Autoconfiguration and Security Schemes for OLSR Protocol for Mobile Ad Hoc Networks

Soutenance de Thèse de Doctorat
Saadi BOUDJIT

25 Septembre 2006

INRIA

UNIVERSITÉ PARIS-SUD 11

SB

Plan

SB

Plan

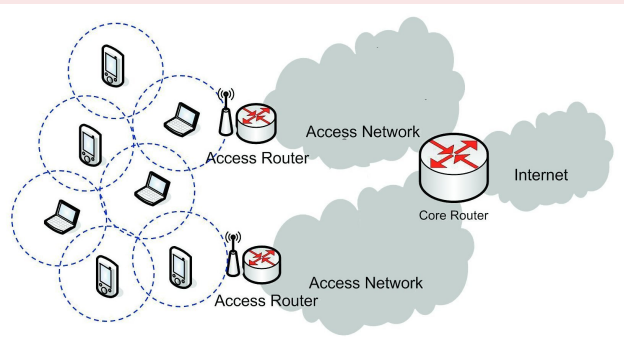
Explosion des réseaux sans fils

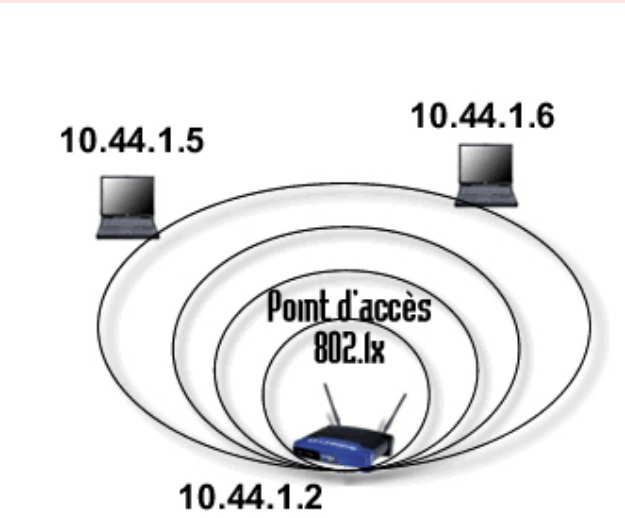
- Grands progrès dans le domaine de la radio:
  1. Composants permettant de transmettre à haut débit sur plusieurs dizaines de mètres (WLAN) ou moyen débit sur des distances de l'ordre du kilomètre (réseau cellulaire).
- Emergence de normes très répondues:
  1. GSM, DECT
  2. IEEE 802.11 (WIFI)
  3. Bluetooth

Les réseaux MANETs

Aperçu

- Une généralisation des architectures de réseaux cellulaires (GSM) ou à point d'accès IEEE 802.11.





Les réseaux MANETs

Applications

Problèmes techniques

Problèmes dans les réseaux ad hoc

Les réseaux ad hoc:

- Posent de nouveaux problèmes
- Modifient le contenu technique des problèmes déjà existants
- Apportent de nouvelles hypothèses

Problèmes techniques

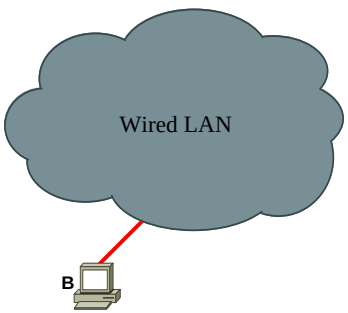
Problèmes dans les réseaux ad hoc

- Routage: AODV - DSR - OLSR - TBRPF (premier problème attaqué dans le domaine);
  - particularité: faible bande passante et mobilité.
- QoS: problème des interférences
- Sécurité: intégrité du réseau, nœuds compromis
- Economie d'énergie (n'a pas d'équivalent dans les réseaux filaires)
- Autoconfiguration: détection d'adresses dupliquées

Autoconfiguration

Autoconfiguration dans les réseaux filaires

Un nœud *B* arrive dans le réseau et demande une adresse IP



Le nœud **B** se voit attribuer une adresse IP manuellement ou via un serveur DHCP.
Il gardera cette adresse tant qu'il est connecté au même réseau.

Autoconfiguration

Autoconfiguration dans les réseaux ad hoc

Plus compliquée que l'autoconfiguration dans les réseaux filaires:

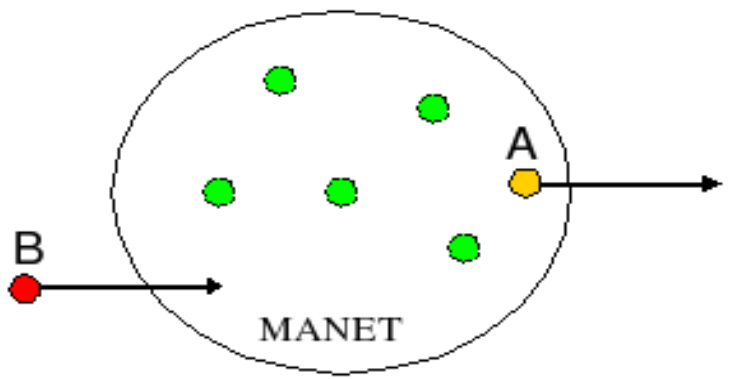
- Instabilité du réseau;
- Ouverture des réseaux MANETs;
- Absence d'une administration centrale dans un réseau MANET.

Pour illustrer cette difficulté, examinons les scénarios suivants:

Autoconfiguration

Scénario 1: un nœud rejoint le réseau et le quitte une fois

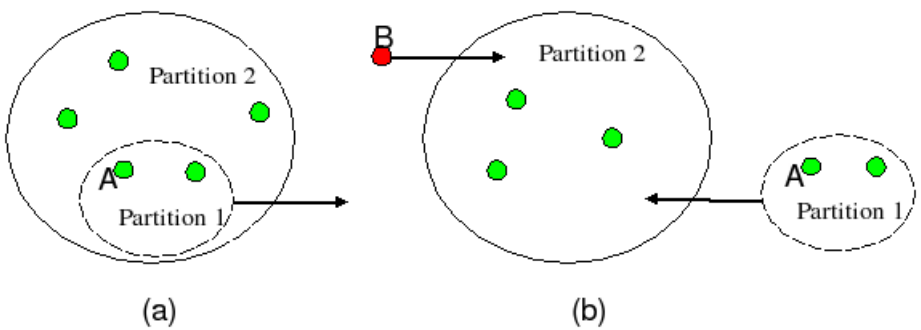
- Une adresse libre est allouée au nœud B à son arrivée et est libérée à son départ.



Autoconfiguration

Scénario 2: partitionnement et fusion de réseaux

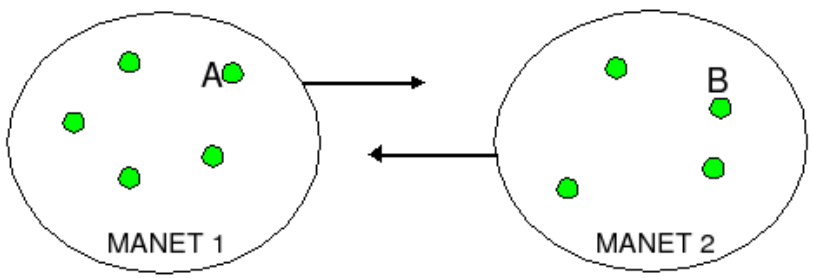
- Partitionnement du réseau en deux ou plusieurs partitions;
- Quand ces deux partitions se rapprochent de nouveau l'une de l'autre, elles fusionnent pour former un seul réseau $\Rightarrow$ possibilité de conflits d'adresses.



Autoconfiguration

Scénario 3: fusion de deux réseaux indépendants

- Dans ce cas il peut y avoir des duplications d'adresses
  $\Rightarrow$ des nœuds (ou tous les nœuds) d'un des deux réseaux peuvent devoir changer leurs adresses.



Autoconfiguration

Quelques solutions connues ...

Classifiées en trois catègories:

1. Mécanismes sans détection de conflits:
   - DCDP (Misra et al);
   - Prophet address allocation (Zhou et al).
2. Mécanismes best effort: DDHCP (Nesargi et al);
3. Mécanismes avec détection de conflits:
   ADAD (Perkins et al) - PDAD (PACMAN: Kilian Weniger).

Mes contributions

1. Conception d'une solution entièrement IPv6 pour OLSR;
2. Conception d'un protocole d'autoconfiguration pour OLSR;
   - optimisé pour OLSR
   - prouvé correct en cas de conflits simples ou multiples
   - fonctionne dans le cas d'un réseau mono-interface ou multi-interfaces
   - évaluation de performances de ce mécanisme
3. Conception d'un protocole de création de clé de groupe symetrique (autoconfiguration d'une clé) pour un réseau ad hoc;

Plan

Adressage IPv6

Types d'adresses IPv6

1. Type unicast: interface unique
2. Type multicast: groupe d'interfaces
3. Type anycast: groupe d'interfaces

Remarque

Pas de type broadcast en IPv6.

Adressage IPv6

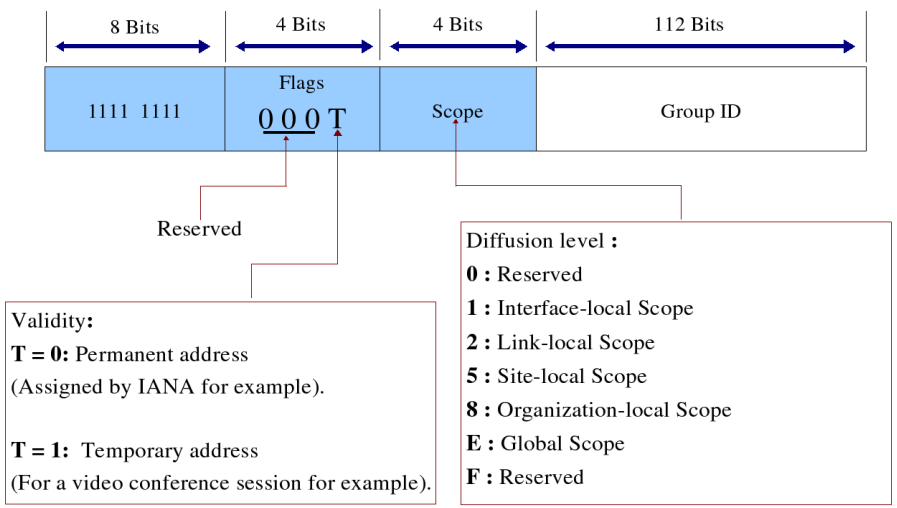
Principaux types d'adresses unicast

1. Adresse *lien-local* (*link-local* address)
   - Adresse non routable;
   - Préfixe FE80::/64 + 64 bits de l'identifiant de l'interface.
2. Adresse *site-local* (*site-local* address)
   - Adresse routable sur un site uniquement;
   - Préfixe FEC0::/48 + un *subnet-ID* de 16 bits + 64 bits de l'identifiant de l'interface.
3. Adresse unicast globale
   - Adresse routable sur Internet;
   - Caracterisée par le préfixe 2000::/3.

