulation et les méthodes empiriques basées sur des mesures. Lorsque des méthodes analytiques ou des simulations sont utilisées, les nœuds et les liaisons de réseau peuvent être modélisés pour capturer les caractéristiques opérationnelles pertinentes telles que la topologie, la bande passante, l'espace tampon et les politiques de service nodal (ordonnancement des liaisons, hiérarchisation des paquets, gestion des tampons, etc.). Les modèles de trafic analytique peuvent être utilisés pour décrire les caractéristiques de trafic dynamiques et comportementales, telles que la rupture en rafale, les distributions statistiques et la dépendance.

En règle générale, les concepts et les mécanismes d'ingénierie du trafic doivent être suffisamment spécifiques et bien définis pour répondre aux exigences connues, tout en étant flexibles et extensibles pour répondre à des demandes futures imprévues.

1.1. Les taxonomies des systèmes d'ingénierie de trafic

Cette section présente une courte taxonomie des systèmes d'ingénierie de trafic selon Awduche [ACE01]. Une taxonomie des systèmes d'ingénierie de trafic peut être construite en fonction des styles et des vues d'ingénierie de trafic énumérés ci-dessous :

- Dépend du temps vs Dépend de l'état (Les méthodologies).
- Hors Ligne vs En Ligne.
- Contrôle Centralisé vs Contrôle Distribué.
- Informations locales vs globales.
- Prescriptive vs Descriptive.
- Boucle Ouverte vs Boucle Fermée.
- Tactique vs Stratégique.

1.1.1. Les méthodologies d'ingénierie de trafic

Les méthodologies d'ingénierie du trafic sont classées en deux types de base : dépendant du temps et dépendant de l'état [ACE02].

Dépend du temps (Time-Dependent) :

Dans l'ingénierie du trafic en fonction du temps, des algorithmes de contrôle du trafic sont utilisés pour optimiser l'utilisation des ressources en réponse aux variations de trafic à grande échelle (heures, jours, semaines). Les mécanismes dépendant du temps utilisent des informations historiques sur les modèles de trafic pour préprogrammer la présentation et l'attribution de trafic LSP (Label Switch Path) 1. Un exemple d'algorithme dépendant du temps pour l'optimisation des ressources globales est proposé par Mitra [MR99a]. L'algorithme formule le problème d'ingénierie du trafic avec plusieurs classes de services et plusieurs chemins en tant que problème linéaire multi-produits.

Dépend de l'état (State-Dependent) :

Des mécanismes dépendant de l'état sont utilisés pour gérer des variations considérables de la charge de trafic réelle, impossibles à prédire à l'aide d'informations historiques. Ces mécanismes sont utilisés pour traiter l'affectation adaptative du trafic aux LSP établis en

fonction de l'état actuel du réseau (utilisation du trafic, retard de paquet, perte de paquet, etc.). Des exemples d'algorithmes dépendants de l'état sont le routage basé sur des contraintes et l'équilibrage de charge entre des trajets multiples. Le routage basé sur les contraintes tente d'acheminer les nouvelles demandes de connexion en minimisant les retards sous réserve des contraintes de ressources. Le Partage de Charge (Load Balancing) tente de répartir le trafic sur plusieurs chemins entre des nœuds source et destinateur. Un paquet entre dans le réseau dans un nœud d'entrée et quitte le réseau dans un nœud de sortie. Une route est une séquence de nœuds entre les nœuds d'entrée et de sortie. Un paquet traverse le réseau en utilisant un itinéraire donné.

1.1.2. Hors Ligne vs En Ligne

L'ingénierie du trafic nécessite le calcul de plans de routage. Le calcul peut être effectué en ligne ou hors ligne [ACE02].

Les systèmes TE hors ligne utilisent toutes les informations de chemin pour calculer les placements de chemin de coût minimal. Le calcul peut être effectué hors ligne pour les scénarios où les plans de routage ne doivent pas nécessairement être exécutés en temps réel. En règle générale, le calcul hors ligne est également utilisé pour effectuer des recherches approfondies sur des espaces de solution multidimensionnels. D'autre part les systèmes TE en ligne calculent les LSP à l'arrivée des demandes entrantes. Le calcul en ligne est requis lorsque les plans de routage doivent s'adapter à l'évolution des conditions du réseau, comme dans les algorithmes dépendant de l'état. Contrairement au calcul hors ligne (qui peut être exigeant en calcul), le calcul en ligne est orienté vers des calculs simples et rapides relatifs permettant de sélectionner des itinéraires, d'ajuster les allocations de ressources et d'effectuer un équilibrage de charge (voir Figure 1).

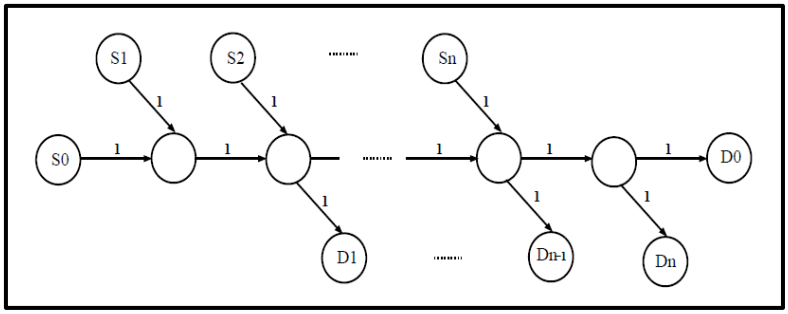


Figure 1 : Les performances de l'ingénierie de la circulation en ligne et hors ligne peuvent varier considérablement [ACE02].

1.1.3. Contrôle Centralisé vs Contrôle Distribué

Le contrôle centralisé [ACE02] a une autorité centrale qui détermine les plans de routage et peut-être d'autres paramètres de contrôle de IT pour le compte de chaque routeur. L'autorité centrale collecte périodiquement les informations sur l'état du réseau auprès de tous les routeurs et les renvoie aux routeurs. Le cycle de mise à jour de routage est un paramètre critique ayant une incidence directe sur les performances du réseau contrôlé. Le contrôle centralisé peut nécessiter une puissance de traitement élevée et des canaux de contrôle de bande passante élevée. En revanche Le contrôle distribué [ACE02] détermine la sélection de route par chaque

routeur de manière autonome en fonction de la vue des routeurs de l'état du réseau. Les informations d'état du réseau peuvent être obtenues par le routeur à l'aide d'une méthode de vérification ou distribuées périodiquement par d'autres routeurs au moyen d'annonces d'état de liaison. Les informations sur l'état du réseau peuvent également être diffusées dans des conditions exceptionnelles.

1.1.4. Informations locales vs informations globales

Les algorithmes d'ingénierie de trafic peuvent nécessiter des informations d'état de réseau locales ou globales [ACE02].

Les informations locales : Concernent l'état d'une partie du domaine. Les exemples incluent la bande passante et le taux de perte de paquets d'un chemin particulier. Les informations d'état local peuvent être suffisantes pour certaines instances de terminaux gérés contrôlés.

Les informations globales : Concernent l'état de l'ensemble du domaine en cours d'ingénierie du trafic. Les exemples incluent une matrice de trafic global et des informations de chargement sur chaque lien dans le domaine d'intérêt. Les informations d'état global sont généralement requises avec un contrôle centralisé. Les systèmes TE distribués peuvent également avoir besoin d'informations globales dans certains cas.

1.1.5. Prescriptive et Descriptive

Les systèmes d'ingénierie du trafic peuvent également être classés comme prescriptif ou descriptif [ACE02]. L'ingénierie de trafic prescriptive évalue les alternatives et recommande un plan d'action, elle peut également être classée comme corrective ou perfectionniste. La première consiste a prescrit un plan d'action pour remédier à une anomalie existante ou prévue et l'autre fournit a prescrit un plan d'action pour faire évoluer et améliorer les performances du réseau même en l'absence d'anomalies évidentes. D'autre part, l'ingénierie de trafic descriptive caractérise l'état du réseau et évalue l'impact de diverses politiques.

1.1.6. Boucle Ouverte vs Boucle Fermée

Comme dans [ACE02] Le contrôle d'ingénierie du trafic en boucle ouverte est l'endroit où l'action de contrôle n'utilise pas les informations de retour provenant de l'état actuel du réseau. L'action de contrôle peut toutefois utiliser ses propres informations locales à des fins comptables. Tandis que le contrôle d'ingénierie du trafic en boucle fermée est l'endroit où l'action de contrôle utilise les informations de retour provenant de l'état du réseau. Les informations de retour peuvent être sous la forme d'informations historiques ou de mesures actuelles.

1.1.7. Tactique vs Stratégique

L'ingénierie de trafic tactique vise à résoudre des problèmes de performances spécifiques (tels que les points chauds) qui surviennent dans le réseau d'un point de vue tactique, sans tenir compte des impératifs stratégiques généraux. Sans planification ni perspicacité adéquates, l'ingénierie de trafic tactique a tendance à être de nature ad hoc. Alors que l'ingénierie de trafic stratégique aborde le problème de l'ingénierie de trafic dans une perspective plus organisée et

systématique, en prenant en compte les conséquences immédiates et à long terme de politiques et d'actions spécifiques [ACE02].

1.2. La mesure du trafic

L'utilisation de la mesure du trafic est pour la collection des données de trafic aux fins suivantes [SLCWT01] :

- Caractérisation du trafic.
- Surveillance du réseau.
- Contrôle du trafic.

1.2.1. Caractérisation du trafic

Dans ce titre, nous mentionnons quelques points prenant qui décrivent la caractérisation du trafic, ces points sont les suivants [SLCWT01] :

- Identification des modèles de trafic, en particulier des modèles de pics de trafic, et leurs variations dans l'analyse statistique. Consiste notamment à développer des profils de trafic afin de capturer les variations quotidiennes, hebdomadaires ou saisonnières.
- Détermination des répartitions du trafic sur le réseau en fonction des flux, interfaces, liens, nœuds, paires de nœuds, chemins ou destinations.
- Estimation de la charge de trafic en fonction des classes de service de différents routeurs et du réseau.
- Observer les tendances de la croissance du trafic et prévoir les demandes de trafic.

Par exemple, les mesures d'ingénierie du trafic sont généralement utilisées pour déterminer les moments statistiques d'un flux de trafic. Comme suggéré dans [RASH00], étant donné la série chronologique des arrivées de paquets, un modèle stochastique paramétrique approprié basé sur la moyenne et la variance de la série temporelle peut être construit. Ce modèle de trafic est ensuite utilisé dans les phases suivantes de l'ingénierie du trafic, telles que le dimensionnement des liaisons pour répondre aux objectifs de service.

1.2.2. Surveillance du réseau

Sur la base des capacités de surveillance du réseau, nous pouvons tirer parti des fonctionnalités comme le suivant [SLCWT01] :

- Elle peut détermine l'état opérationnel du réseau et aussi détecte des pannes. Elle peut aussi contrôler la continuité et de la qualité des services réseau, pour l'objectif de garantir le respect des objectifs QoS / GoS pour différentes classes de trafic et de vérifier les performances des services fournis par un client.
- Sur la base de l'utilisation de données d'historique de performances on peut : le déclenchement de certaines actions basées sur des stratégies d'ingénierie du trafic (telles que la génération d'alarmes ou la préemption de chemin) lors du franchissement de seuil, ou l'évaluation de l'efficacité des stratégies d'ingénierie du trafic.
- La surveillance du réseau peut jouer un rôle important dans la vérification des accords de peering entre fournisseurs de services, d'où dans laquelle la surveille et la mesure des

flux de trafic sur les liaisons d'interconnexion au niveau des routeurs fronteaux, cela inclut l'estimation du trafic inter et intra-réseau, ainsi que du trafic d'origine, de terminaison et de transit échangé entre homologues.

1.2.3. Contrôle du Trafic

Dans les réseaux informatiques, le contrôle du trafic réseau est le processus de la gestion ou de la réduction du trafic réseau permettant les fonctionnalités résumées dans les points suivants [SLCWT01] :

- Optimisation adaptative des performances du réseau en réponse à des événements réseau telles que réacheminement pour contourner la congestion ou les défaillances.
- Fournir un mécanisme de retour d'information dans la messagerie à flux inversé de la signalisation RSVP-TE ou CR-LDP dans MPLS afin de générer des informations sur l'état actuel de la topologie, telles que la disponibilité de la bande passante du lien.
- Il prise en charge du contrôle d'admission basé sur la mesure, c'est-à-dire en prévoyant les futures demandes de l'ensemble des flux existants, de manière à ce que les décisions d'admission puissent être prises pour les nouveaux flux.

Un exemple consisterait à utiliser les résultats de mesure pour les informations en retour dans les décisions de routage IGP, par exemple pour ajuster les poids de lien en fonction de ceux-ci. Un autre exemple de mesures d'ingénierie du trafic utilisées pour appliquer un mécanisme de contrôle du trafic consiste à configurer des mécanismes de contrôle en réponse à des mesures de charge de trafic et de performances. Un opérateur de réseau pourrait restreindre de manière sélective les flux de faible priorité afin d'améliorer les performances en temps quasi réel des flux de priorité supérieure et de maintenir des enveloppes de qualité de service plus étroites.

1.3. Modélisation des abstractions et des transformations

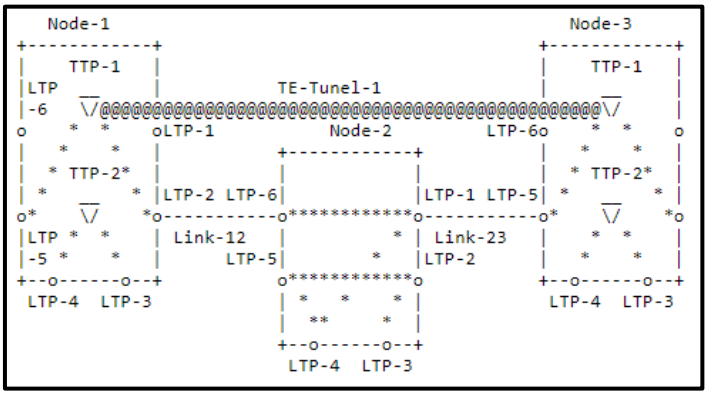


Figure 2 : Abstractions de modélisation de topologie TE [ACE01].

1.3.1. Les topologies de l'ingénierie de trafic

La topologie d'ingénierie du trafic (TET) est une représentation d'ingénierie du trafic d'une ou de plusieurs couches de topologies de réseau. La topologie d'ingénierie du trafic est composée de nœuds d'ingénierie du trafic (sommets de graphe TE) interconnectés via des

liaisons d'ingénierie du trafic (bords de graphe TE). La topologie d'ingénierie du trafic est mappée sur un graphique TE [LJB17].

1.3.2. Le nœud d'ingénierie du trafic

L'élément d'une topologie TE qui présenté comme un sommet sur un graphe TE et qui peut être un ou plusieurs nœuds (commutateurs physiques) s'appelle le nœud d'ingénierie de trafic, ou une fraction d'un nœud, Le nœud TE se voit attribuer l'ID unique d'étendue de topologie TE. Chaque nœud a des attributs chacun ont des informations relatives aux aspects du plan de données des nœuds associés, ainsi que des données de configuration [LJB17].

Les nœuds TE multicouches fournissant des fonctions de commutation au niveau de plusieurs couches réseau constituent un exemple dans lequel un nœud physique peut être décomposé en plusieurs nœuds TE logiques (fractions de nœud). Certains de ces nœuds TE (logiques) peuvent résider dans la topologie TE de la couche client, tandis que les nœuds TE restants appartiennent à la topologie TE de la couche serveur [LJB17].

Dans *la figure 2*, Nœud1, Nœud2 et Nœud3 sont des nœuds d'ingénierie du trafic.

1.3.3. Le lien d'ingénierie de trafic

L'élément d'une topologie TE qui présenté comme une arête sur le graph TE, les flèches indiquent l'une ou les deux directions du lien TE s'appelle le lien d'ingénierie de trafic, Le lien TE est attribué avec l'ID unique d'étendue de topologie TE. Chaque lien a des attributs chacun comprennent des paramètres liés aux aspects du plan de données de la ou des liens associés, ainsi que les données de configuration, chaque lien TE est connectée au nœud TE, terminant le lien TE via exactement un point de terminaison de lien TE (**Link Termination Point** en anglais ou LTP[1]) [LJB17].

Dans *la figure 2*, Link-12 et Link-23 sont des liens TE.

2. La congestion du trafic

Dans cette partie, la définition de la congestion du trafic serait discutée. De plus, nous parlerons des raisons de la congestion du trafic, puis nous présenterons quelques principes ou phénomènes importants qui ne devraient pas être ignorés lorsqu'il s'agissait de congestion du trafic. Enfin, des méthodes théoriques de réduction de la congestion du trafic seraient discutées.

Une congestion peut survenir sur une liaison lorsqu'un routeur atteint sa capacité de mise en mémoire tampon. La congestion pourrait être due à la quantité de trafic dépassant le débit de la liaison. Cela peut se produire lorsque les données transitant par une liaison réseau plus rapide sont routées vers une liaison plus lente [WLi13].

En outre, une accumulation de trafic peut être présente sur un routeur lorsque la quantité de trafic entrant vers un routeur dépasse la quantité de trafic sortant. Cela peut se produire lorsque la charge de trafic n'est pas équilibrée sur le réseau. Plus de trafic est dévié par un routeur du réseau que par d'autres routeurs, ou un routeur peut être confronté à une rafale de

[1] TE **Link Termination Point** (LTP) : est un point conceptuel de connexion d'un nœud TE à l'une des liaisons TE, terminé par le nœud TE.

trafic à fort volume sur une courte période. En conséquence, le trafic entrant sur le routeur dépasse la capacité de la mémoire tampon du routeur et essentiellement, le débit des paquets entrants dépasse le débit des paquets sortants du routeur.

Cet événement entraîne la perte de paquets sur le réseau [WLi13], À mesure que le volume de paquets transitant par le réseau augmente, le débit augmente également. Lorsque le trafic réseau commence à atteindre la capacité du réseau, la vitesse à laquelle le débit augmente commence à ralentir et la congestion se produit. Pour atténuer cet événement, le routeur utilise des schémas de gestion du trafic pour hiérarchiser et supprimer les paquets de moindre importance [JITA04]. En conséquence, le débit des paquets avec une priorité plus élevée augmente aux dépens des autres trafics.

Compte tenu des informations ci-dessus, les pirates peuvent exploiter la vulnérabilité d'un réseau face à la congestion afin de la perturber et d'empêcher le flux de données. Les attaques peuvent être utilisées délibérément pour causer de la congestion sur un routeur ou dans une zone spécifique d'un réseau. Un type d'attaque pouvant générer une accumulation de trafic et créer un encombrement est une attaque par déni de service.

3. L'ingénierie de trafic dynamique

Parmi de nombreuses technologies qui implémentent l'ingénierie du trafic dynamique, nous avons choisi **MPLS** (en anglais **Multiprotocol Label Switching**) pour l'introduire. En MPLS, l'attribution d'un paquet particulier à une classe d'équivalence de transmission (**Forwarding Equivalence Classes** FEC) particulière est effectuée une seule fois, au moment où le paquet entre dans le réseau. La FEC à laquelle le paquet est affecté est codée sous la forme d'une valeur de longueur fixe courte appelée "étiquette" (Ces étiquettes demandent aux routeurs du réseau de transmettre les paquets sur la base de chemins préétablis (qui pourraient être déterminés au moyen de l'IGP ou d'un routage sous contrainte avec ingénierie du trafic MPLS). Lorsqu'un paquet est transmis à son saut suivant, l'étiquette est envoyée avec lui ; c'est-à-dire que les paquets sont "étiquetés" avant d'être transférés. Dans le paradigme de transmission MPLS, une fois qu'un paquet est attribué à une FEC, aucune analyse d'en-tête supplémentaire n'est effectuée par les routeurs suivants. Tout le transfert est conduit par les étiquettes. Cela présente un certain nombre d'avantages par rapport au transfert de couche réseau classique.

Pour le routage, on considère l'algorithme CSPF (Constrained Shortest Path First) [EOAS02], en raison de sa capacité à trouver le chemin le plus court actuel pour une paire de destination source qui satisfait un ensemble de contraintes. CSPF calcule le chemin le plus court entre deux nœuds sur un sous-ensemble du réseau comprenant des liens qui obéissent aux contraintes spécifiées.

Lorsque TE statique est déployé, les TE-LSP sont configurés avec une bande passante réservée fixe associée qui est généralement considérée comme le pic de volume de trafic. Dans ce scénario, il peut arriver que, dans certains cas, le trafic traversant TE-LSP soit bien inférieur à la bande passante qui lui a été réservée sur toutes les liaisons qui se trouvent sur son itinéraire. Inversement, si un TE-LSP est dimensionné avec une valeur de bande passante inférieure au

pic de son volume de trafic, cela peut entraîner des problèmes de congestion et de violation de la qualité de service. Il est clair qu'il faut optimiser ce système [DJOC08].

Le mécanisme dynamique doit trouver un compromis entre redimensionner les connexions chaque fois que la charge de trafic change et le redimensionner moins souvent, mais risquer de ne pas acheminer les connexions sur des trajets plus longs du réseau en raison d'une surréservation ou de risquer des connexions afin de suivre un trajet plus encombré.

3.1. L'ingénierie du trafic IP

La configuration appropriée des métriques IGP permet de mettre en œuvre une ingénierie de trafic. Les fournisseurs de services ne préfèrent pas de modifier la métrique IGP en raison de la charge de configuration, et de l'impact global de la convergence IGP sur les modifications de métrique de lien et également du fait que cela peut conduire à la création de micro-boucles dans le réseau. L'ingénierie du trafic IP ne doit être effectuée que globalement. Dans la plupart des cas, le fournisseur de services ne peut pas connaître la matrice de trafic, ce qui rend difficile la tâche de produire de bonnes métriques IGP [DOV08].

3.2. L'ingénierie du trafic statique

Dans le TE statique, la matrice de trafic est difficile à connaître à l'avance par ce que sa connaissance est nécessaire pour un déploiement robuste. Les avantages du TE statique permettent de mieux utiliser les ressources du réseau en ce qui concerne les demandes de trafic estimées, le trafic suit les plus longs chemins car les tailles de TE-LSP sont généralement basées sur les pointes de trafic. Les TE-LSP peuvent même ne pas être routés, par exemple en cas d'échec [DOV08].

3.3. L'ingénierie de trafic dynamique

Dans l'ingénierie de trafic dynamique, chaque source dans le réseau échantillonne périodiquement le trafic de chacun de ses TE-LSP, après lequel plusieurs méthodes peuvent être utilisées pour décider de la nouvelle taille du TE-LSP [DOV08].

L'ingénierie du trafic dynamique présente plusieurs avantages. De plus en plus de TE-LSP sont acheminés via le chemin le plus court IGP, ce qui réduit le coût total du trajet. Il n'est pas nécessaire de connaître a priori la matrice de trafic, dans la mesure où ingénierie de trafic dynamique prend des mesures du trafic actuel (avantage considérable, car il est difficile pour les fournisseurs de services de disposer de ces données). Un fournisseur de services utilisant l'ingénierie de trafic dynamique est en mesure d'adapter davantage de trafic sur le réseau, car les réservations reflètent le taux de trafic actuel pour le moment et non son pic. L'ingénierie de trafic dynamique est encore plus intéressante lorsque les fuseaux horaires sont pris en compte dans les réseaux mondiaux. L'ingénierie de trafic dynamique pourrait également présenter un intérêt particulier lorsque divers types de TE-LSP (acheminant différents types de trafic) sont mélangés au sein d'un même réseau (par exemple, voix et données). Etant donné que les pics de voix et de données ne se chevauchent pas, la bande passante réservée peut être déplacée d'un type de trafic à l'autre une fois le pic atteint. Dans l'ingénierie de trafic statique, la somme des pics pour la voix et les données serait prise en compte dans ce cas, ce qui réduirait considérablement le trafic circulant sur le réseau [DOV08].

Dans ce contexte, l'hypothèse de grande capacité ne suffit plus. Les opérateurs réseau sont maintenant, et peut-être plus que jamais, en besoin de mécanismes d'Ingénierie Trafic qui soient efficaces (conduisant à une bonne utilisation des ressources disponibles), robustes par rapport aux variations de trafic injecté dans le réseau (changements dans les volumes ou les caractéristiques des flux transportés) et plus tolérants (en cas de panne d'un nœud ou un lien). Au fur et à mesure que la taille du réseau augmente, la gestion du réseau peut devenir une tâche très complexe. Les administrateurs réseau sont donc très intéressés par l'automatisation (un minimum de configuration n´nécessaire) des mécanismes TE qu'ils mettent en pratique dans leur réseau [FeLa10].

Le Partage de Charge Dynamique (Dynamic Load-Balancing ou DLB en anglais) est un mécanisme TE qui a pour l'objectif de répartir le trafic entre ces chemins en temps réel, de manière à ce que certains critères ou objectifs soient remplis. Dans ces schémas dynamiques, les chemins sont établis a priori et la quantité de trafic envoyée par chacun d'eux (distribution du trafic) dépend de la demande de trafic actuelle et de l'état du réseau. DLB est généralement utilisé pour répartir le trafic entrant sur le réseau en détournant efficacement la demande sur plusieurs nœuds, et pour la réactivité et la haute disponibilité sont maintenues en redirigeant les demandes uniquement vers les nœuds disponibles sur le réseau.

Dans cette section étudie plusieurs schémas DLB possibles. En ce sens, il est séparé en deux parties : les ressources réservées et les ressources partagées.

3.4. Les ressources réservées

La première partie considère un réseau dans lequel des ressources sont réservées et utilisées exclusivement par chaque chemin basé sur un mécanisme qui gère ces chemins appelé protection croisée (Cross-Protect en anglais). Cette technique d'ingénierie du trafic (TE) (flow-aware) qui offre des garanties de performances pour le flux de trafic et le trafic élastique, et sa configuration ne repose que sur deux paramètres, qui peuvent facilement être mappés sur les garanties de performances cibles. L'avantage de Cross-Protect en ce qui concerne, par exemple, DiffServ, est qu'aucun marquage de paquet n'est requis. Au lieu de cela, les flux sont classés implicitement en fonction de leur vitesse de transmission. Dans ce cas, des formules approximatives pour ses paramètres de QoS sont dérivées. Nos simulations indiquent que les résultats obtenus avec ce nouveau schéma sont bien meilleurs que les chimies classiques d'équilibrage de charge statique [FeLa10].

3.4.1. Protection Croisée

Le trafic IP classé en deux catégories avec des exigences de qualité de service clairement différentes : élastique et en continu. Le trafic élastique est généré par les transferts de documents (page Web, fichier de musique MP3, par exemple). Les flux élastiques associés nécessitent des transferts « aussi rapides que possible ». Le trafic en streaming, quant à lui, est produit par des applications audio et vidéo en temps réel (par exemple, streaming vidéo, conversation VoIP) et nécessite une transmission transparente, c'est-à-dire un faible taux de perte de paquets et un faible retard.

Les réseaux IP sont conçus pour prendre en charge toutes sortes de services, chacun ayant ses propres exigences. Celles-ci sont presque toujours satisfaites dans les réseaux dorsaux IP actuels, en particulier grâce à une surapprovisionnement substantielle. En effet, la capacité des opérateurs de réseau à distinguer les types de trafic entraîne un traitement non discriminant des paquets en transit et des paquets élastiques (mise en file d'attente FIFO). Bien sûr, un marquage explicite utilisant Diffserv serait possible, mais cela a un coût et pose plusieurs autres problèmes, tels que la confiance dans un environnement inter-domaine.

Le surapprovisionnement est en fait une solution satisfaisante, parce qu'il satisfait la plupart des besoins des utilisateurs et faire un induisant coûteuse opérationnels très bas. Cependant, le réseau reste vulnérable aux utilisateurs mal intentionnés, car la qualité de service attendue dépend de la coopération des utilisateurs pour la mise en œuvre du contrôle de congestion de bout en bout (protocole TCP ou autres protocoles « amicaux TCP »). Par exemple, à une défaillance de la liaison ou de l'équipement, tout le trafic risque de subir une dégradation de la qualité de service, y compris des applications critiques telles que la communication vocale ou émission de télévision.

