

Chapitre 5+6

Routage dans les réseaux de mobiles et MAC 802.11- Recherche

Partie 1

■ Références :

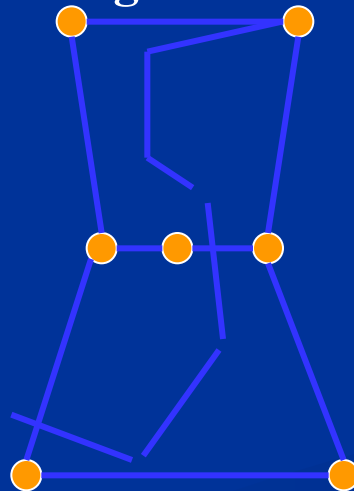
1. **K. AL AGHA, G. PUJOLLE, G. VIVIER, Réseaux de mobiles et réseaux sans fil, Eyrolles, 2001.**
2. **P. MÜHLETHALER, 802.11 et les réseaux sans fil, Eyrolles, 2002.**
3. **K. Pahlavan, P. Krishnamurthy, Principles of Wireless Networks (Prentice Hall), 2002.**
4. **G. Pujole. LES RÉSEAUX Édition 2008**
5. **T. Lemlouma. Le routage dans les réseaux mobiles ad hoc. Technical report, Université des Sciences et de la Technologie Houari Boumèdiene. Institut d'Informatique, 2000.**
6. **F. Risson and N. Gaona. Le routage au sein des réseaux ad hoc. Projet Bibliographique, Décembre 2004.**
7. **T. Clausen and P. Jacquet. Optimized Link State Routing Protocol (OLSR). RFC3626 (Experimental), October 2003.**
8. **C. Perkins, E. Belding-Royer, and S. Das. Ad hoc On-Demand Distance Vector (AODV) Routing. RFC 3561 (Experimental), July 2003.**
9. **Z.J. Hass and M.R. Pearlman. The Zone Routing Protocol(ZRP) for Ad Hoc Networks. Internet Draft, Mobile Ad-Hoc Network(MANET) Working Group, IETF, Springer, August 1998.**
10. **Yacine Challal , Réseaux Mobiles Ad hoc, ReSyD'08.**

1. Introduction

- Le concept des réseaux mobiles ad hoc essaie d'étendre les notions de la mobilité à toutes les composantes de l'environnement.
- Ici, contrairement aux réseaux basés sur la communication **cellulaire**, aucune administration centralisée n'est disponible, ce sont les hôtes mobiles eux-mêmes qui forment, d'une manière **ad hoc**, une infrastructure du réseau.
- Aucune supposition ou limitation n'est faite sur la taille du réseau ad hoc, le réseau peut contenir des centaines ou des milliers d'unités mobiles.

2. Définition

- Un réseaux ad hoc (MANET) est une collection de nœuds, fixes ou mobiles, communiquant au moyen de liens radio pour former un réseau multi-sauts.
- Applications : civile, militaire, ...
- Caractéristiques : topologie dynamique, absence d'infrastructure, bande passante limitée, énergie limitée, sécurité physique et logique limitée.; forment un cahier des charges pour la conception des protocoles de routage.



3. Routage

- Le routage est la méthode d'acheminement des informations à la bonne destination à travers un réseau de connexions défini.
- La prédominance du groupe MANET (<https://www.ietf.org/proceedings/55/177.htm>), nous adoptons leur classification.

3.1. Classification du groupe MANET

1. **Protocoles proactifs**, ou table driven : Ces protocoles entretiennent toutes les routes du réseau avec l'échange périodique des paquets de contrôle.
2. **Protocoles réactifs**, ou on demand : Ces protocoles ne cherchent à calculer une route qu'à la demande d'une application.
3. **Protocoles hybrides** : Les protocoles hybrides combinent les deux principes des protocoles proactifs et réactifs.

3.1.1 Les protocoles proactifs

- Echange périodique de paquets de contrôle
- Plusieurs types de paquets de contrôle.
- Chaque nœud maintient une ou plusieurs tables,
- Les nœuds diffusent des messages de mise à jour à travers tout le réseau
- Les protocoles de cette famille se différencient par la manière dont cette information de mise à jour est transmise à travers le réseau ainsi que par le nombre de tables de routage utilisées.

