Réseaux Mobiles Ad hoc

Yacine Challal

Références

- **Sridhar Iyer Tutorial at CIT'2000**
- **Nitin Vaidya's MobiCom'2000 tutorial**
- **Camille Diou LICM, Université de Metz**
- **Mawloud Omar,**
- **Boushra Alkubeily**

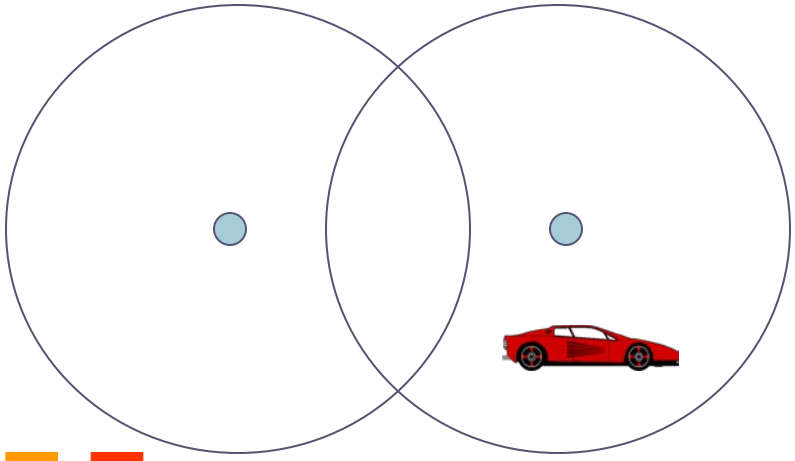
Introduction

- **Réseaux à base d'infrastructure**
  - Réseaux filaires
  - Réseaux cellulaires (Stations de base)

- **Ad hoc Networks**
  - Utiles lorsque l'infrastructure n'est pas disponible, impraticable, ou coûte très chère
  - Applications militaires, opérations de sauvetage, home networking

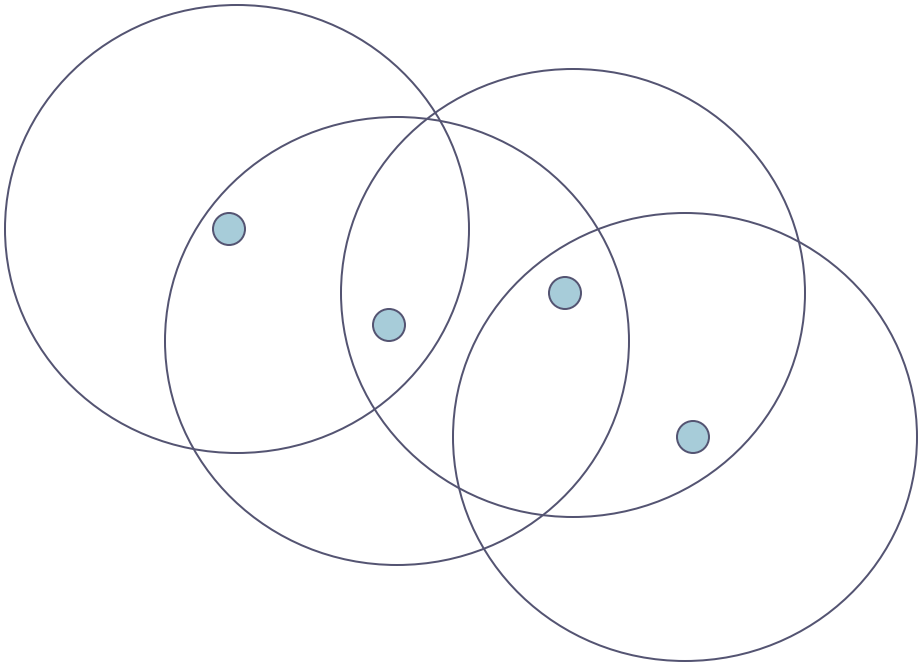
Cellular Wireless

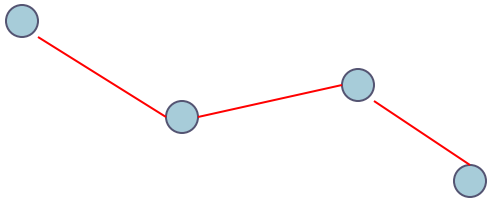
- **Connectivité à 1 seul saut sans fil au réseau filaire**
  - Espace divisé en cellules
  - Une station de base est responsible de communiquer avec les noeuds dans la cellule
  - Les noeuds mobiles peuvent changer de cellule durant la communication
  - Un Hand-off a lieu quand un mobile commence la communication via une nouvelle satation de base



