Schéma DHT hiérarchique pour la tolérance aux pannes dans les réseaux P2P-SIP

Ibrahima Diané, Ibrahima Niang

CARI'10

Schéma DHT hiérarchique pour la tolérance aux pannes dans les réseaux P2P-SIP

Ibrahima DIANE

Dépt. Mathématiques et informatique informatique
Université Cheikh Anta Diop de Dakar de Dakar
BP 5005 - Dakar-Fann
SENEGAL
ibrahima.diane@ucad.edu.sn

Ibrahima NIANG

Dépt. Mathématiques et

Université Cheikh Anta Diop

BP 5005 - Dakar-Fann
SENEGAL
iniang@ucad.sn

RÉSUMÉ. Cet article met l'accent sur la tolérance aux pannes de super-nœuds dans les systèmes P2P-SIP. Ces systèmes sont caractérisés par une forte volatilité des super-nœuds. La plupart des solutions tolérant aux pannes proposées traitent des défaillances physiques et ne prennent pas en compte les défaillances temporelles qui sont aussi importantes pour des applications multimédia telle que la téléphonie. Cet article propose un mécanisme de tolérance aux pannes physiques et temporelles basé sur un réseau de recouvrement P2P à deux niveaux pour les systèmes P2P-SIP. Les résultats de simulation ont montré que notre proposition diminue considérablement la latence de localisation des nœuds ordinaires et augmente la probabilité de les retrouver.

ABSTRACT. This paper focuses on fault tolerance of super-nodes in P2P-SIP systems. These systems are characterized by high volatility of super-nodes. Most fault-tolerant proposed solutions are only for physical defects. They do not take into consideration the timing faults that are very important for multimedia applications such as telephony. This paper proposes a timing and physical fault tolerant mechanism based on P2P overlay with two levels for P2P-SIP systems. The simulation results show that our proposition reduces mostly the nodes location latency and increases the probability to find the called nodes.

MOTS-CLÉS : VoIP, P2P, SIP, P2P-SIP, DHT, super- nœuds, tolérance aux pannes.

KEYWORDS: VoIP, P2P, SIP, P2P-SIP, DHT, super-nodes, fault tolerance.

1. Introduction

Les réseaux Pair-à-Pair (P2P) sont des systèmes de très grande taille à forte disponibilité. Ils reposent sur un grand nombre de nœuds non fiables. Ce qui fait qu'ils ne peuvent atteindre une grande fiabilité que grâce à des mécanismes de réplication. Au delà du partage de fichiers, ces mécanismes permettent de mettre en œuvre des systèmes de fichiers distribués, de la multidiffusion au niveau applicatif ou encore de la voix sur un réseau IP. Ces réseaux P2P sont classifiés en non structurés, structurés et hybrides. Cependant, les réseaux P2P non structurés, basés sur les graphes aléatoires qui utilisent des inondations, ne passent pas à l'échelle à cause des surcharges [10]. Contrairement aux réseaux P2P structurés, basés sur l'utilisation de la DHT (Distributed Hash Table), qui sont plus efficaces et ont une meilleure évolutivité [5].

Récemment, des travaux ont été proposés pour intégrer le système P2P et les services de téléphonie sur IP avec l'utilisation du protocole SIP (P2P-SIP). En effet, un réseau de recouvrement P2P-SIP [1] [9], est une collection de super-nœuds organisés en pair-à-pair pour permettre la communication en temps réel entre nœuds clients, en utilisant le protocole SIP. Ces super-nœuds fournissent les fonctions du serveur d'enregistrement et de localisation aux nœuds clients. Cependant, avec la forte volatilité des nœuds, leur gestion de tolérance aux pannes devient cruciale surtout pour des services de voix sur IP.

Dans cet article, nous proposons une solution efficace de tolérance aux pannes des super-nœuds dans les systèmes P2P-SIP. Notre approche s'appuie sur un schéma DHT hiérarchique à trois niveaux. Elle améliore la gestion des pannes physiques existantes et introduit une solution pour gérer les pannes temporelles. Le reste de cet article est organisé comme suit. La section 2 présente les problématiques de recherche. La section 3 présente notre schéma DHT hiérarchique. Une validation expérimentale et théorique est proposée dans la section 4. Enfin, une conclusion est formulée dans la section 5.

2. Gestion des défaillances dans les réseaux P2P

2.1. Les réseaux P2P et P2P-SIP

2.1.1. Les réseaux P2P

Les réseaux P2P non structurés reposent sur la génération de graphes aléatoires entre les nœuds. Chaque nouveau nœud se connectant doit connaître un nœud appartenant au réseau. Ce dernier lui sert de *bootstrap* pour s'insérer dans le réseau. Les requêtes se passent ensuite sous la forme d'inondation ou de marche aléatoire. Les paramètres importants pour ce type de réseau sont les degrés entrant et sortant (nombre de connexions) de chaque nœud. En effet, ils conditionnent directement la robustesse et la connectivité du réseau.