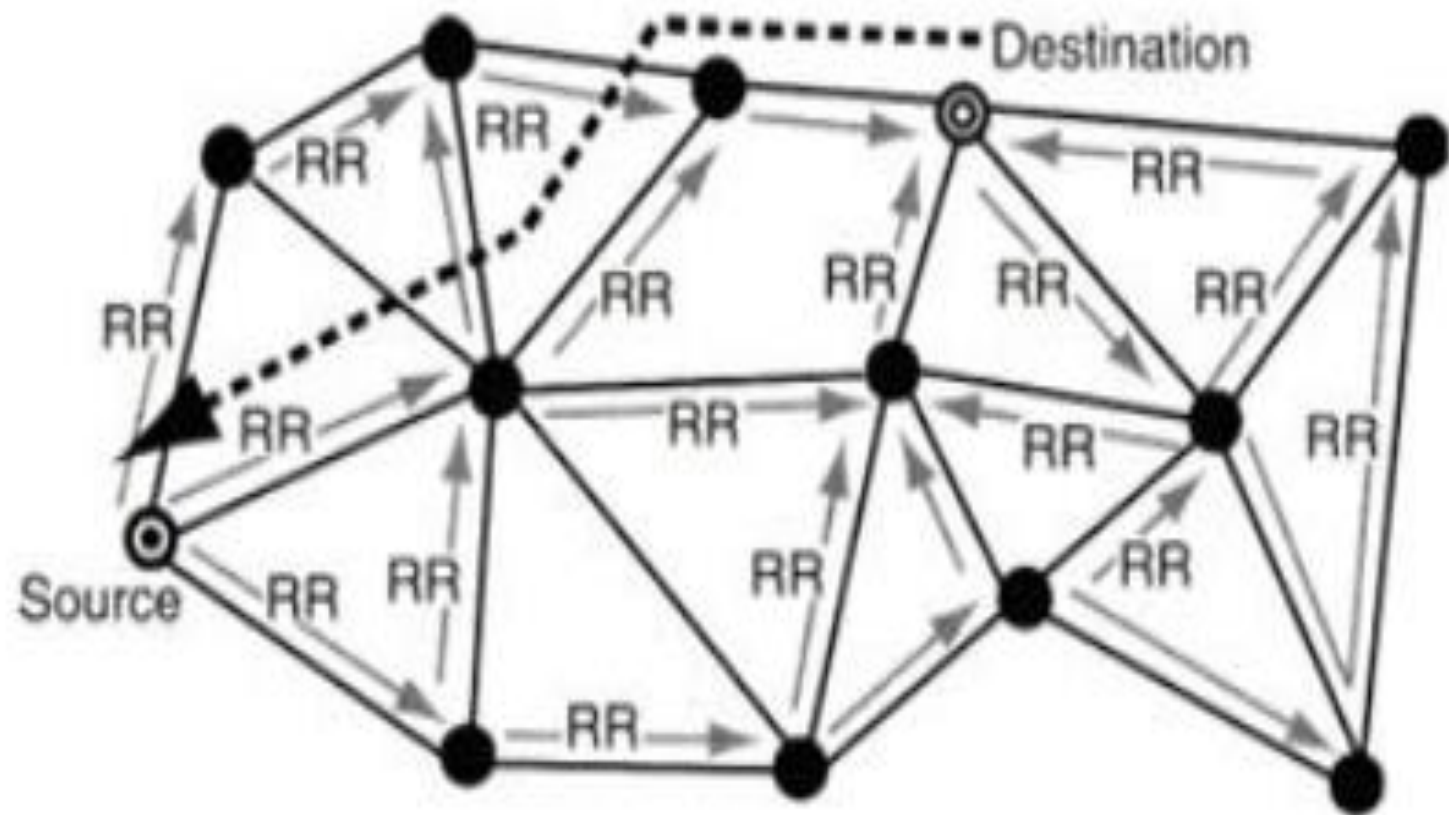
Les principaux protocoles proactifs

- OLSR (Optimized Link State Routing)
- FSR (Fisheye State Routing)
- TBRPF (Topology Broadcast Based on Reverse-path Forwarding)

3.1.2 Les protocoles réactifs

- Un protocole réactif ne calcule pas l'information topologique avant que celle-ci soit rendue nécessaire par la demande de route d'un paquet vers une destination par une application.
- La Figure suivante, illustre le fonctionnement des protocoles réactifs. La source envoie une requête en diffusion pour la recherche d'une route vers la destination ; la destination adresse en retour une réponse vers la source. Sur son chemin de retour, le paquet crée la route vers la destination.

cont



Les principaux protocoles réactifs

- AODV (Ad-Hoc On demand Distance Vector Routing)
- DSR (Dynamic Source Routing)

3.1.3 Les protocoles hybrides

- Ces protocoles, qui combinent les **modes proactif** et **réactif**, fonctionnent dans l'un ou l'autre mode suivant des conditions prédéfinies. Dans cette classe, on peut garder la connaissance locale de la topologie jusqu'à un **nombre prédéfini - a priori petit - de saut** par un échange périodique de paquets de contrôle, autrement dit par une technique proactive. Les routes vers **les nœuds plus lointains** sont obtenues par schéma réactif.
- Les principaux protocoles hybrides sont :
 1. ZRP (Zone Routing Protocol)
 2. CBRP (Cluster Based Routing Protocol)

4. Le protocole OLSR

- OLSR est un protocole de routage proactif pour les réseaux ad hoc qui utilise **un routage saut par saut** et une technique par état des liens pour déterminer dynamiquement les tables de routage.
- Il n'utilise que quelques nœuds, appelés **relais multipoint** (Multipoint Relays), pour diffuser les messages de contrôle.
- Le protocole fonctionne de façon **complètement distribuée** et ne dépend de ce fait d'aucune entité centrale.

4.1 Les relais multipoint

- L'idée des relais multipoint est de réduire l'overhead des messages d'inondation dans le réseau par la réduction des retransmissions inutiles lors de la diffusion générale d'un message.
- Chaque noeud dans le réseau choisit un ensemble de noeuds dans son voisinage symétrique à un saut qui peut retransmettre ses messages aux noeuds se trouvant à deux sauts.

MPRs

- Cet ensemble de nœuds choisis s'appelle "les relais multipoints" (MPRs) pour ce nœud.
- Les voisins du nœud N qui ne sont pas dans son ensemble des MPRs, reçoivent et traitent les messages à diffusion générale envoyés par N mais ne les retransmettent pas.
- Chaque nœud maintient des informations sur l'ensemble des voisins qui l'ont choisi comme MPR, cet ensemble s'appelle "le sélecteur de relais multipoint " (MPR selector set) d'un nœud. Un nœud obtient ces informations à partir des messages HELLO envoyés périodiquement par ses voisins.

4.2 Fonctionnement du protocole

4.2.1 Détection de voisinage

- Chaque nœud doit détecter les voisins avec qui, il a un lien symétrique direct. **L'incertitude** de la propagation radio peut rendre quelques liens asymétriques : **comment ?**
- Par conséquent, tous les liens doivent être testés dans les deux sens afin d'être considérés valides. **Comment ?**

Réponse

- Pour accomplir cela, chaque nœud diffuse périodiquement des messages HELLO qui contiennent l'information concernant ses voisins et leur type de lien, les messages HELLO sont reçus par tous les voisins à un saut mais ne sont pas relayés aux autres nœuds.

Exemple

A $\longrightarrow$ B (message vide)

B : (A est asymétrique)

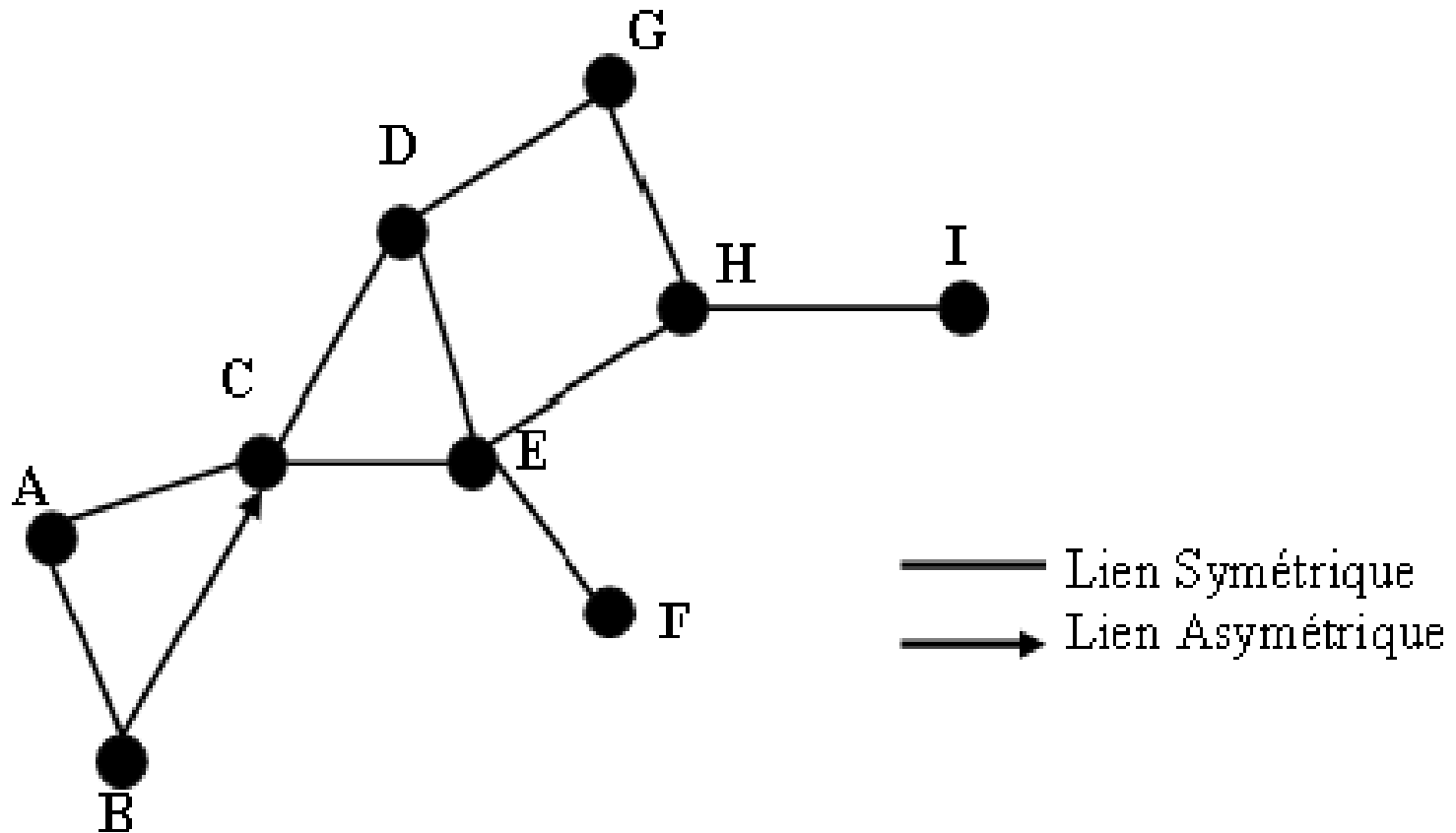
B $\longrightarrow$ A (A est asymétrique)