Multi-Hop Wireless

- **Nécessité de traverser plusieurs liens avant d'atteindre la destination**

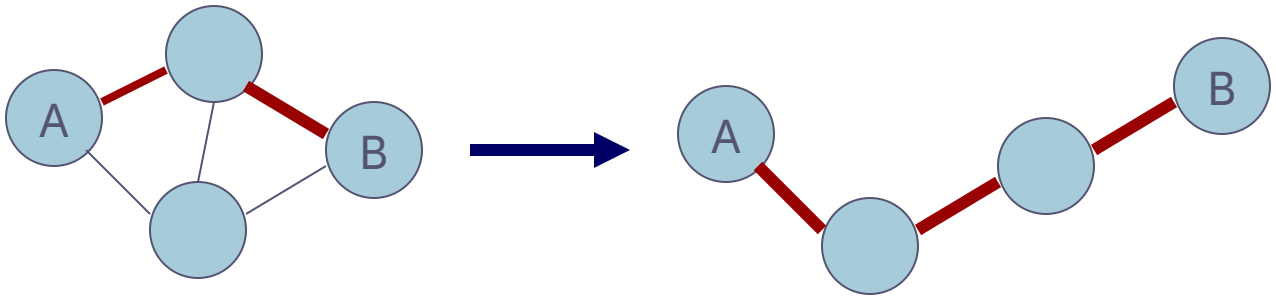




- **La mobilité cause le changement de routes**

Mobile Ad Hoc Networks (MANET)

- **Mouvement fréquent des noeuds**
- **Changement fréquent de la topologie**



- **Pas d'infrastructure cellulaire. Liens sans fils multi-sauts.**
- **Les données doivent être routées via des noeuds intermédiaires.**

Pourquoi MANET ?

- **Il n'est pas toujours possible d'installer des points d'accès ou une infrastructure d'accès (backbone)**
  - Une infrastructure peut ne pas exister suite à une catastrophe ou dans une zone de bataille
  - Une infrastructure peut ne pas être pratique pour des portées radios limitées; Bluetooth (range ~ 10m)

- **Ad hoc networks:**
  - Aucune infrastructure n'est nécessaire
  - Faciles à déployer
  - Utils lorsque l' infrastructure est absente, détruite ou impraticable

Plusieurs Applications

- **Personal area networking (PAN)**
  - cell phone, laptop, ear phone, etc.
- **Environments militaires**
  - soldats, chars, avions
- **Environments civils**
  - Réseau de taxi
  - meeting rooms
  - Réseaux de capteurs (à nuancer)
- **Opérations de secours**
  - Recherche et sauvetage
  - Extinction de feux de forêts

Challenges dans les Environnements Mobiles

- **Limitations du réseau sans fils**
  - Perte de paquets due aux erreurs de transmission
  - Capacité des liens variable
  - Déconnexions / partitionnements fréquents
  - Bande passante limitée
  - Nature broadcast des communications

- **Limitations dues à la mobilité**
  - Changement dynamiques des topologies et des routes
  - Pas de prise en compte de la mobilité par les apllications

- **Limitations du noeud Mobile**
  - Durée de vie limitée de la batterie
  - Capacités limitées (calcul, stockage, etc.)