Les réseaux P2P structurés s'appuient sur la DHT (Distributed Hash Table). Une DHT est une fonction distribuée qui, à partir d'un hash, rend une valeur. Les deux principales fonctions fournies sont *insert (hash, data)* qui insère une donnée dans la DHT et *lookup (hash)* qui retourne la donnée stockée en *hash* [5, 6]. Tout comme pour les réseaux non structurés, un nœud doit en connaître un autre pour s'inscrire dans le réseau. Ensuite, chaque nœud et chaque ressource se voient attribuer un identifiant unique (par exemple, *hash(ip)* pour un nœud, *hash(data)* pour un fichier, etc.), situé dans un espace commun. Le routage d'un nœud vers une ressource s'effectue par "bonds" successifs dans cette espace, en se rapprochant de l'identifiant de la ressource demandée. Afin de passer à l'échelle, les algorithmes de routage sont en O(log(N)) ou O(1), N étant le nombre de nœuds du réseau.

Au niveau de la DHT, les requêtes sont limitées aux ressources dont l'identifiant est connu (pas de requêtes complexes comme dans les réseaux non structurés). Il est néanmoins possible de fournir un système de recherche au dessus de la DHT.

2.1.2. Les réseaux P2P-SIP

Notons que la VoIP utilisant le protocole standard SIP, peut être considérée comme un système P2P avec un ensemble statique de super-nœuds (serveurs SIP). Dans ce cas, la localisation est basée sur le service DNS, à la place d'une clé de hachage. Cependant, l'utilisation d'une architecture P2P pure améliore considérablement la fiabilité et permet au système de s'adapter dynamiquement aux défaillances des nœuds. Il existe deux architectures pour la téléphonie P2P-SIP [1] [9] : *SIP-using-P2P* et *P2P-over-SIP*. La seule différence est que dans

P2P-over-SIP, le protocole SIP est utilisé dans la localisation et la maintenance des pairs. *SIP-using-P2P* remplace le service de localisation et de maintenance SIP par le protocole P2P. Cette architecture utilise une DHT externe. Par contre, *P2P-over-SIP* implémente le protocole P2P lui-même en utilisant des messages SIP. Cette architecture utilise principalement des messages SIP pour assurer la localisation et la maintenance. Son implémentation intègre Chord [11] comme DHT interne. Le protocole P2P-SIP pour la VoIP distribuée a été proposé pour éviter la maintenance et la configuration manuelles comme dans l'architecture SIP client/serveur. En effet, en raison de la surcharge du serveur qui constitue, par ailleurs, un point unique de défaillance, l'architecture SIP centralisée ne permet pas le passage à l'échelle.

L'architecture d'un réseau P2P-SIP correspond à celle d'un réseau à large échelle. Elle définit deux catégories de nœuds : le nœud ordinaire, qui est un client (un PC ou un téléphone IP) demandant un service; le super-nœud, qui est un nœud stockant localement une partie de la DHT. On distingue généralement deux catégories de super-nœuds : ceux qui ont des répliques en lecture seule (les pairs successeurs) et ceux ayant des répliques en lecture et écriture (les pairs responsables et les pairs d'attache).

Le réseau P2P-SIP fonctionne comme suit : un nœud ordinaire se connecte à son super-nœud d'attache et lui envoie un message de localisation concernant un autre nœud ordinaire. Le message est relayé au super-nœud responsable de la clé de destination. Ce dernier l'envoie au super-nœud d'attache du nœud ordinaire distant. Ce pair d'attache traite et envoie ainsi la réponse (contenant l'adresse du nœud distant) au nœud ordinaire local en passant par son super-nœud d'attache. Après la localisation, la communication passera directement entre les deux nœuds ordinaires. L'appel sera ainsi initié.

2.2. Structuration hiérarchique dans les systèmes P2P

La plupart des schémas DHT existants sont basés sur une architecture plate. Toutefois, des solutions de DHTs hiérarchiques proposées visent à améliorer l'évolutivité et la latence dans les réseaux P2P. Dans [6], Coral, un anneau Chord hiérarchisé à trois niveaux, est présenté. Cette solution est un système pair à pair de distribution de contenu. Dans [7], il a été proposé un réseau hiérarchique nommé HP2P, où Chord est utilisé pour la couche supérieure, alors que l'inondation est utilisée pour la couche inférieure.

En effet, La DHT Chord repose sur une structure en anneau, représentant 2^{160} valeurs. Les identifiants de nœuds et de ressources sont des hash SHA-1 (donc sur 160 bits), réalisés à partir de l'IP pour les nœuds. Chord fournit uniquement le routage d'un message vers le nœud possédant la ressource.

Chaque ressource est assignée à un nœud de la manière suivante : une ressource d'identifiant *id* est assignée au nœud possédant le premier identifiant supérieur à *id*. Étant donnée la nature volatile des réseaux Pair-à-Pair, un nœud entrant peut donc prendre le contrôle d'une ressource existante.