A : (B est symétrique)

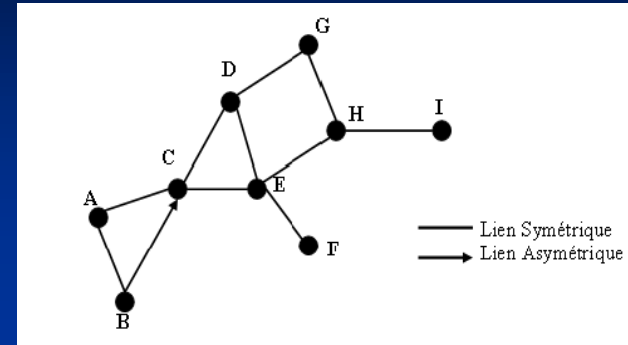
A $\longrightarrow$ B (B est symétrique)

B : (A est symétrique)

Exemple d'un réseau ad hoc déployé avec neuf nœuds, chaque nœud est équipé d'une seule interface réseau



Question 1 : La Table 5.1 montre les voisins du nœud C avec leurs types de liens



Nœus voisin	Statut
A	Symétrique
B	Asymétrique
D	Symétrique
E	Symétrique

Question 2 :

4.2.2 Sélection des relais multipoints

- Chaque nœud du réseau sélectionne indépendamment son ensemble de relais multipoint.
- Cet ensemble est calculé de manière à contenir un sous-ensemble de voisins à un saut qui couvre tous les voisins à deux sauts, c'est-à-dire : l'union des voisins des MPRs contient tous les voisins à deux sauts du nœud.
- L'ensemble de MPRs d'un nœud doit être optimal (**assez petit**) pour accomplir les avantages des MPRs.

Réponse :

Heuristique de calcul des relais multipoints

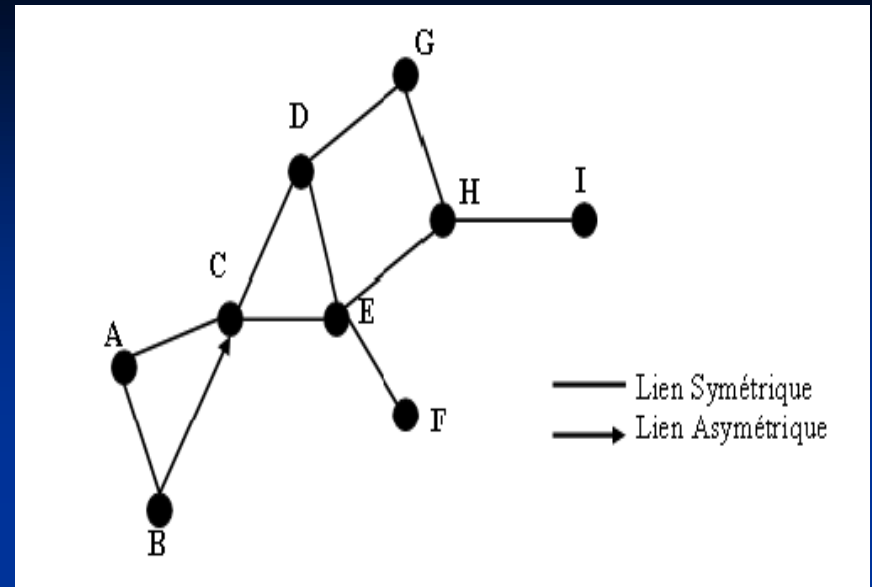
- TD et éventuellement TP ...

4.2.3 Gestion de la topologie

- Chaque nœud, qui a été choisi comme MPR, diffuse des messages de contrôle spécifiques appelés : messages de contrôle de topologie.
- Le message TC contient la liste des voisins qui ont sélectionné l'émetteur comme MPR.
- Construction de la table topologique pour chaque nœud.

- Si on considère que le résultat de processus d'élection des MPRs est le suivant :

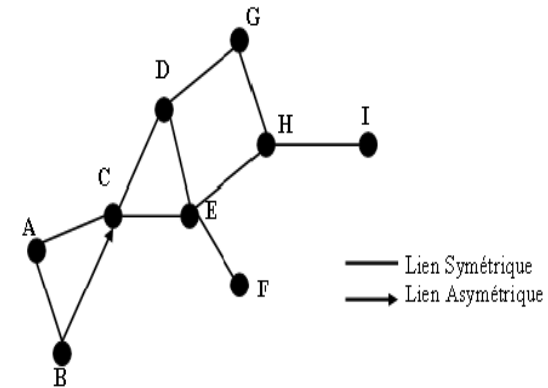
- $MPR(A)=\{C\}$
- $MPR(B)=\{A\}$
- $MPR(C)=\{D,E\}$
- $MPR(D)=\{C,E\}$
- $MPR(E)=\{C,H\}$
- $MPR(F)=\{E\}$
- $MPR(G)=\{H,D\}$
- $MPR(H)=\{E\}$
- $MPR(I)=\{H\}$



■ Question

- $MPR_Selector_Set(C) = \{?\}$
- $MPR_Selector_Set(D) = \{?\}$
- $MPR_Selector_Set(E) = \{?\}$
- $MPR_Selector_Set(H) = \{I\}$
- $MPR_Selector_Set(A) = \{?\}$

Table topologique du noeud C



Nœud destinataire	Nœud du dernier saut	Numéro de sé- quence	Temps de validité
G	D	N1	T1
D	E	N2	T2
F	E	N3	T3
H	E	N4	T4
E	H	N5	T5
I	H	N6	T6
G	H	N7	T7
B	A	N8	T8

4.2.4 Déclaration des interfaces multiples

- Périodiquement, les nœuds possédant plusieurs interfaces, diffusent dans tout le réseau un message MID contenant la liste des adresses des interfaces rattachées à ce nœud ainsi que l'adresse principale associée.
- Chaque nœud maintient un ensemble de tuples de la forme $(I_if_addr, I_main_addr, I_time)$ pour chaque destination possédant plus d'une seule interface qui sera détruite à l'expiration du I_time .