Adressage IPv6

Adresses multicast

- Caracterisées par le préfixe FFOO::/8



Nouvelles fonctionnalités IPv6

Découverte des voisins

Le protocole NDP(*Neighbor Discovery Protocol*) est utilisé pour:

- La résolution d'adresses sur le lien;
- La découverte des routeurs présents sur le lien;
- La DAD: Détection d'Adresses Dupliquées sur le lien ...

Nouvelles fonctionnalités IPv6

Découverte des voisins

Pour se faire, NDP utilise les messages suivants:

1. NS (*Neighbor Sollicitation*): sollicitation des voisins;
2. NA (*Neighbor Advertisement*): annonce d'un voisin;
3. RS (*Router Sollicitation*): sollicitation des routeurs;
4. RA (*Router Advertisement*): annonce d'un routeur.

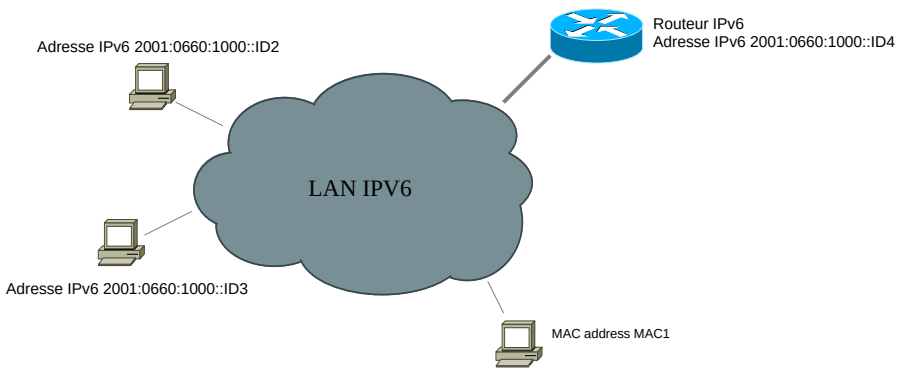
Nouvelles fonctionnalités IPv6

Configuration automatique sans état: Stateless Address Autoconfiguration

1. Basée sur le protocole NDP(Neighbor Discovery Protocol) pour la découverte des voisins;
2. Informations pour l'autoconfiguration d'une machine fournies par un routeur sur le lien.

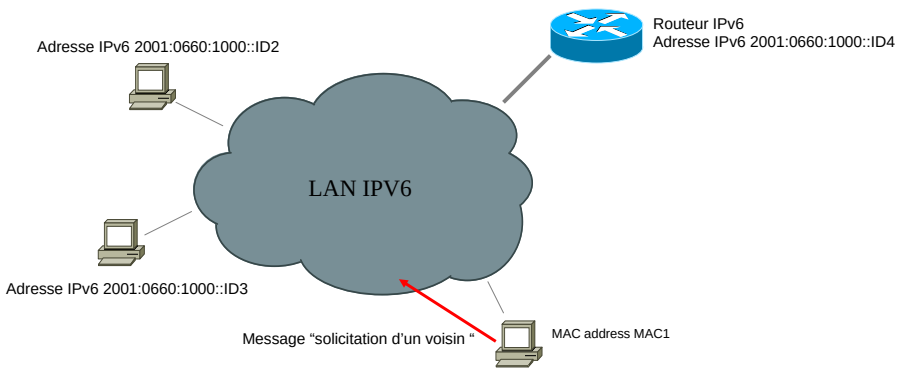
Nouvelles fonctionnalités IPv6

SAA: Stateless Address Autoconfiguration



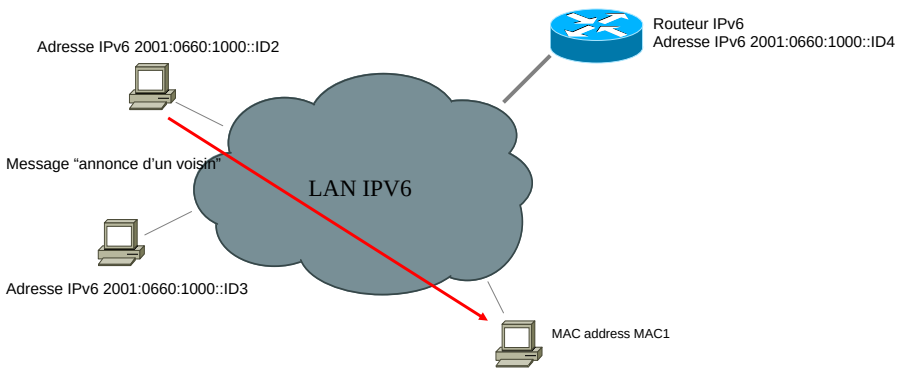
Nouvelles fonctionnalités IPv6

SAA: Stateless Address Autoconfiguration



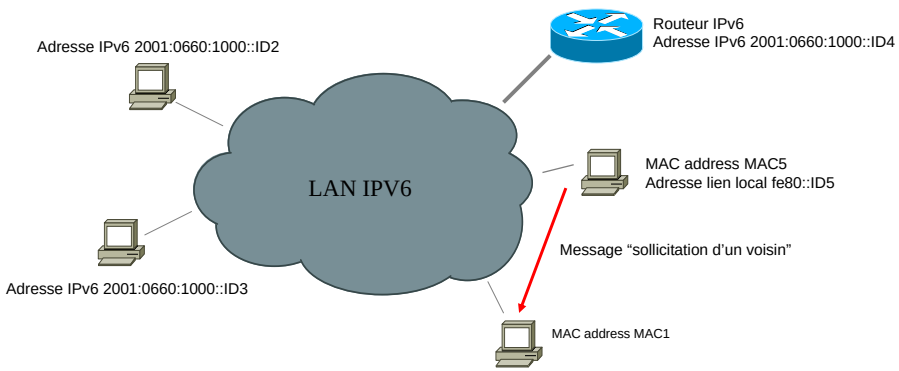
Nouvelles fonctionnalités IPv6

SAA: Stateless Address Autoconfiguration



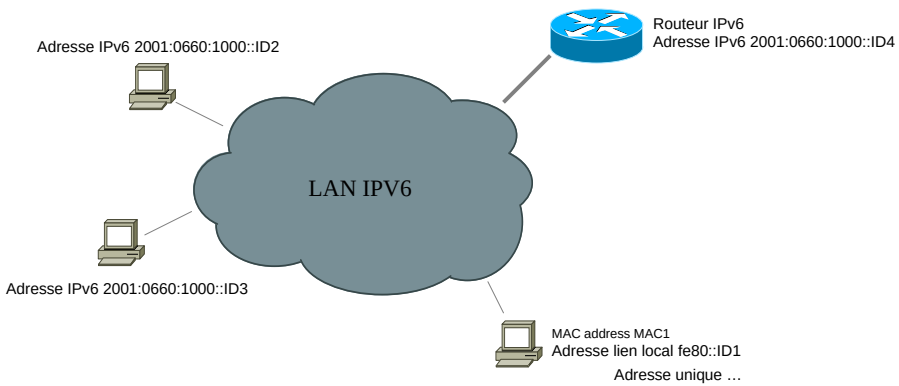
Nouvelles fonctionnalités IPv6

SAA: Stateless Address Autoconfiguration



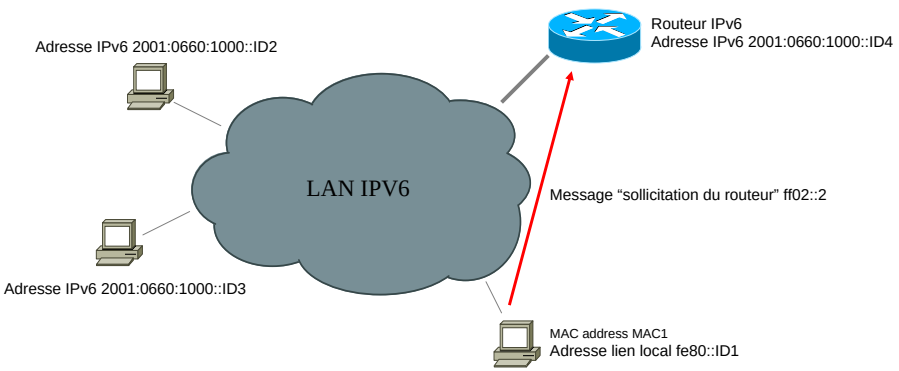
Nouvelles fonctionnalités IPv6

SAA: Stateless Address Autoconfiguration



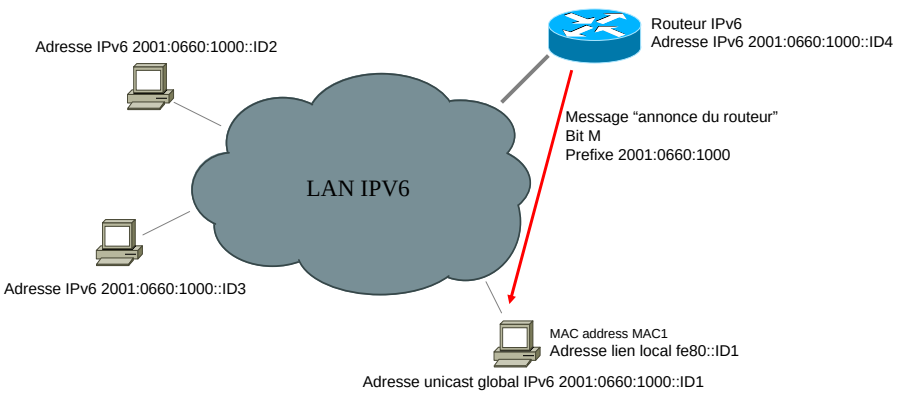
Nouvelles fonctionnalités IPv6

SAA: Stateless Address Autoconfiguration



Nouvelles fonctionnalités IPv6

SAA: Stateless Address Autoconfiguration



Fonctionnement d'OLSR en IPv6

1. Adressage;
2. Autoconfiguration;
3. Modifications à apporter au protocole OLSR.

Adressage

Adresses des interfaces

Un nœud OLSR IPv6 doit reconnaître les adresses suivantes:

1. Adresse **lien-local**: non routable dans un contexte ad hoc;
2. Adresse **unicast globale**: pas de garantie de connexion du réseau à une passerelle IP;
3. Adresse **site-local**: solution intermédiaire entre les deux adresses précédentes pour notre solution d'autoconfiguration pour OLSR:
   - utilisation d'un *subnet-ID* pour OLSR: *OLSR-SUBNET*;
   - une adresse *site-local* d'un nœud OLSR est caractérisée par le préfixe: FEC0:0:0:*OLSR-SUBNET*::/64.

Adressage

Adresses de diffusion

Pour atteindre tous les voisins à un saut

- Utilisation de l'adresse multicast *lien-local* *ALL-LINK-NODES* = FF02::1 avec le champ *Scope* = 2 .