2.3. Tolérance aux pannes dans les réseaux P2P

La quasi-totalité des travaux concernant la tolérance aux pannes dans les systèmes P2P traitent des partages de fichiers mais pas des services de voix sur IP [2, 3, 4]. Dans [4], la méthode de tolérance aux pannes des super pairs proposée est basée sur une technique de redondance. Dans chaque groupe, les *k* super-pairs sont spécifiés pour former un super-pair virtuel. Ensuite, le super-pair virtuel sert les pairs réguliers au sein de son groupe. Chacun des *k* Super pairs doit avoir un index cohérent des fichiers partagés. [3] présente une approche hiérarchique de tolérance aux pannes similaire à [4], où les pairs sont organisés en plusieurs groupes. Dans chaque groupe, il y a un pair spécial appelé super-pair pour servir les pairs réguliers au sein du groupe. Dans cette architecture hiérarchique, si le super-pair échoue, ses pairs réguliers ne pourront plus répondre aux requêtes. Les auteurs proposent une technique de publication multiple pour faire de chaque pair régulier un pair logiquement connecté à deux ou plusieurs super-pairs dans d'autres groupes.

2.4. Problématiques de recherche sur la tolérance aux pannes dans P2P-SIP

Tout système P2P tolérant aux pannes de nœud comprend un mécanisme chargé de détecter les défaillances et de les gérer d'une manière transparente. Dans les réseaux P2P-SIP [1] [9], jusqu'alors proposés, les mécanismes de détection ne font pas de différence entre les défaillances physiques et les défaillances temporelles. Si, après un certain délai de garde, un super-nœud n'envoie pas de messages de rafraîchissement à ses successeurs ou d'accusés de réception à ses nœuds ordinaires, il sera alors considéré comme étant en panne physiquement. En plus, il n'existe pas de mécanisme de reprise automatique après la panne de super-nœuds d'attache pour un nœud ordinaire déterminé. En cas de panne de son super-nœud d'attache, un nœud ordinaire ne peut ni passer ni recevoir un appel jusqu'au prochain rafraîchissement. Une autre limite de ces solutions est qu'elles ne prennent pas en compte la défaillance temporelle des super-nœuds qui constitue un aspect très important pour les applications multimédia comme la téléphonie.

3. Schéma DHT hiérarchique pour la tolérance aux pannes dans les réseaux P2P-SIP

Dans cette section, nous présentons un nouveau mécanisme de tolérance aux pannes des super-nœuds dans les systèmes téléphoniques P2P-SIP. Comme le montre la figure 1, les nœuds ordinaires sont organisés autour des super-nœuds. Chaque nœud ordinaire est lié à un super-nœud. Par conséquent, la défaillance d'un super-nœud met temporellement hors réseau tous les nœuds ordinaires qui lui sont attachés. Notre proposition permet d'atteindre n'importe quel nœud ordinaire même en cas de panne de son super-nœud d'attache. Nous proposons également une optimisation des pannes physiques et introduisons la gestion des défaillances temporelles.

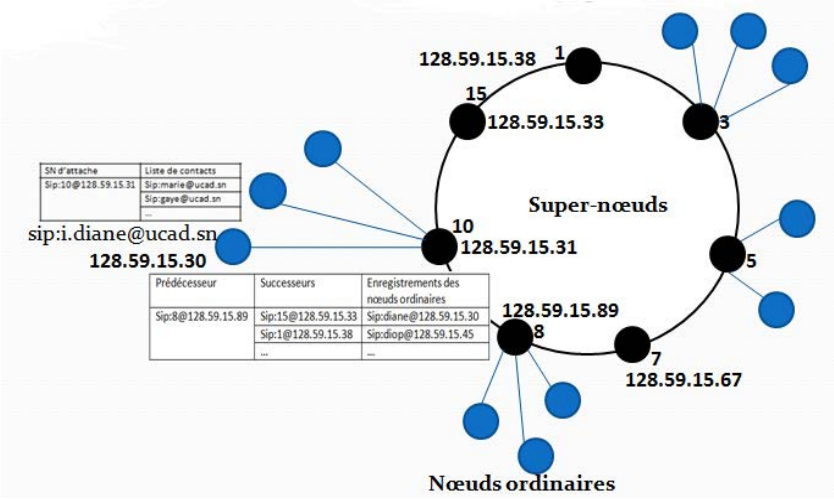


Figure 1. *Architecture du système P2P-SIP*

3.1. Architecture de la solution proposée

Notre solution est basée sur une architecture hiérarchique à trois niveaux contrairement à l'architecture de P2P-SIP classique qui repose lui sur deux niveaux : c'est-à-dire un premier niveau pour les nœuds ordinaires et un deuxième niveau pour les super-nœuds. Notre architecture utilise aussi ces deux niveaux (voir Figure 2). Nous proposons un troisième niveau pour des super-nœuds complexes qui participent au routage des messages de localisation en cas de défaillances des super-nœuds. Les super-nœuds complexes sont

sélectionnés parmi les super-nœuds et le choix est basé sur les paramètres suivants : la durée de vie du nœud dans le réseau, la bande passante, la vitesse du CPU, la taille de la mémoire.

Cette structure à trois niveaux est dictée par les éléments suivants :

1) le problème d'accessibilité des nœuds ordinaires en cas de défaillance physique de leur super-nœud d'attache ;
2) le problème relatif à la latence de localisation des nœuds ordinaires en cas de défaillance temporelle des super-nœuds qui interviennent dans le routage ;
3) le problème relatif à la surcharge du réseau dû au nombre de messages de rafraîchissement.