L'ingénierie du trafic et le contrôle du trafic pour une QoS prévisible sont plus commodément réalisés au niveau du flux, plutôt qu'au niveau du paquet ou de l'agrégat. Un flux correspond à une instance d'application, transportée par le réseau. C'est précisément à ce niveau que l'utilisateur perçoit la QoS. Un flux peut, par exemple, correspondre à un téléchargement de page Web, à un appel vocal ou à une diffusion de musique ou de vidéo. Bien qu'en pratique une définition plus précise soit nécessaire, il suffit de définir un flux en tant que flux de paquets partageant des attributs d'en-tête communs (par exemple, le tuple TCP / IP 5 ou l'étiquette de flux IPv6 combinée à l'adresse source ou de destination) et une durée maximale entre paquets [JWR04].

L'intégration des flux [JWR01, BR03] en continu et des flux élastiques peut être réalisée sans détériorer leur qualité de service respective, à condition que les conditions de multiplexage sans tampon soient garanties pour les flux en continu (traités en priorité) et que les ressources restantes soient équitablement réparties entre les flux élastiques. Un moyen possible de réaliser cette intégration consiste à utiliser la protection croisée (Cross-Protect), une implémentation de la mise en réseau dite Flow-Aware décrite dans [SR05].

Un routeur Cross-Protect est constitué de deux composants de contrôle du trafic. D'un côté, un ordonnanceur de file d'attente équitable (Priority Fair Queueing ou PFQ en anglais), qui est un simple ajustement d'un PFQ, qui implicitement différencie flux et flux élastiques. D'autre part, un mécanisme de contrôle d'admission garantissant une qualité de service minimale aux flux acceptés (ou protégés), ainsi que l'évolutivité de l'ordonnanceur en limitant le nombre de flux devant être traités par l'ordonnanceur à un moment donné.

Le planificateur PFQ classe implicitement les flux en flux ou en mode élastique à la volée sur la base du principe suivant. Si un flux de transmission transmet à un taux inférieur au taux équitable actuel, ses paquets sont alors classés comme étant des flux et prioritaires, alors que les flux élastiques (c'est-à-dire les flux encombrés) se partagent la capacité restante d'une manière de partage de processeur (PS). Par conséquent, le partage équitable est imposé par la

discipline de la mise en file d'attente et ne repose pas sur la convivialité TCP du protocole de contrôle de congestion mis en œuvre par les utilisateurs finaux. Le contrôle d'admission est utilisé pour limiter la charge de streaming (appelée charge prioritaire dans le reste, notée PL) à un seuil relatif γs, et le taux actuel obtenu par les flux élastiques (c'est-à-dire le taux équitable, noté dans la suite FR). Au-dessus d'un autre seuil γe. Si l'une de ces conditions n'est pas remplie, les nouveaux flux sont bloqués. De cette manière, une bande passante minimale pour les flux élastiques est garantie et la charge induite par le trafic en flux continu est contrôlée. Les valeurs typiques pour γs et γe sont respectivement d'environ 80% et 1%, valeurs qu'ils ont été utilisés tout au long des simulations selon [FeLa10].

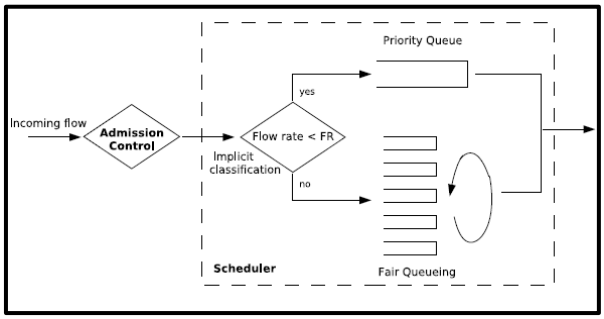


Figure 3 : Schéma de protection croisée.

Un schéma simplifié du mécanisme est illustré à *la Figure 3*. Il est à noter que la classification implicite est appliquée en permanence à tous les flux en cours et pas seulement à l'arrivée des flux vers le routeur. Cela signifie que, à mesure que le débit des flux évolue, leur classification peut également changer. Par exemple, les premiers paquets d'une connexion TCP en mode de démarrage lent sont généralement assimilés à la transmission en continu de paquets [FeLa10].

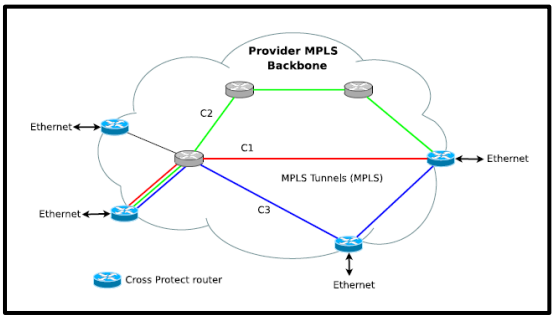


Figure 4 : L'architecture proposée dans MPLS.

La proposition de TE dans les architectures Metro Ethernet consiste à implémenter Cross-Protect dans les routeurs de périphérie (sans aucun impact sur les routeurs principaux). Etant donné que les routeurs périphériques sont connectés via des tunnels d'une capacité donnée, le contrôle de surcharge (sous la forme de contrôle d'admission) peut uniquement être effectué aux nœuds d'entrée. Cela présente l'avantage de limiter les opérations sensibles au flux au bord du réseau et de préserver la simplicité de la transmission de paquets dans le cœur. Un exemple d'une telle architecture TE, dans le cas de tunnels MPLS, est illustré à *la précédante*

Figure 4. Le profil de bande passante peut maintenant être spécifié avec la capacité totale du trajet et les deux seuils (γs et γe).

3.4.2. Analyse de performance

Analyse :

L'analyse générale du modèle intégré n'est pas réalisable, même en supposant une hypothèse simpliste de charges de travail exponentielles. Au lieu de cela, la même idée a été appliquée comme dans [BFDO01] et supposait qu'ils peuvent séparer les échelles de temps des flux et des flux élastiques. Ceci permet d'étudier la file d'attente élastique comme si elle se trouvait dans le régime stationnaire (également appelée hypothèse de quasi-stationnarité (QS)).

L'hypothèse QS se justifie comme suit : en général, la durée moyenne (τs) des flux en flux continu est beaucoup plus grande que la durée moyenne correspondante des flux élastiques. Pour un niveau de charge donné d_s, de, cela signifie que le taux d'arrivée des écoulements en flux et des flux élastiques vérifie que λ_s λ_e. Cette relation implique que les événements associés aux flux de flux se produisent dans le temps et permet à la file d'attente élastique de se comporter dans un régime quasi statique, sous lequel les flux élastiques voient la file d'attente comme un serveur à débit constant.

L'hypothèse QS permet d'analyser la file d'attente élastique en tant que file d'attente *M / G / 1 - PS* de capacité *C - rx*$_s$ pour les flux de transmission x_s présents dans le système. En conséquence, il peut écrire la probabilité de x_e flux élastiques dans le système, car il existe des flux x_s dans la file d'attente de transmission en continu, comme suit :

$$P(N\mathrm{e} = x\mathrm{e}|\mathrm{Ns})) = x\mathrm{s} = \frac{1 - \rho\mathrm{e}(x\mathrm{s})}{1 - \rho\mathrm{e}(x\mathrm{s})^{\mathrm{Nmax\,e}(\mathrm{xs})+1}} \rho e(x_s)^{x_e} \quad 1.1$$

Pour $0 \leq x_e \leq N_e^{max}(x_s)$ où :

$$x = \frac{\lambda_e \mathrm{b}_e}{\mathrm{C} - rx_s} \quad 1.2$$

$$N_e^{max}(xs) = \left\lfloor \frac{C - rx_s}{\gamma_e C} \right\rfloor \quad 1.3$$

Ecrivez donc la probabilité de blocage conditionnée à xs à partir de (1.1) en faisant $N_e = N_e^{max}(x_s)$:

$$B_e(x_s) = \frac{1 - \rho_e(x_s)}{1 - \rho_e(x_s)^{N_e^{\max(x_s)+1}}} \rho_e(x_s)^{N_e^{max(x_s)}} \quad 1.4$$

Pour calculer la probabilité de blocage en régime stationnaire, il doit établir une moyenne de la probabilité de blocage conditionnel $B_e(x_s)$ par rapport à la distribution stationnaire $\pi_s(x_s)$ de la file d'attente de transmission en continu :

$$B = \sum_{x_s=0}^{N_s^{max}} B_e(x_s)\pi_s(x_s) \quad 1.5$$

Où : $N_s^{max} = \left\lfloor \gamma_e \frac{C}{r} \right\rfloor$.

La file d'attente de diffusion en continu se comporterait exactement comme une file d'Erlang avec $A_s = \lambda_s \tau_s$ charge (dans Erlangs), si les flux de diffusion étaient uniquement rejetés en raison de la condition de chargement prioritaire. Mais ce n'est pas le cas, car les deux conditions de charge prioritaire et de tarif équitable sont appliquées indépendamment du type de trafic. Le processus qui en résulte est donc un processus naissance-mort, avec un taux de natalité égal à $\lambda_s\ (1 - B_e(x_s))$ (pour tenir compte de l'état bloquant de la file d'attente élastique) et un taux de mortalité égal à x_s / τ_s dans Etat x_s. La distribution stationnaire devient alors :

$$\pi_s(x_s) = \pi_s(0) \frac{A_s^{x_s}}{x_s!} \prod_{i=0}^{x_s-1} \left(1 - b_e(i)\right) \quad 1.6$$

Où $\pi_s(0)$ peut être obtenu à partir de la condition de normalisation. Les équations (1.4), (1.5) et (1.6) donnent alors la probabilité de blocage B du système.

3.4.3. Simulations au niveau des paquets

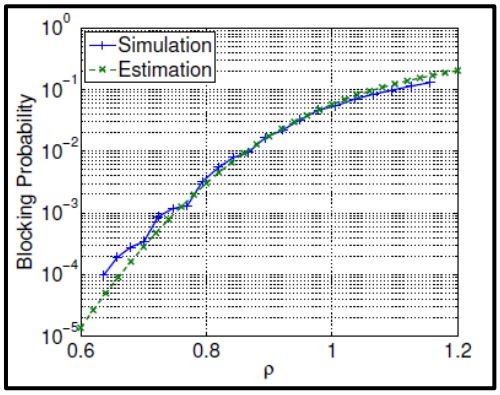


Figure 5 : Estimation de probabilité de blocage et résultats de simulation pour un routeur à protection croisée isolé.

Afin de vérifier l'analyse précédente, ils ont effectué plusieurs simulations au niveau du paquet en utilisant ns-2 [TNS], avec l'implémentation Cross-Protect utilisée dans [KOR04]. Une comparaison entre la probabilité de blocage obtenue par simulation et l'estimation correspondante est visible à *la Figure 5* pour le cas d'un serveur unique, où l'axe des x est l'utilisation de la liaison (c.-à-d. $\rho = (d_e + d_s\ C)$ Le scénario de cas est un mélange de trafic élastique dont la charge de travail suit une distribution de Pareto avec une moyenne de 20 kb et un trafic de streaming avec un débit fixe de 10 kbits / s et une durée de 20 secondes. Le trafic en streaming représente 20% du trafic et le canal a une capacité totale de 1 Mbps.

Bien que l'analyse n'ait pas tenu compte de la dynamique de TCP au niveau des paquets (par exemple, démarrage lent), l'estimation s'avère très précise. Cependant, en présence d'une dynamique au niveau des paquets TCP, le système de classification implicite assimile une partie du trafic TCP au trafic en continu, notamment pendant la phase de démarrage lent. Cela se traduit par un trafic plus prioritaire que prévu par le modèle. Si la probabilité qu'un flux soit bloqué en raison de la condition PL est négligeable, le modèle d'estimation produira des prévisions précises. Sinon, le modèle a tendance à sous-estimer la probabilité de blocage. Cet effet est plus net lorsque la charge est faible, et que la convergence des flux TCP vers leur taux de transfert prend plus de temps, ce qui entraîne un trafic prioritaire plus important que prévu par le modèle, comme expliqué précédemment.

3.4.4. Multiple tunnels et l'analyse du Partage de Charge

Supposons que le trafic consiste uniquement en trafic élastique. Dans cette situation, le problème devient un problème de routage entre plusieurs files d'attente de partage de processeur en parallèle Ce problème a d'abord été étudié par [FBO90], et plus récemment Ce problème a été étudié pour la première fois par [GKAH92].

Leurs résultats montrent que la politique optimale, en termes de probabilité de blocage et de débit, sur la base des informations sur l'état actuel, consiste à envoyer les flux entrants à la file avec le plus petit nombre de flux / clients (Joindre la file la plus courte, JSQ) dans le cas de deux serveurs identiques et des charges de travail exponentielles.

Pour le paramètre général, c'est-à-dire les charges de travail générales et les systèmes non symétriques, le problème est ouvert et la stratégie optimale inconnue. Hajek dans [BH84] a analysé un système plus général permettant différentes capacités dans un cadre markovien. Il a montré, sur la base d'une approche de programmation dynamique, que la politique optimale est toujours le type de commutateur (c'est-à-dire que la probabilité de choisir l'une des files d'attente est 1 ou 0), mais aucune formule explicite pour la courbe de commutateur n'a été fournie. Dans [GKAH92], les auteurs effectuent des calculs numériques pour approximer la courbe de commutation du modèle de Hajek dans un paramètre de routage. Le résultat pour les charges de travail exponentielles, dans le cas de deux serveurs, est que la stratégie optimale en termes de débit est donnée par la stratégie gloutonne exacte (EGP) :

Route vers la file d'attente $i \Leftrightarrow i = arg_j^{max} \frac{Cj}{xj+1}$ 2.1

Où xj est le nombre de clients dans la j -ème file. Il s'agit d'une politique gourmande en ce sens que chaque flux entrant maximisera le tarif équitable qu'il recevra lors de la mise en service dans le système. Dans le cas symétrique, cela se résume à la politique JSQ.

Les auteurs de [BJP04] ont étudié l'approche de Le Partage de Charge dans le cas élastique quand ils ont proposé une autre classe de politiques, le routage équilibré (Balanced Routing), ils sont insensibles à la répartition des charges de travail des flux. L'optimum en termes de probabilité de blocage est défini et se caractérise par les probabilités suivantes dans la classe de stratégies de routage équilibrées :

Route à la file d'attente avec prob. $P_i(x) = \frac{ni-xi}{\sum_j nj-xj}$ 2.2

Où xj est à nouveau le nombre de clients dans la j-ème file d'attente et $n = (n_1, \ldots, n_n)$ correspond au nombre maximal de clients autorisés dans chaque file d'attente. Cette politique s'appelle la politique optimale équilibrée (OBP). La probabilité de blocage B_{obp} dans ce cas peut être facilement calculée [FeLa10].

3.5. Les ressources partagées

Dans la deuxième partie, un réseau « à ressources partagées » sera examiné. Dans ce cas, DLB est défini mathématiquement en termes de fonction objectif à optimiser qui est une nouvelle fonction objective, basée sur les idées du contrôle de la congestion. L'objectif est de maximiser encore l'utilité obtenue par chaque flux, mais sans changer le mécanisme de contrôle de congestion. Au lieu de cela, cette maximisation est réalisée par l'équilibrage de charge, qui contrôle indirectement le débit obtenu du flux en choisissant son chemin [FeLa10].

3.5.1. Routage statique pour le trafic dynamique

Routage robuste

Tous les réseaux ont un trafic de plus en plus complexe et difficile à prévoir pour cela dans [BAK05] [DAEC03] trouve que le routage robuste comme un solution à cet aspect problématique du trafic du point de vue du routage. *Le routage robuste* dont l'objectif est de trouver une configuration de routage statique unique qui réponde à certains critères pour une large gamme de matrice du trafic (Une *matrice de trafic* (TM) représente l'existence du volume de trafic dans un réseau entre toutes les paires de sources et de destinations possibles [PTMR13] *(voir la Figure 6)*, généralement celle qui minimise l'utilisation maximale de la liaison sur tous les matrices du trafic.

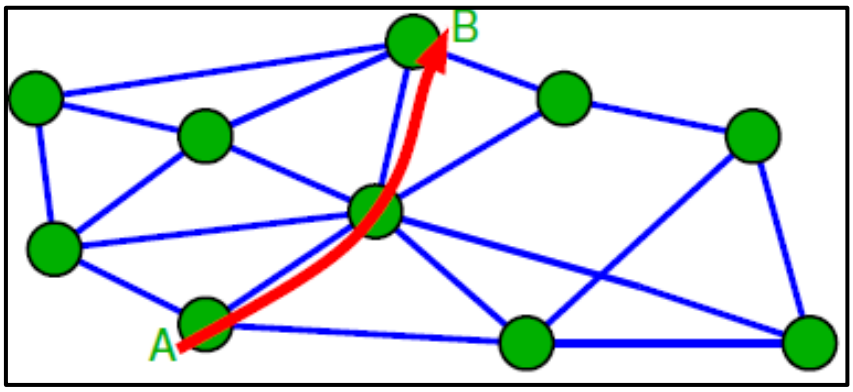


Figure 6 : un exemple d'une matrice de trafic.

Valiant Load-Balancing

Le schéma de routage statique dont nous allons parler est le *Valiant Load-Balancing* en anglais ou **VLB** qui a proposé l'idée de router des paquets par des points centraux aléatoires pour la communication entre des ordinateurs parallèles peu connectés [LGV82], [LVJB81]. Plusieurs groupes ont appliqué l'idée de *Valiant Load Balancing* à l'ingénierie du trafic afin de

prendre en charge efficacement toutes les matrices de trafic possibles [KLS04], [KLS06], [NPKWZ05], [SW06], [ZSMc04], [ZSMc05].

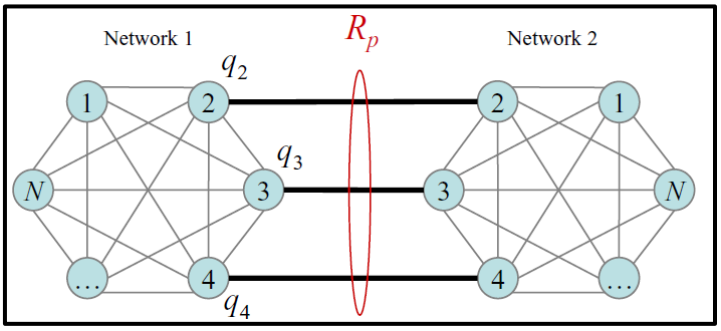


Figure 7 : Deux réseaux VLB se connectent à un ensemble de nœuds de peering.

Le fonctionnement de VLB a un mécanisme simple comme suivant : le trafic entrant sur le réseau est être équilibré entre tous les nœuds qui envoient à leur tour les paquets à leur destination finale. Il existe un seul moyen d'éviter la congestion du réseau : considérons un réseau de *n* nœuds, chacun avec une capacité *r*, chaque nœud pouvant initier et recevoir du trafic au même débit maximal de *r*. dans ce cas, le trafic réseau satisfait à cette contrainte d'agrégat de nœud. Un lien logique de capacité $\frac{2r}{n}$ est établi entre chaque paire de nœuds sur les liens physiques, comme illustré à *la Figure 7* et *la Figure 8*.

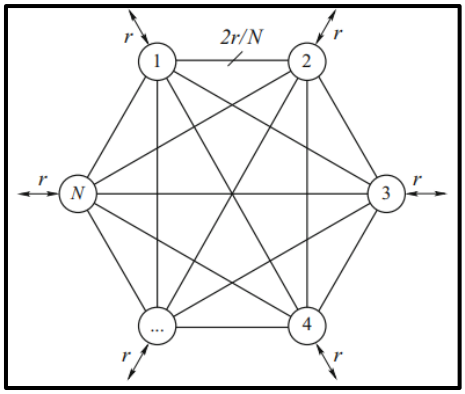


Figure 8 : VLB dans un réseau de *n* nœuds.

Dans [ZSNMc] utilisent la convention selon laquelle un *flux* sur le réseau est défini par le nœud source et le nœud de destination, sauf indication contraire. Chaque flux entrant dans le réseau est également divisé en *n* chemins de deux sauts entre les nœuds (source et destinataires), c'est-à-dire qu'un paquet est transmis deux fois dans le réseau : lors du premier saut, un nœud source distribue uniformément chacun de ses flux entrants à tous les flux entrants. Les *n* nœuds, quelles que soient les destinations. Au deuxième saut, tous les paquets sont envoyés aux destinations finales par les nœuds intermédiaires. Le Partage de Charge (**Load-balancing**) peut se faire paquet par paquet ou flux par flux au niveau du flux d'application [SW]. La division du trafic peut être aléatoire ou déterministe.

3.5.2. Le Partage de Charge Dynamique

Le Partage de Charge Dynamic (Dynamic Load-Balancing en anglais ou DLB) vise à optimiser la répartition du trafic en fonction de la demande de trafic actuelle [KKDC05], en évitant le compromis performance-taille, en obtenant les meilleures performances des ressources disponibles. DLB inclut les défaillances possibles des liens ou des nœuds, il effectue également l'optimisation pour la situation de réseau actuelle. De plus, compte tenu des ressources réseau et tant que les contraintes de capacité sont appliquées, l'ensemble de TM pris en charge est au moins celui pris en charge par les mécanismes statiques [FKF06]. En raison relativement du short time scale (de l'ordre de quelques secondes), les chemins sont établis a priori et la seule adaptation possible est la modification de la quantité de trafic envoyée le long de chacun d'eux. De plus, cette échelle de temps (time-scale) nécessite également que l'algorithme qui contrôle ces adaptations soit exécuté sur chaque routeur d'entrée. La conception de ces algorithmes distribués est probablement l'aspect le plus difficile de DLB. C'est précisément en raison de sa nature dynamique et distribuée que le déploiement de DLB a été quasiment nul [FeLa10]. Les opérateurs de réseau hésitent à l'utiliser principalement parce qu'ils craignent un éventuel comportement oscillatoire de l'algorithme de partage de charge, même lorsque des travaux récents indiquent le contraire par le biais de simulations et de théories [Elwalid] [KKDC05] [FKF06].

Les trois propositions les plus notables dans ce domaine sont TeXCP [KKDC05], RE-Plex [FKF06] et MATE [Elwalid]. Chacun d'eux a sa fonction objective et c'est la première différence entre eux. Nous mentionnons d'abord la fonction objective et sa différence entre les propositions évoquées ci-dessus, TeXCP et REPLEX ils ont un fonction objective commun que ce soit minimiser l'utilisation maximale de la liaison dans le réseau, comme dans RR. Autrement, MATE a une fonction objective de minimiser la somme sur tous les liens de fl (ρl) $(fl(pl)$ est une fonction de lien croissante convexe où ρl est la charge sur le lien *l),* cette fonction représente la congestion sur le lien qui s'efforcer de minimiser l'encombrement total sur le réseau par le DLB. La convexité est intuitivement justifiée par le fait qu'à des charges plus élevées, une augmentation de la charge génère plus de congestion qu'à des charges plus faibles [Elwalid]. Dans [XCR08] les auteurs définissent l'ingénierie du trafic comme un procédure minimisé par l'opérateur de réseau et cela a rendu la fonction cible plus populaire.

L'algorithme de partage de charge distribué (Distributed Load-Balancing) est une différence très importante entre ces trois propositions. TeXCP utilise un algorithme spécialement conçu pour sa fonction objectif, et cela peut être décrit grossièrement comme une augmentation de la quantité de trafic envoyé le long du chemin avec l'utilisation maximale la plus basse. L'algorithme utilisé dans REPLEX est basé sur les méthodes d'échantillonnage adaptatif présentées dans [FRV06]. Concernant MATE l'algorithme de partage de charge est basé sur l'algorithme classique de projection sur gradient [DPB99]. C'est-à-dire qu'à chaque itération, la quantité de trafic envoyée le long du chemin P est mise à jour sous la forme $[dp(t) - \gamma \phi p(t)]^{+}$, où le coût du chemin ϕp est égal à $\sum_{l \in P} f_l(\rho l)$. L'inconvénient majeur de cet algorithme est sa vitesse de convergence [KKDC05]. De plus, pour que la convergence soit garantie, le pas de taille γ doit remplir une condition qui dépend de $f_l(\rho l)$, qui n'est pas nécessairement connue à l'avance.

4. L'adaptation du trafic

Le transfert basé sur la destination dans les routeurs IP traditionnels n'a pas été en mesure de tirer pleinement parti des multiples chemins qui existent fréquemment dans les réseaux de fournisseurs de services Internet. En conséquence, les réseaux peuvent ne pas fonctionner efficacement, en particulier lorsque les modèles de trafic sont dynamiques. MATE adopte une approche minimaliste en ce sens que les nœuds intermédiaires ne sont pas obligés d'effectuer une ingénierie de trafic ou des mesures en plus du transfert de paquets. D'autre part, la congestion sur le réseau entraîne un débit médiocre et de longs retards pour les utilisateurs finaux, ainsi qu'une utilisation inefficace des ressources du réseau. Il a été proposé de gérer le trafic sur plusieurs chemins, MATE et TeXCP Tous deux ont fait de grands progrès en démontrant qu'il est possible de réaliser une ingénierie de trafic dynamique, stable et adaptative aux besoins des utilisateurs et des fournisseurs de services Internet. Un autre algorithme proposé dans [HMC] qui se distingue des travaux antérieurs en répondant simultanément aux besoins des utilisateurs et des fournisseurs de services Internet.

4.1. MATE et DATE comme méthodes de gestion de la congestion.

Nous avons été choisis deux techniques qui gèrent le trafic de manière adaptative qui sont les suivantes :

4.1.1. MATE (Multipath Adaptive Traffic Engineering):

Les auteurs dans MATE décrit un schéma d'ingénierie de trafic adaptatif par trajets multiples, afin d'éviter la congestion du réseau qui établit sur des bases en équilibrant de manière adaptative la charge entre plusieurs chemins qui se base sur l'analyse et le mesure de la congestion des chemins. Ce mécanisme (MATE) *(voir la figure 9)* adopte une approche minimaliste en ce sens que les nœuds intermédiaires ne sont pas obligés d'effectuer une ingénierie du trafic ou des mesures en dehors du transfert de paquets [ACSI02].

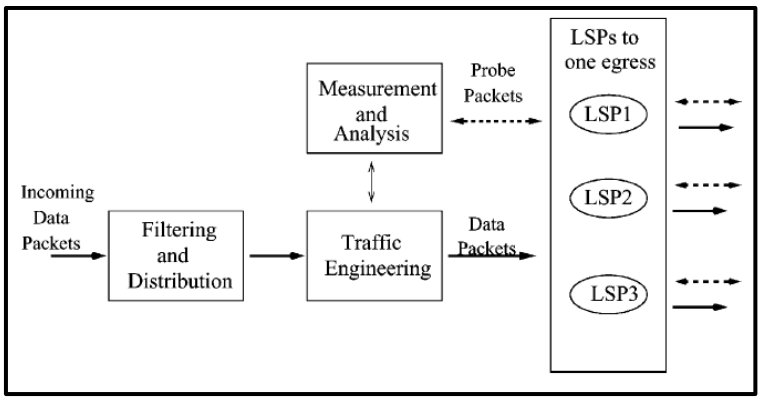


Figure 9 : Fonctions de MATE dans un nœud Ingress.

Il est supposé que plusieurs LSP explicites entre les pairs IE dans un domaine MPLS ont été établis à l'aide d'un protocole standard tel que CR-LDP [JAL02] ou RSVP-TE [WAL01], ou configurés manuellement. Le nœud Ingress est le responsable de l'opération d'équilibrage du trafic dans le but de répartir le trafic sur les LSP afin que les charges soient

équilibrées et que la congestion soit réduite au minimum [ACSI02]. MATE fonctionne en deux phases : une phase de surveillance et une phase d'équilibrage de charge.