Autoconfiguration

Algorithme d'autoconfiguration IPv6 pour OLSR

Une approche à deux étapes:

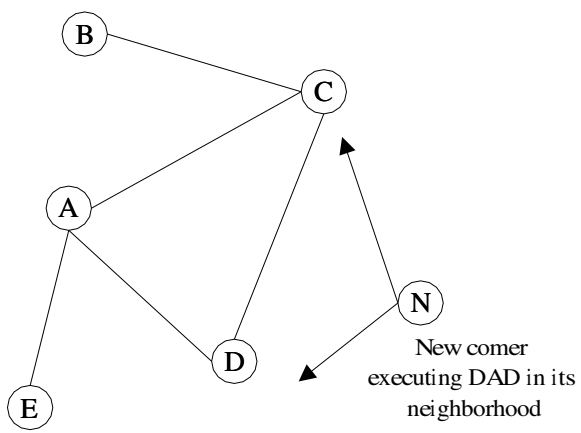
1. Vérification immédiate de l'unicité de l'adresse *site-local* d'un nouveau nœud à son arrivée dans le réseau;
2. Vérification périodique de l'unicité de cette adresse dans le réseau pour traiter les scénarios décrits précédemment.

Autoconfiguration

DAD immédiate

Lorsqu'un nouveau nœud N rejoint le réseau:

- Il calcule son adresse *lien-local* ;
- Il exécute la DAD IPv6 classique dans son voisinage direct;

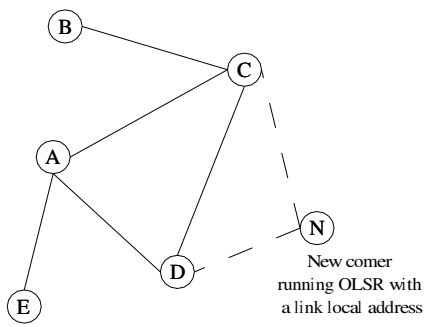


(a)

Autoconfiguration

DAD immédiate

- Si pas de réponse de ses voisins, il commence à exécuter OLSR utilisant son adresse *lien-local* ;
- Avec l'échange de messages HELLO, le nœud N calcule ses MPRs et choisit l'un d'eux, ici le nœud D, pour vérifier l'unicité de l'adresse dans tout le réseau;

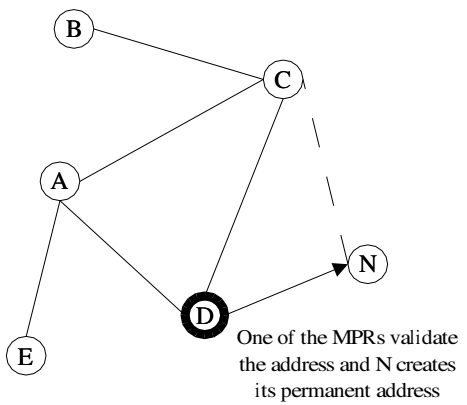


(b)

Autoconfiguration

DAD immédiate

- Le nœud D vérifie l'unicité de l'adresse *lien-local* du nœud N dans tout le réseau;
- Si l'adresse est unique, le nœud D valide cette adresse et le nœud N peut construire son adresse *site-local*.



(c)

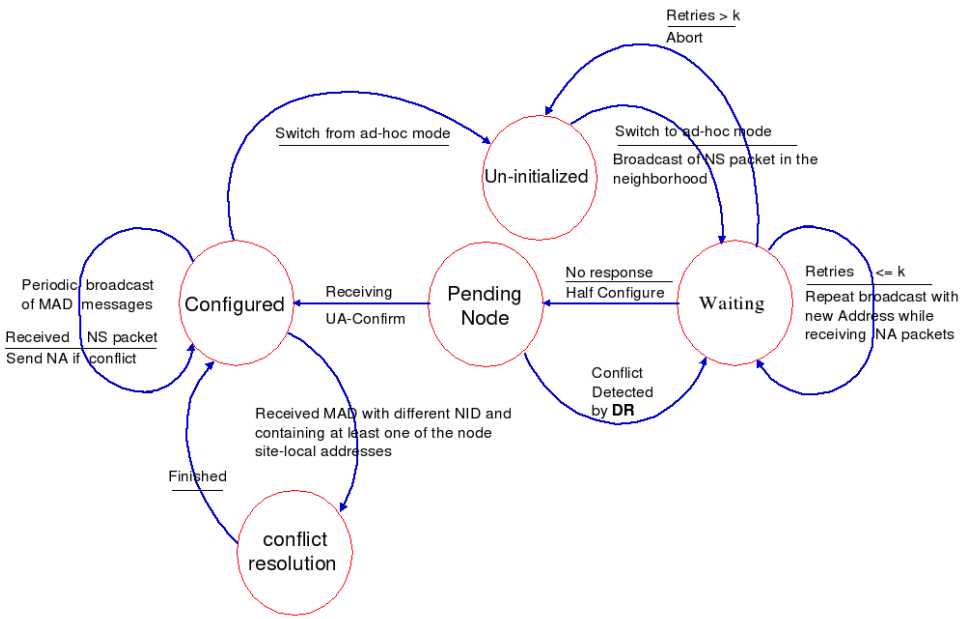
Autoconfiguration

DAD périodique

- Introduction d'un nouveau message de contrôle MAD (Multiple Address Declaration) pour la détection d'adresses dupliquées;
- Le nœud N envoie périodiquement ce message MAD (contenant son adresse) dans tout le réseau pour détecter les conflits d'adresses qui peuvent arriver en cours d'exécution.

Autoconfiguration

Automate d'états finis pour un nœud OLSR IPv6 exécutant l'algorithme d'autoconfiguration



Modifications à apporter au protocole OLSR

Utilisation temporaire de l'adresse *lien-local*

OLSR est modifié de sorte que:

- L'adresse *lien-local* est utilisée uniquement durant la phase d'autoconfiguration du nœud;
- Un nœud doit ignorer les voisins ayant uniquement des adresses *lien-local* lors:
  1. du calcul de ses MPRs;
  2. du calcul des tables de routage;
  3. de la génération des messages TC (Topology Control).

Plan

Principe de notre algorithme d'autoconfiguration

Notre algorithme comprend 3 étapes:

1. Allocation d'une adresse initiale à un nœud nouvellement arrivé dans le réseau;
2. Détection d'adresses dupliquées (chaque nœud vérifie périodiquement qu'aucun autre nœud ne détient son adresse);
3. Résolution de conflits.

Hypothèse

Chaque nœud dans le réseau est identifié par un identifiant unique *Node-ID* de longueur *L* bits.

Principe de notre algorithme d'autoconfiguration

Notre algorithme comprend 3 étapes:

1. Allocation d'une adresse initiale à un nœud nouvellement arrivé dans le réseau;
2. Détection d'adresses dupliquées (chaque nœud vérifie périodiquement qu'aucun autre nœud ne détient son adresse);
3. Résolution de conflits.

Hypothèse

Chaque nœud dans le réseau est identifié par un identifiant unique *Node-ID* de longueur *L* bits.

Principe de notre algorithme d'autoconfiguration

Allocation d'une adresse initiale

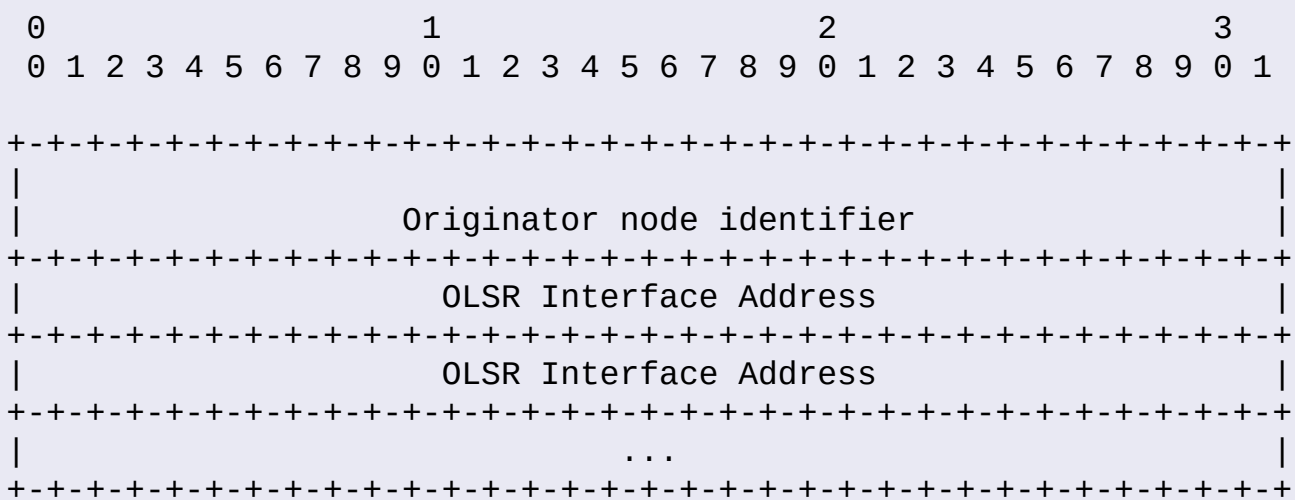
Deux propositions:

1. Sélection aléatoire d'une adresse IP dans un pool d'adresses bien connu et exécution de la DAD par la suite
   - refaire la procédure jusqu'à obtention d'une adresse non dupliquée.
2. Demander son adresse IP à un des voisins déjà configurés
   - les nœuds configurés sont sensés garder une trace des adresses IP déjà allouées dans le réseau.

Principe de notre algorithme d'autoconfiguration

Détection d'adresses dupliquées

- Introduction d'un nouveau message MAD pour la détection d'adresses dupliquées;



Principe de notre algorithme d'autoconfiguration

Détection d'adresses dupliquées

- Ce message est diffusé périodiquement dans le réseau en utilisant le mécanisme des MPRs;
- Un conflit est détecté si un nœud reçoit un message MAD contenant son adresse avec un identifiant différent.

Problème

Le mécanisme des MPRs suppose qu'il n'y a pas d'adresses dupliquées dans le voisinage à deux sauts d'un nœud

- en présence d'adresses dupliquées dans le réseau, les messages MAD risquent de ne pas atteindre tous les nœuds.

Principe de notre algorithme d'autoconfiguration

Détection d'adresses dupliquées

- Ce message est diffusé périodiquement dans le réseau en utilisant le mécanisme des MPRs;
- Un conflit est détecté si un nœud reçoit un message MAD contenant son adresse avec un identifiant différent.