L'analyse des mécanismes de tolérance aux défaillances de super-nœuds a montré que les problèmes cités dans 1) et 2) restent des cas non résolus pour les super-nœuds.

Les super-nœuds complexes sont proposés, d'une part pour gérer la tolérance aux défaillances physiques des super-nœuds d'attache, et d'autre part pour introduire la gestion de la tolérance liée aux défaillances temporelles des super-nœuds. Dans notre solution, chaque nœud ordinaire est à la fois rattaché à un super-nœud et à un super-nœud complexe pour créer une certaine redondance. Ce choix est guidé par le fait que chaque nœud ordinaire doit rafraîchir son enregistrement auprès de ses nœuds d'attache, après un certain temps. Par conséquent, le nombre de messages de rafraîchissement sera multiplié par le nombre de nœuds d'attache pour chaque nœud ordinaire. Nous utilisons Chord dans notre proposition parce qu'il comporte un service pair à pair évolutif de recherche de ressources pour les applications Internet.

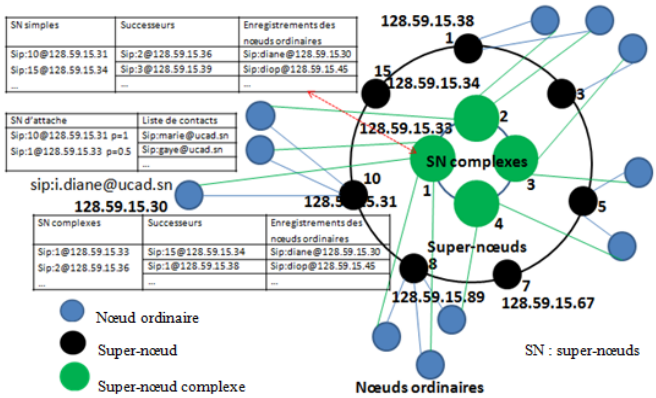


Figure 2. *Architecture de la tolérance aux pannes dans les réseaux P2P-SIP*

3.2. Gestion de la tolérance aux pannes des super-nœuds

Notre système fonctionne comme suit : au démarrage, un nœud ordinaire tente de se connecter à un super-nœud et à un super-nœud complexe. Pour cela, le nœud ordinaire cherche à découvrir un super-nœud qui lui servira de bootstrap (passerelle). Après cette découverte, le nœud ordinaire va essayer de s'enregistrer auprès de son super-nœud responsable via le bootstrap. Avant de confirmer l'enregistrement, le super-nœud responsable va répliquer l'enregistrement du nœud ordinaire sur un super-nœud complexe. Après la phase d'enregistrement, le super-nœud responsable va répliquer l'enregistrement du nœud ordinaire sur ces successeurs. Une fois dans le réseau, le nœud ordinaire peut découvrir d'autres nœuds pour d'éventuelles communications.

1) Découverte de Super-nœud : Tout d'abord, le nœud ordinaire cherche à découvrir un super-nœud. Il envoie ainsi un message multicast à l'adresse 224.0.1.75 qui se trouve être l'adresse multicast SIP.

Le message envoyé est, par exemple, le suivant :

REGISTER sip:224.0.1.75 SIP/2.0

To : <si :@128.59.15.30>

From : <sip:@128.59.15.30>

Si un super-nœud reçoit le message multicast, il répond avec un message unicast en indiquant sa propre adresse, par exemple :

SIP/2.0 302 Redirect to unicast

To : <sip:@128.59.15.30>

Contact : <sip:128.59.15.67> *// adresse du super-nœud*

Si le nœud ordinaire reçoit plusieurs réponses, il choisit l'adresse du super-nœud qui a répondu le premier. Ce dernier peut être considéré comme étant le super-nœud le plus proche.

2) Procédure d'enregistrement : Apres avoir découvert un super-nœud, le nœud ordinaire cherche à s'enregistrer auprès du super-nœud responsable de sa clé. Pour cela, le nœud envoie son enregistrement au super-nœud découvert qui va, à son tour, l'envoyer au super-nœud responsable. Ainsi, le nœud ordinaire sera lié à son super-nœud responsable (voir figure 3).

(1), (2) et (3) représentent les messages échangés.

(1) Envoi de l'enregistrement du nœud ordinaire au 1er super-nœud découvert

REGISTER sip:128.59.15.67 SIP/2.0 //adresse du 1er super-nœud

To : <sip:i.diane@ucad.sn> // adresse du nœud ordinaire

From : <sip:i.diane@128.59.15.30>

(2) Le 1er super-nœud découvert envoie, à son tour, l'enregistrement au super-nœud responsable.