IEEE 802.11

Introduction

- **1990: groupe IEEE 802.11**
- **1997: standard IEEE 802.11**
- **1 couche MAC, 3 couches physiques:**
- **Norme d'interopérabilité:**
  - WiFi (Wireless Fidelity) délivré par le WECA (Wireless Ethernet Compatibility Alliance)

IEEE 802.11 : normalisation des WLAN

Norme d'interopérabilité du WECA

Technologie Apple

Architecture

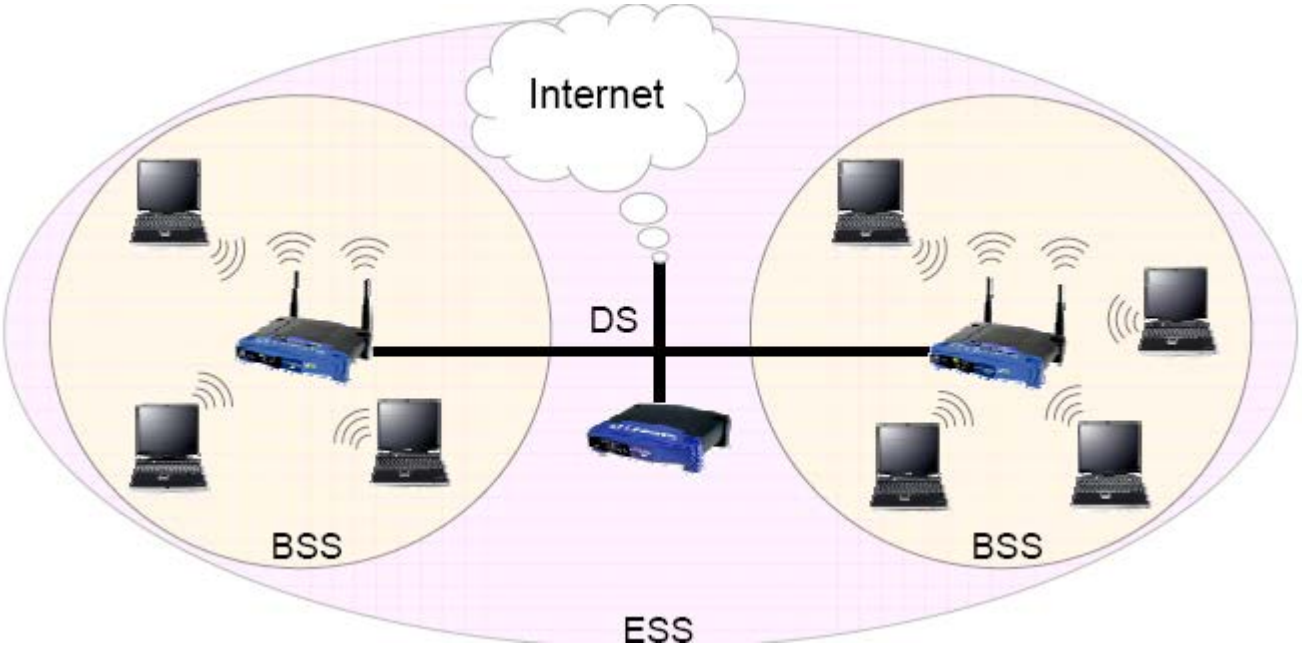
- **Architecture cellulaire**
  - Similaire à la téléphonie mobile: téléphones + stations
  - Un ou plusieurs points d'accès: unifier le réseau et servir de pont
  - ➔ cellule
- **Deux types de topologies**
  - Mode infra-structure
    - ✓ BSS: Basic Service Set
    - ✓ ESS: Extended Service Set
  - Mode ad-hoc
    - ✓ IBSS: Independent Basic Service Set

Le mode infrastructure: BSS

- **Le mode infrastructure désigne un réseau composé d'une infrastructure permettant l'échange d'information entre les stations: l'infrastructure est le point d'accès**
- **1 cellule = 1 Basic Service Set (BSS) = 1 point d'accès**
- **100 stations: support partagé entre toutes les stations, ainsi que le débit (11 Mbits/s)**