Problème

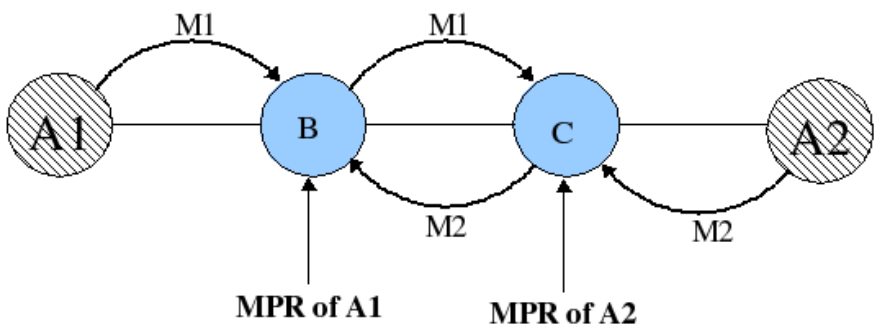
Le mécanisme des MPRs suppose qu'il n'y a pas d'adresses dupliquées dans le voisinage à deux sauts d'un nœud

- en présence d'adresses dupliquées dans le réseau, les messages MAD risquent de ne pas atteindre tous les nœuds.

Principe de notre algorithme d'autoconfiguration

Détection d'adresses dupliquées: exemple

1. Les nœuds *A*1 et *A*2 sont en conflit;
2. Les nœuds *B* et *C* ne se choisissent pas mutuellement comme MPRs
   - chacun des nœuds *B* et *C* voit un réseau à un saut.



Principe de notre algorithme d'autoconfiguration

Détection d'adresses dupliquées: solution

Modification du mécanisme de diffusion MPR d'OLSR

- Introduction du mécanisme DAD-MPR flooding : Duplicate Address Detecting MPR flooding.
- Le mécanisme DAD-MPR fonctionne même en présence d'adresses dupliquées dans le réseau.

Principe de notre algorithme d'autoconfiguration

Résolution de conflits

Deux propositions:

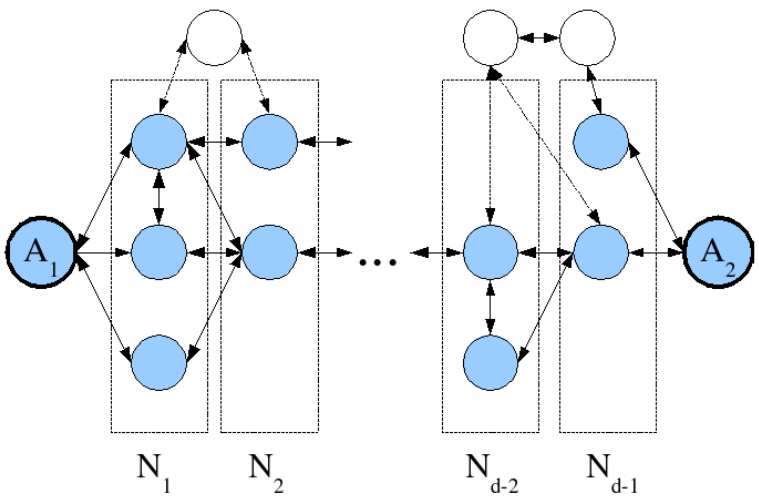
1. Le nœud en conflit ayant le plus petit identifiant change d'adresse.
2. Une partie des premiers bits de l'identifiant peut être utilisée pour indiquer la priorité du nœud:
   - Le nœud moins prioritaire change d'adresse.

Conception et preuve du mécanisme DAD-MPR

1. Problèmatique;
2. DAD-MPR pour réseaux OLSR mono-interface;
3. DAD-MPR pour réseaux OLSR multi-interfaces.

Problèmatique

- On suppose que deux nœuds A_1 et A_2 ayant les identifiants ID_{A_1} et ID_{A_2} respectivement, partagent la même adresse A;
- Les ensembles de nœuds N_i qui sont à une distance i de A_1 et à une distance $d - i$ de A_2 pour $i \in \{1, ..., d-1\}$, sont sur le plus court chemin entre A_1 et A_2.



Problèmatique

- On cherche les règles à ajouter au mécanisme MPR pour faire propager les MADs entre A_1 et A_2.
- On va raisonner sur la distance d du plus court chemin entre A_1 et A_2.

DAD-MPR pour réseaux OLSR mono-interface

Hypothèse 1

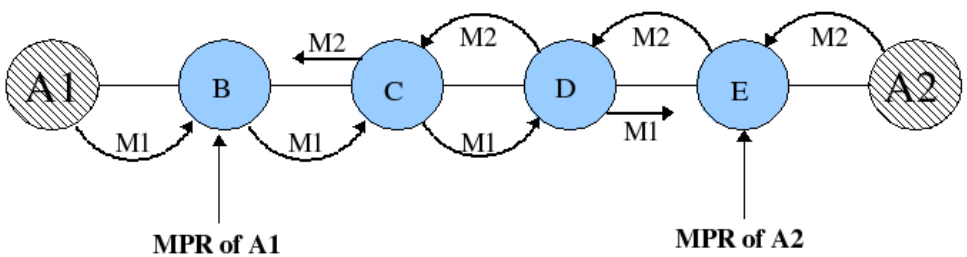
On suppose qu'il y a un seul conflit dans le réseau.

- $d \geq 5$: Les règles des MPRs suffisent.
- $d = 4$: On va introduire une nouvelle règle (*Règle 1*).
- $d = 3$: On introduit une deuxième règle (*Règle 2*).
- *Règle 1* et *Règle 2* couvrent également les cas où $d = 2$ et $d = 1$.

DAD-MPR pour réseaux OLSR mono-interface

$d \geq 5$

Il n'y a pas de conflit à deux sauts donc les MPRs sont bien choisis et les MADs se propagent bien entre A_1 et A_2.

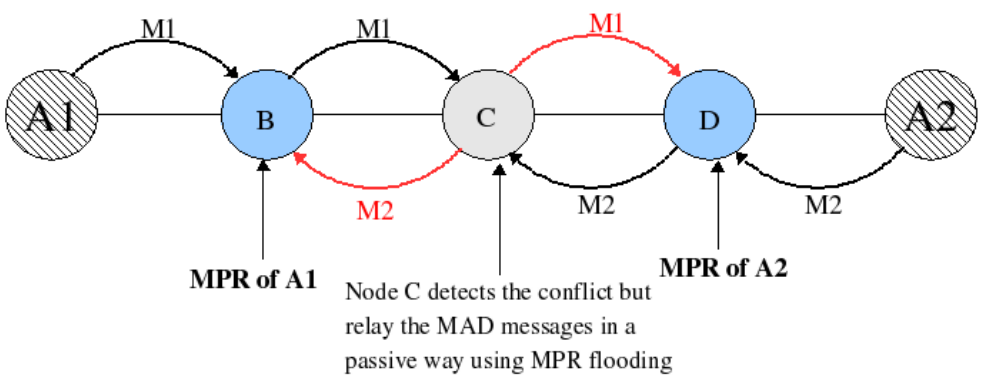


DAD-MPR pour réseaux OLSR mono-interface

$d = 4$

La propagation des MADs risque d'être arrêtée par le numéro de séquence.

Règle 1: la table des duplications doit prendre en compte l'identifiant du MAD.

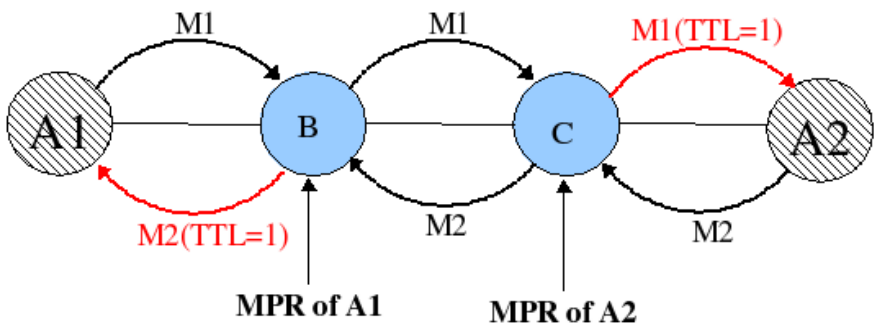


DAD-MPR pour réseaux OLSR mono-interface

$d = 3$

- Le nœud B voit un réseau à 1 saut (nœud C et nœud $A1$);
- Le nœud C voit un réseau à 1 saut (nœud B et nœud $A2$).

$\Rightarrow$ B et C ne se choisissent pas mutuellement comme MPRs.



DAD-MPR pour réseaux OLSR mono-interface

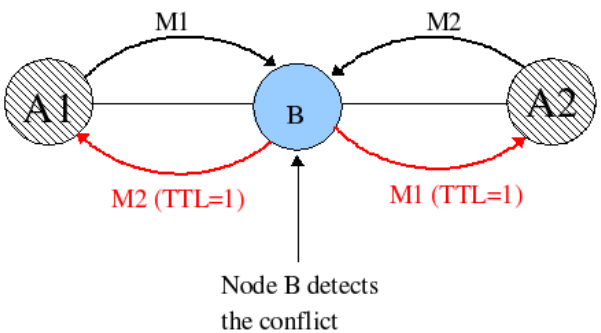
$d = 3$

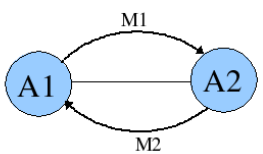
Règle 2: Lorsqu'un nœud B reçoit un message MAD et détecte un conflit entre deux nœuds $A1$ et $A2$, il relaye ce message MAD s'il est lui même voisin direct de $A1$ ou de $A2$.
Le TTL du paquet est remis à 1.

DAD-MPR pour réseaux OLSR mono-interface

$d = 2$ et $d = 1$

Les règles précédentes suffisent pour assurer la propagation des messages MAD entre les nœuds A_1 et A_2.

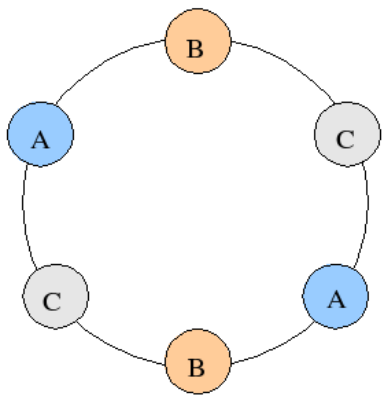




DAD-MPR pour réseaux OLSR mono-interface

Hypothèse 2

On suppose qu'il y a des conflits multiples dans le réseau.



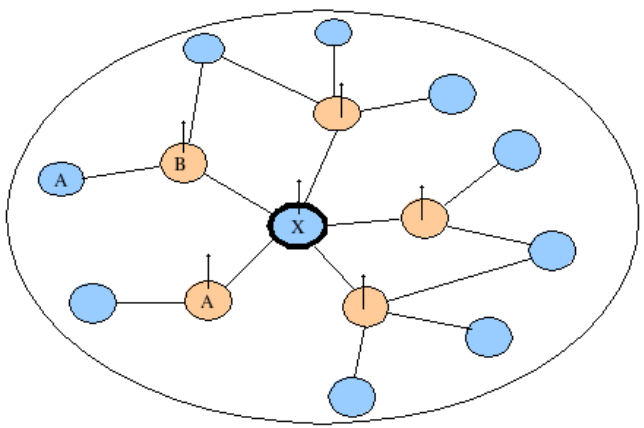
Les règles *Règle 1* et *Règle 2* ne suffisent pas.