REGISTER sip:128.59.15.31 SIP/2.0 //adresse du super-nœud responsable

To : <sip:i.diane@ucad.sn>

From : <sip:i.diane@128.59.15.30>

(3) La réponse du super-nœud responsable vers le nœud ordinaire. Cette réponse contient également l'adresse du super-nœud complexe qui sera utilisé en cas de défaillance du super-nœud responsable

SIP/2.0 200 OK // ACK

To : <sip:i.diane@128.59.15.30>

Contact : <sip:10@128.59.15.31>;

Contact : <sip:1@128.59.15.33>; p

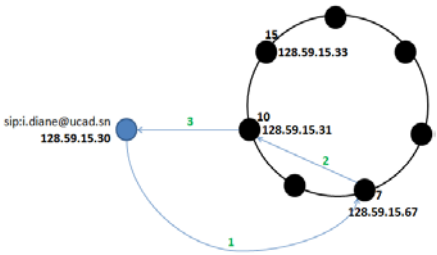


Figure 3. *Connexion du nœud ordinaire à son super-nœud*

En fait, avant d'accuser réception, le super-nœud responsable va répliquer l'enregistrement sur un super-nœud complexe en fonction de la clé d'enregistrement. La réplication utilisée à cet effet est active.

(1) et (2) représentent les messages échangés.

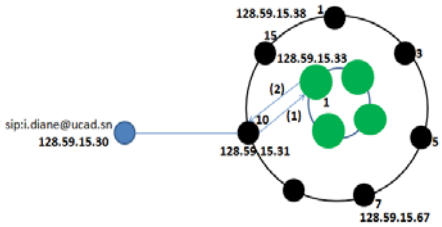
(1)

REGISTER sip:128.59.15.33 SIP/2.0

To : <sip:i.diane@ucad.sn>

From : <sip:i.diane@128.59.15.30>

Contact: <sip:10@128.59.15.31>; p=1



(2)

SIP/2.0 200 OK // ACK

To : <sip:i.diane@128.59.15.30>

Contact: <sip:10@128.59.15.31>; p=1

Contact: <sip:1@128.59.15.33>; p=0.5

Figure 4. *Connexion du nœud ordinaire à son super-nœud complexe*

Après ces étapes, le super-nœud responsable de la clé va répliquer l'enregistrement sur ses ***m*** successeurs dans le but de tolérer les défaillances physiques ; ***m*** étant par ailleurs la taille (en bits) des clés dans le réseau considéré. La réplication utilisée à cet effet est semi-active.

3) Localisation d'un nœud ordinaire : Pour localiser un nœud ordinaire distant, le nœud ordinaire local envoie un message de localisation à son super-nœud d'attache qui se trouve être son super-nœud responsable. Le message est relayé au super-nœud responsable de la clé de destination. Ce dernier traite le message et envoie ainsi la réponse (contenant l'adresse du nœud ordinaire distant) au nœud ordinaire local en passant par son super-nœud d'attache. Après la localisation, la communication passe directement entre les deux nœuds ordinaires (voir figure 5).

(1), (2), (3) et (4) représentent les messages échangés.

(1)

INVITE sip:128.59.15.31 SIP/2.0 // adresse du super-nœud responsable

To : <sip:marie@ucad.sn> // adresse du nœud ordinaire distant

From: <sip:i.diane@128.59.15.30> // adresse du nœud ordinaire

(2)

INVITE sip:128.59.15.38 SIP/2.0 // adresse du super-nœud responsable distant

To : <sip:marie@ucad.sn>

From: <sip:i.diane@128.59.15.30>

(3)

SIP/2.0 200 OK // ACK

To : <sip:i.diane@128.59.15.3

Contact: <sip:marie@128.59.1

(4)

SIP/2.0 200 OK // ACK

To : <sip:i.diane@128.59.15.3

Contact : <sip:marie@128.59.15.50>

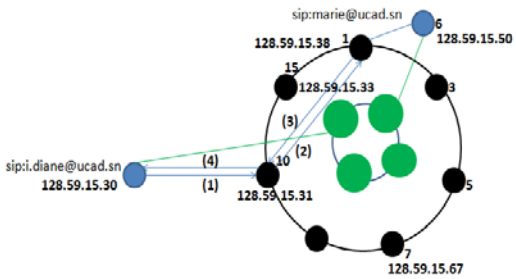


Figure 5. *Localisation d'un nœud ordinaire*

3.3. Gestion de la tolérance aux pannes des super-nœuds

Cette section présente les mécanismes que nous utilisons pour mettre en œuvre la gestion des défaillances physiques et temporelles de super-nœuds dans notre système P2P-SIP.

3.3.1. Gestion des pannes physiques

a) Détection : Toute technique de gestion de pannes comprend un mécanisme chargé de les détecter. Nous utilisons, comme dans l'architecture P2P-SIP classique, l'approche basée sur un anneau logique pour mettre en œuvre la détection des pannes physiques. En pratique, les défaillances physiques sont détectées en utilisant les messages de rafraîchissement. Ainsi, un nœud ordinaire détecte la panne de son super-nœud d'attache s'il ne reçoit pas de réponse à son rafraîchissement. Dans ce cas, le nœud ordinaire reprend à nouveau la procédure de découverte de super-nœud. Cela pose des problèmes aux applications VoIP où le délai de localisation doit être minimisé.

b) Recouvrement : Trois cas de figure sont considérés : i) Si le super-nœud défaillant est le nœud responsable de la clé du nœud ordinaire local, alors le système fait recourt à un super-nœud complexe. Le nœud ordinaire envoie à nouveau son message à son super-nœud complexe. Ce dernier envoie le message au super-nœud complexe du nœud ordinaire distant qui va traiter le message et renvoyer les informations de localisation du nœud ordinaire recherché. ii) Si le super-nœud défaillant est un successeur du nœud responsable de la clé du nœud ordinaire local, alors il sera ignoré au profit de

son successeur immédiat. iii) Si le super-nœud défaillant est le nœud responsable de la clé du nœud ordinaire distant, alors son successeur immédiat se chargera de traiter le message et d'envoyer les informations de localisation du nœud ordinaire.