4.2.5 Gestion des sous réseaux

- Pour permettre l'accès à d'autres types de réseaux les **nœuds passerelles (?)** doivent déclarer ces associations via un autre type de message HNA (Host and Network Association) périodiquement.
- Chaque nœud dans le réseau MANET doit maintenir un ensemble de tuples :
(**A_gateway_addr, A_network_addr, A_netmask, A_time**)

4.2.6 Le calcul de la route

- Chaque nœud maintient une table de routage.
- Pour qu'un nœud source **S** arrive à voir le chemin vers une destination **R**, celui-ci doit avoir; premièrement une paire connectée de nœuds (**X;R**), puis la paire (**Y;X**), et ainsi de suite jusqu'à voir le nœud **Y** dans la table des voisins de la source.
- Chaque entrée dans la table de routage consiste en une adresse destinataire (**R_dest_addr**), adresse du saut suivant (**R_next_addr**) et le nombre de sauts (**R_dist**) qui sépare la source de la destination.

cont

- La table de routage est calculée en se basant sur la **table des voisins** et la **table topologique**, donc si l'une de ces tables a été modifiée, la table de routage sera recalculée.
- Notons que chaque noeud calcule indépendamment sa table de routage sans la génération d'aucun message dans le réseau ; il s'agit d'un simple re-calcule local.

Procedure

- Toutes les entrées de la table de routage sont supprimées.
- Tous les voisins symétriques à un saut seront insérés dans la table de routage avec une distance de 1 ($h = 1$).
- Boucle s'arrête lorsqu'il n'y a plus de nouvelles entrées à **ajouter** dans la table de routage

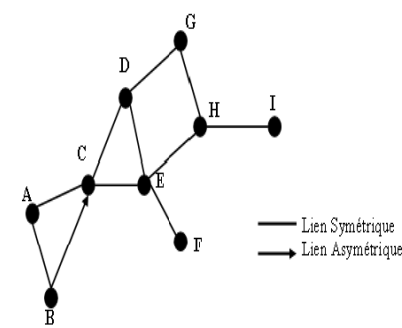
- Pour chaque destination à plus d'un saut ($h+1$), la procédure suivante est exécutée :
- Pour chaque entrée dans la table topologique, si l'adresse de destination ne correspond à aucune adresse de destination dans la table de routage *ET* l'adresse du last-hope node correspond à une adresse destination dans la table de routage avec une distance h , on insère une nouvelle entrée dans la table de routage telle que :
 - **R_dest_addr égale à dest_addr.**
 - **R_next_addr égale à R_next_addr dont le R_dest_addr est égale à l'adresse de lasthope.**
 - **R_dist = $h+1$.**

Nœud destinataire	Nœud du dernier saut	Numéro de sé- quence	Temps de validité
G	D	N1	T1

cont

- Par la suite, la table de routage est complétée par l'ensemble des associations des interfaces en ajoutant des entrées pour toutes les interfaces non présentes dans la table de routage mais dont l'adresse principale associée y figure déjà.
- Finalement, on termine par l'insertion des routes vers l'ensemble des associations des réseaux et les hôtes rattachés.

Table de routage du nœud C



Destination	Nœud suivant	Nombre de sauts	Interface
A	Directe	1	Interfac_C
D	Directe	1	Interfac_C
E	Directe	1	Interfac_C
B	A	2	Interfac_C
F	E	2	Interfac_C
G	D	2	Interfac_C
H	E	2	Interfac_C
I	E	3	Interfac_C

cont.

- Au fait, OLSR ne fait pas le routage des données lui-même, mais il se contente de mettre à jour la table de routage du noyau du système d'exploitation.
- Le routage se fait conformément aux spécifications du RFC1812.

Pratique

- Regarder le code source du protocole OLSR.

5. Le protocole AODV (Ad-Hoc On demand Distance Vector Routing)

- Comme tout protocole réactif, pour effectuer le routage, AODV exécute deux tâches : la création des routes et la maintenance de celles-ci.

5.1 Création de la route

1. Lorsqu'un noeud reçoit une demande d'une application pour une route vers une destination, il cherche d'abord à savoir s'il en possède une, si tel est le cas, le protocole n'a pas d'algorithme particulier à mettre en oeuvre. Dans le cas contraire, le noeud source diffuse une demande de route **RREQ** (Route REQuest).