DAD-MPR pour réseaux OLSR mono-interface

Règles en cas de conflits multiples

On substitue à la *Règle 2* la *Règle 3*.

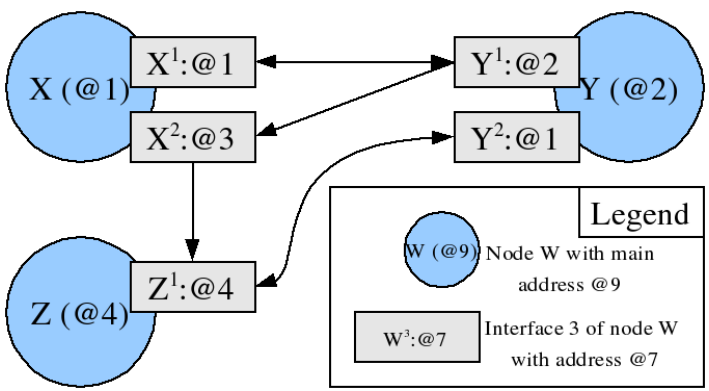
- *Règle 3*: lorsqu'un nœud *B* a un lien symétrique ou asymétrique avec la source d'un message MAD, le nœud *B* relaye le message.



DAD-MPR pour réseaux OLSR multi-interfaces

Noeuds multi-interfaces

- Chaque nœud peut avoir plusieurs interfaces
- Chaque interface a une adresse
- Chaque nœud choisit aléatoirement une de ses adresses comme *main address*. Elle sera l'adresse source de tout ses messages.



DAD-MPR pour réseaux OLSR multi-interfaces

Définition

Deux nœuds multi-interfaces X et Y sont en conflit s'il existe au moins une adresse partagée entre les deux nœuds.

Nouvelles règles

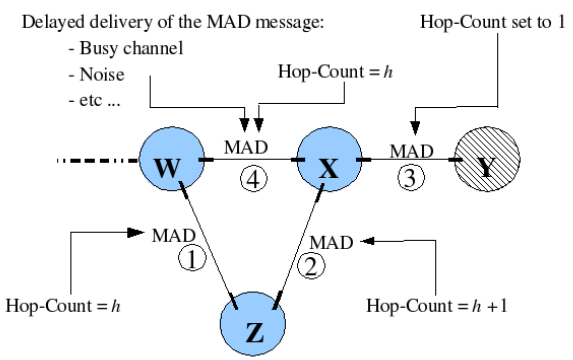
Deux nouvelles règles pour traiter les nœuds à interfaces multiples

- *Règle 1*: pour assurer le relayage des messages MAD.
- *Règle 2*: pour un calcul correct des MPRs en cas de conflits d'adresses.

DAD-MPR pour réseaux OLSR multi-interfaces

Relayage des MADs

- *Règle 1*: lorsqu'un nœud *X* reçoit un message MAD contenant la même *main address* que celle d'un nœud *Y* avec lequel il a un lien symétrique ou asymétrique, le nœud *X* relaye le message.
  - le champ *Hop-Count* du message MAD est mis à 1.

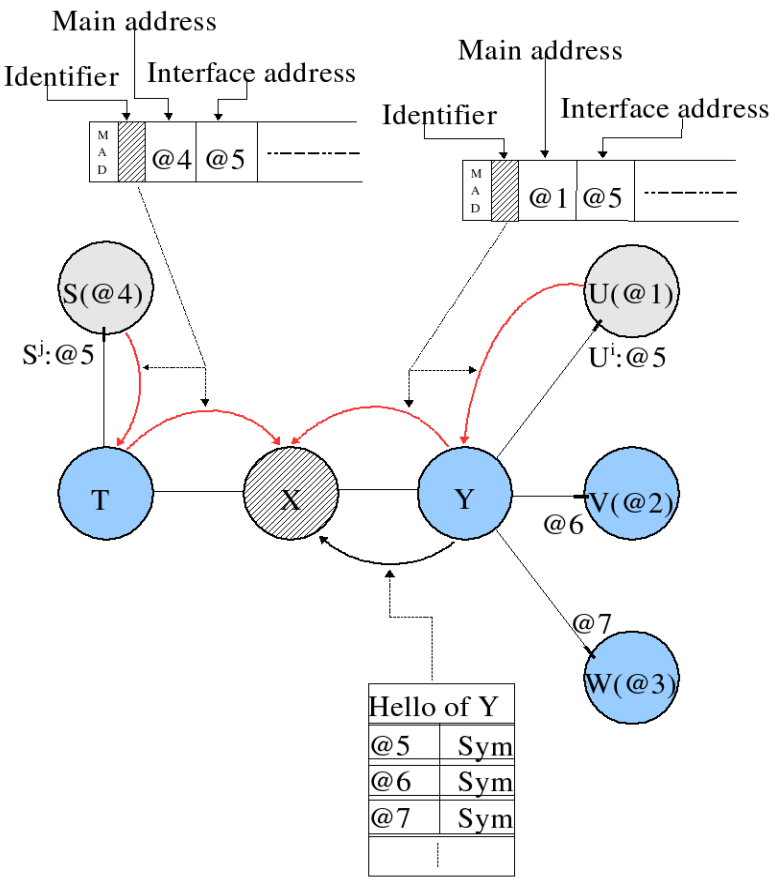


DAD-MPR pour réseaux OLSR multi-interfaces

Calcul correct des MPRs

La *Règle 2* permet à un nœud X d'éviter une mauvaise conversion des adresses de ses voisins à 2 sauts en leurs adresses principales (*main address*)
$\Rightarrow$ calcul correct des MPRs de X.

DAD-MPR pour réseaux OLSR multi-interfaces



DAD-MPR pour réseaux OLSR multi-interfaces

Calcul correct des MPRs

En appliquant la *Règle 2*, le nœud X construit deux tuples pour les adresses U^i:@5 et S^j:@5 comme suit:

- U^i:@5 (*main address* de $Y \rightarrow$ *main address* de U(@1)).
- S^j:@5 (*main address* de $T \rightarrow$ *main address* de S(@4)).

DAD-MPR pour réseaux OLSR multi-interfaces

Calcul correct des MPRs

Règle 2:

1. Un message *HELLO* en provenance d'un nœud Y et reçu par un nœud X, contient les adresses des interfaces des voisins à 2 sauts de X (voisins à 1 saut de Y);
2. Pour convertir ces adresses en leurs *main address*, le nœud X doit utiliser uniquement les messages MAD relayés par le nœud Y et originaires des voisins à 1 saut de Y (*Hop-Count* = 1).

Simulations et évaluation des performances

1. Allocation d'une adresse initiale;
2. Overhead du message MAD;
3. Convergence du protocole DAD-MPR.

Allocation d'une adresse initiale

Variables

- Soit N_n le nombre de nœuds dans le réseau, et N_a le nombre total d'adresses IP dans le pool d'adresses.

Première technique: choix aléatoire d'adresses

- Probabilité de choisir une adresse dupliquée est $p = \frac{N_n}{N_a}$.
- Si on note par D_1 la durée de détection d'une adresse dupliquée, le temps moyen pour obtenir une adresse non dupliquée est

$$\sum_{i \geq 1} (1-p) i D_1 p^{i-1} = D_1 \frac{1}{1-p} = D_1 \frac{1}{(1-\frac{N_n}{N_a})}$$

Allocation d'une adresse initiale

Variables

- Soit N_n le nombre de nœuds dans le réseau, et N_a le nombre total d'adresses IP dans le pool d'adresses.

Première technique: choix aléatoire d'adresses

- Probabilité de choisir une adresse dupliquée est $p = \frac{N_n}{N_a}$.
- Si on note par D_1 la durée de détection d'une adresse dupliquée, le temps moyen pour obtenir une adresse non dupliquée est

$$\sum_{i \geq 1} (1-p) i D_1 p^{i-1} = D_1 \frac{1}{1-p} = D_1 \frac{1}{(1-\frac{N_n}{N_a})}$$

Allocation d'une adresse initiale

Deuxième technique: demande d'adresse à un voisin

- On suppose qu'une fraction h des nœuds configurés N_n ne sont pas connus par ce nœud voisin
  $\Rightarrow$ la probabilité d'obtenir une adresse dupliquée est $p = \frac{hN_n}{N_a - N_n(1-h)}$.
- D_2 = la durée de demande d'adresse à un voisin + la durée de détection éventuelle d'adresse dupliquée
  $\Rightarrow$ le temps moyen pour obtenir une adresse non dupliquée peut être exprimé par

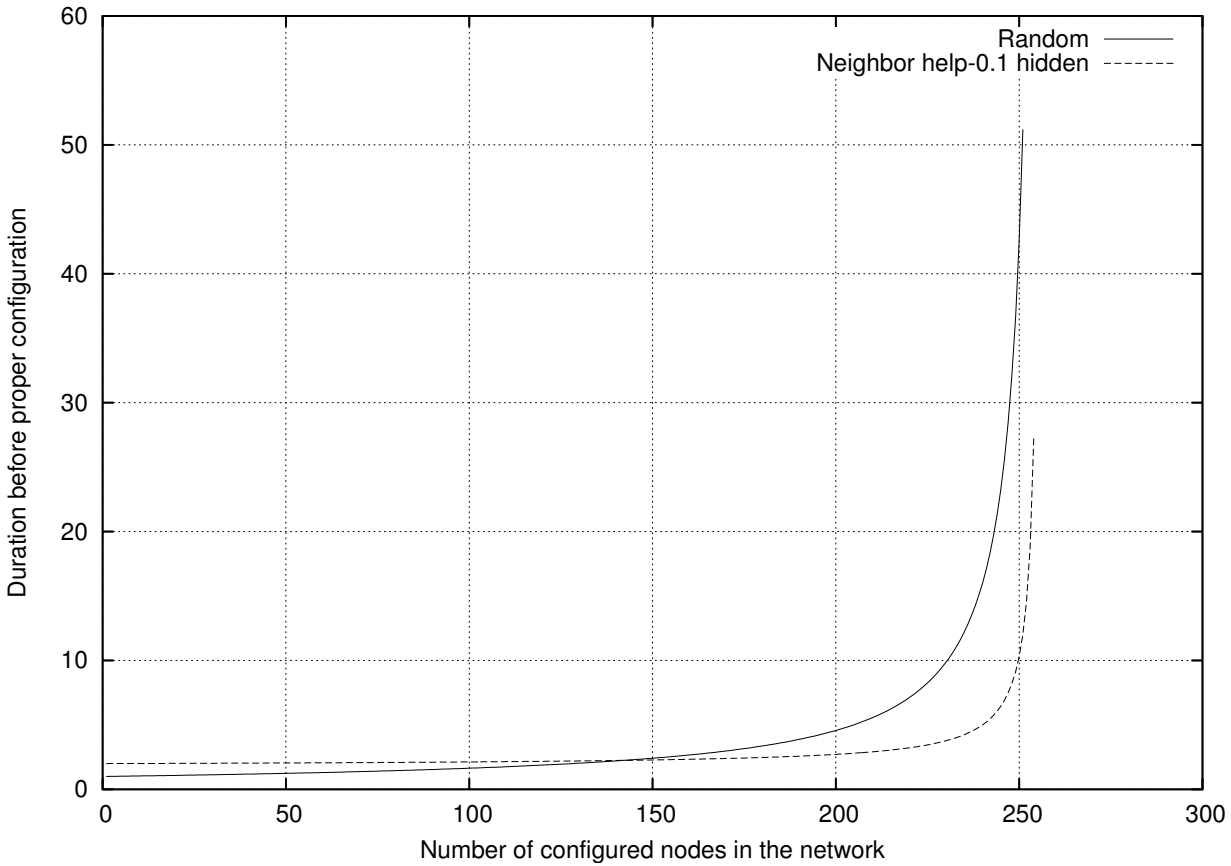
$$\sum_{i \geq 1} (1-p) i D_2 p^{i-1} = D_2 \frac{1}{(1 - \frac{hN_n}{N_a - N_n(1-h)})}$$