En résumé, les super-nœuds complexes n'interviennent que dans la gestion des pannes de super-nœuds locaux.

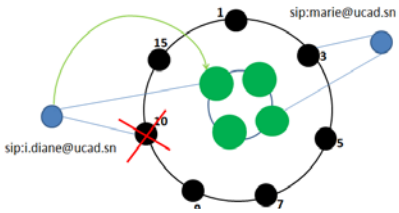


Figure 6. *Gestion de la défaillance physique du super-nœud responsable*

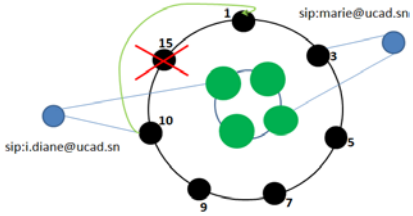


Figure 7. *Gestion de la défaillance physique d'un successeur du super-nœud*

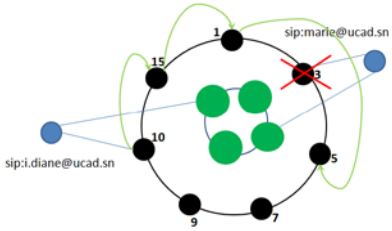


Figure 8. *Gestion de la défaillance physique du super-nœud responsable distant*

3.3.2. Gestion des pannes temporelles

a) Détection : A la différence du mécanisme utilisé dans la gestion des pannes physiques, nous utilisons ici la technique de messages "ping/pong" pour détecter les défaillances temporelles. Pour cela, de manière périodique, un nœud envoie un message "ping" à un autre. Cette technique permet une détection plus ciblée car chaque message "ping" réclame explicitement un message "pong".

b) Recouvrement : La principale technique pour atteindre cet objectif est de répliquer les enregistrements. Nous considérons aussi trois scénarios pour la gestion des pannes temporelles: i) Si le super-nœud défaillant est le responsable

de la clé du nœud ordinaire, alors le nœud ordinaire annule le message envoyé au super-nœud défaillant et renvoie le même message à nouveau à son super-nœud complexe. Ce dernier va traiter le message, c'est-à-dire, envoyer le message au super-nœud complexe du nœud ordinaire distant. ii) Si le super-nœud défaillant est un successeur du super-nœud responsable de la clé du nœud ordinaire, alors le message est envoyé à un super-nœud complexe connu par le super-nœud responsable. Ce dernier envoie le message au super-nœud complexe du nœud ordinaire distant. iii) Si le super-nœud défaillant est le responsable de la clé du nœud ordinaire distant, alors le message est envoyé à un super-nœud complexe connu par le prédécesseur du super-nœud défaillant. Ce super-nœud complexe envoie le message au super-nœud complexe du nœud ordinaire distant.

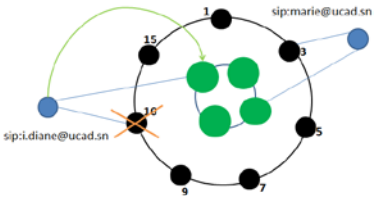


Figure 9. *Gestion de la défaillance temporelle du super-nœud responsable*

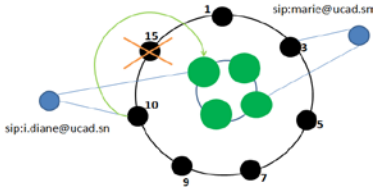


Figure 10. *Gestion de la défaillance temporelle d'un successeur du super-nœud*

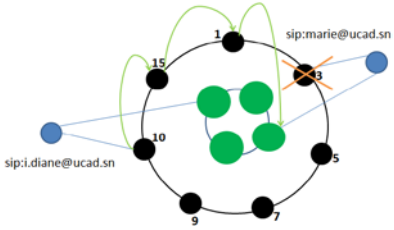


Figure 11. *Gestion de la défaillance temporelle du super-nœud responsable distant*

A la différence des pannes physiques, dans la gestion des pannes temporelles, nous utilisons toujours les super-nœuds complexes.

Lorsque le super nœud défaillant est un successeur du nœud responsable de la clé du nœud ordinaire local, la procédure de recouvrement n'est pas la même selon qu'il s'agit d'une panne physique ou d'une panne temporelle. Ceci s'explique par le fait que nous évitons que le successeur immédiat du nœud

défaillant met à jour sa table, considérant ainsi que son prédécesseur est physiquement défaillant dans le cas d'une panne temporelle.