Au cours de la phase de surveillance, les paquets de sondage sont envoyés périodiquement et les mesures de congestion sur les LSP et leurs dérivés sont estimées. Si un changement sensible et persistant de l'état du réseau est détecté, la phase d'équilibrage de la charge est effectuée. Dans la phase d'équilibrage de la charge, l'algorithme continue de surveiller les mesures d'encombrement sur les LSP et tente d'égaliser leurs marges. Une fois que les mesures sont approximativement égalisées, l'algorithme passe à la phase de surveillance et l'ensemble du processus se répète [AlWalid].

4.1.2. DATE (Distributed Adaptive Traffic Engineering):

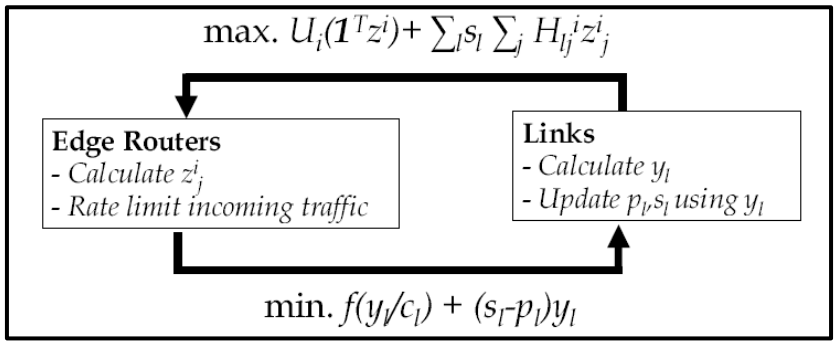


Figure 10 : Vue graphique de l'algorithme DATE.

La technique DATE utilise deux types de prix de lien *(voir la figure 10)* : le prix de la congestion {pl} et le prix de cohérence {sl}. Le premier garantit que les contraintes de capacité ne sont pas violées à l'équilibre et qui existe implicitement sur Internet. L'algorithme de routage réagit uniquement à la charge mesurée sur chaque lien, ce qui en fait l'une des causes potentielles d'instabilité dans un algorithme dynamique distribué. Pour assurer une correspondance entre la charge de liaison mesurée et la charge de liaison cible à l'équilibre, le prix de cohérence a été introduit. Laissez la topologie underlay définie par H, où j indexe les chemins multiples de i. Tp est le temps de réponse de chaque routeur principal, où Tp doit être supérieur au temps d'aller-retour (round trip time ou RTT) plus le temps nécessaire à chaque routeur central pour calculer son retour. Dans un réseau DATE, les routeurs frontal et central travaillent ensemble pour équilibrer la charge, limiter le taux de trafic entrant et contourner les défaillances. Chaque routeur central mesure d'abord la charge de liaison de tous les liens qui lui sont connectés. Ensuite, il calcule la nouvelle charge cible yl pour chaque lien en utilisant les informations des deux prix qui sont mises à jour à l'aide de la méthode du gradient, en fonction des informations locales à chaque lien.

En général, DATE nécessite une fonction supplémentaire au niveau des routeurs fronteaux. Les routeurs fronteaux déterminent le débit autorisé de chaque flux et limitent le trafic entrant en supprimant les paquets envoyés au-dessus du débit autorisé. Le mécanisme de contrôle de congestion existant devrait permettre aux hôtes d'extrémité d'adapter leur débit lorsque leurs paquets sont rejetés. Les mises à jour des prix sont des multiplications matricielles simples. La mise à jour de y_l et z_j^i implique la résolution d'un problème d'optimisation convexe qui n'a pas non plus besoin de beaucoup de calcul [HMC].

Conclusion

Ce chapitre a d'abord défini l'ingénierie du trafic comme l'aspect de l'ingénierie de réseau traitant du problème de l'évaluation et de l'optimisation des performances des réseaux IP, et nous avons décrit les principes de l'ingénierie de trafic et ses styles de taxonomie selon Awduche [ACE 01]. Ensuite, nous avons mentionné la mesure du trafic en tant que collecte de données de trafic aux fins de la caractérisation du trafic, de la surveillance du réseau et du contrôle du trafic. Nous avons également discuté de la définition de la congestion du trafic et de la dynamique de l'ingénierie du trafic en introduisant le système MPLS. Après cela, comme exemple pour un mécanisme TE visant à répartir le trafic entre les chemins en temps réel, nous avons mentionné le Dynamic Load-Balancing (DLB). Enfin, nous avons terminé le chapitre en donnant un aperçu général de certaines techniques permettant l'adaptation du trafic, telles que MATE et DATE.

Chapitre 02 : La virtualisation

Introduction

Avant de discuter en détail des différentes catégories de virtualisation, il est utile de définir le terme dans un sens abstrait. La virtualisation consiste à créer une version virtuelle d'un périphérique ou d'une ressource, telle qu'un serveur, un périphérique de stockage, un réseau ou même un système d'exploitation, dans laquelle l'infrastructure répartit la ressource en un ou plusieurs environnements d'exécution. Aujourd'hui, le terme virtualisation est largement appliqué à un certain nombre de concepts, qui comprend : une virtualisation de serveur, une virtualisation de stockage et virtualisation de réseau.

Dans ce chapitre nous allons concentrer sur la virtualisation des réseaux qui fournit une nouvelle approche qui permet d'exécuter plusieurs réseaux virtuels sur une infrastructure de réseau physique partagée. Ensuite, nous présentons une brève discussion des techniques de virtualisation des réseaux. D'une autre main, les recherches continues sont en cours pour améliorer le routage, nous avons présente un petite rappelle sur le terme routage, et des certains protocoles de routage proposés sont décrits dans la section suivante. Nous présentons quelques systèmes capables de gérer les fluctuations inattendues du trafic avec des performances réseau.

L'ingénierie du trafic récemment reçu de nombreuses attentions dans la communauté de recherche Internet. Il a été créé pour le contrôle de performance d'un réseau quelconque en analysant et en prévoyant la nature de la transmission de données sur un réseau. Pour cela, nous allons discuter les différentes approches et techniques utilisé dans ces systèmes, sans oublier les topologies de routage virtualisées utilisé par les ingénieries de trafic dynamique.

1. La virtualisation

La virtualisation a commencé dans les années 1960, en tant que méthode de division logique des ressources système fournies par les ordinateurs centraux entre différentes applications. Depuis lors, le sens du terme s'est élargi [GC13]. La virtualisation est une nécessité absolue dans l'environnement de travail actuel. Les chances sont que toute personne utilisant un ordinateur physique dans le monde d'aujourd'hui sera exposée à une certaine forme de virtualisation. La virtualisation implique la création d'une version virtuelle de quelque chose pouvant être utilisé sans que celle-ci ne soit physiquement présente là où elle est requise.

1.1. Types de technologies de virtualisation

La virtualisation est classée principalement en fonction de ce qui est virtualisé ou de ce qu'elle résout. Il existe trois types de classification : Virtualisation de serveur, Virtualisation de stockage et Virtualisation de réseau.

1.1.1. Virtualisation de serveur

La virtualisation de serveur est le modèle le plus populaire et le plus difficile, il implémente une couche virtuelle au-dessus d'un système physique, les périphériques physiques sont masqués pour créer plusieurs nombres de machines virtuelles isolées [AM10]. La virtualisation de serveur permet de diviser un serveur physique en plusieurs serveurs virtuels come illustré dans *la figure 11* [GS07].

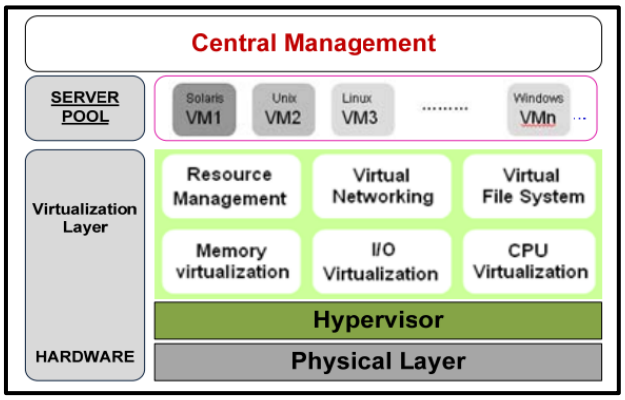


Figure 11 : Architecture du modèle conceptuel de virtualisation de serveur.

La virtualisation de serveur est une technique qui modifie l'architecture de modèle de serveur et établit une nouvelle couche appelée hyperviseur entre la couche physique et les systèmes d'exploitation. L'hyperviseur (*est un environnement logiciel*) qui comprend plusieurs blocs d'activités (*mémoire, E/S, CPU, système de fichiers*) contrôlés par un système de gestion (*blocs de gestion des ressources*), Dans un serveur virtuel, un serveur physique avec toutes ses ressources devient plusieurs serveurs virtuels de sorte que chaque serveur virtuel dispose des fonctionnalités du serveur physique et fonctionne séparément des autres machines virtuelles [AM10]. La virtualisation de serveur réduit le nombre de serveurs physiques requis, tout en optimisant l'utilisation des ressources et en améliorant la facilité de gestion, réduisant ainsi les coûts [GS07].

1.1.2. Virtualisation de stockage

L'utilisation de votre ordinateur qui doit être connecté au périphérique qui stocke toutes vos données, ce qui vous permet d'écrire et de récupérer des données à partir de ce périphérique de stockage. La quantité de données pouvant être écrite sur le périphérique de stockage est limitée par la capacité de stockage de ce périphérique. La virtualisation du stockage (*voir la figure 12*) combine un ensemble de périphériques de stockage en réseau dans ce qui apparaît aux utilisateurs comme une entité de stockage unique. Un matériel ou un logiciel spécialisé gère la complexité d'un réseau de stockage et permet à chaque périphérique souhaitant accéder au stockage de se connecter directement au support de stockage.

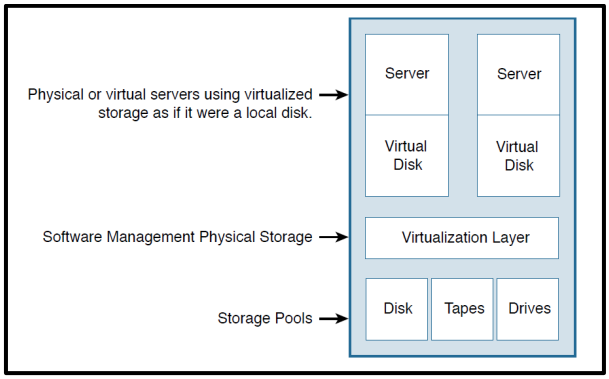


Figure 12 : Virtualisation du stockage.

La virtualisation du stockage (voire *la Figure 1.1*) est généralement associée à un réseau SAN (Storage Area Network) de grande taille gérée par une couche de virtualisation matérielle ou logicielle qui présente ce vaste stockage sous forme de bloc unique aux serveurs nécessitant du stockage [DLS16].

De manière générale, la virtualisation du stockage a été catégorisée de trois manières :

Basé sur l'hôte :

Avec la virtualisation basée sur l'hôte, le provisioning est effectué sur le serveur pour définir les volumes logiques.

Basé sur le périphérique de stockage :

Avec ce type, la virtualisation est transmise au matériel de stockage lui-même.

Basé sur le réseau :

Avec ce type de virtualisation, un périphérique réseau situé entre l'hôte et le périphérique de stockage va virtualiser et rediriger les demandes d'E / S.

1.1.3. Virtualisation de réseau

La virtualisation de réseau est devenue un sujet populaire ces dernières années et elle est souvent mentionnée dans les magazines techniques et les documents de recherche. La virtualisation de réseau fait référence à la technologie qui permet de partitionner ou d'agréger une collection de ressources réseau et de les présenter à différents utilisateurs de manière à ce que chaque utilisateur bénéficie d'une vue unique et unique du réseau physique [WIDRB13]. Selon la définition a mentionné dans [MSS15], La virtualisation des réseaux a été présentée comme un nouveau paradigme pour les nouvelles architectures réseaux et pour l'Internet du futur. Elle permet d'offrir une diversité de réseaux en masquant l'hétérogénéité de l'infrastructure physique et une flexibilité en contournant la rigidité des équipements réseaux. La virtualisation est une technique utilisée pour modifier les propriétés d'un service de réseau sans introduire de modifications au niveau des clients et des serveurs. Elle permet la coexistence de multiples réseaux hétérogènes dans une seule infrastructure. Pour cela, cette technologie doit assurer un niveau adéquat d'isolation afin de permettre l'utilisation des ressources physiques du réseau en temps réel et à grande échelle. Elle a promis de garantir la qualité de service requise [SWPM09].

1.1.4. Les techniques de virtualisation de réseau

La virtualisation du réseau est distinguée en deux catégories : des techniques basées sur la virtualisation des protocoles et des techniques basées sur la virtualisation des machines.

1.1.4.1. Techniques basées sur la virtualisation des protocoles :

Les auteurs de [CB09] disent que les approches basées sur le protocole appliquent un protocole pour identifier et isoler les réseaux virtuels. Ce type d'approche exige que l'équipement physique soit capable de supporter le protocole choisi. Les approches couramment utilisées sont : les réseaux locaux virtuels (VLAN) et les réseaux privés virtuels

(VPN). Les VLANs sont caractérisés par le contrôle d'accès qui donne à l'utilisateur l'accès à un segment particulier du réseau. Les VLANs divisent logiquement un réseau local en plusieurs réseaux virtuels et ils se caractérisé aussi par l'isolation. L'autre approche (VPN) est un réseau dédié fournissant un canal de communication sécurisé entre plusieurs sites géographiquement distants.

A. Les réseaux locaux virtuels (VLANs)

Les VLANs sont généralement utilisés pour regroupent un ensemble des hôtes logique et non physique [PL12] (*voir la Figure 13*). Le VLAN apporte des solutions nouvelles dans la configuration et l'administration physique des réseaux locaux, il est un regroupement de plusieurs hôtes de façon logique et non physique indépendamment de la localisation géographique de ces hôtes. Il permet de gérer des domaines de diffusion (Broadcast Domain) d'une manière logique sans se soucier de l'emplacement de ses hôtes. Selon la définition du standard *IEEE 802.1Q*, Les réseaux locaux virtuels fonctionnent au niveau des couches liaison de données en modèle OSI.

NB : Pour définir des VLANs, il faut que les commutateurs supportent cette extension de la technologie Ethernet (IEEE 802.1q).

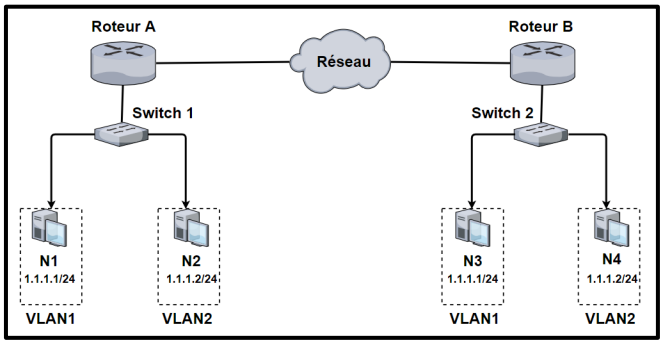


Figure 13 : Regroupement des nœuds en VLANs.

Plusieurs types de VLANs sont définis qui sera comme le suivant [RV97] :

VLAN de niveau 1 ou VLAN par port (Port-Based VLAN) :

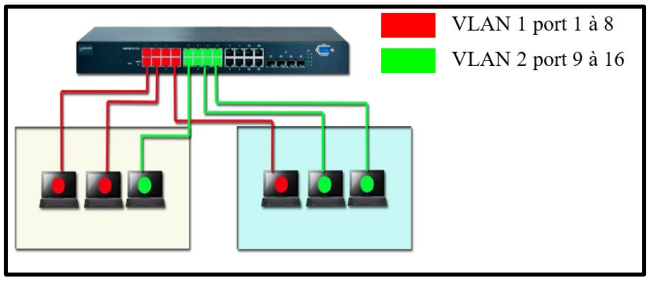


Figure 14 : VLAN par port.

Il définit un réseau virtuel en fonction des ports de raccordement sur le commutateur (*voir la Figure 14*). On associe un port physique de ce commutateur à un numéro de VLAN. Le numéro de VLAN a associé avec un port physique (Lorsqu'un nœud se déplace il doit être

configurer et modifier le nouveau port auquel elle s'associe et l'ancien port auquel elle était associée).

VLAN de niveau 2 ou VLAN MAC (MAC Address-Based VLAN) :

En principe, Il définit un réseau virtuel qui associent des hôtes par leur adresse MAC (*voir la Figure 15*). Les différents VLANs peuvent contient plusieurs hôtes raccordés à un même port(segment). Ces VLAN peuvent contenir des hôtes partagés.

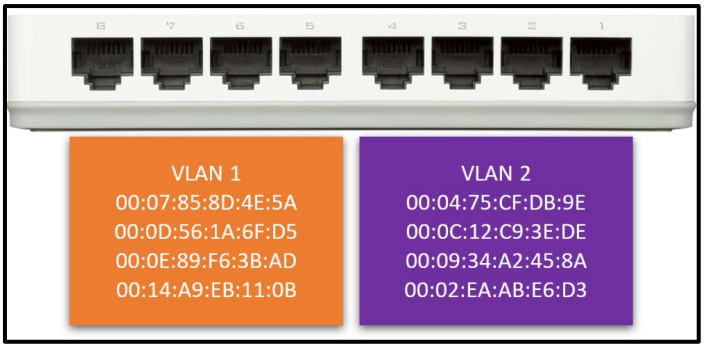


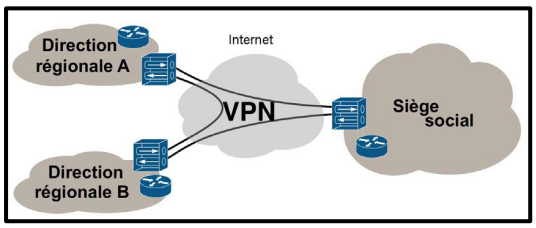
Figure 15 : VLAN par adresse MAC.

VLAN de niveau 3 :

On distingue deux types de VLAN de niveau 3 :

- **VLAN par sous-réseau (Network Address-Based VLAN)**
  Il partage le même principe des VLANs de niveau 2 (*voir la Figure 16*), mais il définies par leur adresse réseau (plage d'adresses) ou par masque de sous-réseau (subnet d'IP). Ceci permet de modifier automatiquement la configuration des commutateurs lors d'un changement ou d'un déplacement de l'hôte.
- **VLAN par protocole (Protocol-Based VLAN)**
  Il définit un réseau virtuel en fonction des protocoles. Dans ce cas, chaque VLAN doit regrouper ces hôtes qui utilisent le même protocole.

B. Les réseaux privés virtuels (VPN)



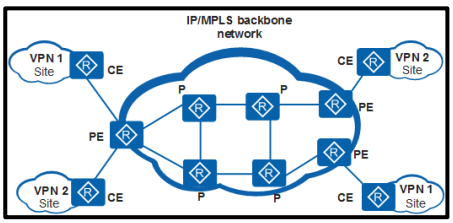


Figure 16 : Réseau privé virtuel.

Un réseau privé virtuel (**Virtual Private Network**) est un réseau connectant plusieurs sites via des tunnels privés et sécurisés sur des réseaux de communication partagés ou publics, les VPN connectent des sites répartis géographiquement [CB09]. Ces réseaux reposent sur un protocole, appelé protocole d'encapsulation (tunneling), qui permet de sécuriser les informations circulantes entre des bouts par des algorithmes de cryptographie. Le VPN est utilisé pour le masquage de distance entre les sites.

Dans [FRPRB08], chaque site VPN comporte un ou plusieurs périphériques *(Customer Edge CE)* et un ou plusieurs routeurs *(Provider Edge PE)* qui sont reliés entre eux. Autrement, La technologie VPN a été utilisée dans MPLS (*Multiprotocol Label Switching)*, appelée MPLS VPN, qui transporte et route plusieurs types de trafic réseau à l'aide d'un backbone MPLS [RR06] ((voir *Figure 16*)).

Les VPN peuvent être classés dans les trois couches suivantes :

- VPN de couche 1 (L1VPN)

Il a créé pour louer ou échanger des ressources entre les clients, et pour fournit le type de la connectivité entre les sites clients du réseau virtuel. Il offre aux clients les moyens de proposer leurs propres services. Il servit un service par la première couche du modèle OSI.

- VPN de couche 2 (L2VPN)

Dans lequel ou les trames sont transportés entre les sites participants. Mais l'inconvénient est qu'il n'y a pas de plan de contrôle pour gérer l'accessibilité via le VPN [MKCB08]. Dans MPLS L2VPN, les PE communiquent avec d'autres routeurs PE, ils peuvent envoyer des informations au tunnel approprié.

- VPN de couche 3 (L3VPN)

Les L3VPN peuvent à nouveau être classés en deux approches : les VPN basés sur CE a connecté peut se comporter comme s'il était connecté à un réseau privé et ceux basés sur PE d'où le réseau du fournisseur est responsable de la configuration et de la gestion des VPN [MKCB08]. D'autre manière, les informations de routage d'un client sont complètement séparées des autres clients et transmises via le réseau MPLS du fournisseur de services [PK]. L'avantage de L3VPN est de garantir la séparation du trafic privé entre des autres utilisateurs connectés.

1.1.4.2. Techniques basées sur la virtualisation des machines

Les approches basées sur la virtualisation des machines incluent l'isolation et l'abstraction des ressources informatiques [JSR10].

Dans ce qui suit nous allons présenter : la virtualisation complète et la paravirtualisation qui sont des techniques basées sur la virtualisation de machines.

La virtualisation complète

La virtualisation complète (Full Virtualization) permet aux logiciels existants, que ce soit des systèmes d'exploitation (invités) ou des logiciels, de s'exécuter sur une machine virtuelle sans aucune modification [SHW11]. Elle offre une réplique virtuelle du matériel du système. L'hyperviseur est chargé d'assurer l'isolation entre les systèmes d'exploitation invités et le matériel. Le principal avantage de cette approche est qu'il est très facile à utiliser c.-à-d. votre SE invité n'a pas besoin d'être modifié pour fonctionner dans un tel environnement. D'autre part, le principal inconvénient de cette approche est la faible performance, qui peut être jusqu'à 30% inférieure à celle utilisée directement sur du matériel [SML10]. Par exemple, un utilisateur commun peut installer un logiciel tel que VMware Workstation. Dans VMware

Workstation, un système d'exploitation invité peut-être installer et utilisé exactement comme s'il s'exécutait directement sur du matériel (*voir Figure 17).*

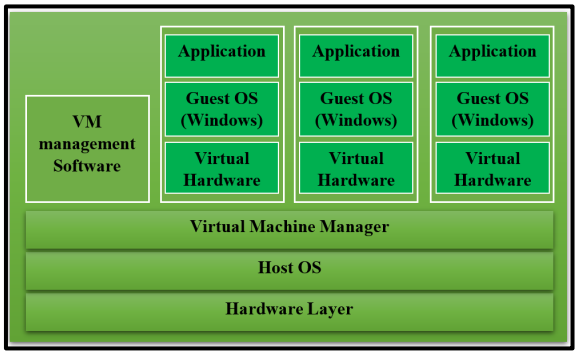


Figure 17 : La virtualisation complète (*Full-Virtualization*).

La paravirtualisation

L'approche de la paravirtualisation est un peu différente par rapport la virtualisation complète, dans la paravirtualisation le système d'exploitation invité nécessite quelques modifications pour pouvoir être utilisé dans l'environnement virtuel. La paravirtualisation est un sous-ensemble de la virtualisation de serveur [SML10]. Un fait intéressant dans cette technologie est que Le système d'exploitation invités sont conscients, car ils savent qu'ils fonctionnent dans un environnement virtualisé. Cette approche a une caractéristique très importante qui permet à la paravirtualisation d'atteindre des performances plus proches du matériel non virtualisé. L'interaction de périphérique dans un environnement paravirtualisé est très similaire à l'interaction de périphérique dans un environnement virtualisé complet (*Voir la Figure 18).*

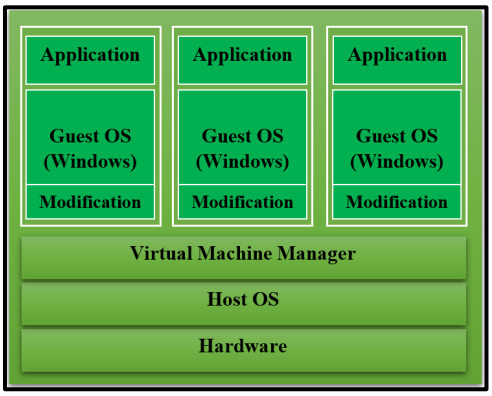


Figure 18 : La paravirtualisation (*Para-Virtualization*).

2. Le routage

Le terme routage a référencé à l'envoi d'un paquet d'un nœud à travers le réseau vers un autre nœud sur un réseau différent. Les routeurs ne se soucient pas vraiment de l'hôte, ils se soucient seulement des réseaux et du meilleur chemin d'accès à chaque réseau. Chaque routeur doit renseigner par l'adresse de destinateur, il doit également connaître les routeurs voisins à partir desquels il peut s'informer sur les réseaux distants. Ce dernier doit trouver des routes possibles vers tous les réseaux distants et en choisir le meilleur. Les informations de routage

de chaque routeur doivent être maintenir et vérifier [TL05]. L'adresse réseau logique de l'hôte de destination est utilisée pour acheminer des paquets vers un réseau via un réseau de routes, puis l'adresse matérielle de l'hôte est utilisée pour transmettre le paquet d'un routeur à l'hôte de destination approprié.

2.1. Routage Statique et Routage Dynamique

Dans le routage statique, la table de routage est rarement modifiée, la topologie ne change pas fréquemment, les liaisons sont fiables et le type de liaisons entre tous les nœuds est connu. Il nécessite moins de puissance de calcul au niveau des nœuds de routage, car il ne nécessite pas de calcul de la topologie du réseau ni de construction fréquente de la table de routage.

Par contre dans le routage dynamique, les nœuds partagent régulièrement des informations sur tous les liens qui leur sont connectés avec leurs nœuds voisins. Il fournit à un nœud de routage peut avoir une bonne idée de l'ensemble du réseau. Il enrichit un nœud de routage par une bonne idée de tous les autres nœuds du réseau. En cas de défaillance d'un lien ou d'un nœud, tous les nœuds sont informés par les mises à jour reçues directement ou indirectement de voisins concernant des nœuds défaillants. Dans le cas d'un réseau énorme, les nœud être occupés en calcul sur le routage. Toutefois, comme ces nœuds disposent d'informations mises à jour sur la topologie du réseau, ils peuvent éviter de transmettre des paquets sur des routes comportant des liens encombrées ou défaillantes.

2.2. Les protocoles de routage

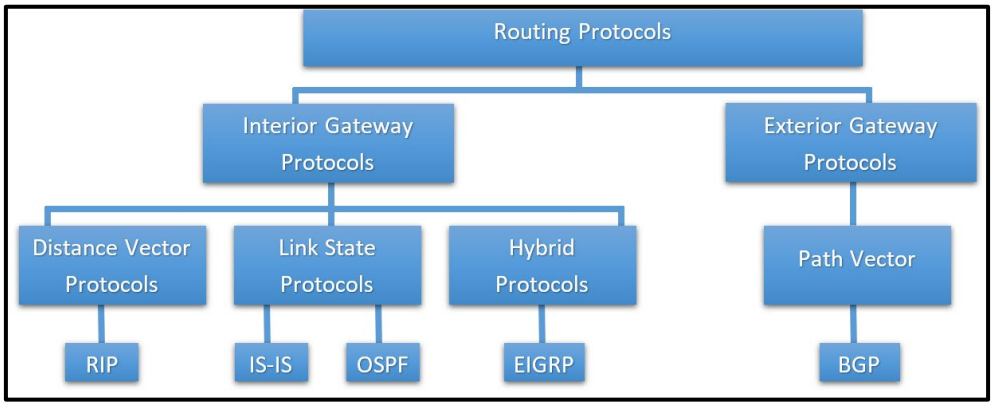


Figure 19 : Classification de protocole de routage.