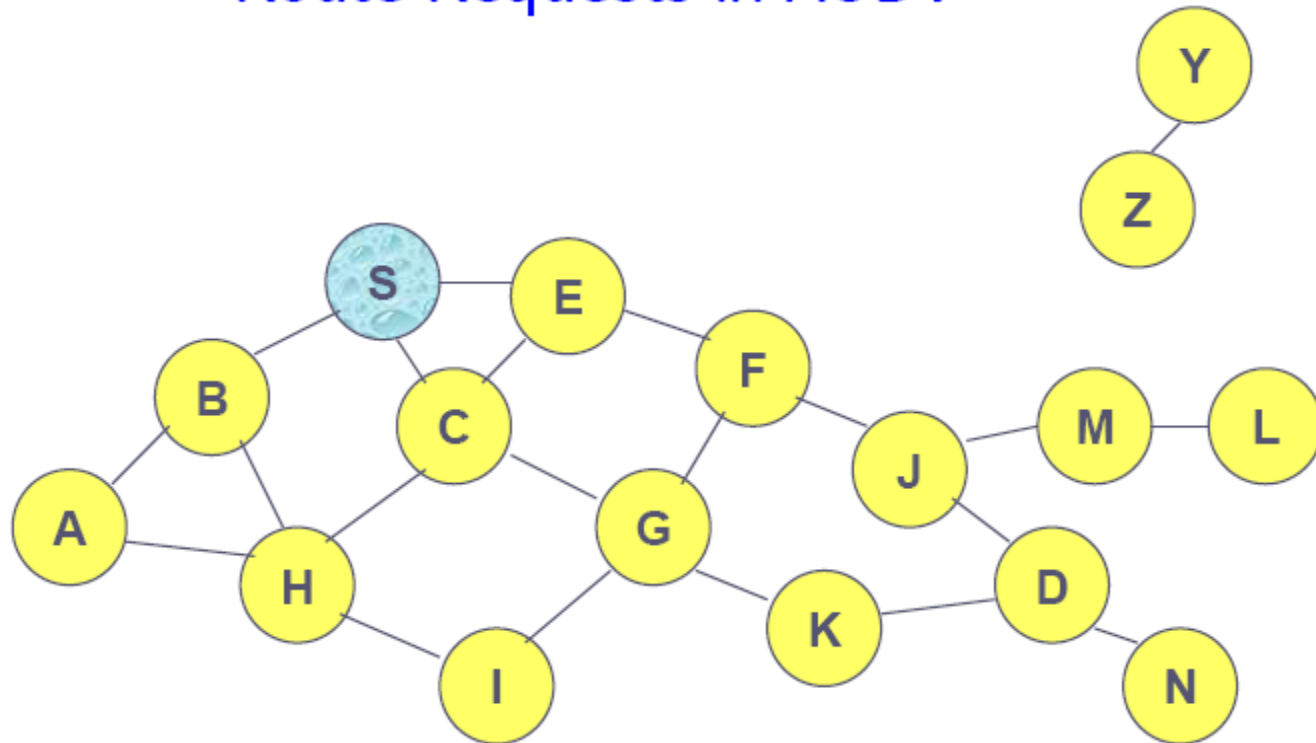
cont

2. Les nœuds qui reçoivent ces paquets les diffusent à leur tour jusqu'à atteindre la destination ou au moins un nœud qui possède une information de routage récente vers la destination recherchée.
3. Les nœuds situés sur le parcours de la requête de route conservent dans leur cache **l'adresse du nœud qui leur a relayé la requête RREQ**, cette information est utilisée lors du retour de la réponse '**RREP**' de demande de route pour permettre d'aiguiller cette réponse jusqu'à la source initiale.

5.2 Entretien des routes

- AODV incorpore un mécanisme pour signaler les ruptures de lien. Lorsque le nœud i repère la rupture d'un lien sur un trajet d'une route reliant une source S à une destination D , i envoie à S un paquet **RERR** (Route ERROR) d'erreur de route, cette dernière relance une nouvelle procédure de recherche de route.