En résumé, contrairement au système P2P-SIP classique, notre proposition prend en charge les défaillances temporelles. Nous utilisons des messages "ping/pong" pour détecter ces défaillances. Si un nœud détecte la défaillance temporelle d'un super-nœud, alors il l'ignore au profit d'un super-nœud complexe. Ce procédé permet ainsi de réduire considérablement les délais de localisation.

4. Validation expérimentale et théorique

Dans cette validation expérimentale, nous avons utilisé le logiciel de simulation de réseau pair-à-pair appelé OverSim [8]. Nous avons fixé le pourcentage de pannes à 70%, varié le nombre de super-nœuds de 100 à 2000 et mesuré à chaque fois la latence de localisation et la probabilité de localiser un nœud ordinaire.

Les expériences menées ont pour objectif :

a. de montrer l'impact des défaillances sur la latence de localisation ;

b. de montrer l'impact des défaillances sur le ratio de localisation (c.-à-d. la probabilité de localiser un nœud ordinaire) ;

c. de montrer les avantages et limites de notre solution, par rapport à la solution existante.

4.1. Notre solution Vs. P2P-SIP Classique

Dans cette étude, nous comparaisons notre proposition et le système P2P-SIP classique par rapport à la latence et à la probabilité de localiser un nœud ordinaire.

a) Latence de localisation : Les résultats montrent qu'il ya, quelque soit le type de panne considéré, une nette différence entre le système P2P-SIP classique et notre proposition vis-à-vis de la latence de localisation des nœuds ordinaires. Nous remarquons aussi que le type de panne n'influe pas sur la latence dans le système P2P-SIP classique. Ceci s'explique par le fait que toute panne détectée était traitée comme une panne physique. Contrairement au système classique, notre proposition est sensible au type de défaillance avec l'utilisation de super-nœuds complexes qui optimisent le temps de recouvrement.

b) Ratio de localisation : Cette comparaison est faite par rapport à la probabilité de trouver un nœud ordinaire. Nous remarquons que notre solution permet de mieux localiser un nœud ordinaire lorsque des pannes de super-nœuds surviennent. En effet, de 100 à 2000 nœuds et à 70% de pannes de super-nœuds, la probabilité de localiser un nœud ordinaire passe :

- **Pannes physiques** : de 0,789 à 0,597 pour notre proposition et de 0,536 à 0,327 pour le système P2P-SIP classique.
- **Pannes temporelles** : de 0,913 à 0,709 pour notre proposition et de 0,540 à 0,342 pour le système P2P-SIP classique.

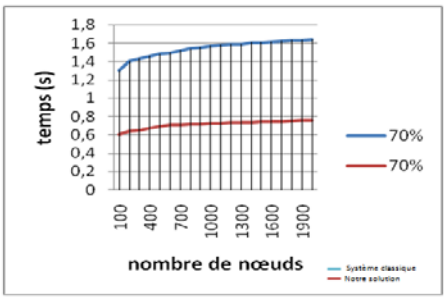


Figure 12.a *Latence pour 70% de pannes physiques*

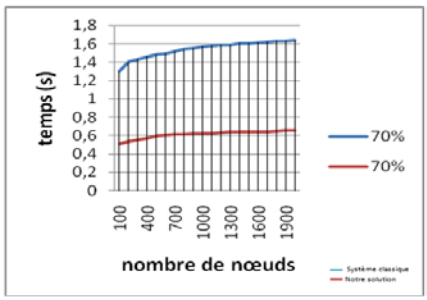


Figure 12.b *Latence pour 70% de pannes temporelles*

Ces résultats montrent la fiabilité de notre solution par rapport au système classique. La variation des résultats de notre proposition en fonction du type de panne est due au fait qu'avec les défaillances temporelles, les messages de localisation sont toujours envoyés aux super-nœuds complexes. Ce qui n'est toujours pas le cas avec les pannes physiques où les messages peuvent être supprimés.

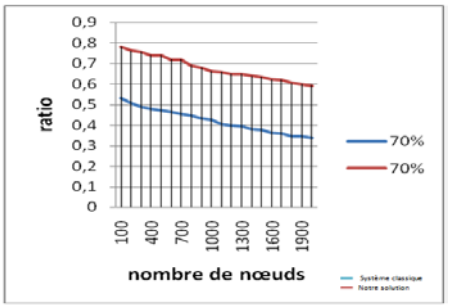


Figure 13.a *Ratio pour 70% de pannes physiques*

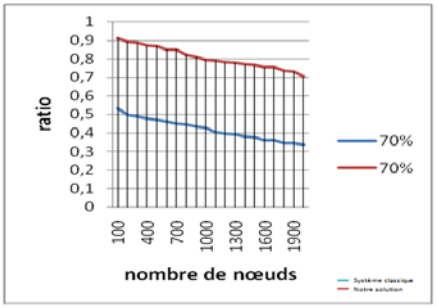


Figure 13.b *Ratio pour 70% de pannes temporelles*

4.2. Surcharge du réseau

Cette sous section est une comparaison de notre proposition et du système P2P-SIP classique par rapport à la surcharge du réseau. Nous considérons un réseau avec ***n*** nœuds ordinaires, ***n'*** super-nœuds et ***m*** le nombre de répliques des enregistrements.