Un protocole de routage indique la communication entre différents routeurs. Il est utilisé pour déterminer les routes. Chaque routeur contient les détails de ses réseaux voisins uniquement. Un protocole de routage partage ces informations d'abord entre voisins immédiats, puis sur l'ensemble du réseau. De cette façon, les routeurs acquièrent des connaissances sur la topologie du réseau. La classification du routage se divise en deux types : le IGP (*Interior Gateway Protocol utilisés pour le routage au sein de systèmes autonomes*) et le EGP (*Exterior Gateway Protocol utilisés pour l'acheminement entre différents systèmes autonomes*) se sont des protocoles de routage qui sont utilisés pour la communication réseau interne et externe (*voir la Figure 19*).

2.2.1. Interior Gateway Protocols (IGP)

Interior Gateway Protocols ou IGP sont utilisés au sein d'un domaine de routage. Ils sont utilisés pour les réseaux sous une administration réseau unique. Chaque réseau utilise également un IGP pour la détermination du chemin le plus court dans ses propres domaines de routage. Les IGP peuvent être classés en protocoles de vecteur de distance (*Distance Vector*) et d'état de lien (*Link State*) [ATM16].

La principale différence entre les protocoles de vecteur de distance et les protocoles d'état de lien est que les informations de routage sont stockées sous forme un tableau de routage de vecteur de distance et sous forme d'une base de données pour le routage d'état de lien. Les protocoles de routage Interior Gateway courants sont RIP, IGRP, EIGRP, OSPF et IS-IS. IGP est généralement utilisé pour le routage intra-domaine, c'est-à-dire le routage au sein du système autonome[2] [AAAY12].

A- Classification du protocole Interior gateway (IGP)

IGP peuvent être classés en deux types :

1) Protocoles de routage à vecteur de distance

Le routage à vecteur de distance partage la totalité de sa table de routage avec ses voisins à intervalles réguliers. Ces mises à jour de routage peuvent générer un trafic important sur les liens. Dans lequel il n'a pas d'informations sur la topologie complète du réseau pare ce qu'ils fournissent à tout nœud les informations nécessaires pour atteindre le nœud directement connecté. Ces protocoles utilisent généralement l'algorithme de Bellman-Ford pour la détermination du meilleur chemin [ATM16].

Les protocoles de vecteur de distance fonctionnent mieux dans les situations où le réseau est simple et ne nécessite pas de conception hiérarchique. RIP est un algorithme de routage à vecteur de distance utilisant le nombre de sauts comme métrique [JRB15].

2) Protocoles de routage à état de liens

A l'aide de l'algorithme de Dijkstra, les protocoles de routage à état de liens peuvent calcule le meilleur chemin de la source à la destination afin de recueillir des informations sur l'état des liens, puis présentent les a tous les routeurs voisins, avec cela tous les nœuds du réseau ont une vue topologique complète du réseau [AAAY12]. Les protocoles à état de liens fonctionnent mieux dans les situations où la conception du réseau est hiérarchique, généralement dans les grands réseaux et où la convergence rapide du réseau est cruciale. Ils sont en outre classés en OSPF et IS-IS [GJ08].

Open Shortest Path First (OSPF)

OSPF est un protocole de routage à état de liens, Il envoie des paquets Hello chaque 10 secondes, des requêtes d'état des liens, des mises à jour et des descriptions de base de données, il est basé sur un algorithme de calcul du plus court chemin appelé algorithme de Dijkstra (*voir la Figure 20*). Lorsqu'un changement a eu lieu, OSPF multidiffuse les informations mises à jour (informe toutes les nœuds voisins) [JRB15].

[2] Un système autonome (AS), également appelé domaine de routage, est un ensemble de routeurs administrés sous une administration commune.

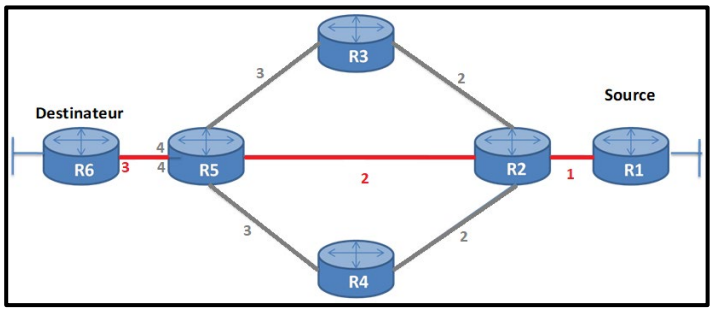


Figure 20 : Open Shortest Path First (OSPF).

Intermediate System to Intermediate System (IS-IS)

IS-IS est un protocole d'état des liens et se comporte presque comme OSPF, car il utilise également des zones pour décomposer le domaine de routage en un plus petit. OSPF et IS-IS utilisent tous deux le même algorithme pour calculer le meilleur chemin, utilisent le même multitâche pour vérifier les mises à jour de routage [AAAY12]. IS-IS utilise quatre types de paquets : paquet IS-IS Hello, paquet d'état de lien, paquet de numéro de séquence partiel, paquet de numéro de séquence complet.

OSPF prend en charge le lien virtuel, contrairement à IS-IS qui ne supporte pas.

2.2.2. Border Gateway Protocols (BGP)

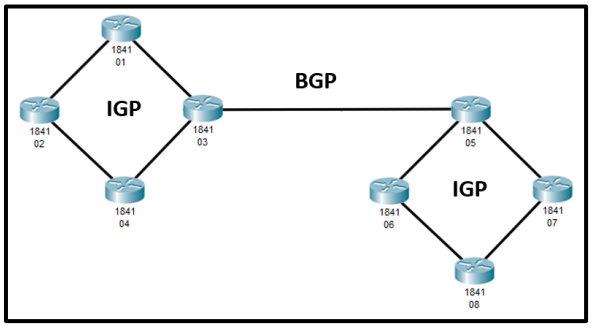


Figure 21 : Différence entre BGP et IGP.

BGP a été créé pour remplacer le protocole EGP (*Exterior Gateway Protocol*), qui agit et effectue le routage entre plus de systèmes autonomes. Il est décrit comme un protocole de vecteur de chemin (*path vector protocol*). Le BGP peut être interne ou externe, BGP interne lorsqu'il connecte deux nœuds du même système autonome, BGP externe lorsqu'il interconnecte différents systèmes autonomes [NSF07]. BGP utilise un message ouvert (*Open Message*) dans le cas où il souhaite démarrer une session entre deux nœuds différents du réseau, dans le cas contraire (l*orsqu'il existe plus qu'un Border Gateway Message (BGM)*), il utilise le message *Update Message* qui fournit la mise à jour du routage, il utilise Message de notification (*Notification Message*) quand il y a un problème de routage, et le dernier type de message est utilisé pour maintenir la connectivité entre les nœuds qu'il s'appelle *Keep Alive Message* [AAAY12]. Un point très important qu'il doit être mentionné est la différence entre IGP et iBGP (voir *Figure 21*), IGP fait le routage à l'intérieur d'un système autonome vers une destination interne et iBGP fait le routage à l'intérieur d'un système autonome vers une destination externe.

2.2.3. Ingénierie de trafic basée sur IGP multi-topologie adaptative

L'ingénierie du trafic intra-domaine basé sur IGP multi-topologie (MT-IGP) est un système capable de gérer les fluctuations inattendues du trafic avec des performances réseau quasi optimales. Le réseau est dimensionné via une optimisation du poids des liens hors connexion à l'aide d'IGP multi-topologies afin d'obtenir une diversité de chemins maximale dans plusieurs topologies de routage. Un algorithme d'ingénierie de trafic adaptatif effectue un ajustement de la répartition dynamique du trafic pour équilibrer la charge sur plusieurs topologies de routage en réaction à la dynamique du trafic surveillé [WHP08], Cet algorithme étant basé sur une configuration MT-IGP optimisée.

Si l'ingénierie du trafic est en mode hors ligne (*offline TE*), il est suggéré d'optimiser simultanément le poids des liens IGP et le ratio de fractionnement[3] du trafic [MHN02], en fonction de la matrice de trafic estimée et supposée a priori et de la topologie du réseau en entrée, tout ça afin d'obtenir des performances réseau optimales. Malheureusement, cette hypothèse n'est généralement pas valable dans les réseaux opérationnels réels en raison de la présence fréquente de dynamiques de trafic telles que des pics de trafic inattendus [WX06], Les méthodes TE qui ne sont pas connectées au réseau peuvent entraîner de mauvaises performances, dans ce cas elles doivent être réaffecter les poids de lien IGP d'une manière dynamique, cette réaffectation à la volée peut provoquer des boucles de transmission transitoires au cours de la phase de convergence, ce qui entraîne souvent des interruptions de service et une instabilité du trafic. La technique la plus connus pour résoudre ce problème consiste à gérer de manière adaptative la dynamique du trafic dans les réseaux IP opérationnels qui s'appelle AMPLE.

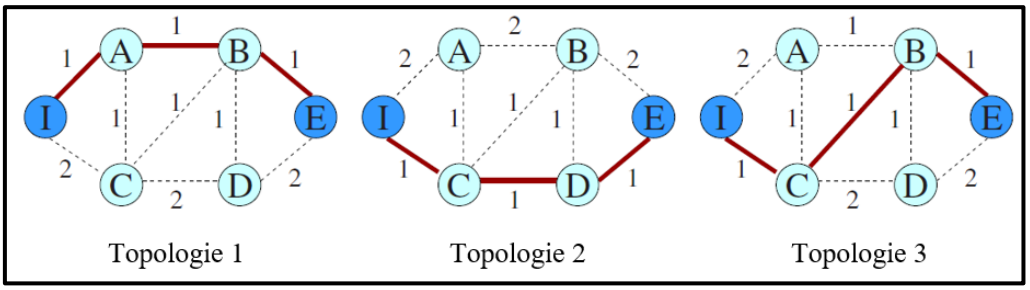


Figure 22 : Paramétrage de poids du lien MT-IGP pour la diversité des chemins.

L'idée mentionnée dans [WHP08], les IGP multi-topologies adoptés pour permettre la diversité de chemins, reposent sur le fractionnement adaptatif du trafic sur plusieurs topologies de routage pour l'équilibrage dynamique de la charge (*dynamic load balancing*). Comme ils l'ont déjà mentionné, AMPLE comprend deux tâches distinctes comme nous le discutons dans la section suivante, le dimensionnement de réseau hors ligne et l'ajustement adaptatif du ratio de fractionnement du trafic à travers les topologies de routage, le premier, qui permet d'obtenir une diversité de chemins intra-domaine maximale entre plusieurs topologies de routage MT-

[3] Cela permet potentiellement de modifier facilement la topologie du réseau ou d'ajouter de nouveaux flux sans effectuer toute la procédure d'optimisation, quelle proportion du flux entrant devant être envoyée sur chaque lien sortant [MHN02].

IGP (voir *Figure 22*), et l'autre pour obtenir un équilibrage dynamique de la charge en cas de dynamique inattendue du trafic.

Dans AMPLE, la configuration MT-IGP produite dans la phase hors ligne offre la possibilité d'utiliser plusieurs chemins IGP différents pour transporter le trafic avec une division arbitraire sur plusieurs topologies de routage.

Le contrôle de trafic adaptatif doit être doté d'un algorithme efficace pour l'ajustement adaptatif du ratio de fractionnement du trafic au niveau des nœuds sources PoP individuels. Le responsable TE central doit effectuer certaines opérations de manière périodique à un intervalle de temps relativement court.

Ces opérations incluent à la fois de faire : mesurez le volume de trafic entrant et la charge du réseau pour l'intervalle actuel, calculez les nouveaux ratios de fractionnement du trafic pour tous les nœuds PoP en fonction de la demande de trafic mesurée et de la charge du réseau pour l'équilibrage dynamique de la charge et demandez aux différents nœuds PoP d'appliquer le nouveau ratio de fractionnement du trafic sur leur trafic d'origine locale.

2.2.4. L'évaluation de performance d'AMPLE

Les performances dans AMPLE [WHP08] a été évalué, dans lequel ils utilisent les topologies réelles et les matrices de trafic des réseaux GEANT qui contient 23 nœuds PoP et 74 liens, et Abilene qui contient 12 nœuds et 30 liens.

Les performances de diversité de chemins :

Dans cette section, les résultats de la simulation selon [WHP08] présentés pour l'optimisation du poids de lien MT-IGP hors ligne qui comprendre une métrique de performance basé sur la proportion de paires source-destination. La *Figure 23* affiche les performances de la diversité de chemins dans la topologie GEANT qui inclus un paramétrage optimisé du poids de lien MT-IGP pour maximiser la diversité de chemins intra-domaine, et un paramétrage aléatoire aux poids de lien dans toutes les topologies de routage. Le paramétrage optimisé du poids de lien surperforme sensiblement la solution aléatoire en termes de diversité de chemins.

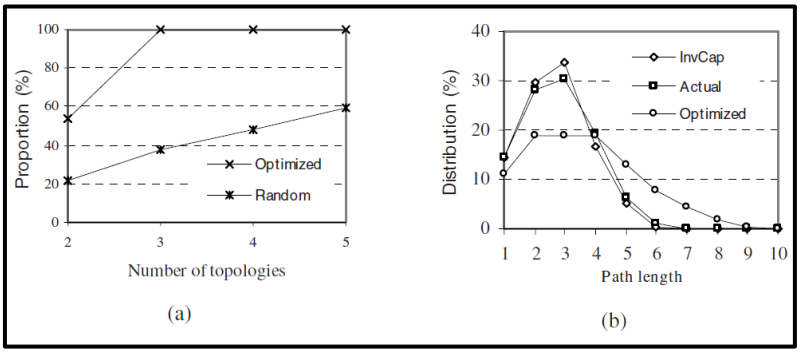


Figure 23 : Performances de paramétrage du poids de lien MT-IGP (GEANT).

La figure 23 annonce que l'algorithme supporté dans AMPLE en mesure de garantir à 100% l'évitement des liens critiques partagés par toutes les topologies avec seulement trois

topologies de routage. En cas de congestion du réseau et pour contourner le lien congestionné, les sources associées sont toujours en mesure de remarquer leur trafic local pour appliquer une autre sélection de chemin IGP.

On peut voir que l'algorithme proposé conduit à des chemins plus longs en raison des efforts déployés pour maximiser la diversité des chemins sur plusieurs topologies de routage, ce qui représente une augmentation du coût total du réseau. D'autre côté, les performances du réseau Abilene disent que ce plus élevé nombre de topologies de routage conduit à une plus grande diversité de chemins. Il est référencé que ce n'est pas aussi bonne que la topologie GEANT. Les performances de diversité de chemins correspondantes peuvent atteindre 100% avec quatre topologies de routage [WHP08].

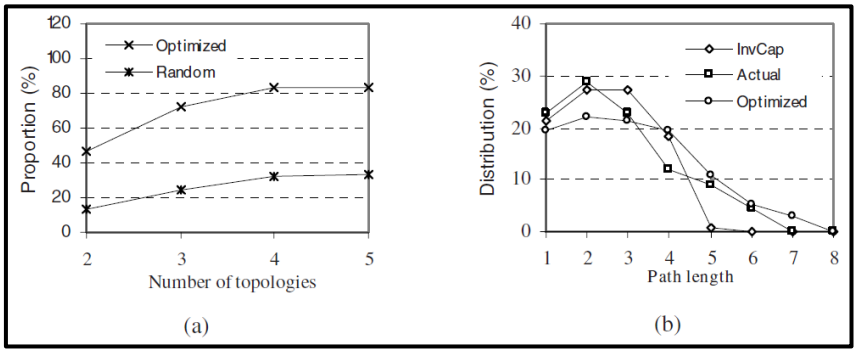


Figure 24 : Performances de paramétrage du poids de lien MT-IGP (Abilene).

L'évaluation de l'ingénierie adaptative du trafic :

Les auteurs de [WHP08] comparent les approches suivantes dans leur évaluation de l'ingénierie adaptative du trafic : **Actuel** ce qui signifie le paramétrage du poids de lien actuelles dans les réseaux opérationnels actuels. **InverCap** ce qui signifie paramétrage du poids de lien proportionnel à la capacité inverse. **Multi-TM** qu'ils ont utilisé le TOTEM toolbox pour calculer un ensemble du poids de lien pour plusieurs matrices de trafic afin de rendre le TE IGP robuste face à l'incertitude de la demande de trafic. **AMPLE-n** qui s'exécute leur algorithme TE adaptatif proposé sur n-topologies de routage MT-IGP optimisées. **Optimal** qui représente une base de référence pour leurs comparaisons, ils ont utilisé le GLPK dans le TOTEM toolbox pour calculer la MLU optimale pour les topologies et matrices de trafic données.

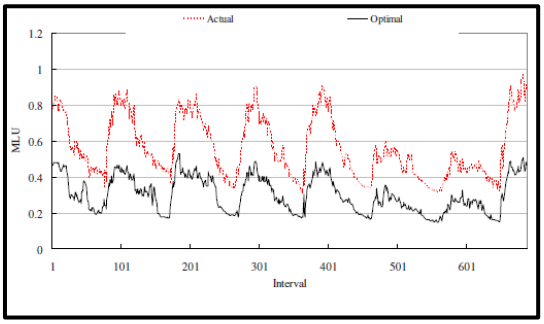


Figure 25 : MLU dans GEANT.

Le graph a présenté dans *la Figure 25* affiche une réalisation de MLU pour tous les TM du réseau GEANT par Actuel et Optimal au cours d'une semaine qui dénote que l'écart de performance entre Actuel et Optimal est très grand. Cet écart de performance révèle que les ressources du réseau sont loin d'être utilisées avec la plus grande efficacité. Il est souhaitable de maintenir l'utilisation du réseau aussi proche que possible d'Optimal afin de minimiser ou d'éviter la congestion potentiel.

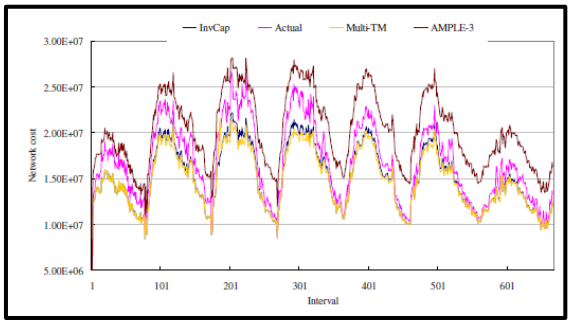


Figure 26 : Coût du réseau dans GEANT.

La figure 26 montre les performances correspondantes sur le réseau GEANT, dont la structure de la dynamique du trafic est assez régulière au quotidien. Globalement, Multi-TM est le plus performant, car il optimise le coût du réseau comme objectif principal. Bien qu'AMPLE ait un coût de réseau plus élevé, petit et acceptable. En revanche, la performance des coûts de réseau sont similaires dans Abilene et GEANT. InvCap et Multi-TM fonctionnent mieux qu'Actuel.

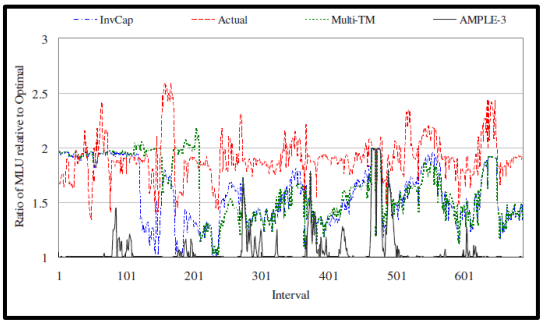


Figure 27 : Ratio de MLU par rapport à Optimal dans GEANT.

En se basant sur les mêmes matrices de trafic que celles utilisées dans *la Figure 25,* et *La Figure 27* représente le ratio entre MLU et Optimal qu'il est calculé comme étant la MLU d'une méthode spécifique divisée par celle d'Optimal. AMPLE peut atteindre une MLU quasi optimale pour la plupart des matrices de trafic sur la base des poids des liens MT-IGP optimisés. L'approche Multi-TM n'atteint pas de bonnes performances en minimisant la MLU.

3. Les systèmes basés sur les topologies de routage virtuel

L'ingénierie du trafic a été créé pour le contrôle de performance d'un réseau quelconque en prévoyant, analysant et régulant la nature de la transmission de données sur un réseau. La motivation diffère des propositions existantes axées sur le provisioning de réseau virtuel pour soutenir la différenciation des services, le partage de ressources ou les plates-formes

hétérogènes coexistantes. Au lieu de considérer la manière dont plusieurs topologies de réseau virtuel « équivalentes » ont chacune leur propre configuration de routage. L'ingénierie du trafic peut être effectué en ligne ou hors ligne, l'approche TE hors ligne vise à optimiser les ressources du réseau de manière statique, qui prend en entrée la topologie du réseau physique et tente de produire une diversité de chemin de routage maximale sur plusieurs topologies de routage virtuelles pour un fonctionnement à long terme grâce au réglage optimisé des poids de liaison avec l'algorithme de contrôle de trafic d'admission. Comme nous le savons, l'internet est un ensemble de réseaux, où chacun contrôlé par différentes administrations. Les fournisseurs de réseau Internet sont intéressés sur le mécanisme de l'ingénierie du trafic qui optimise les performances du réseau et distribue le trafic. Dans l'ingénierie du trafic, L'optimisation du routage est très importante afin de trouvant des routes efficaces pour atteindre les performances réseau souhaitées. AMPLE [SR15], [WHP12], [PG13] est un système d'ingénierie et de gestion du trafic efficace qui effectue un contrôle adaptatif du trafic en utilisant plusieurs topologies de routage virtualisées (TRVs).

3.1. Ingénierie de trafic adaptatif basé sur TRV

AMPLE est un système d'ingénierie du trafic adaptatif basé sur plusieurs topologies de routage virtualisées, est un système holistique basé sur des topologies de routage IGP virtualisées pour une ingénierie de trafic dynamique. Il a récemment reçu de nombreuses attentions dans la communauté de recherche Internet. L'ingénierie du trafic concerne le contrôle de la performance et la gestion du réseau en prévoyant la nature et l'organisation de la transmission de données sur le réseau. Les systèmes proposés se composent de deux éléments complémentaires dans [SSD15], [WHP12], [SR15] et par contre ils se composent de trois composants complémentaires dans [PG13]. Les systèmes AMPLE partagent les deux suivants éléments qui sont : *Offline Link Weight Optimization* et *Adaptive Traffic Control*, les autres de [PG13] ajoute un troisième élément qui nommée *Admission Control Algorithm*.

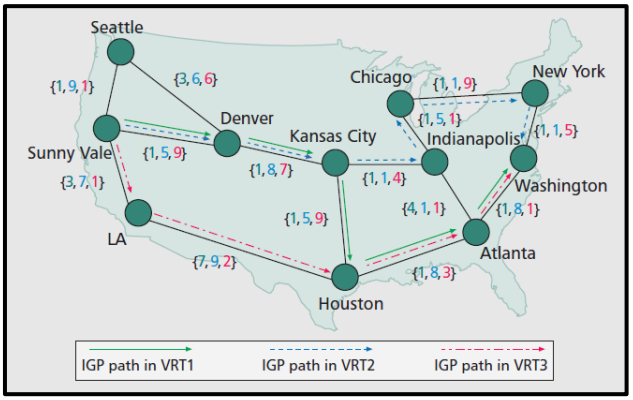


Figure 28 : Diversité de chemins dans la topologie du réseau Abilene.

Ces dernières années, la communauté des chercheurs s'intéresse aux réseaux virtuels contenant de nombreuses ressources telles que des routeurs ou des liens, et aussi des topologies de réseau logiques (*soft resources*), L'idée préconisé dans [CCK10] suit la stratégie de provisioning hors ligne de plusieurs chemins différents dans le routage et de répartition en ligne de la charge de trafic pour un équilibrage dynamique de la charge (*Dynamic Load Balancing*)

dans la transmission. L'approche a été décrite comme suit : Les MT-IGP sont utilisés en tant que protocole de routage sous-jacent pour fournir une diversité de chemins intra-domaines indépendante du trafic entre toutes les paires source-destination. Le trafic client attribué à différentes topologies de routage virtuel (VRT) suit des chemins IGP distincts en fonction des configurations de poids de lien IGP dédiées au sein de chaque VRT, le tout se passe en utilisant le routage MT-IGP. En prenant comme exemple, de Sunny Vale à Washington, qui illustré à la *Figure 28*, ce qui signifie comment la diversité de chemins peut obtenue pour les paires Source-Destinateur (S-D) dans la topologie de réseau Abilene au niveau du *Point-of-Presence* (PoP) [SSD15].

Un système AMPLE qui se compose de deux composants principaux. Le OLWO *(Offline Link Weight Optimization)* ce composant peut brièvement fonctionne comme suit, il se concentre sur le dimensionnement statique du réseau sous-jacent, avec poids de lien MT-IGP sont calculées pour maximiser la diversité de chemins intra-domaine sur plusieurs VRT. Une fois que la configuration optimisée du poids de la liaison a été appliquée sur le réseau. Le deuxième composant appeler contrôle de trafic adaptatif (ATC) effectue un ajustement du ratio de fractionnement du trafic sur une courte délais pour un équilibrage de charge adaptatif sur divers chemins IGP dans les VRT techniques, en fonction des conditions de trafic surveillées actuelles. Le système TE offre une solution prometteuse pour gérer efficacement la dynamique du trafic [SAY14].

3.1.1. Vue générale du système AMPLE (MT-IGP)

La dernière *Figure 29* présente une vue générale du système AMPLE TE proposé, AMPLE qu'il a inclus comme nous l'avons déjà mentionné les deux derniers composants clés (OLWO et ATC). Une nouveauté remarquable est que l'optimisation du poids des liens hors ligne est uniquement basée sur les caractéristiques du réseau lui-même. Les poids de lien MT-IGP calculés sont configurés dans des routeurs individuels et les chemins IGP correspondants dans chaque VRT sont renseignés dans leurs bases d'informations de routage locales (MT-RIB) [SAY14], [WHP12], [SSD15], [SSD15]. L'ATC fournit des fonctionnalités complémentaires à OLWO pour permettre un contrôle sur une courte délais (par exemple, horaire) en réponse au comportement du trafic qui ne peut généralement pas être anticipé après que l'OLWO se soit concentré sur la configuration de routage statique un court délai (par exemple, mensuelle). D'après *la même figure*, l'entrée pour l'ATC inclut les divers chemins MT-IGP en fonction des poids de lien calculés par OLWO et du réseau surveillé et des données de trafic telles que le volume de trafic entrant et les utilisations de lien. L'ATC calcule un nouveau ratio de fractionnement du trafic entre les différents VRT afin d'optimise les divers chemins IGP entre chaque paire S-D chaque intervalle de temps court. Le responsable TE centralisé gère cette fonctionnalité, il possède une connaissance complète de la topologie du réseau, cela il est aussi rassemblé pleinement à la collecte des conditions de trafic surveillées à jour [WHP12]. Ensuite il configure ces nouveaux ratios de fractionnement pour des nœuds PoP sources individuels, ils utilisent cette configuration pour remarquer en conséquence les identificateurs multi-topologies (MTID) du trafic provenant de leur localité située dans [SAY14] comme un module appelé allocation du trafic virtuel (*Virtual Traffic Allocation*).

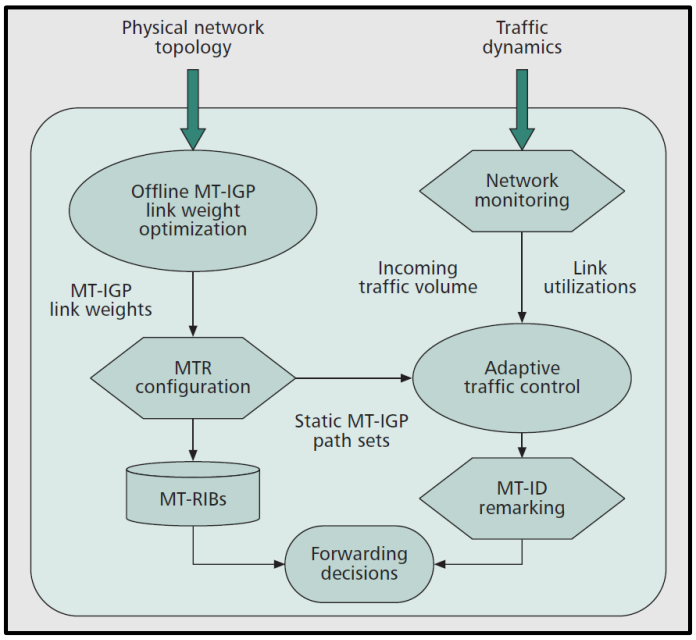


Figure 29 : Le système AMPLE (MT-IGP).