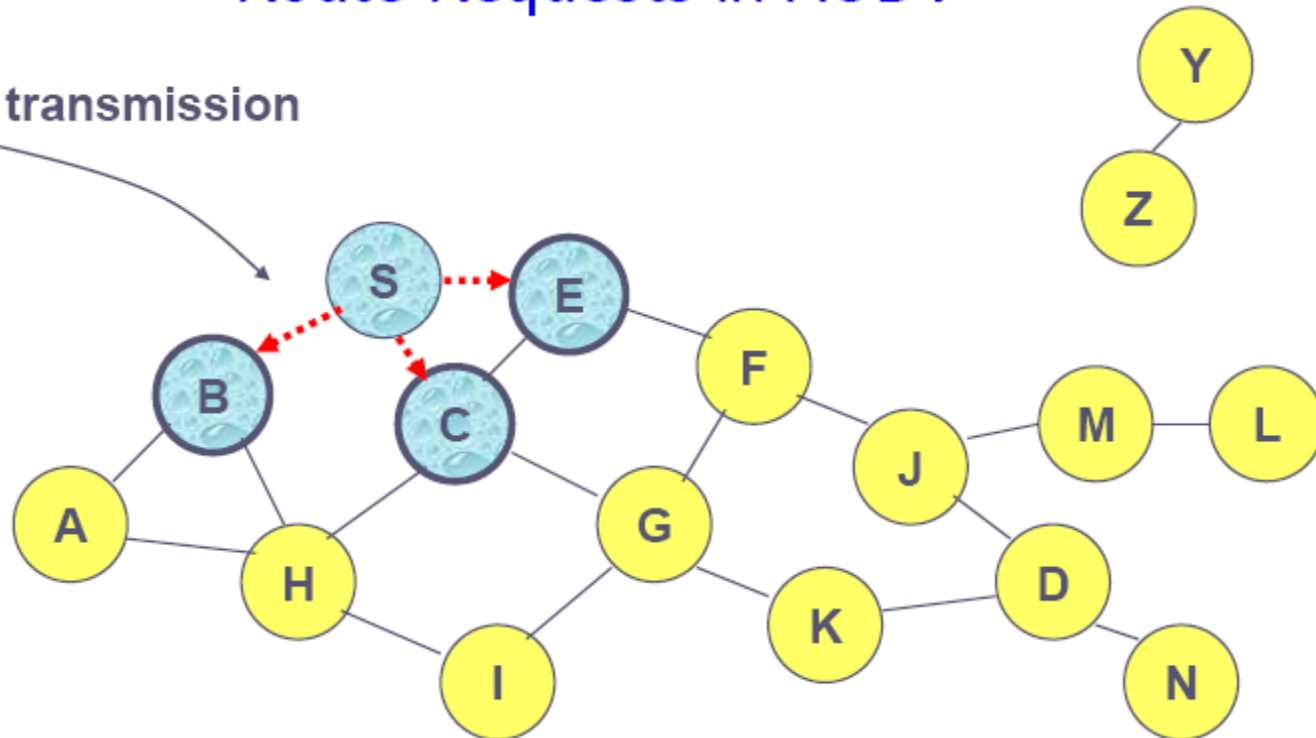
Route Requests in AODV



Represents a node that has received RREQ for D from S

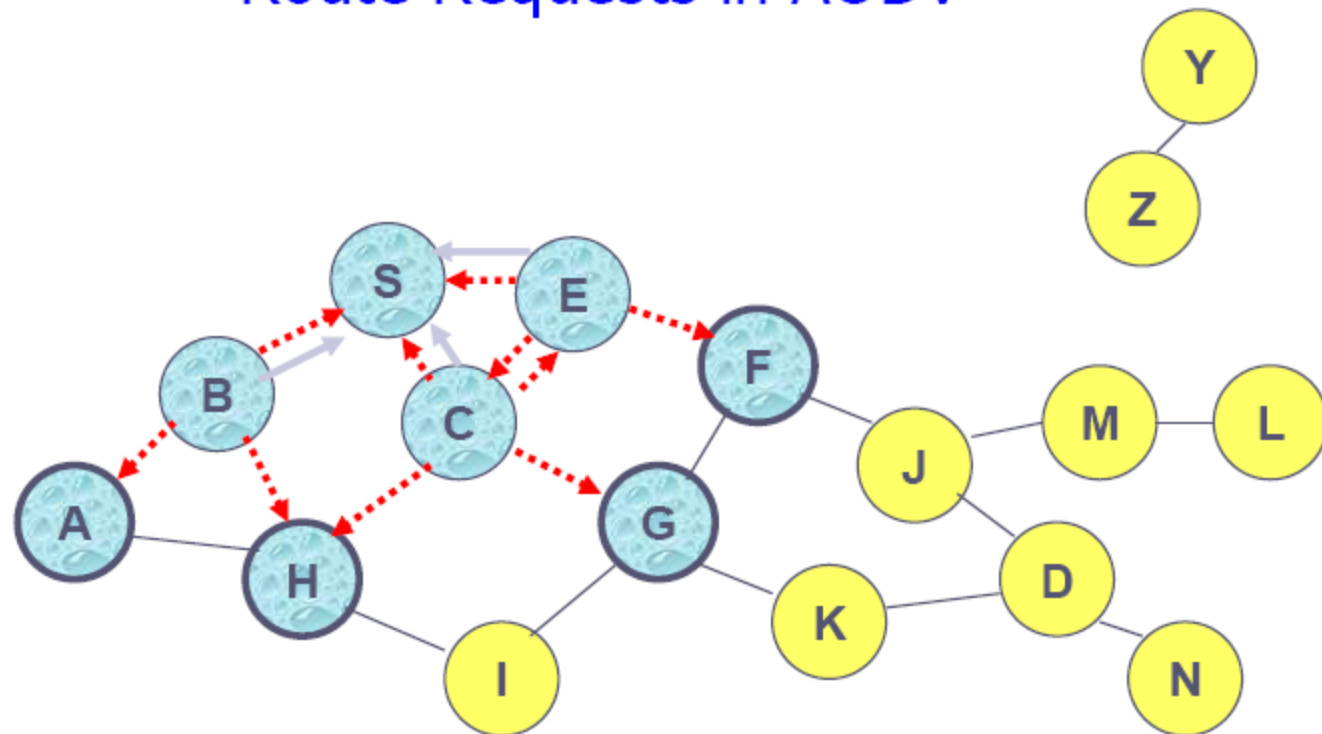
Route Requests in AODV

Broadcast transmission



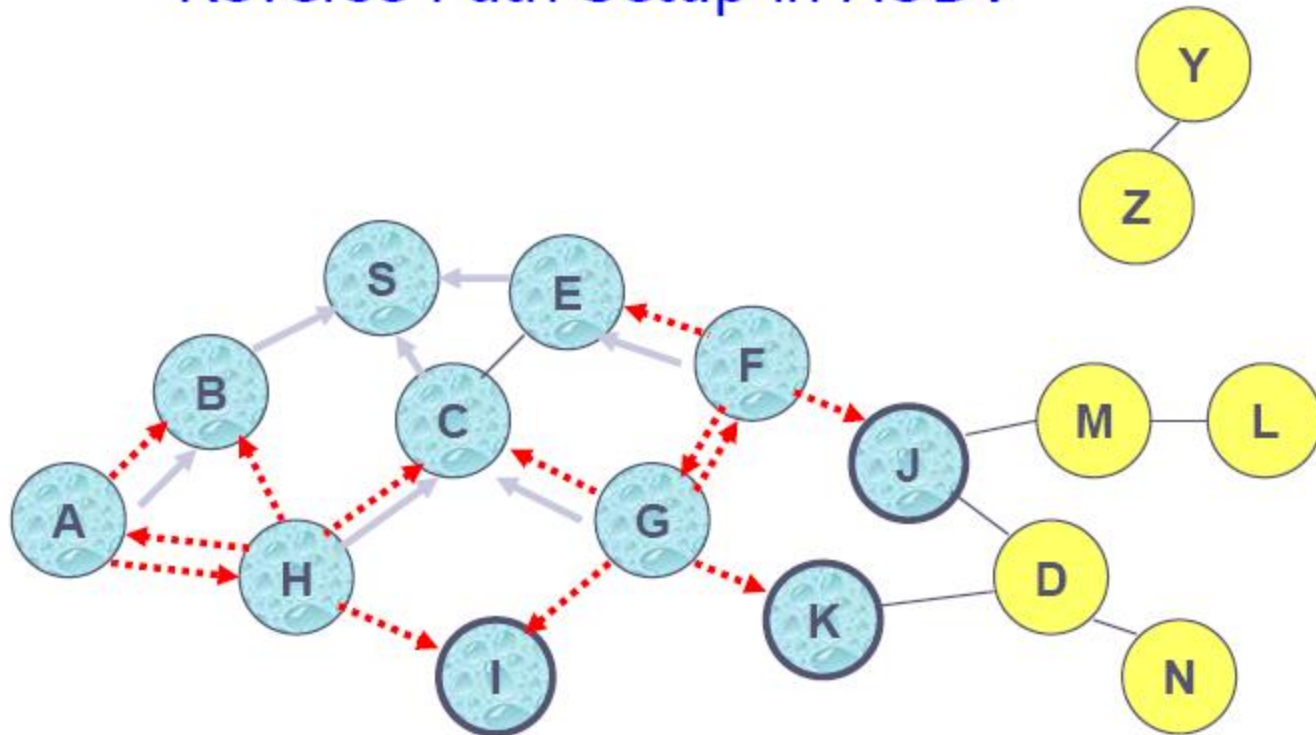
.....> Represents transmission of RREQ

Route Requests in AODV



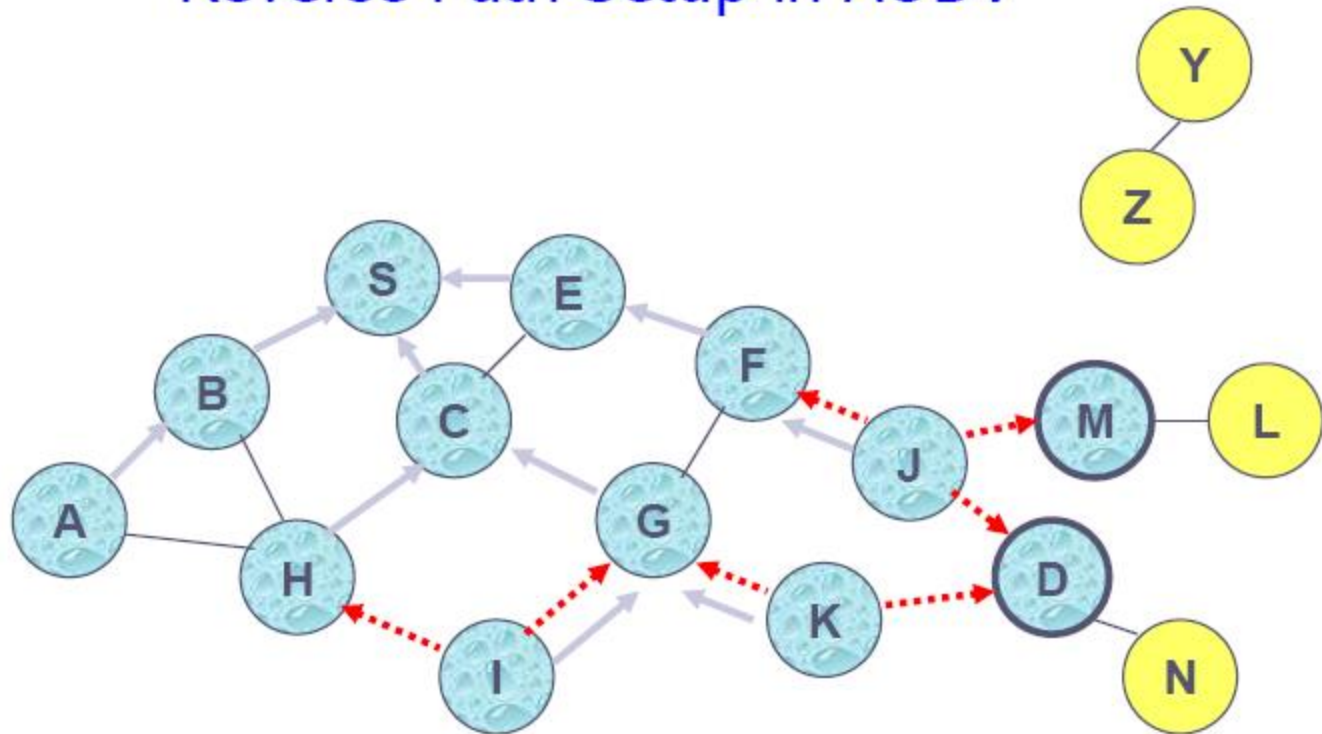
← Represents links on Reverse Path