Allocation d'une adresse initiale

Paramètres de simulations

- Pour prendre en considération la durée d'échanges de messages entre un nouveau nœud et un de ses voisins configurés; on suppose que $D_2 = 2D_1$;
- On suppose aussi que 10% des messages MAD sont perdus ($h = 0.1$);
- On prend un pool d'adresses de 256 adresses ($N_a = 256$).

Allocation d'une adresse initiale



Overhead du message MAD

Modéle analytique

- $T_m \leq$ overhead des voisins + overhead de la diffusion MPR

$$T_m \leq \alpha T_h + \beta T_t \quad (1)$$

Où

- $$\alpha = \frac{\tau_m}{\tau_h}\frac{L_m}{L_a} \quad (2)$$

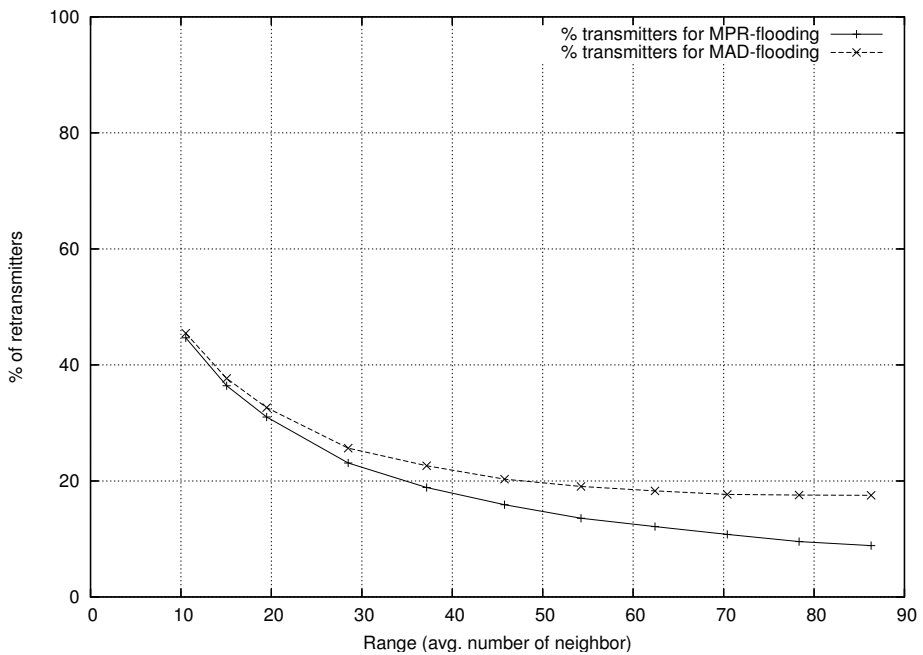
- $$\beta = \frac{\tau_m}{\tau_t}\frac{L_m}{L_t}\frac{1}{\rho} \quad (3)$$

Varia- ble	Meaning
δ	average degree of a node
N	number of nodes in the network
τ_h	Hello message rate
L_h	size of Hello messages
τ_t	TC message rate
L_t	size of TC messages
o	broadcast optimization factor, $\frac{1}{\delta} \leq o \leq 1$
ρ	proportion of nodes which are MPR of at least one node
τ_m	MAD message rate
L_m	size of MAD messages
T_h	total overhead of Hello messages (in bytes)
T_t	total overhead of TC messages (in bytes)
T_m	total overhead of MAD messages (in bytes)
L_a	size of one address
N_n	avg. number of neighbors of one node

Overhead du message MAD

Simulations

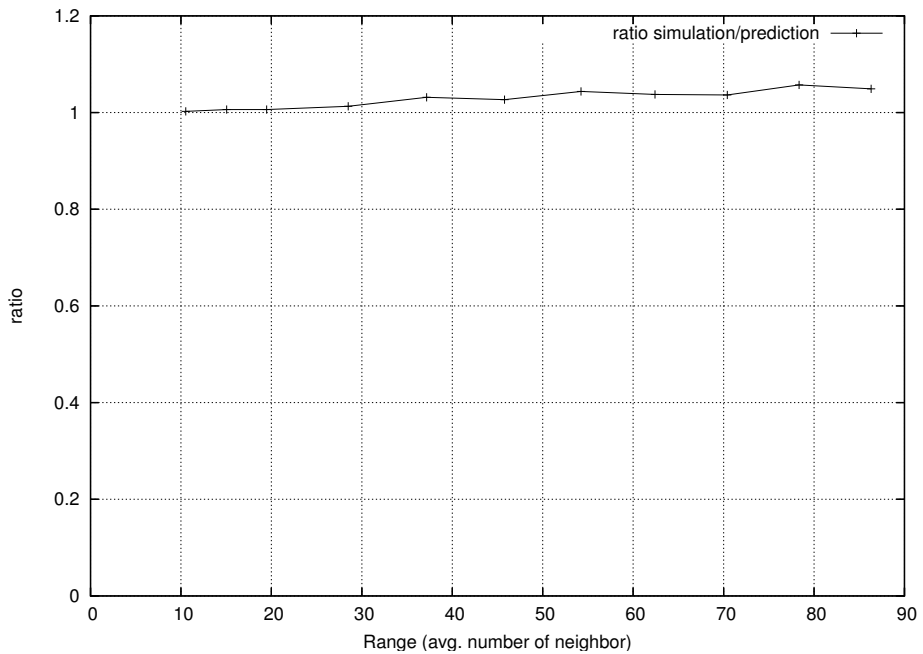
Taux de nœuds dans le réseau retransmettant un message MAD.



Overhead du message MAD

Simulations

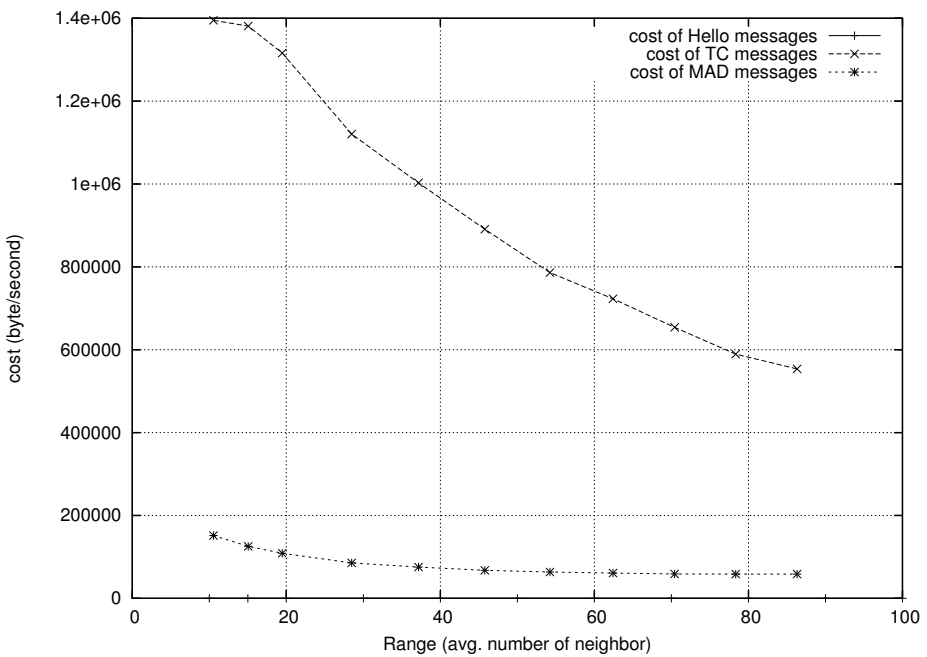
Taux réel de nœuds retransmettant un message MAD versus taux estimé.



Overhead du message MAD

Simulations

Overhead du message MAD comparé à celui des autres messages de contrôle.



Convergence du protocole DAD-MPR

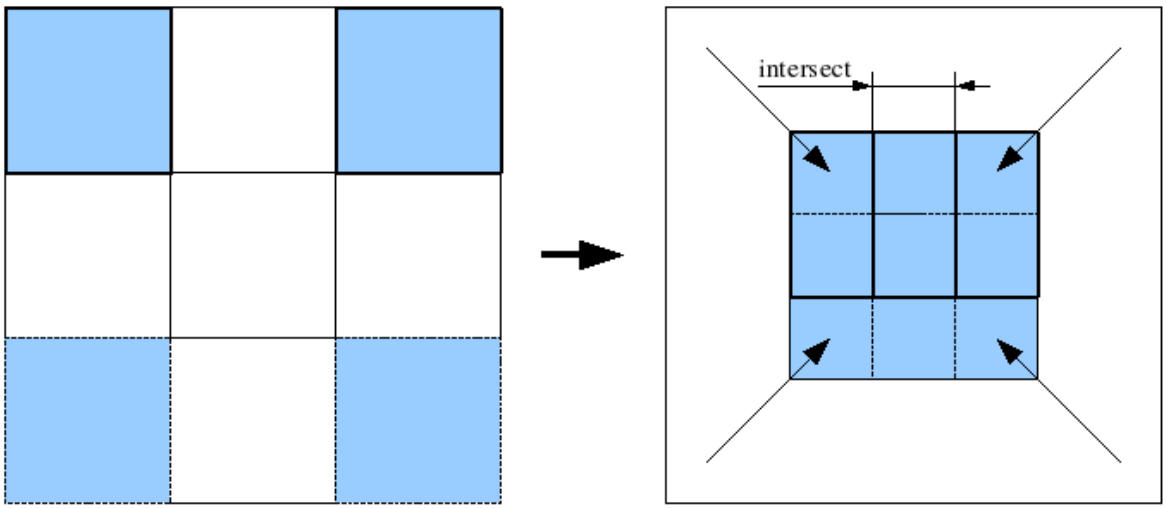
Principe

L'idée est:

1. De simuler la fusion de plusieurs réseaux en générant des duplications massives d'adresses;
2. De calculer par la suite le temps de détection et de correction de ces adresses par le protocole DAD-MPR.