3.2. Ingénierie de trafic adaptatif MT-BGP basé sur TRV

Il existe deux types de routage : le routage intra-domaine qui est le processus de routage au sein d'un AS et le routage inter-domaine qui est le processus de routage entre différents AS. Le BGP est le protocole de routage inter-domaine sur Internet (BGP) [SM02]. Il existe également deux types de BGP : BGP intérieur (IBGP), utilisé par les ISPs (*Internet service providers*) pour échanger des informations de routage au sein d'un systèmes autonomes, et BGP externe (EBGP), utilisé pour échanger des routes entre systèmes autonomes.

Le système proposé utilisant le protocole BGP comprend trois composants complémentaires : comme nous l'avons mentionné dans la dernière partie, l'optimisation du poids de lien hors ligne (***offline link weight optimization***) prend en compte la topologie du réseau physique et tente de produire une diversité maximale de chemins de routage sur plusieurs topologies de routage virtuelles pour un fonctionnement à long terme grâce au réglage optimisé des poids de liens. Sur la base de ces divers chemins, le contrôle de trafic adaptatif (***adaptive traffic control***) effectue un fractionnement intelligent du trafic sur des topologies de routage individuelles en réaction à la dynamique du réseau surveillé à court terme. L'algorithme de contrôle d'admission (***Admission control algorithm***) utilisant dynamiquement crée un nouveau chemin à l'aide des topologies de routage virtuel [PG13]. Le système capable de gérer de manière optimale les dynamiques de trafic inattendues et constitue une nouvelle proposition visant à améliorer la qualité de service et les performances du réseau dans les réseaux IP utilisant le protocole BGP. L'ajustement du ratio de fractionnement du trafic adaptatif sur la topologie de routage MT-BGP réalise un équilibrage dynamique de la charge (*en cas de dynamique de trafic inattendue*).

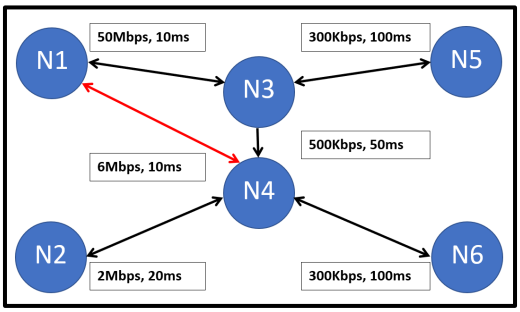


Figure 30 : Création d'un nouveau chemin avec l'aide de l'ADC.

La Figure 31 donne une structure globale du système AMPLE (MT-BGP) proposé, nous avons déjà expliqué l'objectif d'OLWO, et nous l'avons dit qui c'était un élément complémentaire de l'ATC.

Les auteurs dans [PG13] ajoute un troisième élément complémentaire à ces deux derniers. Les poids de lien MT-BGP calculés sont configurés dans des routeurs individuels et les chemins BGP correspondants au sein de chaque VRT sont renseignés dans leurs bases d'informations de routage locales.

L'ATC fournit des fonctionnalités complémentaires à OLWO pour permettre un contrôle sur une courte délais (par exemple, horaire) en réponse au comportement du trafic qui ne peut généralement pas être anticipé après que l'OLWO se soit concentré sur la configuration de routage statique un court délai (par exemple, mensuelle). L'objective principale de l'algorithme de contrôle d'admission (ADC) est de rechercher le chemin le moins fréquenté. S'il n'y a pas de chemin, le ADC informe immédiatement les topologies de routage virtuel et il crée son propre chemin (*la Figure 30*).

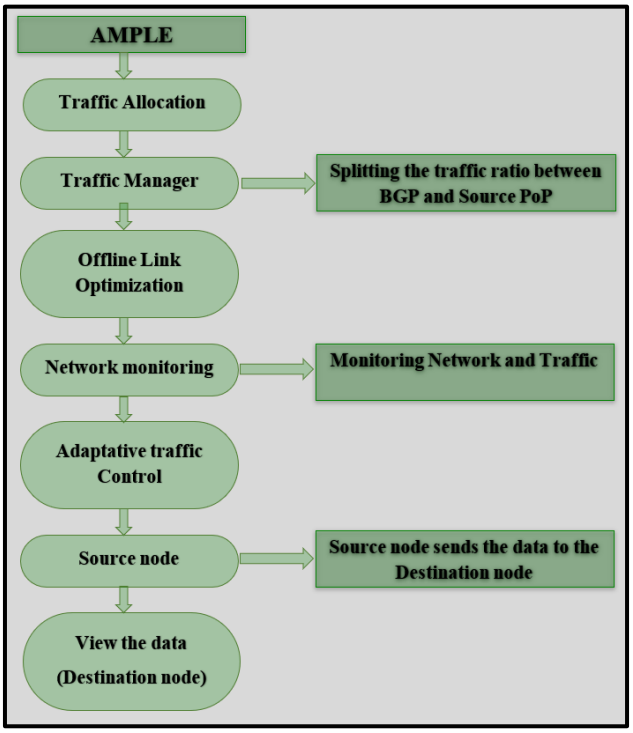


Figure 31 : Le système AMPLE (MT-BGP).

Conclusion

Dans ce chapitre nous avons présenté une étude détaillée des techniques de virtualisation des réseaux qui classée principalement en trois types de classification : virtualisation de serveur, virtualisation de stockage et virtualisation de réseau, il est distinguée en deux catégories : des techniques basées sur la virtualisation des protocoles, nous avons mentionné les VLANs et les VPNs et la virtualisation complète et la paravirtualisation comme des techniques basées sur la virtualisation des machines, nous avons introduit un rappel sur le terme de routage et nous expliquons plusieurs protocoles de routage (protocoles de routage statiques et dynamiques) et décrivons leurs forces et faiblesses relatives, après cela, nous avons mentionné la classification des protocoles de routage qui sont basés sur la communication réseau interne et externe (IGP et EGP) et leurs types. Nous avons terminé avec un état de l'art qui contient des systèmes basés sur des topologies de routage virtuel et nous avons introduit AMPLE, un nouveau système TE basé sur le routage IGP ou BGP virtualisé.

Chapitre 03 : Contribution

Introduction

De nos jours, le monde des réseaux est en train de devenir viral en termes de développement, donnant naissance à de nombreux types de réseaux. Une fois qu'on a dit qu'il était question de réseaux câblés et sans fil, une nouvelle marque de réseau est apparue dans notre vie. Le réseau de capteurs sans fil, ou comme il s'appelle WSN, ouvre vraiment un nouvel horizon dans de nombreux domaines tels que la science, la biologie, l'armée, la santé. Par sa flexibilité, sa fiabilité, sa reproductivité. De ce point de vue, les progrès récents de la technologie MEMS (Micro-Electro-Mechanical Systems) ont accru la recherche sur les réseaux de capteurs sans fil.

Ce n'est pas tout ce que cela apporte entre ses mots, un nouveau domaine fertile, plein de défis et de mystères, qui attendent d'être résolus pour s'améliorer afin que WSN devienne un meilleur outil au service de l'humanité.

1. Les réseaux de capteurs sans fil (WSN) :

Les réseaux de communication sans fil suscitent un intérêt croissant au sein des communautés de la recherche scientifiques d'où elle a réussi de nombreux avantages et en s'instaurer comme un terme clé et incontournable dans les architectures réseaux actuelles. Actuellement, les réseaux de capteurs sans fil (WSN) connu sous le nom de réseaux de capteurs, composé d'appareils à bas prix, autonomes en énergie, capables de surveiller et enregistrer les conditions physiques ou environnementales qui fonctionner de manière indépendante et en collaboration pour collecter, traiter et transmettre les données nécessaires sur l'environnement (température, humidité, bruit, vibration, pression, mouvement, pollution, etc.) [MJM05].

Dans les réseaux de capteurs sans fil, les nœuds sont dispersés de manière organisée ou aléatoire pour l'objectif de collecter des données et d'acheminer les données vers le puit et les utilisateurs finaux qui les analyser afin de prédire ou anticiper certains phénomènes (*voir la figure 32*).

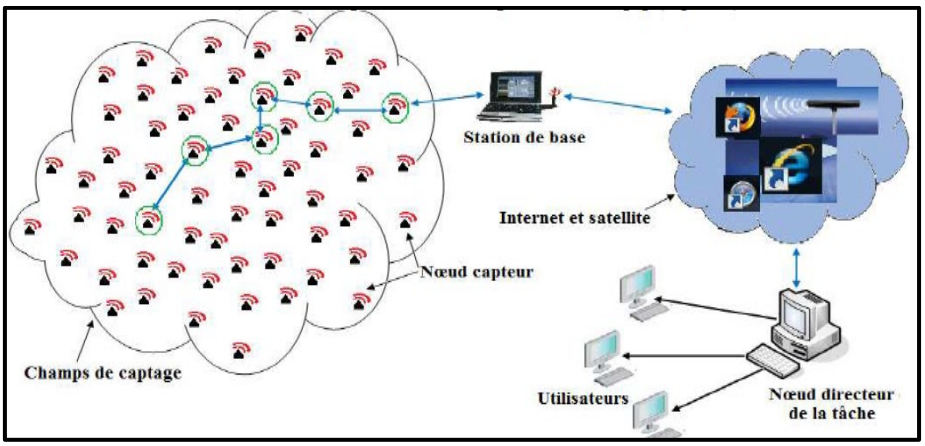


Figure 32 : Topologie d'un réseau de capteurs sans fil.

Chaque nœud de capteur sans fil est composé de quatre composants de base [AWYE02] comme le montre *la figure 33* : l'unité d'acquisition, l'unité de traitement, l'unité de communication et l'unité source d'énergie. Des réseaux de capteurs sans fil Multimédia ont été proposés pour permettre le suivi et la surveillance d'événements sous forme multimédia, tels que l'imagerie, la vidéo et l'audio. Ces réseaux sont constitués de nœuds de capteurs à faible coût équipés de microphones et de caméras. Ces nœuds sont interconnectés via une connexion sans fil pour la compression, la récupération et la corrélation de données.

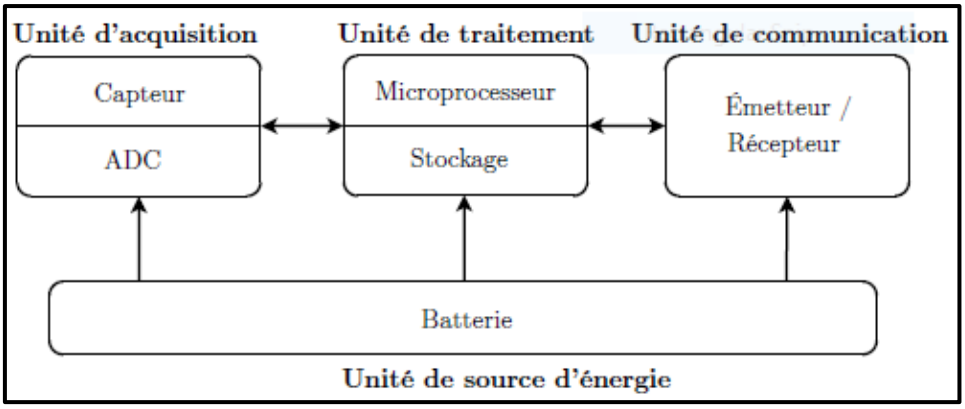


Figure 33 : Les composants d'un nœud capteur.

2. Les contraintes les plus courantes dans WSN :

Les réseaux de capteurs sans fil rencontrent des problèmes pendant le temps de travail. Ces problèmes peuvent se situer au niveau du capteur ou au niveau du réseau dans son ensemble, voici les problèmes les plus connus liés aux réseaux de capteurs.

2.1. Qualité De Service (QOS) :

Le niveau de service offert par les réseaux de capteurs sans fil est la qualité de service fournie à l'utilisateur. Les différents problèmes de qualité de service dans les réseaux de capteurs sont [DCH04], [MYO04] :

- En raison des changements constants de la topologie des réseaux de capteurs sans fil et des informations de routage, il est difficile d'assurer la qualité de service.
- Les réseaux de capteurs doivent disposer de la bande passante requise pour pouvoir atteindre la qualité de service minimale requise.

2.2. L'énergie :

Un grand problème courant dans le WSN est appelé l'énergie, car toute opération ou tâche à accomplir nécessite une certaine quantité d'énergie, si nous parlons de l'énergie consommée par le nœud lors de la capture et du traitement sans négliger les plus exigeants. L'énergie de communication et repose sur les deux opérations importantes que sont l'énergie de réception et l'énergie de transmission.

2.3. Sécurité :

La sécurité dans les réseaux de capteurs est l'un des piliers de base pour créer des réseaux de capteurs robustes et fiables. Elle est très importante autant que les performances et la faible consommation d'énergie.

Le RCSF est déployé dans des applications de champ de bataille, également pour la surveillance de bâtiments, dans des systèmes critiques tels que les aéroports et les hôpitaux et les alarmes antivols.

Les réseaux de capteurs étant une technologie en plein développement, les chercheurs et les développeurs conviennent que leurs efforts devraient être concentrés sur le développement et l'intégration de la sécurité dès les phases initiales du développement d'applications de capteurs.

Ce faisant, ils espèrent assurer une protection renforcée et complète contre les activités illégales tout en maintenant la stabilité des systèmes.

Chaque application RSF doit respecter les exigences de sécurité de base et se présente comme le suivant :

- **La confidentialité :**

  Elle est nécessaire dans les réseaux de capteurs pour protéger les informations transitant entre les nœuds de capteurs du réseau ou entre les capteurs et la station de base ; sinon, la communication pourrait être indiscrète.

- **Authentification :**

  Chaque nœud de capteur et la station de base doivent pouvoir vérifier que les données reçues ont bien été envoyées par un expéditeur de confiance et non par un adversaire ayant incité des nœuds légitimes à accepter de fausses données.

- **La sécurité et la qualité de service :**

  Elles sont deux pôles opposés dans les réseaux de capteurs. Les mécanismes de sécurité tels que le cryptage doivent être légers afin de minimiser la surcharge et ne pas affecter les performances du réseau.

2.4. Le trou de couverture :

Il a été interprété de diverses manières, l'auteur dans [CHF03] définit le problème des trous de couverture comme suit : avec un ensemble de capteurs et une zone cible, il n'existe au début aucun trou de couverture, si chaque point de cette zone cible est recouvert d'au moins k capteurs, les capteurs continuent de se déplacer pour répondre aux exigences de l'application jusqu'à ce que les trous deviennent.

2.5. La congestion :

Dans les réseaux de capteurs sans fil (WSN), une congestion se produise lorsque les nœuds sont distribués de manière dense ou que l'application produit un débit élevé près du puits en raison de la nature convergente du trafic en amont. La congestion peut entraîner une perte de paquets, ce qui réduit le débit et gaspille de l'énergie. Pour

minimiser la congestion dans les réseaux WSN ils doivent être contrôlés afin d'obtenir une efficacité énergétique élevée, de prolonger la durée de vie du système et d'améliorer l'ingénierie du trafic en termes d'utilisation des liaisons et de taux de perte de paquets, ainsi que du délai de transmission des paquets.

3. Motivation

Trop de protocoles ont été proposés pour éviter la congestion et affiner la consommation d'énergie. Des travaux ont déjà été réalisés pour fournir un meilleur réseau de distribution d'énergie (WSN) comme produit pour servir davantage dans notre vie quotidienne. Nous avons constaté que ces deux points sont vraiment des points chauds où ils ont eu la part du lion en causant de nombreux problèmes liés au routage des données du réseau. Nous allons ici changer le calibre de notre périmètre pour l'ajuster et faire clignoter le bulbe pour parler sur des topologies virtuelles et comment les problèmes de routage les plus fréquents sont survenus et affectés. Afin de dépasser les deux derniers points, nous avons parlé plus tôt de la congestion et de l'énergie, il devrait y avoir un mécanisme adaptatif avec un contrôle de mesure basé sur une structure hiérarchique utilisant le clustering pour réduire la quantité de communications sur le réseau, en ajoutant le goût d'être sélectif dans l'élection des nœuds pouvant participer au chemin de routage virtuel.

4. Une méthode pour la gestion dynamique du trafic dans les réseaux virtuels

Après avoir découvert plusieurs approches et méthodes (MATE, DATE ...) pour analyser et contrôler l'ingénierie du trafic réseau, Nous avons réalisé que MATE maîtrisait parfaitement le contrôle du trafic et je voulais l'appliquer sur les réseaux de capteurs virtuels (VSN est formé par un sous-ensemble de nœuds d'un réseau de capteurs sans fil) [KBG16], en couplant avec la puissance des clusters du protocole LEACH pour renforcer la force de connexion et réduire la quantité de données transmises sur le réseau.t Je vais emboîter la précédente avec une contrainte d'énergie lors de l'élection de nœuds où ils s'engageront dans le virtuel chemin de routage et déposer à l'aide de LSP.

Notre contribution consiste à proposer une méthode pour la gestion dynamique du trafic dans les réseaux de capteurs virtuels qui exécute un contrôle adaptatif du trafic en utilisant plusieurs topologies de routage virtualisées. La méthode fonctionne en deux étapes : une étape de surveillance du réseau et une étape d'adaptation du réseau. Elle contient les trois axes suivants :

1- Infrastructure : Conception et déploiement du réseau de capteurs sans fils.
2- Le processus d'adaptation basé trafic
   Phase 1 : Le Clustering.
   Phase 2 : La détection de congestion.
   Phase 3 : Les contraintes énergétiques.
   Phase 4 : L'adaptation du trafic (L'utilisation des topologies de routage virtualisées).
   Phase 5 : Répéter les phases 3 et 4.
3- Outils de simulation et plateformes : OMNET++, INET.

5. Scénario d'étude

Les réseaux de capteurs multimédias sans fil (WMSN) ont fasciné les chercheurs de l'intérêt suscité par l'amélioration des caméras et des microphones. Il existe de nombreuses possibilités de capture de contenu multimédia pour des applications telles que la surveillance du trafic, la détection d'intrusion et la surveillance de l'environnement et les applications militaires. Le contenu multimédia est sensible aux retards, c'est-à-dire aux paquets qui retardent et perdent du contenu dans des données multimédia telles que des données d'image, vidéo ou audio, ce qui engendre une congestion du trafic réseau, en particulier ce problème pendent. En fait, le problème est que les nœuds transmettre des données multimédia entres eux qui faire une surcharge, lorsque ces donnes arrivent retard aux destinataires ou quand perdre ces données.

De cette manière, ce problème justifie notre besoin de développer un scénario d'étude de trafic de réseau de capteur virtuel (VSN) pour la gestion dynamique du trafic qui exécute un contrôle adaptatif et de réduire la congestion du trafic dans les réseaux de capteurs virtuels.

L'étude proposée vise à évaluer le trafic dans un réseau de capteur sans fil pendent une guerre. Notre scénario d'étude (*voir la figure 34*) contient des nœuds qui sont dispersés de manière aléatoire, chaque cluster représente des VSN qui ont son application militaire spécifique. Nous supposons que l'armée s'intéresse à la détection précoce des zones critiques, à la taille des troupes et à la quantité d'équipements, et détecte les attaques et cible l'ennemi à l'aide d'un WSN. Les trois types d'application sont : Surveiller les zones (les zones critiques et les frontières), surveiller le statut (taille des troupes et quantité d'équipement), surveillance du champ de bataille (détecter l'attaque et cibler l'ennemi), dans un cluster chaque groupe des nœuds peut gère un ou plusieurs des applications précédentes.

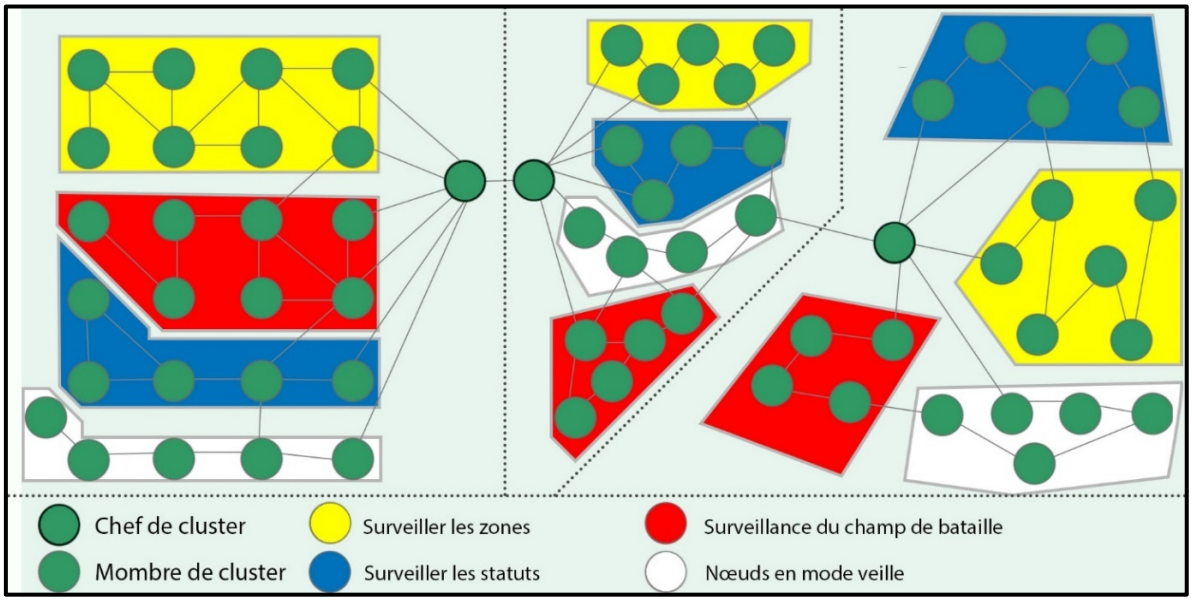


Figure 34 : Un réseau de capteur sans fils virtualisé.

Pour créer une gestion de trafic, nous supposons qu'il notre réseau est flat et supposons qu'il y a un VSN dans lesquels tous les nœuds de capteur été envoyer des données, cela provoquera de créer un grand problème de congestion du trafic qui a montré dans *la figure 35*.

Le trafic entrant arrive au chef de cluster, ce qui facilite le transfert de trafic entre les topologies de routage virtuel de manière à permettre la réception des paquets en ordre aux la destination, et il décide quand et comment distribuer le trafic entre les topologies de routage virtuel. Ceci est effectué sur la base des statistiques obtenues à partir de la phase de détection d'encombrement.

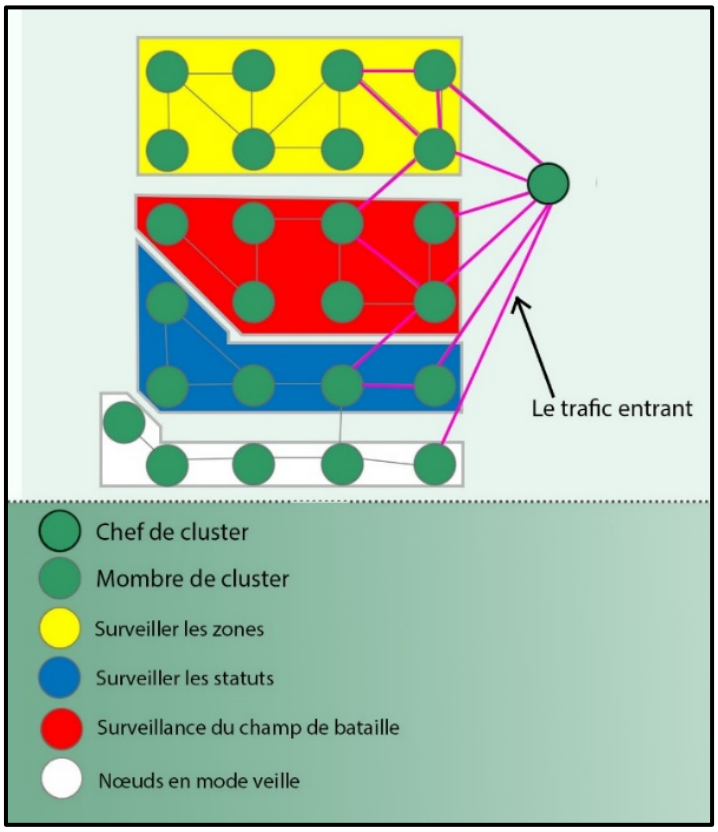


Figure 35 : Congestion du trafic dans un cluster.

Dans la partie suivante, nous allons expliquer notre méthode pour la gestion dynamique du trafic dans les réseaux de capteurs sans fils qui exécute un contrôle adaptatif du trafic en utilisant plusieurs topologies de routage virtualisées. Notre méthode est diffusée de cinq phases, nous montrons comme suite :

5.1. Phase 1 : Le Clustering.

Dans cette phase de notre méthode, nous avons utilisées la technique qu'il gère les économies d'énergie en utilisant des techniques telles que le clustering (figure 36) qui organise notre réseau en groupes (clusters) avec des chefs de groupe (clusterheads) et des nœuds membres. Le réseau doit se regrouper (clustering) de manière aléatoire, nous devons définir une règle pour choisir le chef de cluster (Cluster Head) de chaque cluster de notre réseau.

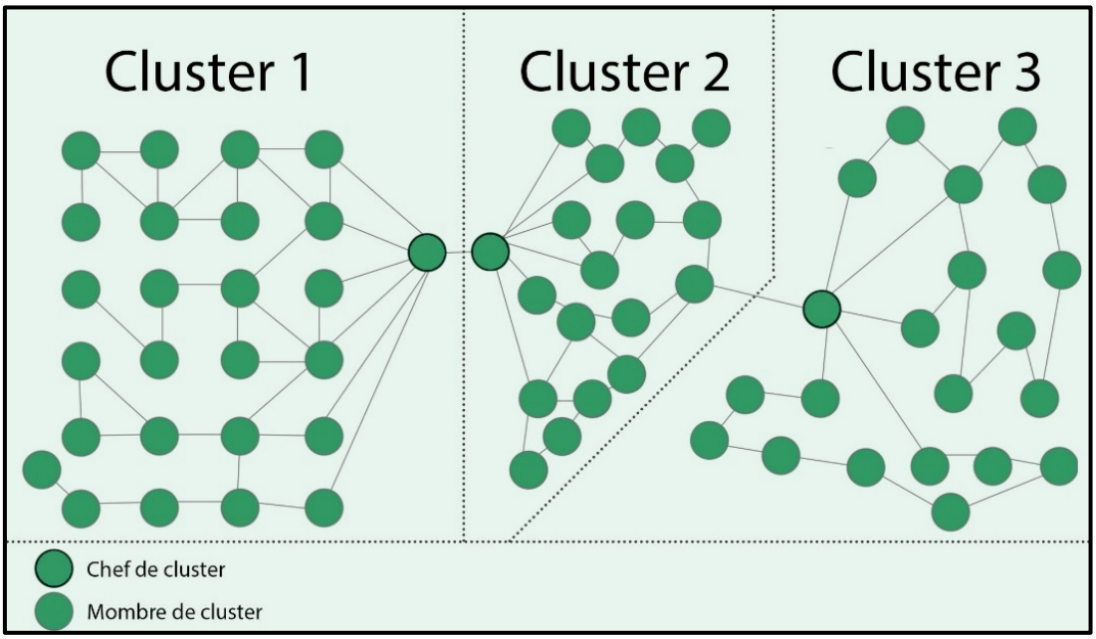


Figure 36 : Le clustering.