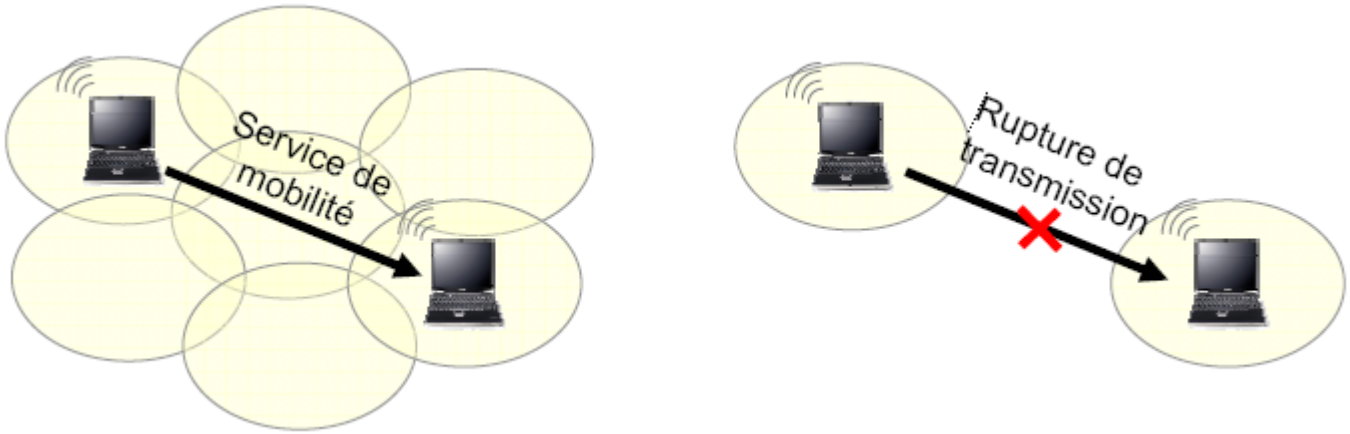
Le mode infrastructure : ESS

- **Extended Service Set: plusieurs points d'accès (BSS) connectés entre eux par un système de distribution (DS)**
- **DS: Ethernet ou un autre réseau LAN**
- **Fourniture d'accès vers un autre réseau: Internet**



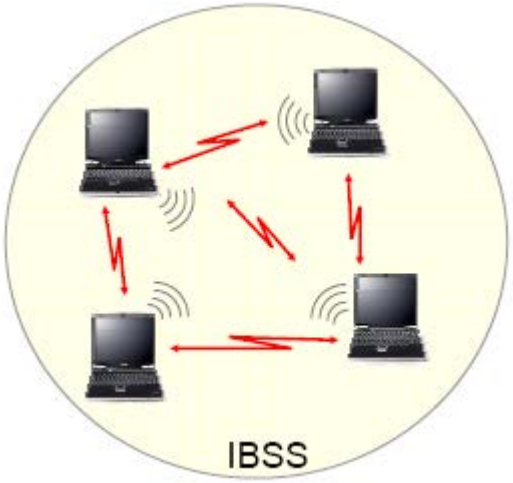
Le mode infrastructure: ESS

- **Topologie ESS variable: cellules recouvrantes ou non**
- **Les cellules recouvrantes permettent d'offrir le service de mobilité (IEEE 802.11f): pas de pertes de connexions**
- **Plus grand nombre d'utilisateurs possibles sans dégradation trop importante des performances**



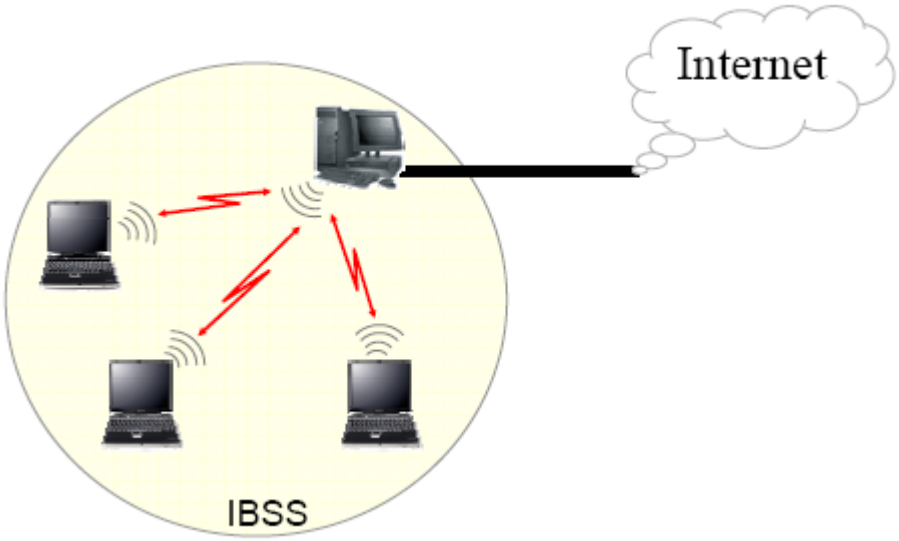
Le mode ad-hoc: IBSS

- **Independent Basic Service Set: mode point à point**
- **Permet l'échange d'informations lorsque aucun point d'accès n'est disponible**