Reverse Path Setup in AODV

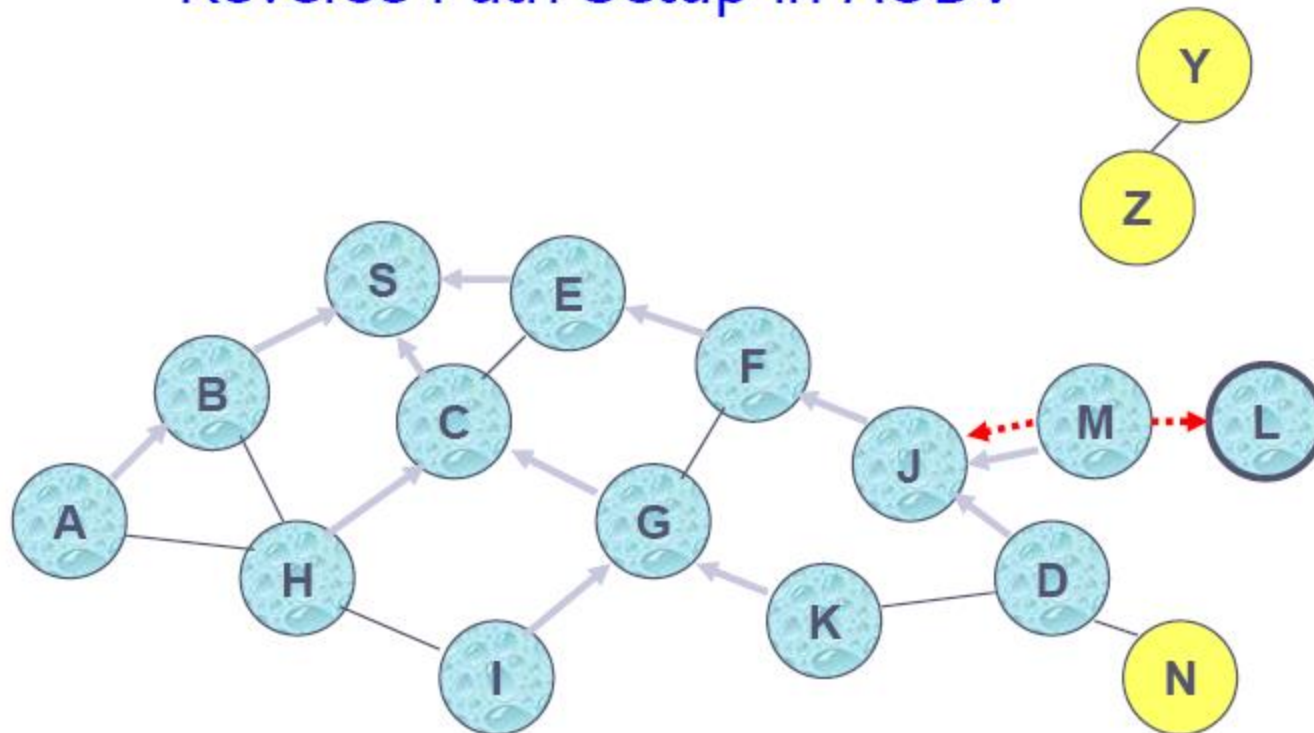


- Node C receives RREQ from G and H, but does not forward it again, because node C has **already forwarded RREQ** once

Reverse Path Setup in AODV

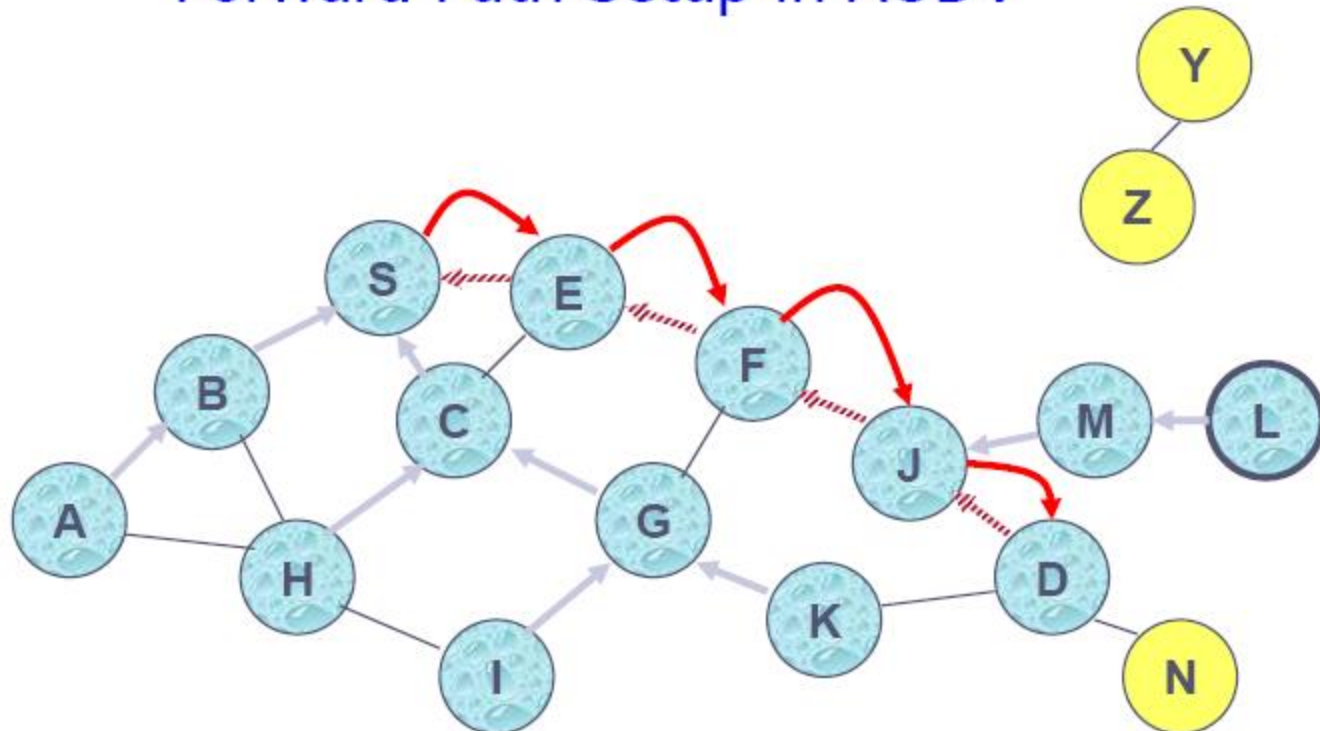


Reverse Path Setup in AODV



- Node D **does not forward** RREQ, because node D is the **intended target** of the RREQ