5.1.1. Le chef de Cluster (Cluster Head) :

Comme nous le savons, l'énergie est la ressource la plus essentielle dans les réseaux de capteurs sans fil par ce que chaque nœud a une batterie limitée, cela nous oblige à choisir et à sélectionner le chef de cluster idéales en termes d'énergie. Aléatoirement chaque nœud de cluster choisit un nombre n compris entre 0 et 1, pour un nœud devient le chef de cluster (Cluster Head) il faut que : n < T(n), selon [AWYE02] qui dit :

$$T(n) = \begin{cases} \dfrac{P}{1 - P \times \left(r \bmod \dfrac{1}{P}\right)} , si\ n\ \in G. \\ 0 , sinon \end{cases}$$

Avec :

P : pourcentage désiré de chef de cluster (Cluster Head) pendant un round.
r : numéro du round.
G : l'ensemble des nœuds qui n^' ont pas été élu le chef de cluster pendant les 1/P rounds précédents.

Après cette étape, les chefs de clusters envoient des paquets de publication pour informer les nœuds du cluster qu'ils sont devenus des chefs de clusters. Une fois que les nœuds de capteur ont reçu la publication, ils déterminent le cluster auquel ils souhaitent appartenir en fonction de la force du signal de la publication des têtes de cluster aux nœuds de capteur. Les nœuds de capteurs peuvent commencer à détecter et à transmettre des données aux clusterheads, ces derniers qui agréger les données des nœuds de leur cluster et après avoir envoyé ces données à la station de base comme *la figure 37* montre.

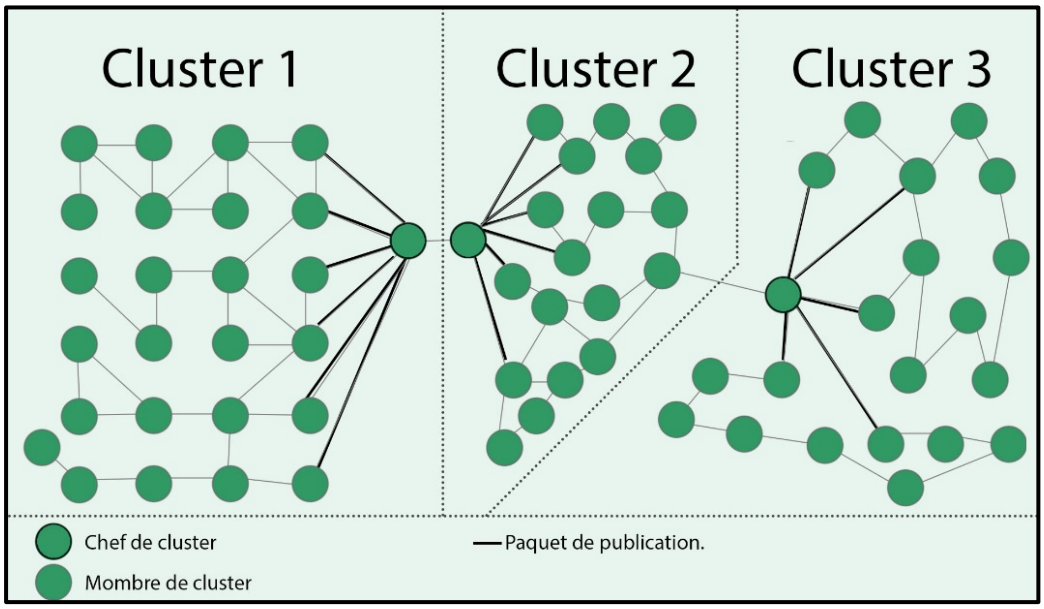


Figure 37 : Les chefs de clusters envoient Paquets de publication.

5.1.2. La virtualisation du réseau de capteur :

La virtualisation est une technologie qui peut potentiellement permettre le partage. Sur la base de la dernière définition, nous devons virtualiser notre réseau comme suit : chaque réseau de capteurs virtuels formé par un sous-ensemble de nœuds WSN regroupés en tant qu'un cluster, chacun d'eux étant dédié à une application à un moment donné, cette formation dynamique de clusters garantit l'efficacité des ressources et les nœuds restants pourraient être disponibles pour différentes applications.

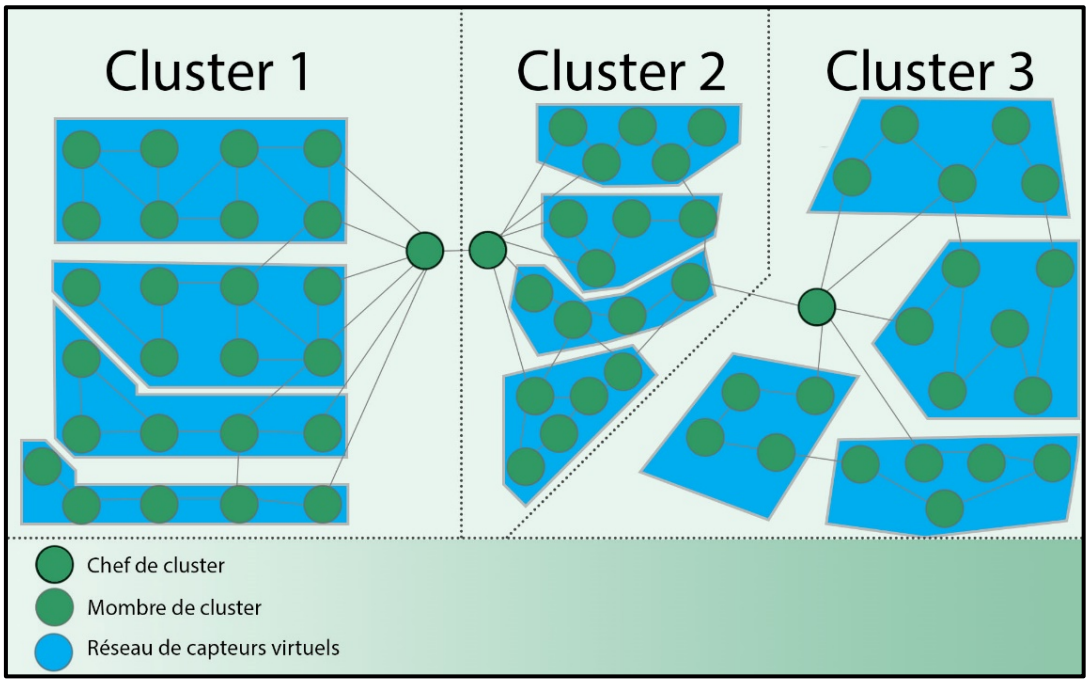


Figure 38 : La virtualisation du réseau de capteur.

Après que nous virtualiser notre réseau, il faut affecter les applications à chaque un des VSN dans chaque cluster, *la figure 39* montre ce dont nous avons parlé.

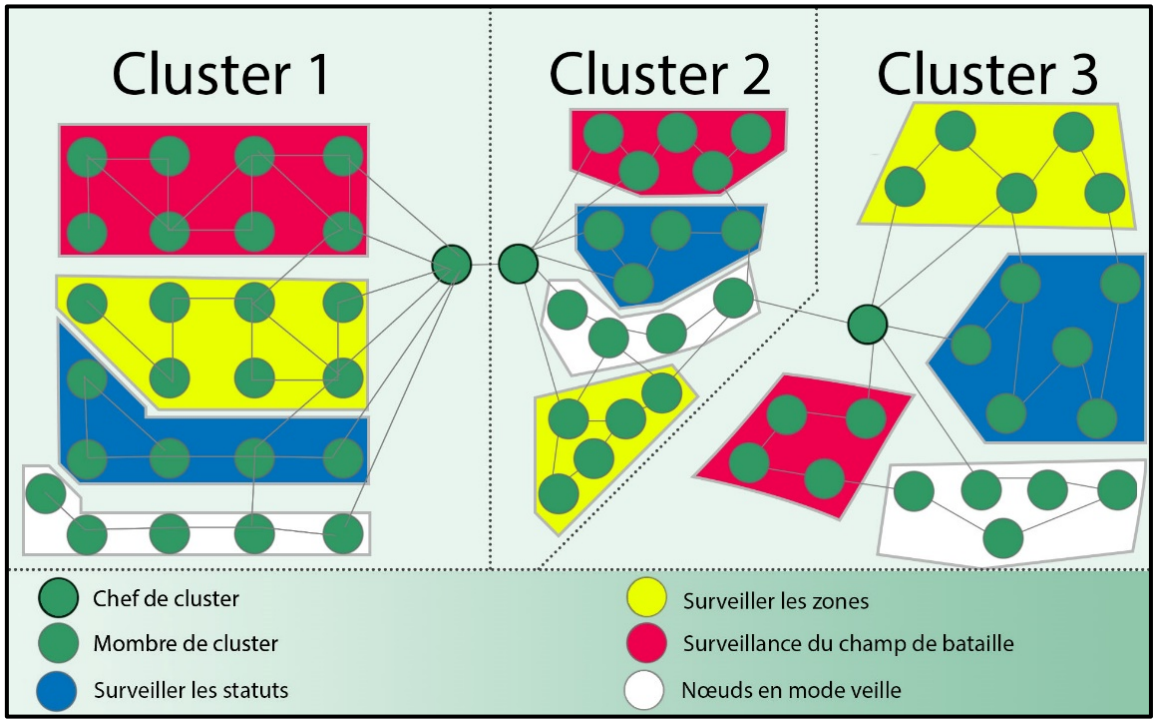


Figure 39 : Affectation des applications.

5.2. Phase 2 : La détection de congestion.

Dans notre méthode, seuls les chefs de cluster et le nœud destination sont requis pour participer à la phase de la détection de congestion. La plupart des études suggèrent que deux métriques ont été utilisé à savoir le retard et la perte de paquets [KDBA14], sont mesurées en transmettant périodiquement des paquets de test au nœud de destination, qui les renvoie ensuite au nœud de chef du cluster, ces deux métriques pouvant être mesurées de manière fiable en cas de congestion sur le trafic.

5.2.1. Le retard de paquet :

Le retard d'un paquet à travers un chemin virtuel (Virtual Path ou VP) peut être obtenu en transmettant un paquet de test par le chef de cluster au nœud de destination. Le paquet de test est horodaté chez le chef de cluster à l'instant T1 et enregistré sur le nœud de destination à l'instant T2 (*voir la figure 40*). Si l'unité de traitement du chef de cluster est plus rapide que l'unité de traitement du nœud de destination par Td, le retard de paquet global (temps de transmission, temps de propagation, temps d'attente et temps de traitement) est alors T2 - T1+Td. Le retard moyen des paquets est estimé par un groupe de paquets de test envoyés simultanément à travers un chemin virtuel par la règle suivante E [T2 - T1] + Td.

Dans la plupart des réseaux informatiques, le retard sera calculé en fonction de la somme cumulée sur le retard de mise en file d'attente, de traitement, de propagation et de transmission [RWW04] :

a- Retard de transmission de paquets (Transmission delay) :

Il représente le temps pris par la couche physique à la source pour placer les paquets sur la liaison. $Transmission\ Delay\ =$ Data size / bandwidth $=$ (L/B) second.

b- Retard de propagation de paquets (Propagation delay) :

Il représente le temps de vol des paquets nécessaires aux bits pour atteindre la destination à partir du nœud source.

$Propagation\ delay\ =\ distance/transmission\ speed\ =\ d/s.$

c- La fille d'attente (Queuing delay) :

Il représente le temps à laquelle le paquet est mis en mémoire tampon (buffer) avant de pouvoir être envoyé. $Queuing\ delay\ =\ (N-1)L/(2*R)$.

$D'ou:\ N\ =\ nombre\ de\ paquets, L = taille\ du\ paquet\ et\ R = bande\ passante.$

d- Retard de traitement de paquets (Processing delay) :

Il représente le temps nécessaire pour examiner l'en-tête du paquet et déterminer la direction du paquet ou le temps nécessaire pour traiter le paquet sur le système de réseau.

$Processing\ Delay\ =\ microsecondes\ ou\ moins.$

En générale le retard global de paquet calculer par la règle suivante :

$$T_d = D_{pro} + D_{queue} + D_{trans} + D_{prop}$$

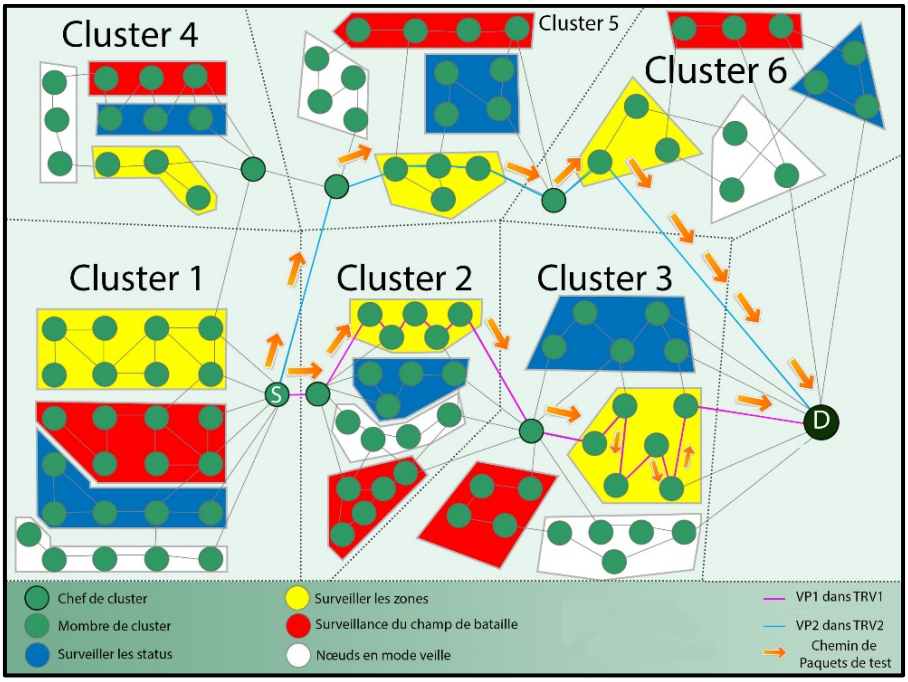


Figure 40 : L'envoi de paquet de test à travers des multiples chemins virtuels.

5.2.2. La perte de paquets :

La perte de paquets est la deuxième métrique que nous avons utilisée pour mesurer la congestion, elle peut être estimée par un groupe de paquets de test. Dans le contexte, un nœud abandonnera le paquet par ce que ce paquet ne trouve pas son emplacement pour le stocker

dans une file d'attente plein, comme cela le paquet sera perdu. Nous pouvons estimer la probabilité de perte de paquets en codant un numéro de séquence (figure 5.7) dans le paquet de test envoyés à travers un chemin virtuel en ajoutant deux champs aux paquets : le premier champ contient le nombre de paquets de test envoyés par le chef du cluster, le second contient le nombre de paquets de test reçus par le nœud de destination.

Toutes ces informations sont référées au chef du cluster pour savoir combien de paquets de test ont été perdus pondant le processus de transmission. Ce qui permet au chef du cluster d'estimer la probabilité de perte de paquets en fonction du nombre de paquets de test qui ont été transmis et du nombre reçu.

Par exemple, le chef de cluster a envoyé 20 paquets de test via deux chemins virtuels, il a envoyé 10 paquets pour chaque chemin, le numéro de séquence des paquets de la première opération de transmission (chemin virtuel 1) est compris entre 1 et 10, et entre 11 et 20 pour la deuxièmement (chemin virtuel 2), lorsque le chef de cluster a fini d'envoyer les paquets de test via un VP, il notifie le nœud de destination qui est le dernier paquet via ce VP, à l'autre extrémité, le nœud de destination reçoit les paquets de test. Ensuite, le chef de cluster sait combien de paquets de test sont transmis via chaque VP (par exemple, 10 paquets via VP1 et VP2), et le nœud de destination ajoute le nombre de paquets de test reçus (par exemple, 10 paquets de VP1 et 5 paquets de VP2).

En conséquence, à travers le premier chemin virtuel : 10 paquets ont été transmis et reçus, ce qui prouve qu'il n'y a pas de congestion sur ce chemin, contrairement au deuxième chemin virtuel : 10 paquets ont été transmis et 5 paquets ont été reçus, ce qui prouve qu'il existe une congestion sur ce chemin (*voir la figure 41*).

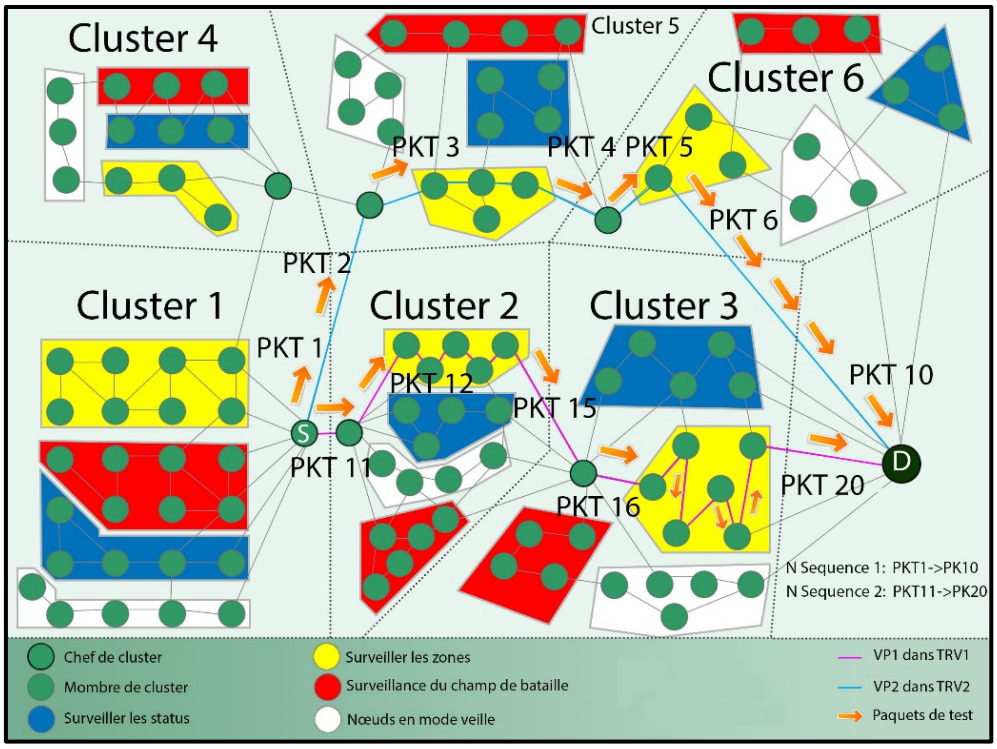


Figure 41 : Codage par numéro de séquence.

5.3. Phase 3 : Les contraintes énergétiques :

Chaque cluster contient des plusieurs réseaux virtuels selon le nombre d'application (service), dans notre scénario nous avons les trois types précédents : surveiller les zones (les zones critiques et les frontières), surveiller le statut (taille des troupes et quantité d'équipement), surveillance du champ de bataille (détecter l'attaque et cibler l'ennemi), dans chaque cluster nous avons des nœuds en mode veille qui représente ¼ de le nombre total des nœud, l'lorsque nous avons détecter qu'il y a un nœud a une faible énergie, nous adapte le VSN par le changement de ce nœud. Le module le plus consommable d'énergie dans le nœud est le module radio car c'est lui qui assure la communication entre les nœuds [MN04]. Il comprend quatre états (émetteur et récepteur) : actif, recevoir, transmettre et veille.

- État actif : la radio est allumée, mais elle est inutilisée, ce qui signifie que le nœud du capteur n'est ni en train de recevoir ni d'émettre, ce qui entraîne une perte de puissance due à une écoute inutile du canal de transmission. Pour éviter le dernier problème, un capteur doit être activé uniquement lorsque cela est nécessaire, et il doit être endormi différemment.
- État de veille : la radio est éteinte.
- État de transmission : la radio transmet un paquet.
- État de réception : la radio reçoit un paquet.

Nous expliquerons comment nous adaptons le réseau de capteurs virtuels, qui basée sur l'énergie des nœuds. Le chef de cluster envoie un paquet à tous les membres de cluster, par ce paquet nous pouvons tester l'état d'un nœud, après les envois nous pouvons extraire deux états pour le nœud: nœud vivant ou nœud mort, nous pouvons le détecter par les paquets envoyés, si le nœud répond par un paquet, cela prouve que le nœud est vivant (nous ne nous inquiétons pas de l'heure), dans le cas où le nœud ne répond pas, la seule possibilité est que le nœud est mort. Si le nœud est mort, le chef du cluster change ce nœud par un autre nœud cela apporte de la liste des nœuds qui étaient en mode veille.

Les conditions énergétiques :

Nous allons préciser les conditions suivantes :

1. En vérifiant l'état énergétique actuel du nœud, plus que le minimum (le minimum est la quantité d'énergie qui peut supporter le travail affecté 2 fois) de 20% à choisir ce nœud dans le chemin de routage, car il peut s'agir d'un nœud épuisé.
2. Estimez la quantité de données à envoyer et vérifiez que le nœud peut gérer la tâche en termes d'énergie.
3. Si la communication établie actuelle prenait plus que la quantité d'énergie calculée, avec plus de 20%, nous abandonnons la connexion pour éviter toute perte d'énergie.

5.4. Phase 4 : L'adaptation du trafic.

Cette phase est la plus importante dans notre méthode, comme nous l'avons mentionné auparavant que le contrôle adaptatif du trafic est une stratégie de gestion du trafic. L'objectif principal de cette phase est consisté a distribué le trafic entrant via plusieurs chemins virtuels

qui peut réduire la congestion sur certains liens et c'est ce qu'on a appelé l'équilibrage de charge (Load Balancing) dans [CNF10].

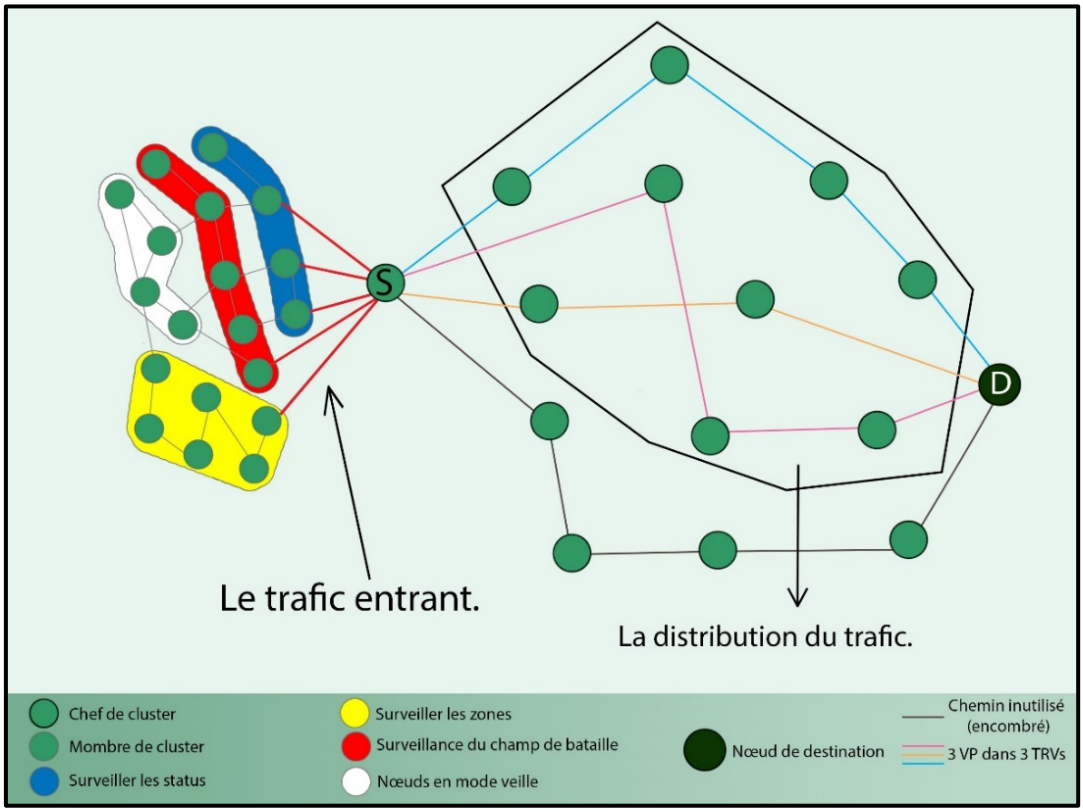


Figure 42 : La phase d'adaptation du trafic.

Après avoir utilisé les deux dernières métriques pour mesurer la congestion et vérifier l'énergie de chaque nœud pour lequel nous avons garanti les contraintes d'énergie lorsque tous les chemins virtuels ne contiennent pas de nœuds morts, de plus, nous n'utilisons pas le chemin que nous détectons qui est un chemin encombré. Nous devrions avoir à contrôler le trafic entrant en le distribuant via plusieurs chemins virtuels (la fonction de clusterhead), lorsqu'il distribue le trafic entrant de manière presque égale via plusieurs chemins vers le nœud de destination.

La distribution est effectuée par paquet (DP) après avoir divisé le nombre total de paquets reçus (NP) pendant le trafic entrant par le nombre de chemins virtuels (NCV), donc : DP = NP / NCV.

5.5. Phase 5 : Répéter les phases 3 et 4.

La dernière phase de notre méthode est de répéter les deux dernières phases qui sont contrôle l'énergie des nœuds et adapter le trafic tout le temps, pour assurer la distribution du trafic et de résoudre et minimiser le problème de congestion.

Conclusion

Dans ce chapitre, nous avons proposé une méthode pour la gestion dynamique du trafic dans les réseaux de capteurs virtuels qui exécute un contrôle adaptatif du trafic en utilisant plusieurs topologies de routage virtualisées pour l'objectif d'éviter et réduire le problème de congestion.

La méthode commence par une phase de regroupement qui regroupe les nœuds et choisit des clusterheads qui sont envoyés à leurs membres de cluster pour les informer qu'ils sont les chefs de cluster. Dans chaque cluster, nous devons virtualiser notre réseau sur plusieurs réseaux virtuels où chacun a son application. Ensuite, nous devons détecter l'encombrement de nos réseaux en utilisant deux métriques : délai de paquet et perte de paquet qui sont des paquets de test, puis nous devons vérifier l'énergie du nœud en envoyant un paquet et en attendant la réponse des nœuds, qu'ils répondent ou non, nous devons connaître l'état du nœud (nœud vivant ou mort).

Dans la phase d'adaptation du trafic, toutes les mesures sont utilisées pour éliminer aux maximum les chemins virtuels encombrés, pour éliminer les nœuds morts et pour éliminer les nœuds qui ne peuvent pas gérer les tâches en termes d'énergie, après que toutes ces fonctions le trafic entrant doit être distribué via plusieurs chemin virtuel dans les topologies de routage virtuel.

Chapitre 04 : Implémentation et simulation.

Chapitre 04 : Implémentation et simulation :

Introduction

Après nous être assuré de notre idée finale de la méthode proposée dans le dernier chapitre, un test de simulation a été réalisé pour réaliser un prototype pour notre méthode en créant un réseau de capteurs sans fil avec des nœuds statiques et en essayant d'envoyer des paquets de test pour détecter la congestion du trafic, et nous allons essayer d'adapter le trafic entrant dans le clusterhead en le distribuant via plusieurs chemins virtuels. Avant de détailler nos simulations, nous allons d'abord parler des outils de simulation fournis et de la motivation pour OMNET ++, nous présenterons l'environnement de simulation, puis nous développerons une implémentation de notre méthode et nous terminerons notre chapitre par une conclusion.

1. Les outils de simulation

Aujourd'hui, les simulateurs de réseau ont mis beaucoup de mal à réaliser de vrais réseaux, car le déploiement d'un banc d'essais complet est extrêmement coûteux. Grâce à ces simulateurs de réseau, nous pouvons facilement vérifier un protocole ou un algorithme spécifique. Pour les simulateurs, il existe deux types commerciaux tels que OPNET, QUALNET et Open Source, tels que NS2, OMNET ++, SSFNET et J-Sim.

Dans cette section, nous présenterons les simulateurs les plus utilisés dans le monde WSN [JIP08].

- **OPNET :**

  Il s'agit de la marque commerciale déposée et du nom du produit présenté par OPENT Technologies incorporation. Il est l'un des simulateurs de réseaux commerciaux les plus célèbres et les plus populaires à la fin de 2008.