a) Avec P2P-SIP classique

- Chaque nœud ordinaire doit rafraîchir son enregistrement : ***n*** messages;
- Chaque super-nœud doit rafraîchir ses répliques sur ses ***m*** successeurs : ***n*** x ***m*** messages;

En résumé, nous avons, au pire des cas, ***n*** x ***m*** messages de rafraîchissement dans le réseau. Ces messages sont utilisés pour rafraîchir les enregistrements d'utilisateurs et pour détecter les pannes physiques.

b) Avec notre proposition

- Chaque nœud ordinaire doit rafraîchir son enregistrement : ***n*** messages;
- Chaque nœud ordinaire doit envoyer un message "ping/pong" à son super-nœud : ***n*** messages;
- Chaque super-nœud doit rafraîchir ses répliques sur ses ***m*** successeurs : ***n*** x ***m*** messages;
- Chaque super-nœud doit rafraîchir les enregistrements sur les super-nœuds complexes : ***n*** messages;
- Chaque super-nœud doit envoyer un message "ping/pong" à ses ***m*** successeurs : ***n'*** x ***m*** messages;

En résumé, nous avons, au pire des cas, ***n*** x ***m*** messages de rafraîchissement et (***n*** + ***n'*** x ***m***) messages "ping/pong" dans le réseau. Ces messages "ping/pong" sont utilisés pour détecter les pannes temporelles.

	P2P-SIP classique	**Notre proposition**
Nombre de messages de rafraîchissement	***n*** x ***m***	***n*** x ***m***
Nombre de messages "ping/pong"	**0**	***n*** + ***n'*** x ***m***

Figure 7. *Surcharge du réseau : P2P-SIP classique vs notre proposition*

5. Conclusion

Dans cet article, nous avons proposé une approche hiérarchique pour la gestion de la tolérance aux pannes dans les réseaux P2P-SIP. Cette approche combine la gestion des pannes physiques et temporelles. Elle est basée sur l'architecture P2P-SIP à trois niveaux qui correspondent aux trois types de nœuds (nœud ordinaire, super-nœud et super-nœud complexe). Notre proposition permet d'améliorer considérablement les performances de la téléphonie P2P-SIP. Toutefois, il est important de noter que notre approche est plus coûteuse en termes de nombre de messages. En plus des messages de rafraîchissement, nous utilisons des messages «ping / pong» pour détecter les pannes temporelles. Cependant, notre approche est meilleure vis à vis de la stabilité, de l'évolutivité et de l'efficacité du système par rapport aux autres réseaux.

6. Bibliographie

[1] Bryan, D., B. Lowekamp, and C. Jennings "*SOSIMPLE: A Serverless, Standard-based, P2P SIP Communication System*," International Workshop on Advanced Architectures and Algorithms for Internet Delivery and Applications, June 2005.

[2] Laban Mwansa, Jan Janeček,, " *Ensuring fault-tolerance in generic network location service*", Procedings on 22nd European conference on Modelling and simulation, 2008.

[3] Jenn-Wei Lin, Ming-Feng Yang, Jichiang Tsai, "*Fault Tolerance for Super-peers of P2P Systems*", Proceedings of the 13th Pacific Rim International Symposium on Dependable Computing, 2008.

[4] B. Yang and H. Garcia-Molina, "*Designing a Super-Peer Network*", Proc. *19th Int'l Conf. Data Eng.*, Mar. 2003. pp. 49-62.

[5] S. Ratnasamy, P. Francis, M. Handley, R. Karp, and S. Shenker, "*A scalable content-addressable network*", In Proc. ACM SIGCOMM, August 2001.

[6] Freedman, M., Mazieres, D., "*Sloppy Hashing and Self-Organising Clusters*", 2nd International Workshop on Peer-to-Peer Systems, Berkley, USA, February 2003.

[7] Peng, Z., Duan, Z., Qi, J., Cao, Y., Lv, E., "*HP2P: A Hybrid Hierarchical P2P Network*", 1st International Conference on the Digital Society (ICDS), Guadeloupe, French Caribbean, January 2007.

[8] Ingmar Baumgart, Bernhard Heep, Stephan Krause, "*OverSim: A Flexible Overlay Network Simulation Framework*", IEEE Global Internet Symposium, 2007.

[9] Singh, K., and H. Schulzrinne, "*Peer-to-Peer Internet Technology Using SIP*," Columbia University Technical Report CUCS-044-04, New York, October 2004.

[10] G.X. Yue, R.F. Li, and Z.D. Zhou, "*A P2P network model with multi-layer architecture based on region*", Journal of Software, 2005,16(6):1140.1150. DOI: 10.1360/jos161140, 2005.

[11] Robert Morris, M. Frans Kaashoek, David Karger, Hari Balakrishnan, Ion Stoica, David Liben-Nowell, Frank Dabek, "*Chord : A scalable peer-to-peer lookup protocol for internet applications*", Networking, IEEE/ACM, Feb 2003.