Forward Path Setup in AODV



Forward links are setup when RREP travels along the reverse path



Represents a link on the forward path

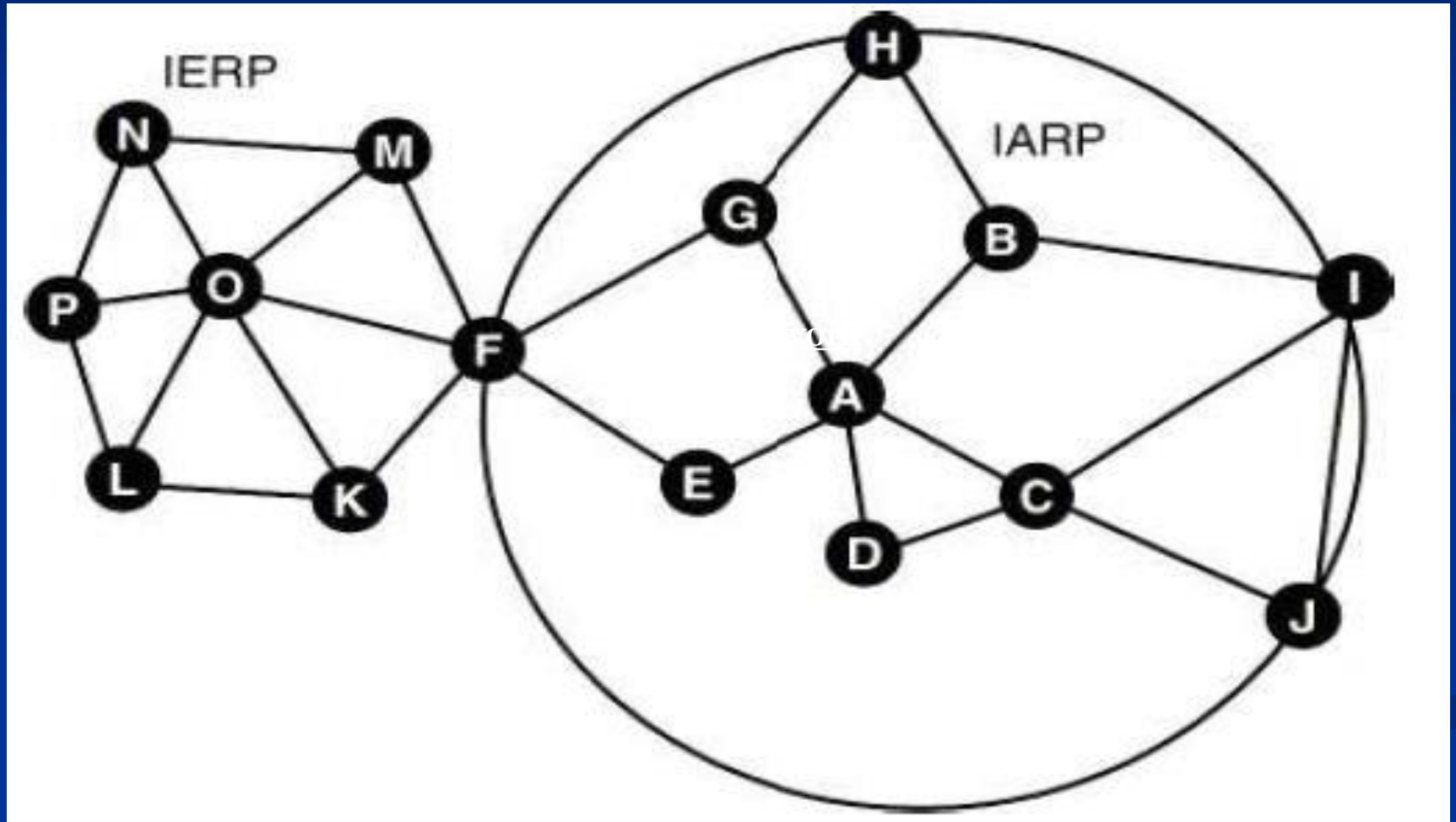
AODV: Résumé

- **Il n'est pas nécessaire d'inclure les routes dans les paquets de données**
- **Les noeuds maintiennent des tables de routage contenant des entrées uniquement pour les routes en utilisation active**
- **Au plus un seul next-hop par destination maintenu à chaque noeud**
 - DSR pourrait maintenir plusieurs routes pour une seule destination
- **Les "Sequence numbers" sont utilisés pour éviter les anciennes et obsolètes routes**
- **Les "Sequence numbers" évitent la formation de boucles**
- **Les routes non-utilisées expirent même si la topologie ne change pas**

6. Le protocole ZRP (Zone Routing Protocol)

- ZRP est un protocole hybride où chaque nœud ZRP définit une zone de routage, qui inclut tous les nœuds dont la distance minimale à ce nœud est x .
- Les nœuds qui sont exactement à la distance x sont appelés nœuds périphériques.
- Pour trouver une route vers des nœuds situés à une distance supérieure à x , ZRP utilise un système réactif, qui envoie une requête à tous les nœuds périphériques.
- ZRP met pour cela deux types de fonctionnement : IARP (IntraZone Routing Protocol) et IERP (InterZone Routing Protocol).

Example



802.11s

- **L'Amendement 802.11s.**
- **Objectif :** Définit comment les dispositifs sans fil peuvent créer un réseau maillé (mesh).
- Permet des topologies fixes (stations) et des réseaux ad hoc (mobiles).
- Des distributions Linux comme OpenWrt et des systèmes comme Google Wifi et certaines Freebox intègrent le support 802.11s

802.11 New

- 802.11ax (Wifi6) Optimisé pour la densité d'appareils, utilise OFDMA, MU-MIMO, et la bande 6 GHz (Wi-Fi 6E) pour des débits très élevés.
- 802.11be (Wifi7) Le standard le plus récent (publié en 2024/2025), promet des débits multi-gigabits, utilise les bandes 2.4, 5 et 6 GHz, et intègre des technologies comme le MLO (Multi-Link Operation) et des canaux plus larges.
- La sécurité (WPA3)

802.11 Recherche Académique

- ACM
- IEEE.
- Science Directe.
- Springer.
- arXiv.