- **Network Simulator 2 (NS2) :**

  Le NS2 est l'un des simulateurs de réseau open source les plus populaires. Le NS original est un simulateur à événements discrets destiné à la recherche en réseau. NS2 est la deuxième version de NS (simulateur de réseau). NS est à l'origine basé sur un simulateur de réseau REAL. La première version de NS a été développée en 1989 et a beaucoup évolué au cours des dernières années.

- **OMNET ++ :**

  Similaire à NS2, OMNET ++ est également un simulateur de réseau public à base de composants avec prise en charge d'interface graphique. Son principal domaine d'application est les réseaux de communication. OMNET ++ possède une architecture générique et flexible qui la rend également performante dans d'autres domaines tels que les systèmes informatiques, les réseaux de mise en file d'attente, les architectures matérielles ou même les processus métier**.**

2. Motivation de choix de OMNET ++ :

OMNET ++ (Objective Modular Network Testbed en C ++) est un framework de simulation de réseau d'événements discrets modulaire orienté objet, basé sur les composants de simulation C++ (bibliothèque et Framework), principalement utilisé pour la construction de simulateurs de réseaux. L'apparition d'OMNeT++ visait à unifier les efforts de la communauté des chercheurs afin de fournir une plate-forme de simulation puissante et reconnue pour les simulations complexes et les conditions proches de la réalité. Le résultat : OMNeT++ est devenu l'un des simulateurs de réseau les plus utilisés par la communauté des chercheurs pour expérimenter de nouvelles idées. Il permet entre autres une simulation complète de toutes les couches réseau et du protocole TCP / IP avec une variété de protocoles et de paramètres de simulation (Routage, mobilité, plage de transmission et densité, etc.).

3. L'environnement OMNET :

OMNeT ++ (Objective Modular Network Testbed en C ++) est une bibliothèque et une structure de simulation C ++ extensibles, modulaires et basées sur des composants, destinées principalement à la construction de simulateurs de réseau. Le terme « réseau » s'entend au sens large et comprend les réseaux de communication filaires et sans fil, les réseaux sur puce, les réseaux de mise en file d'attente, etc.

Figure 43 : L'environnement OMNET++.

Des fonctionnalités spécifiques à un domaine, telles que la prise en charge des réseaux de capteurs, des réseaux ad hoc sans fil, des protocoles Internet, de la modélisation des performances, des réseaux photoniques, etc., sont fournies par des cadres de modèles développés en tant que projets indépendants.

OMNeT ++ propose un environnement de développement intégré basé sur Eclipse, un environnement d'exécution graphique et une multitude d'autres outils. Il existe des extensions

pour la simulation en temps réel, l'émulation de réseau, l'intégration de base de données et plusieurs autres fonctions.

Les principaux modèles de simulation de réseaux informatiques sont disponibles dans plusieurs cadres externes. Le plus couramment utilisé est INET qui offre une variété de modèles pour tous les types de protocoles réseau et de technologies comme IPv6, BGP, etc. INET propose également un ensemble de modèles de mobilité pour simuler le mouvement des nœuds dans les simulations. Les modèles INET sont sous licence LGPL ou GPL.

Le simulateur OMNET++ a des caractéristiques parmi eux les suivants :

- C'est un noyau de simulation et un éditeur de réseau graphique pour les fichiers NED.
- Outils pour tracer des données.
- Compilateur pour les langages de description de topologie NED.
- Utilitaires (outil de génération de graines de nombres aléatoires, outil de création de fichiers, etc.).
- Deux types d'interfaces utilisateur pour l'exécution de la simulation :
    - Une interface utilisateur en ligne de commande.
    - Une interface utilisateur graphique.

4. Le Framework INET pour OMNeT ++ :

INET est construit autour du concept de modules qui communiquent par la transmission de messages. Les agents et les protocoles réseau sont représentés par des composants, qui peuvent être librement combinés pour former des hôtes, des routeurs, des commutateurs et d'autres périphériques réseau. Les nouveaux composants peuvent être programmés par l'utilisateur et les composants existants ont été écrits de manière à être faciles à comprendre et à modifier.

INET bénéficie de l'infrastructure fournie par OMNeT ++. Outre l'utilisation des services fournis par le noyau et la bibliothèque de simulation OMNeT ++ (modèle de composant, paramétrage, enregistrement des résultats, etc.), cela signifie également que les modèles peuvent être développés, assemblés, paramétrés, exécutés et leurs résultats valorisés dans le confort de l'utilisateur. OMNeT ++ Simulation IDE ou à partir de la ligne de commande.

Certaines fonctionnalités :

- Scénario de réseau de capteurs sans fil.
- Implémentations de protocole enfichables pour différentes couches.
- Protocoles MAC pour réseaux de capteurs sans fil.
- Consommation d'énergie.
- Protocoles de la couche de transport : TCP, UDP, SCTP.
- Protocoles de routage (ad-hoc et filaire).
- Large gamme de modèles d'application.
- Support d'émulation de réseau.
- Soutien à la mobilité.

5. Implémentation de notre méthode

Le développement du prototype est passé par quelques étapes et ici, il y a des instantanés de plusieurs étapes.

La première étape est la préparation de OMNeT ++ sous Ubuntu :

Figure 44 : Montre l'OMNeT ++ sous Ubuntu.

Le simulateur OMNeT++ a été configuré sous Linux Ubuntu 18.04 et la raison de l'utilisation de Linux Ubuntu est dû au fait que certains modèles et Frameworks ne fonctionnent que dans cet SE, c'est également le système d'exploitation le plus stable pour OMNeT ++.

Avant de commencer l'installation, nous actualisons la base de données des packages disponibles et nous tapons dans le terminal pour installer les packages requis :

```
$ sudo apt-get update
$ sudo apt-get install build-essential gcc g++ bison flex perl python
python3 qt5-default libqt5opengl5-dev tcl-dev tk-dev libxml2-dev zlib1g-dev
default-jre doxygen graphviz libwebkitgtk-1.0
```

Puis entrez les commandes suivantes :

```
$ . / configure
$ make
```

La deuxième étape consiste à créer un réseau de capteurs sans fils contenant certains nœuds, parmi lesquels des chefs de clusters et des nœuds de capteurs.

Dans cette étape, nous devons présenter deux modèles de nœuds le chef du cluster et le nœud de capteurs qui sont des modules composés qui contient quelques éléments importés de la Framework INET :

Le nœud de capteur :

Nous avons dit que ce module est composé et nous dirons qu'il contient les sous modèles importés de INET (*la figure 45 représente une vue globale d'un nœud de capteur*) qui sont les suivants :

Statu (Status) assure le suivi de l'état du nœud de réseau, **Tableau D'interface (interfaceTable)** qui contient uniquement les propriétés indépendantes du protocole des interfaces **IPv4** ou **IPv6**, **Stockage De L'énergie (energyStorage)** ces modèles décrivent des dispositifs qui absorbent l'énergie produite par des générateurs et fournissent de l'énergie aux consommateurs, **Gestion De L'énergie** (**energyManagment**) cela surveille un stockage d'énergie, en évaluent l'état et contrôlent les consommateurs et les générateurs afin d'empêcher le stockage d'énergie de fonctionner en dehors de sa zone d'utilisation sécurisée, **Générateur D'énergie (energyGenerator)** ce type décrit le processus de génération d'énergie d'appareils au fil du temps, TCP ou UDP (*voir les figures 47*).

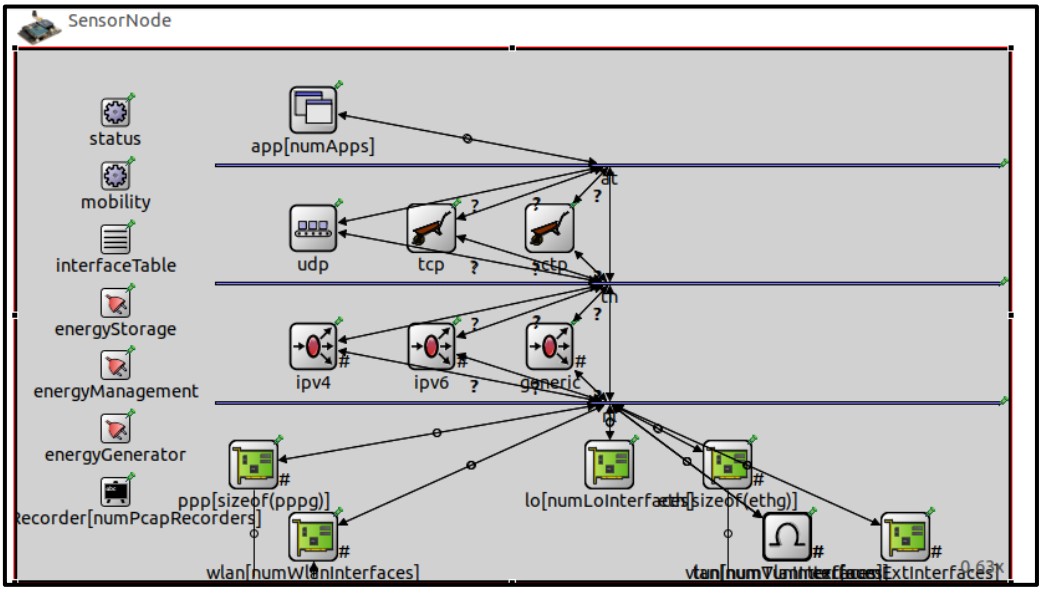


Figure 45 : Description du module de nœud de capteur.

Voilà le code source du nœud de capteur :

```
module SensorNode extends ApplicationLayerNodeBase
{
    parameters:
        @display("i=misc/sensor2");
        @figure[submodules];
        numWlanInterfaces = default(1);
        energyStorage.typename = default("IdealEpEnergyStorage");
        wlan[*].typename = default("Ieee802154NarrowbandInterface");
        wlan[*].radio.energyConsumer.typename = default("SensorStateBasedEpEnergyConsumer");
}
```

Figure 46 : Le code source du nœud de capteur.

```
moduleinterface ITcp
{
    @display("i=block/wheelbarrow");
    gates:
        input appIn @labels(TcpCommand/down);
        input ipIn @labels(TcpHeader,Ipv4ControlInfo/up,Ipv6ControlInfo/up);
        output appOut @labels(TcpCommand/up);
        output ipOut @labels(TcpHeader,Ipv4ControlInfo/down,Ipv6ControlInfo/down);
}
```

```
moduleinterface IUdp
{
    parameters:
        @display("i=block/transport");

    gates:
        input appIn @labels(UdpControlInfo/down);
        input ipIn @labels(UdpHeader,Ipv4ControlInfo/up,Ipv6ControlInfo/up);
        output appOut @labels(UdpControlInfo/up);
        output ipOut @labels(UdpHeader,Ipv4ControlInfo/down,Ipv6ControlInfo/down);
}
```

Figure 47 : Le code source de IUDP et ITCP.

Le nœud de chef de cluster :

Aussi, ce module est composé et il contient des sous modèles listés comme suivants (*la figure 48 représente une vue globale d'un nœud chef de cluster*) : **Statu (Status), Tableau D'interface (interfaceTable), Tableau Des Mac (macTable), Wlan et relayUnit** qui gèrent les fonctions suivantes: mappage entre les ports et les adresses MAC, transmission de trames vers les ports appropriés, relais de trames en fonction de leurs adresses MAC de destination et modélisation de la taille de la mémoire tampon finie et de la puissance de traitement finie.

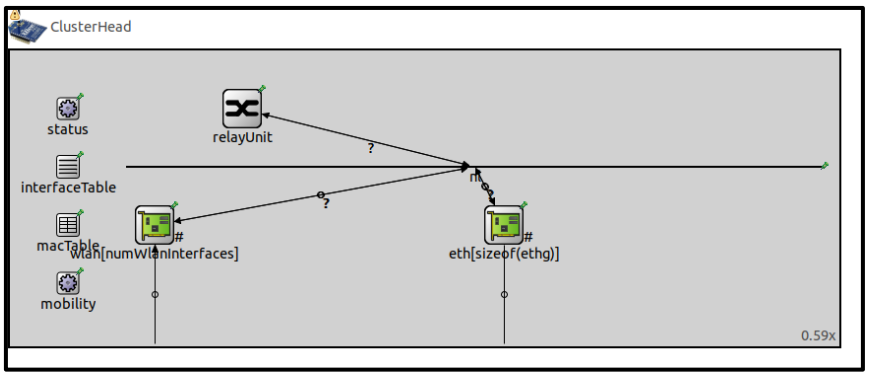


Figure 48 : Description du module de chef de cluster.

Déclaration des paramètres du nœud dans notre simulation :

```
parameters:
    @networkNode();
    @labels(node,ethernet-node,wireless-node);
    @display("i=misc/sensor");
    int numWlanInterfaces = default(1);              // the number of radios in the CusterHead
    bool hasStatus = default(false);
    wlan[*].mgmt.typename = default("Ieee80211MgmtAp");
    wlan[*].llc.typename = default("Ieee80211Portal");
    wlan[*].agent.typename = default("");
    wlan[*].radio.antenna.mobilityModule = default("^.^.^.mobility");
    eth[*].encap.typename = "EtherEncapDummy";
    *.interfaceTableModule = default(absPath(".interfaceTable"));
    relayUnit.hasStp = false;
```

Figure 49 : Le code source du nœud chef de cluster.

Après avoir décrit les modules, nous devons créer un réseau (*illustre dans la figure 50*) de capteurs sans fil contient des chefs de clusters et des nœuds de capteur qui va commencer à échanger des données ultérieurement, avec que tous les nœuds de capteurs sont des nœuds stationnaires.

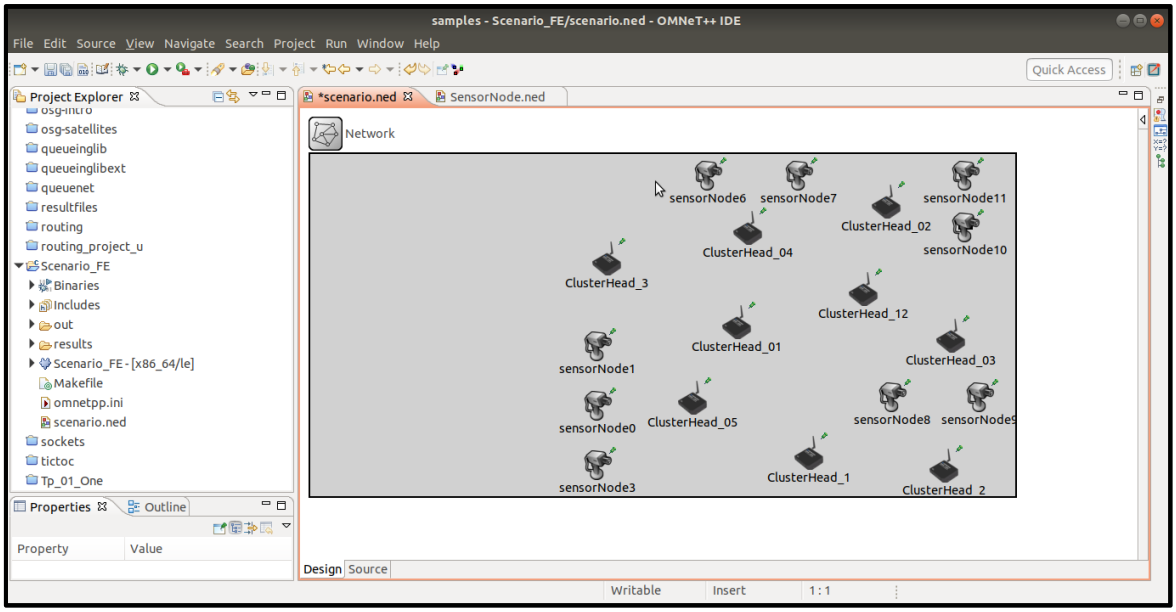


Figure 50 : La création des réseaux de capteurs.

Aussi, nous avons besoin des autres modules pour mise en forme notre réseau, et amélioré notre scenario (*voir la figure 51*) avec des modules importés de INET suivants : **visualiser** qui être pour visualiser un large éventail d'événements et de conditions sur le réseau, **radioMedium** : ce modèle de support radio utilise la puissance de transmission scalaire dans la représentation analogique, et configurator : Ce module attribue des adresses IPv4 et configure le routage. Il peut également optimiser les tables de routage générées.

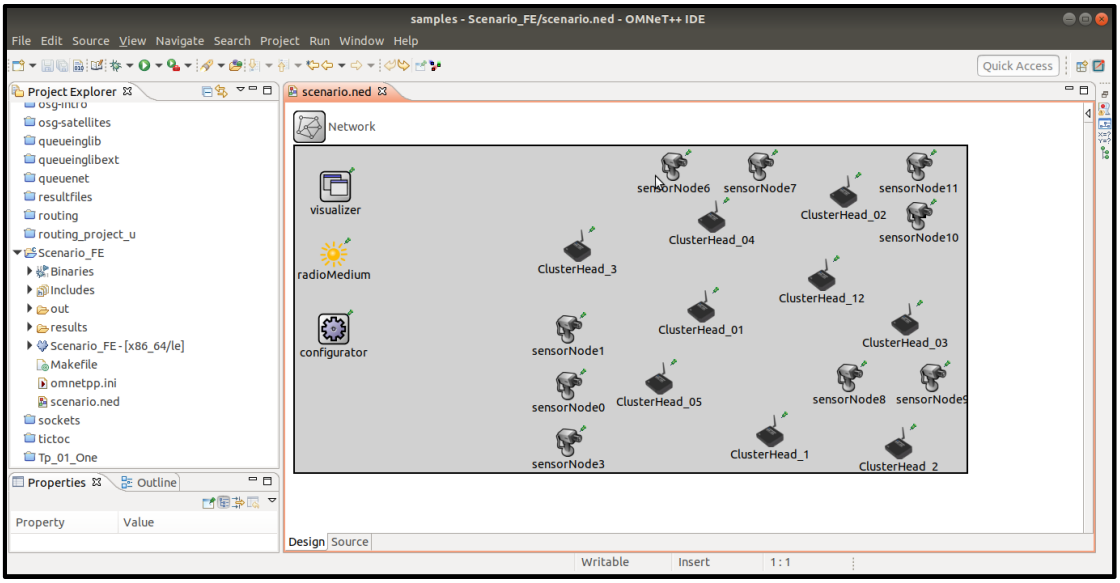


Figure 51 : Un scenario prêt.

La figure suivante montre le code source du notre réseau :

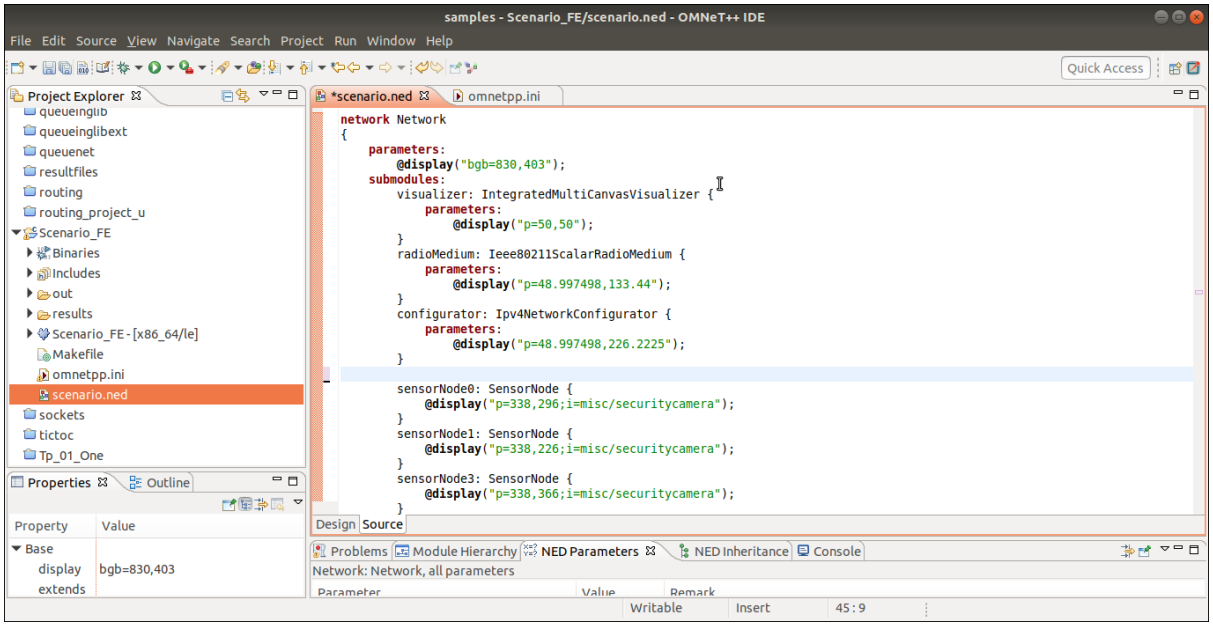


Figure 52 : Le code de notre réseau.

Une fois que nous avons préparé notre réseau et que nous avons configuré tous les modules que nous avons présentés, puis préparé notre scénario en ajoutant les derniers modules, nous devons configurer le fichier omnetini, *la figure 53* montre une partie de la configuration du fichier.

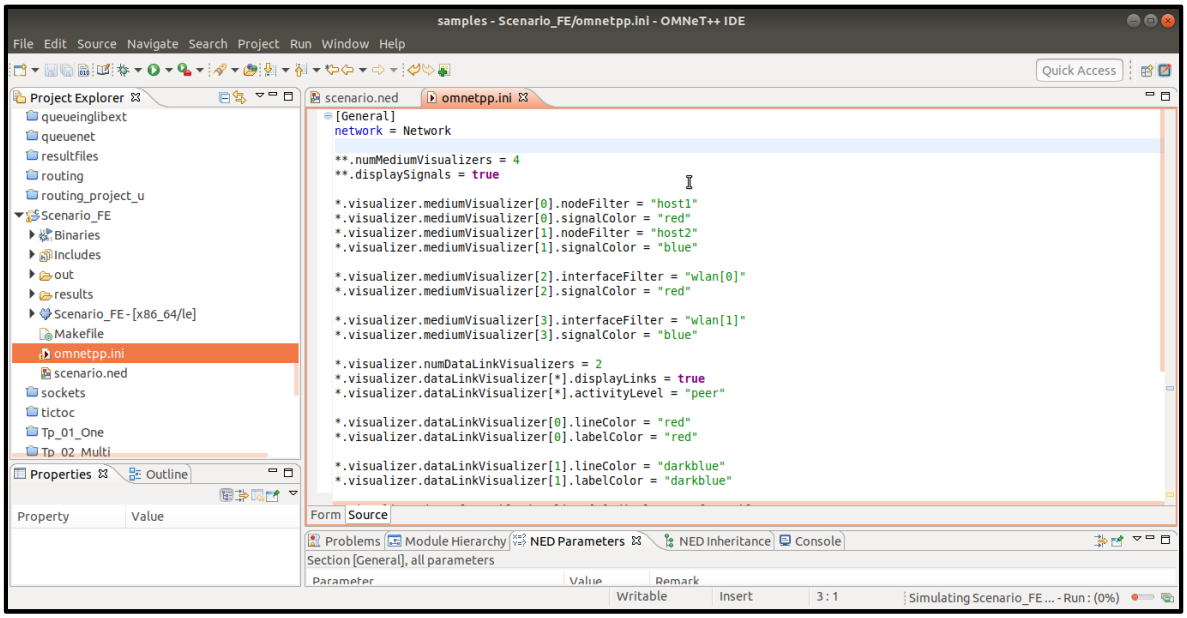


Figure 53 : Une partie de la configuration de fichier omnetini.

5.1. La préparation d'exécution du scénario

Dans cette étape, et après avoir utilisé tous les derniers modules et configurations, nous devons construire et exécuter notre scénario : *voir la figure 54 qui représente un scénario est construit mais pas encore exécuté.*

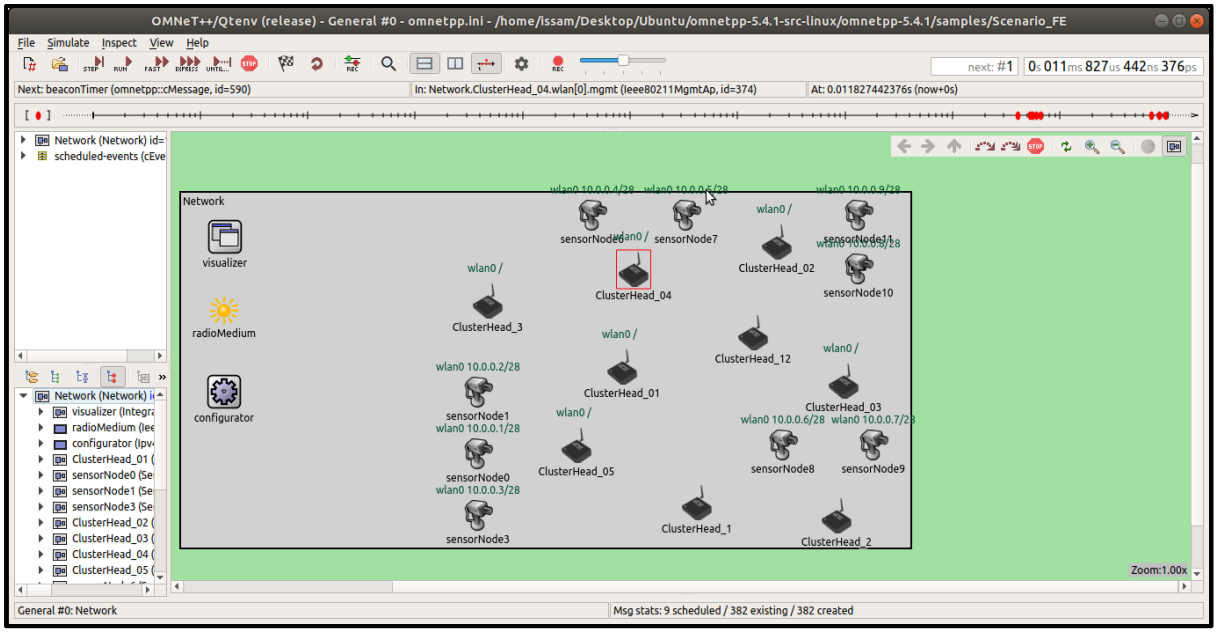


Figure 54 : Un scénario prêt avant l'exécution.

5.2. L'exécution du scénario

Le fonctionnement de la phase de distribution du trafic est réalisé par les chefs des clusters via plusieurs chemins virtuels, *et ceci est illustré dans les figures 55 et 56 :*

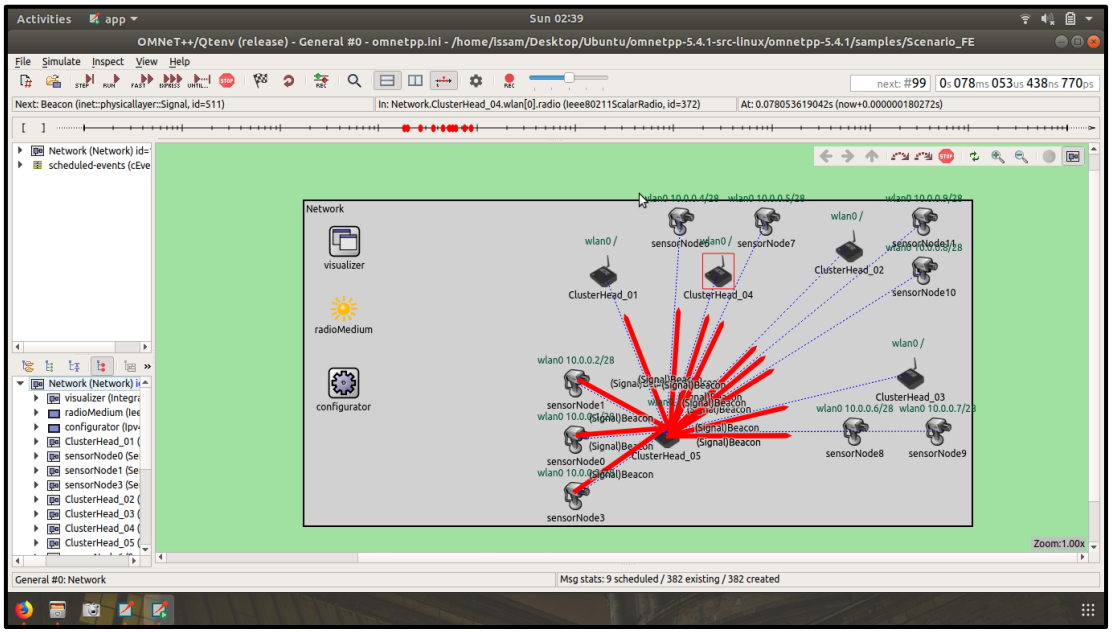


Figure 55 : Un chef de cluster distribue le trafic via plusieurs VP.