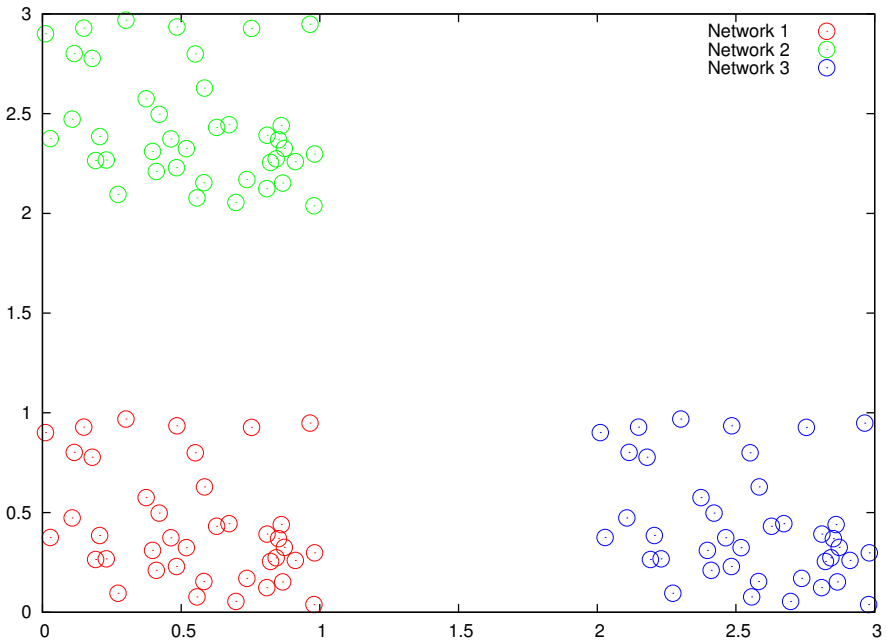
Convergence du protocole DAD-MPR

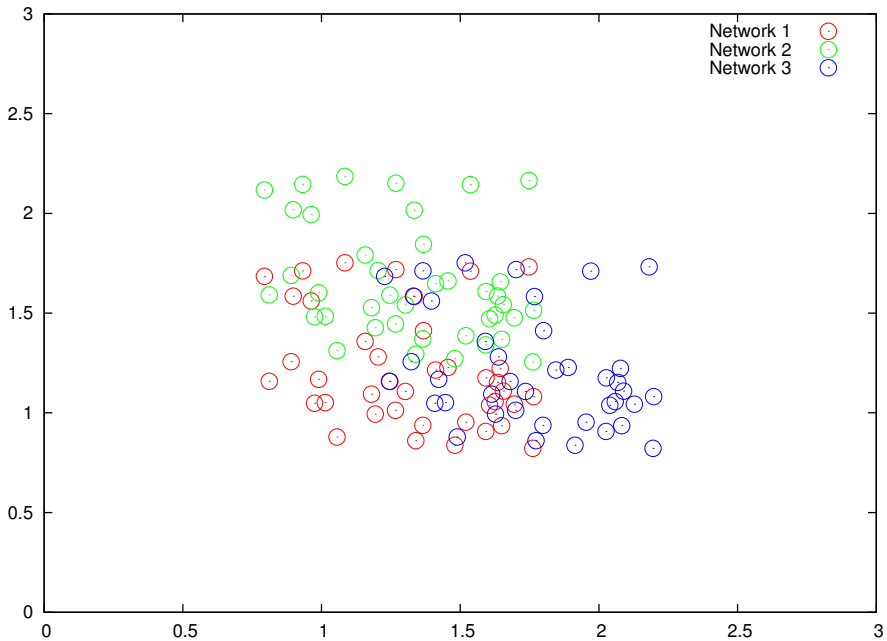
Aire d'intersection des réseaux



Convergence du protocole DAD-MPR

Scénario de fusion de trois réseaux avec $l = 0.70$





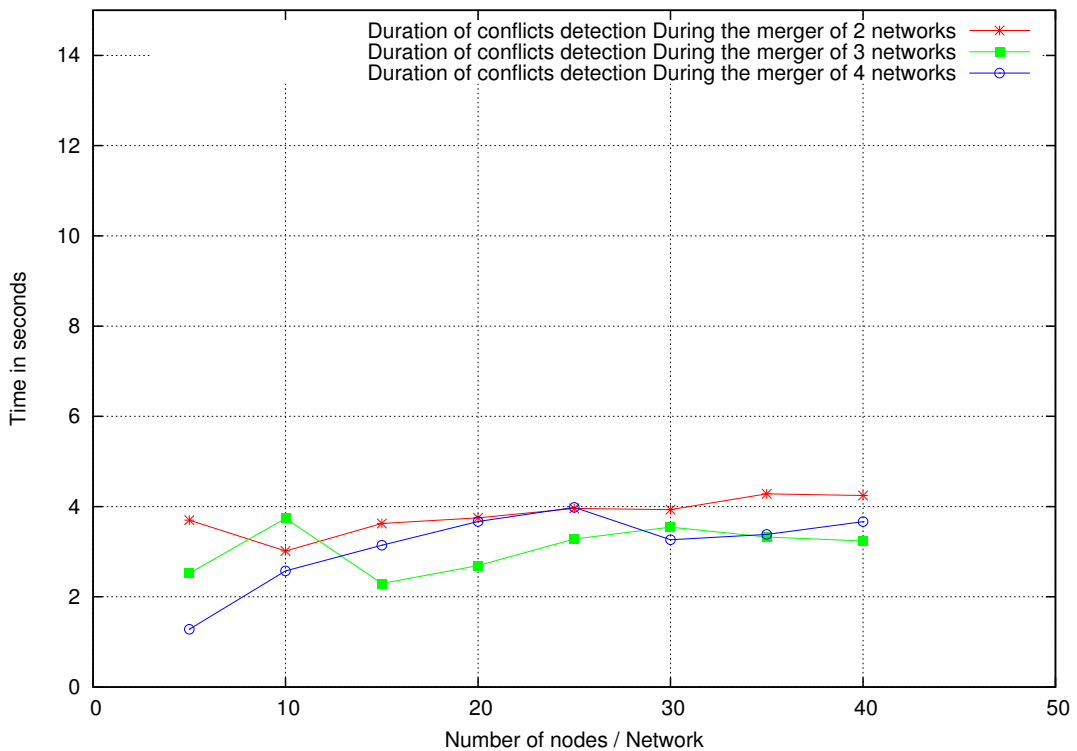
Convergence du protocole DAD-MPR

Paramètres de simulation

- Les nœuds sont placés d'une manière aléatoire dans un carré de 1x1;
- Portée du signal (R: 0 à 1);
- Nombre de réseaux (*Nb-Part*: 1 à 4);
- Nombre de nœuds N dans chaque réseau;
- Nombre d'adresses dupliquées (A: 1 à N) après la fusion;
- Longueur de l'aire d'intersection (l: 0 à 1).

Convergence du protocole DAD-MPR

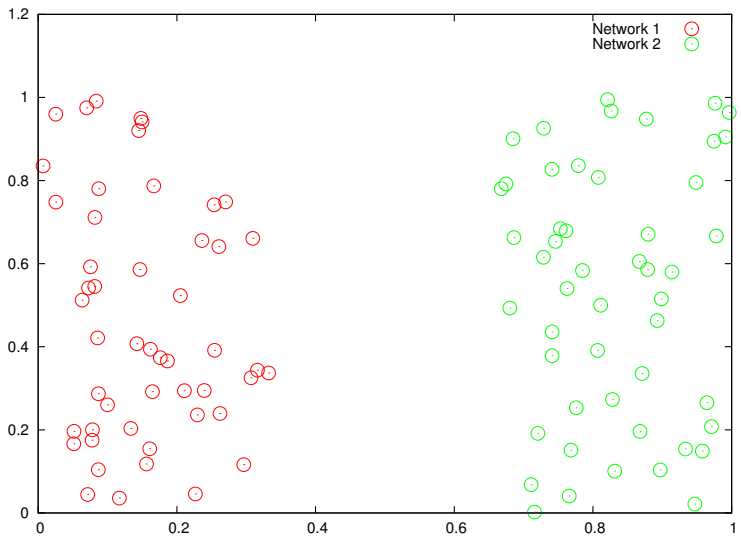
$R = 0.4$ et $I = 0.70$

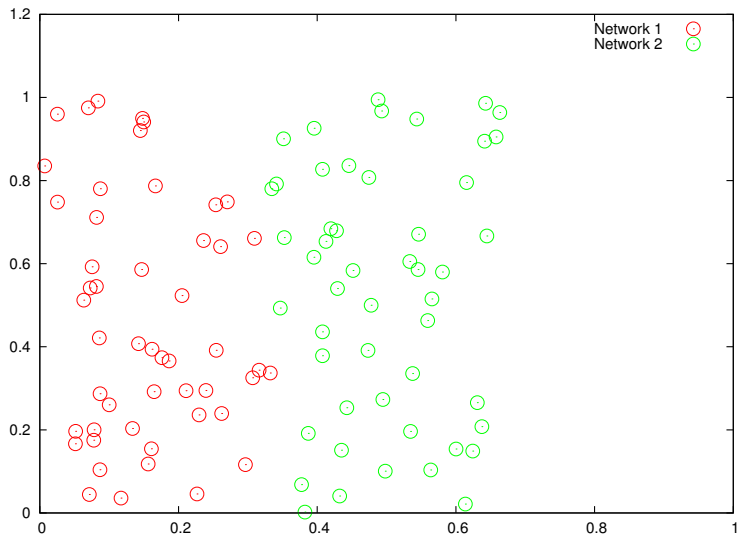


Convergence du protocole DAD-MPR

Problème 1

- Après la fusion, le nombre de sauts dans le réseau est insuffisant pour tester le protocole DAD-MPR
  $\Rightarrow$ augmenter le nombre de sauts en prenant $I = 0$.





Convergence du protocole DAD-MPR

Problème 2

- Après la fusion, le réseau n'est pas connexe.