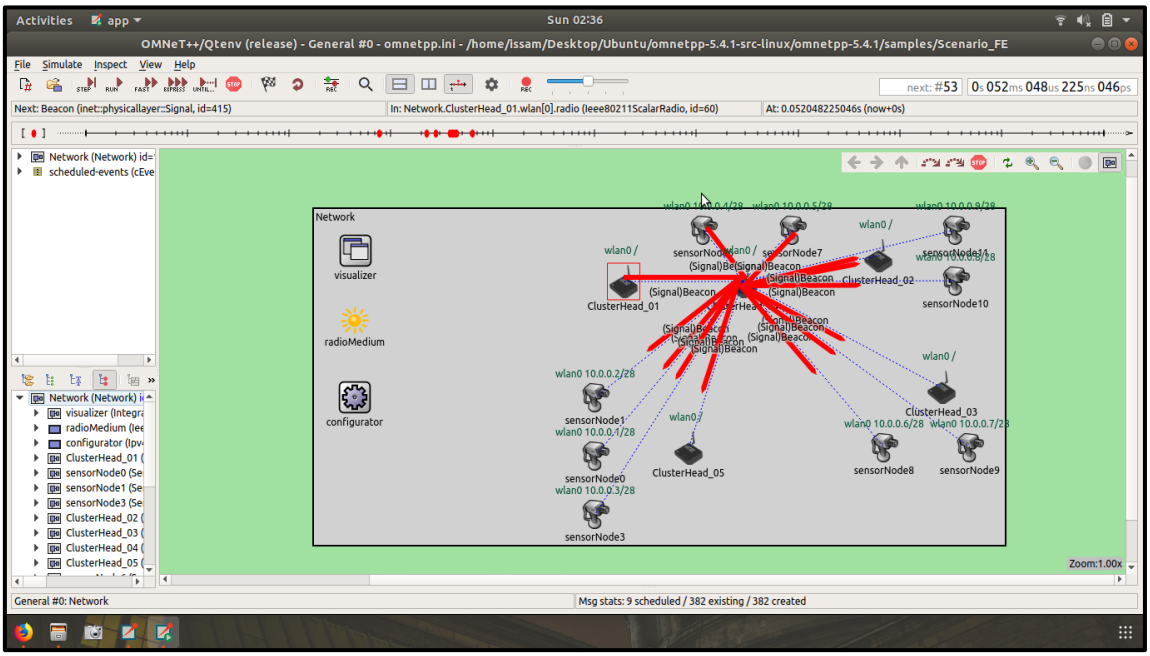


Figure 56 : Un chef de cluster distribue le trafic via plusieurs VP.

La figure 57 montre qu'il y a des chefs de cluster sans congestionnée comme ClusterHead_1, ClusterHead_2 et ClusterHead_3, dans ce cas ces nœuds ne recevoir pas du trafic.

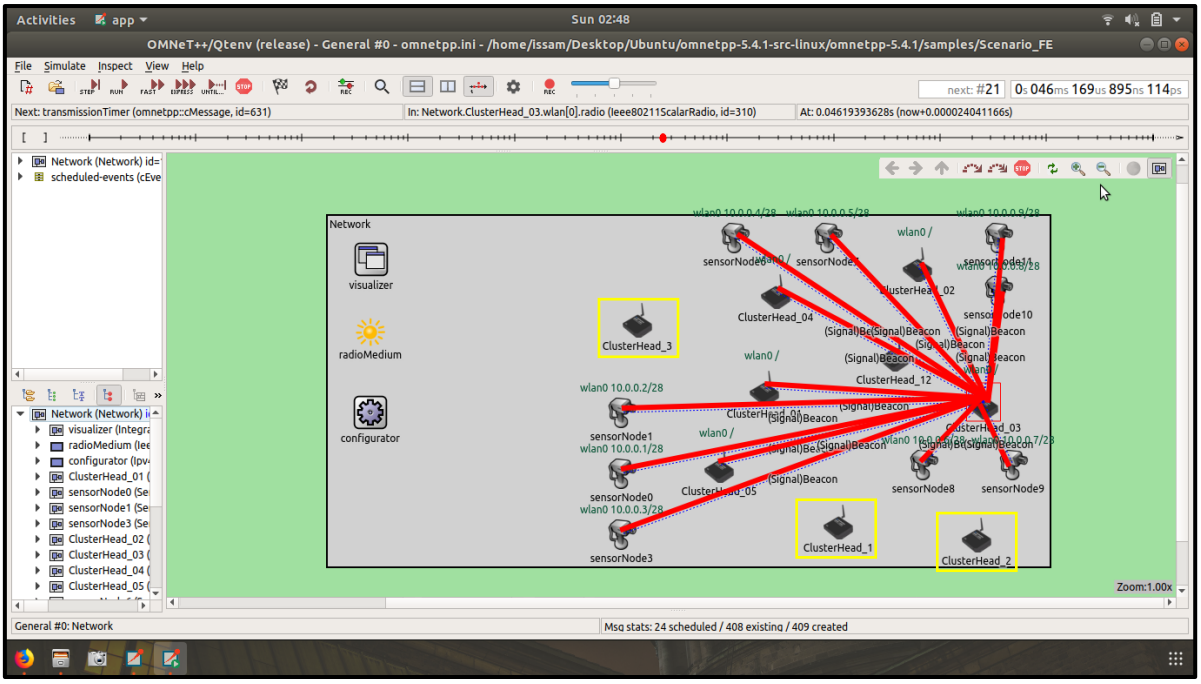


Figure 57 : Les chefs de cluster congestionnés.

Dans ce cas, le CLusterHead_03 est encombré par le trafic entrant, après que la congestion ait été réduite, il est retourné pour recevoir les données.

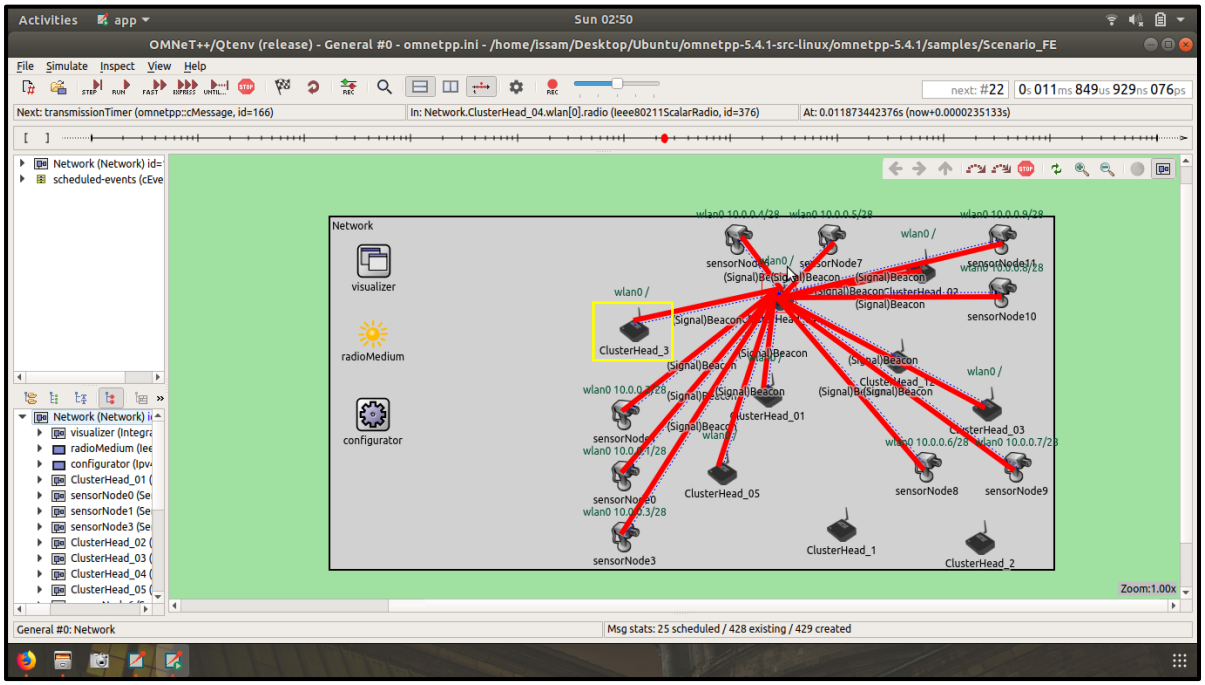


Figure 58 : Le chef de cluster 3 recevoir les données.

Conclusion

Au cours de ce chapitre, nous avons utilisé l'environnement OMNeT++ pour implémenter quelques étapes de base pour notre méthode proposée telles que la création des nœuds de capteurs sans fil (Chef de cluster et Noeud membre), et l'ajout de ces nœuds à un réseau avec une configuration pour l'échange des données, en essayant de montrer du trafic entré dans nœud chef de cluster et le distribue via plusieurs chemins virtuels. Ce travail peut toujours être développé pour couvrir toutes les étapes de notre méthode.

Conclusion générale :

La gestion de l'ingénierie du trafic est susceptible à l'avenir, de constituer un développement technologique majeur apportant des solutions à divers problèmes, tels que la congestion du trafic sur plusieurs réseaux comme le WSN.

Tout au long de notre travail, nous avons constaté que la réalisation d'un RCSF posait de gros problèmes : la congestion du trafic qui se produit lorsque les nœuds sont densément distribués ou que l'application produit un débit élevé près du puits en raison de la nature convergente du trafic en amont. En outre, la consommation d'énergie dans ces réseaux est l'un des plus grands défis. Actuellement, la plupart des recherches sur ces réseaux sont consacrées aux méthodes de conception visant à minimiser l'énergie inhérente aux communications afin de maximiser la durée de vie du réseau.

L'idée principale de notre travail concentre sur la perte et le retard de paquet, qui sont connue comme l'une des métriques les plus prometteuses pour détecter la congestion du trafic. Grâce à ces informations, nous pouvons mesurer la congestion du trafic, et sur cette base nous avons adapter le trafic en distribuant ce trafic entrant via plusieurs chemins virtuels par le chef de cluster. En outre, nous avons étudié quelques approches adaptatives de l'ingénierie du trafic, dans lesquelles il a été constaté que la distribution du trafic était très utile pour réduire la congestion du trafic dans le réseau WSN.

Nous commençons par le clustering, pour simplifier la gestion des nœuds, réduire la consommation d'énergie, augmenter la robustesse, améliorer l'agrégation des données et l'équilibrage de la charge, cela nous a donné la première raison de l'ajouter pour réduire la congestion du trafic, nous avons virtualisé nos clusters sur des réseaux de capteurs virtuels afin de réduire le besoin d'envoyer du trafic vers des destinations inutiles.

L'évaluation des performances de notre solution a été réalisée sous le simulateur OMNeT++. Les simulations des bases des réseaux de capteurs sans fil à partir de la création des nœuds de capteurs quel que soit des chefs de clusters ou des nœuds membres et puis nous créons notre scénario, ou dans lequel les chefs de clusters reçoivent un trafic énorme et le distribuent via plusieurs chemins virtuels dans des topologies de routage virtuelles.

Bibliographie

[WHPH08] Ning Wang, Kin Hon Ho, George Pavlou, And Michael Howarth, An overview of routing optimization for internet traffic engineering, 2008.
[SR15] Kavitha. S 1 BE, Vidhyalakshmi. R, A Survey on Adaptive Traffic Engineering System based on Virtual Routing Topologies, 2015.
[WHP12] Ning Wang, Kin Hon Ho, George Pavlou, AMPLE: An Adaptive Traffic Engineering System Based on Virtual Routing Topologies, 2012.
[PG13] V. Palanisamy, K. Gowri, An Adaptive MT-BGP Traffic Engineering Based on Virtual Routing Topologies, 2013.
[SSD15] Tejashree Kumar Shinde, Yevale Ramesh S,Prakash. B. Dhainje, Adaptive Traffic Engineering System using Virtual Routing Topologies, 2015.
[XCR08] D. Xu, M. Chiang, and J. Rexford, "Link-State Routing with Hop-By-Hop Forwarding can Achieve Optimal Traffic Engineering," Proc. IEEE INFOCOM, 2008.
[ACE01] D. Awduche, A. Chiu, A. Elwalid, I. Widjaja, and X. Xiao. A Framework for internet traffic engineering, 2001.
[ACE02] D. Awduche, A. Chiu, A. Elwalid, I. Widjaja, and X. Xiao. Overview and Principles of Internet Traffic Engineering, 2002.
[SLCWT01] W. Sum Lai, B. Christian, R. W. Tibbs, and S.V.D. Berghe. A Framework for Internet Traffic Engineering Measurement, 2001.
[RASH00] Gerald R. Ash Traffic Engineering & QoS Methods for IP-, ATM-, & TDM-Based Multiservice Networks, 2000.
[AWD99] D. Awduche, "MPLS and Traffic Engineering in IP Networks", IEEE Communications Magazine, Dec. 1999.
[LJB17] Xufeng Liu, Jabil, Igor Bryskin, Vishnu Pavan Beeram,Tarek Saad, Himanshu Shah, Oscar Gonzalez De Dios, YANG Data Model for Traffic Engineering (TE) Topologies, 2017.
[MR99a] D. Mitra and K.G. Ramakrishnan. A case study of multiservice, multipriority traffic engineering design for data communications, 1999.
[WLi13] X. Wei and Z. Li, "Analysis and solution of the network congestions in the local area network", 2013.
[JITA04] G. Jin and H. Tang, "Control transmission pace at IP layer to avoid packet drop, 2004.
[FeLa10] Federico Larroca, Techniques d'ingénierie de trafic dynamique pour l'internet, 2010.
[Elwalid] MATE: MPLS Adaptive Traffic Engineering, 2001.
[ACSI02] Anwar Elwalid, Cheng Jin, Steven Low, Indra Widjaja, MATE multipath adaptive traffic engineering,
[JWR04] J. W. Roberts, "Internet Traffic, QoS and Pricing," Proceedings of the IEEE, 2004.
[JWR01] T. Bonald, A. Proutiere, and J.W. Roberts, "Statistical Performance Guarantees for Streaming Flows using Expedited Forwarding", 2001.
[BR03] T. Bonald and J. W. Roberts, "Congestion at flow level and the impact of user behaviour", 2003.
[SR05] S. Oueslati and J. W. Roberts, "A new direction for quality of service: flow-aware networking", 2005.
[GVC97] P. Goyal, H. Vin, and H. Cheng, "Start-time fair queueing: a scheduling algorithm for integrated services packet switching networks", 1997.
[BFDO01] N. Benameur, S. B. Fredj, F. Delcoigne, S. Oueslati-Boulahia, and J. W. Roberts, "Integrated admission control for streaming and elastic traffic", 2001.
[FBO90] F. Bonomi, "On job assignment for a parallel system of processor sharing queues", 1990.

Bibliographie

[GKAH92] G. Koole and A. Hordijk, “On the Assignment of Customers to Parallel Queues”, 1992.
[TNS] “The Network Simulator - ns.” [Online]. Available: http://nsnam.isi.edu/nsnam/index.php/MainPage
[KOR04] A. Kortebi, S. Oueslati, and J. W. Roberts, “Cross-protect: implicit service differentiation and admission control”, 2004.
[BH84] B. Hajek, “Optimal control of two interacting service stations,”, 1984.
[BJP04] T. Bonald, M. Jonckheere, and A. Proutiere, “Insensitive load balancing,”, 2004.
[BAK05] W. Ben-Ameur and H. Kerivin, “Routing of uncertain traffic demands”, 2005.
[DAEC03] D. Applegate and E. Cohen, “Making intra-domain routing robust to changing and uncertain traffic demands: understanding fundamental tradeoffs,”, August 2003.
[DOV08] Sukrit Dasgupta, Jaudelice C. de Oliveira, J.P. Vasseur, “Dynamic traffic engineering for mixed traffic on international networks Simulation and analysis on real network and traffic scenarios”, 2008.
[EOAS02] Eric Osborne, Ajay Simha, Traffic Engineeering with MPLS, Networking Technology Series, July 2002.
[PTMR13] P. Tune, M. Roughan, “Internet Traffic Matrices: A Primer”, 2013.
[LGV82] L. G. Valiant. A scheme for fast parallel communication. SIAM Journal on Computing, 1982.
[LVJB81] L. G. Valiant and G. J. Brebner. Universal schemes for parallel communication. In ACM Symposium on Theory of Computing, 1981.
[KLS04] M. Kodialam, T. V. Lakshman, and S. Sengupta. Efficient and robust routing of highly variable traffic, November 2004.
[KLS06] M. Kodialam, T. V. Lakshman, and S. Sengupta. Maximum throughput routing of traffic in the hose model, April 2006.
[NPKWZ05] H. Nagesh, V. Poosala, V. Kumar, P. Winzer, and M. Zirngibl. Loadbalanced architecture for dynamic traffic, March 2005.
[SW06] F. B. Shepherd and P. J. Winzer. Selective randomized load balancing and mesh networks with changing demands, 2006.
[ZSMc04] R. Zhang-Shen and N. McKeown. Designing a Predictable Internet Backbone Network, November 2004.
[ZSMc05] R. Zhang-Shen and N. McKeown. Designing a predictable Internet backbone with Valiant Load-Balancing. Thirteenth International Workshop on Quality of Service (IWQoS), 2005.
[ZSNMc] Rui Zhang-Shen and Nick McKeown. Guaranteeing Quality of Service to Peering Traffic.
[SW] F. B. Shepherd and P. J. Winzer, Selective randomized load balancing and mesh networks with changing demands.
[KKDC05] S. Kandula, D. Katabi, B. Davie, and A. Charny, “Walking the tightrope: responsive yet stable traffic engineering,” in Proceedings of the 2005 conference on Applications, technologies, architectures, and protocols for computer communica- tions (SIGCOMM ’05), August 2005.
[FKF06] S. Fischer, N. Kammenhuber, and A. Feldmann, “Replex: dynamic traffic engineering based on wardrop routing policies,” in Proceedings of the 2006 ACM CoNEXT conference (CoNEXT ’06), Lisboa, Portugal, December 2006.
[XCR08] D. Xu, M. Chiang, and J. Rexford, “Link-state routing with hop-by-hop forwarding can achieve optimal traffic engineering”, 2008.
[FRV06] S. Fischer, H. Räcke, and B. Vöcking, “Fast convergence to wardrop equilibria by adaptive sampling methods”, 2006.
[DPB99] D. P. Bertsekas, Nonlinear Programming. Athena Scientific, 1999.

Bibliographie

[KKDC05] S. Kandula, D. Katabi, B. Davie, and A. Charny, “Walking the tightrope: responsive yet stable traffic engineering”, 2005.
[RVC01] E.C. Rosen, A. Viswanathanm, R. Callon, Multiprotocol label switching architecture, IETF RFC 3031, January 2001.
[WAL01] D.O. Awduche et al., RSVP-TE: Extensions to RSVP for LSP Tunnels, IETF RFC 3209, December 2001.
[JAL02] B. Jamoussi et al., Constraint-based LSP setup using LDP, IETF RFC 3212, January 2002.
[FT00] B. Fortz, M. Thorup, Internet traffic engineering by optimizing OSPF weights, 2000.
[MRKR] M.A. Rodrigues, K.G. Ramakrishnan, Optimal routing in shortest-path networks.
[SKCE04] Selin Kardelen Cerav-Erbas, Traffic Engineering in MPLS Networks with Multiple Objectives: Modeling and Optimization, 2004.
[CV98] C. Villamizar, "OSPF Optimized Multipath (OSPF-OMP)," 1998.
[KDH15] Philip Koopman, Kevin Driscoll, Brendan Hall, Selection of Cyclic Redundancy Code and Checksum Algorithms to Ensure Critical Data Integrity, 2015.
[AZB98] A.M. Zoubir, B. Boashash, The bootstrap and its applications in signal processing, IEEE Signal Processing Magazine, 1998.
[LS06] X. Lin and N. B. Shroff, “Utility Maximization for Communication Networks with Multi-path Routing,” IEEE Trans. Automatic Control, 2006. To appear.
[SHST04] H. Han, S. Shakkottai, C. V. Hollot, R. Srikant, and D. Towsley, “Overlay TCP for Multi-Path Routing and Congestion Control,” in Proc. IMA Workshop on Measurement and Modeling of the Internet, January 2004.
[GK02] R. J. Gibben and F. Kelly, “On packet marking at priority queues,” IEEE Trans. Automatic Control, vol. 47, pp. 1016–1020, December 2002.
[HMC] Jiayue He, Mung Chiang, Jennifer Rexford, DATE: Distributed Adaptive Traffic Engineering.
[WHPH08] Ning Wang, Kin Hon Ho, George Pavlou, And Michael Howarth, An overview of routing optimization for internet traffic engineering, 2008.
[GC13] Graziano, Charles. "A performance analysis of Xen and KVM hypervisors for hosting the Xen Worlds Project", 2013.
[AKA06] ADAMS, K., AND AGESEN, O. A comparison of software and hardware techniques for x86 virtualization. In ACM SIGOPS Operating Systems Review, 2006.
[ATDP05] ABELS, T., DHAWAN, P., AND CHANDRASEKARAN, B. An overview of xen virtualization, 2005.
[AM10] Ahmadi, M. R., & Maleki, Performance evaluation of server virtualization in data center applications, 2010.
[GS07] B. Goldworm, A. Skamarock, “Blade Servers and Virtualization”, Transforming Enterprise Computing while Cutting Costs, 2007.
[DLS16] Arvind Durai, Stephen Lynn, Amit Srivastava, Virtual Routing in the Cloud, Copyright© 2016 Cisco Systems, Inc.
[WIDRB13] Anjing Wang, Mohan Iyer, Rudra Dutta, George N. Rouskas, and Ilia Baldine, Network Virtualization: Technologies, Perspectives, and Frontiers, 2013.
[MSS15] Mohamed Said Seddiki, Allocation dynamique des ressources et gestion de la qualité de service dans la virtualisation des réseaux, 2015.
[SWPM09] Schaffrath, G., Werle, C., Papadimitriou, P., Feldmann, A., Bless, R., Greenhalgh, A., Wundsam, A., Kind, M., Maennel, O., and Mathy, L. (2009). Network virtualization architecture: proposal and initial prototype.
[CB09] Chowdhury, N. and Boutaba, R. Network virtualization: state of the art and research challenges. IEEE Communications Magazine, 2009.

Bibliographie

[MSS15] Mohamed Said Seddiki, Allocation dynamique des ressources et gestion de la qualité de service dans la virtualisation des réseaux, 2015.
[PL12] Pillou J and Lemainque, F, Tout sur les réseaux et Internet - 4e éd, 2012.
[RV97] Rajaravivarma, V, Virtual local area network technology and applications,1997.
[FRPRB08] D. Fedyk, Y. Rekhter, D. Papadimitriou, R. Rabbat, L. Berger, Layer 1 VPN Basic Mode, 2008.
[RR06] E. Rosen, Y. Rekhter, BGP/MPLS IP Virtual Private Networks (VPNs), 2006.
[MKCB08] N.M. Mosharaf Kabir Chowdhury and Raouf Boutaba, A Survey of Network Virtualization, 2008.
[RE] https://www.packetdesign.com/blog/a-guide-to-mpls-vpn-fundamentals/, consulté le 21 Mars 2019.
[SHW11] Han, S., & Jin, H.-W, Full virtualization based ARINC 653 partitioning, 2011.
[SML10] Jyotiprakash Sahoo, Subasish Mohapatra, and Radha Lath, Virtualization: A survey on concepts, taxonomy and associated security issues, 2010.
[TL05] Todd Lammle, CCNA™: Cisco® Certified Network Associate Study Guide 5th Edition, 2005.
[AAAY12] Abdulrahman Alkandari, Imad F.T. Alshaikhli, Mohammed Ali Yousef, An Anatomy of IGP and BGP Routing Protocols, 2012.
[ATM16] Amrah Baba Ali, Mujahid Tabassum, Kuruvilla Mathew, A Comparative Study of IGP and EGP Routing Protocols, Performance Evaluation along Load Balancing and Redundancy across Different AS, 2016.
[JRB15] Megha Jayakumar, N Ramya Shanthi Rekha, B.Bharathi, A Comparative study on RIP and OSPF protocols Analysis of RIP and OSPF protocols using GNS-3, 2015.
[GJ08] Rick Graziani, Allan Johnson, Routing Protocols and Concepts, CCNA Exploration Companion Guide, 2008.
[NSF07] Mohamed Nassar, Radu State, Olivier Festor, IBGP confederation provisioning, 2007, Page 3.
[MHN02] John Murphy, Richard Harris and Richard Nelson, Traffic Engineering Using OSPF Weights and Splitting Ratios, 2002.
[WHP08] Ning Wang, Kin-Hon Ho and George Pavlou, Adaptive Multi-topology IGP Based Traffic Engineering with Near-Optimal Network Performance, 2008.
[WX06] Hao Wang, Haiyong Xie, COPE: Traffic Engineering in Dynamic Networks, 2006.
[CCK10] Caesar, M., Casado, M., Koponen, T., Rexford, J., & Shenker, S, Dynamic Route Computation Considered Harmful, 2010.
[SAY14] N.Shanker, Shaik Tanveer Ahmed, M.Yesuratnam Traffic Engineering System Based on Adaptive Multipath Virtual Routing, 2014.
[SM02] S. Murphy, “BGP Security Vulnerabilities analysis”, IETF draft, 2002.
[MMSP16] Maheshwari Marne and, Swapna Patil, The Constraints in Wireless Sensor Network - A Review, January 2016
[MJM05] Ankit Mehta, Deepak T. J, Arpit Mehta, Compendium of Applications for Wireless Sensor Network All the three authors were summer interns at TCS Chennai in summer 2005.
[AWYE02] Ian F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks. IEEE Communications Magazine, pages 102.114, 2002.
[DCH04] D.Chen and P.K. Varshney,”QoS Support in Wireless Sensor Networks:A Survey”, Proceedings of the 2004 International Conference on Wireless Network (ICWN 2004), Las Vegas, Nevada, USA, June 21-24, 2004.
[MYO04] M.Younis, K.Akkaya et.al,”On Handling QoS traffic in Wireless Sensor Network”, Procedings of the 37th Hawaii International Conference on System Science 2004.
[RIT16] Reshma I. Tande, Leach Protocol in Wireless Sensor Network: A Survey, 2016.

Bibliographie

[WAH00] Wendi Rabiner Heinzelman, Anantha Chandrakasan and Hari Balakrishnan, Energy-efficient communication protocol for wireless microsensor networks, 2000.
[RWW04] Ramaswamy Ramaswamy, Ning Weng and Tilman Wolf, Characterizing Network Processing Delay, 2004.
[KBG16] Imran Khan, Fatna Belqasmi, Roch Glitho, Noel Crespi, Monique Morrow and Paul Polakos, Wireless Sensor Network Virtualization: A Survey, 2016.
[MN04] M. Younis and T. Nadeem. "Energy efficient MAC protocols for wireless sensor networks", Technical report, university of Mryland baltimre County, USA, 2004.
[CNF10] C. Neves Fonseca, “Multipath Routing for Wireless Mesh Networks”, (2010).
[KDBA14] M.A.Kafi, D.Djenouri, J,B Othman, A, Ouadjaout, N, Badache Congestion Detection Strategies in Wireless sensor Networks: A Comparative Study with Testbed Experiments, 2014.