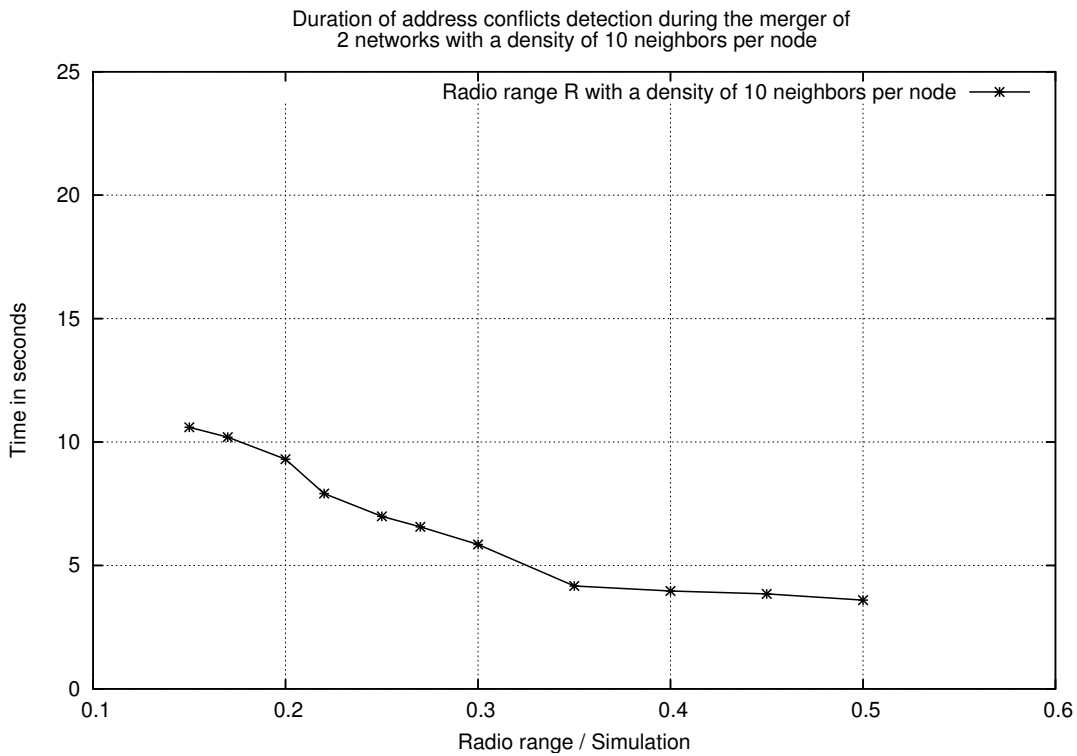
Approche

Une approche pour contrôler la topologie du réseau a été proposée par (*Douglas M. Bough et al*)

- maintenir la densité des voisins de l'ordre de k pour chaque nœud dans le réseau;
- pour $k = 9$, un réseau de 50 à 500 nœuds est connexe avec une probabilité 0.95.

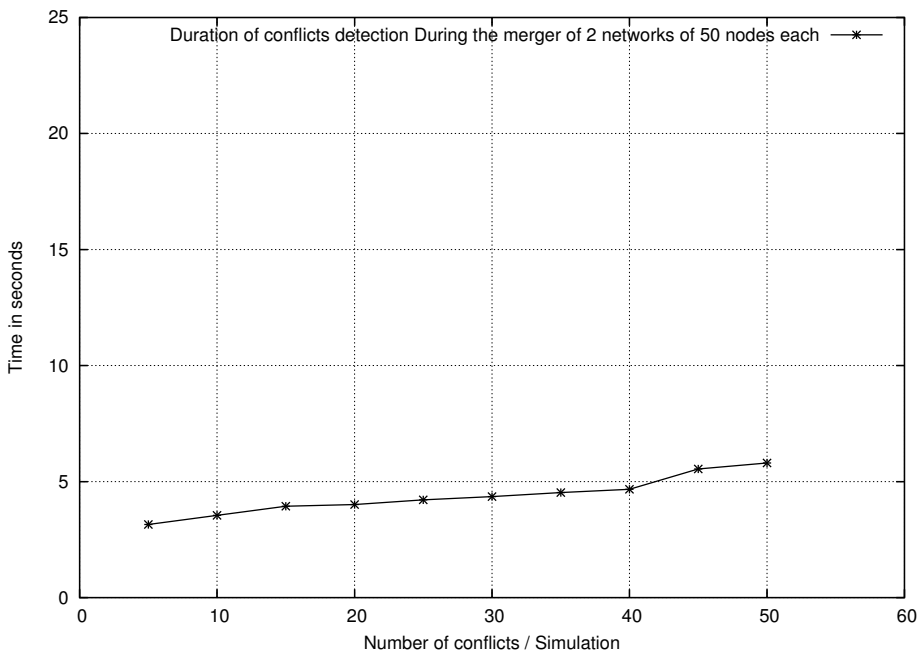
Convergence du protocole DAD-MPR

$D = 10$, $I = 0$ et R varie



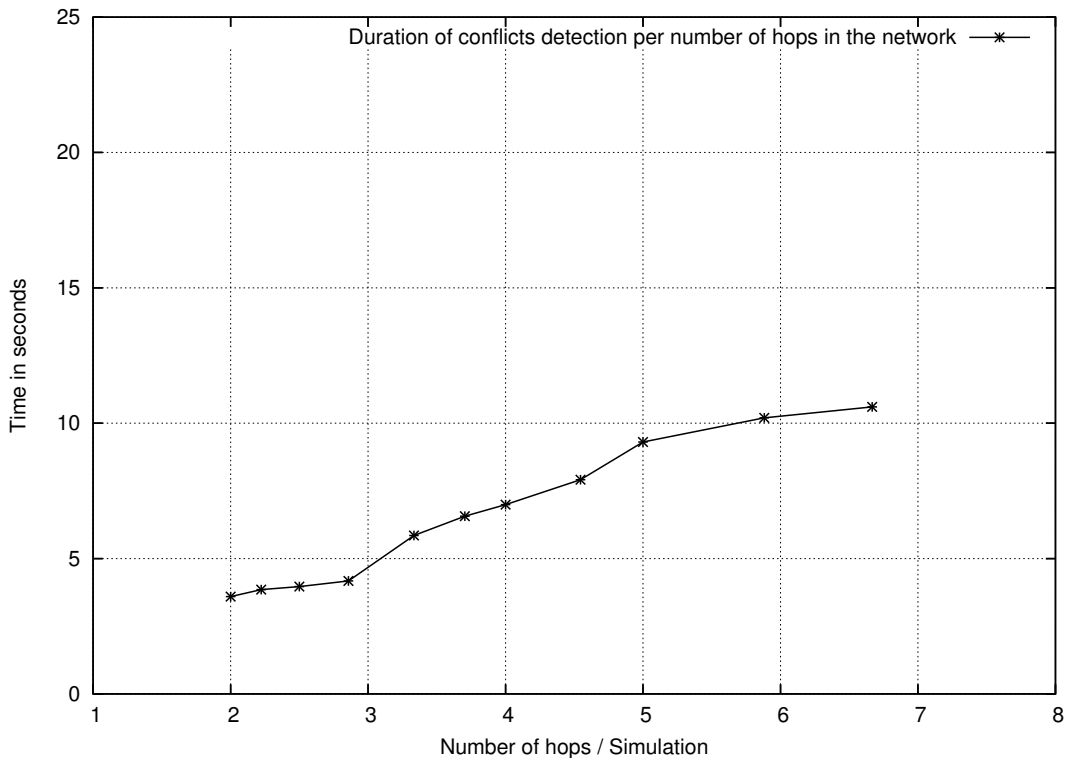
Convergence du protocole DAD-MPR

$R = 0.25$, $I = 0$, $N = 50$ et A varie



Convergence du protocole DAD-MPR

$D = 10$, $I = 0$ et le nombre de sauts varie



Plan

SB

Intérêt d'une clé de groupe symétrique

Clé asymétrique / symétrique

- Les mécanismes de sécurité à clé asymétrique fonctionnent pour des communications en point à point. Ils nécessitent l'existence de paires de clés pour tous les couples (source, destination)
- Ils ne fonctionnent pas pour un trafic multipoint
- Une clé de groupe symétrique permet de réduire le nombre de clés nécessaires dans le réseau et de sécuriser le trafic multipoint.

Sélection d'un algorithme de création de clé de groupe symétrique déjà existant

Critères de sélection pour un réseau ad hoc

1. Pas de structure sous-jacente du réseau (exemple anneau)
2. Nombre d'étapes indépendant du nombre de nœuds
3. Nombre de messages minimum.

Sélection d'un algorithme de création de clé de groupe symétrique déjà existant

Comparaison des protocoles à nombre d'étapes constant

	Expo per U_i	Messages	Broadcasts	Rounds	Structure	FS
Octopus	4	$3m-4$	0	4	Hypercube	Yes
BDB	3	$2m$	m	2	Ring	Yes
BCEP	$2^{\dagger}$	$2m$	0	2	None	No
Catalano	$m+1$	$2m$	0	2	None	Yes
KLL	3	$2m$	$2m$	2	Ring	Yes
NKYW	$2^{\ddagger}$	m	1	2	None	Yes
STR	$(m-i)^{*}$	m	1	2	Skewed tree	Yes
AGDH	2^{**}	m	1	2	None	Yes

†: m exponentiations for the base station.
‡: $m+1$ exponentiations and m-1 inverse calculations for the parent node.
$*$: Up to $2m$ exponentiations for the sponsor node.
$**$: m exponentiations for the leader.

Sélection d'un algorithme de création de clé de groupe symétrique déjà existant

Algorithme AGDH (Asymmetric Group Diffie Hellman) (Augot, Bhaskar)

Algorithme en trois étapes

1. Envoi initial du leader: message de présence,
2. Réponse des membres i: contribution g^{r_i}
3. Réponse du leader l: contributions $g^{r_i}, g^{r_i r_l}$
4. Calcul de la clé $K = g^{r_l(1+\sum_{i \neq l} r_i)}$

Adaptation du protocole AGDH aux réseaux ad hoc

AGDH et réseaux ad hoc

1. Adaptation des messages du protocole AGDH
2. Mécanismes d'élection d'un leader
3. Gestion de la dynamique du réseau
4. Calcul de l'overhead du protocole

Plan

SB

Conclusions et perspectives

Conclusions

- Conception d'une solution entièrement IPv6 pour OLSR;
  - traitement des messages de contrôle d'OLSR
  - autoconfiguration IPv6 d'OLSR
- Proposition d'un mécanisme d'autoconfiguration pour OLSR;
  - DAD-MPR: diffusion optimisée en cas de conflits d'adresses
  - prouvé correct en cas de conflits simples ou multiples
  - fonctionne dans le cas d'un réseau mono-interface ou multi-interfaces

Conclusions et perspectives

Conclusions

- Evaluation de performances de ce mécanisme;
  - l'overhead généré est limité
  - convergence en quelques secondes en cas de conflit
- Conception d'un protocole de création de clé de groupe symetrique (autoconfiguration d'une clé) pour un réseau ad hoc (adaptation du protocole AGDH);

Conclusions et perspectives

Perspectives

- Concevoir une solution d'autoconfiguration pour les réseaux ad hoc indépendante des protocoles de routage
  - si cette solution est en IPv6, elle sera conforme à la charte de l'autoconfiguration à l'IETF.
- Concevoir un modèle de sécurité adapté aux réseaux ad hoc. Cela permettra de bâtir des preuves formelles solides pour les protocoles de sécurité dans les réseaux ad hoc.

Merci !!! Thanmirth

Questions?