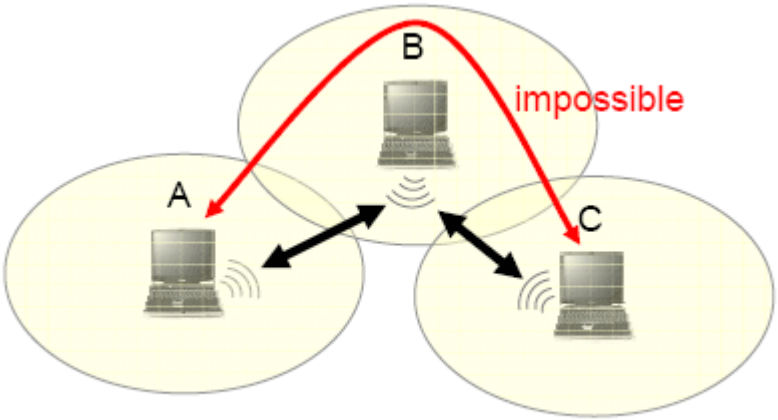
Le mode ad-hoc IBSS

- **Une station peut partager un accès à Internet: le réseau fonctionne comme un BSS**



Le mode ad-hoc IBSS

- **3 stations en mode ad-hoc: différent d'un réseau ad-hoc de trois stations**
- **Il n'y a pas de protocole de routage: A ne peut pas envoyer de données à C car B ne peut effectuer le routage**



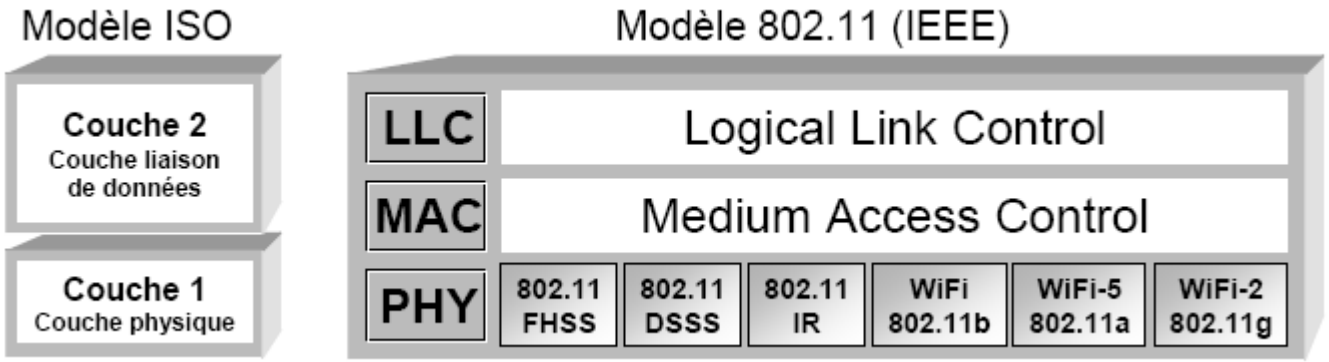
3 stations en mode ad-hoc

Réseaux ad-hoc et routage

- **Le protocole de routage doit être présent dans chaque nœud**
- **Cas le plus classique: nœuds intermédiaires dotés de tables de routages optimisées**
- **Protocoles de routage ad-hoc:**
  - Protocoles réactifs
  - Protocoles proactifs
  - Protocoles hybrides

Architecture de 802.11 (IEEE)

- **Modèle IEEE: couche liaison de données subdivisée en deux sous-couches MAC et LLC**
- **Couche MAC commune à toutes les couches physiques**

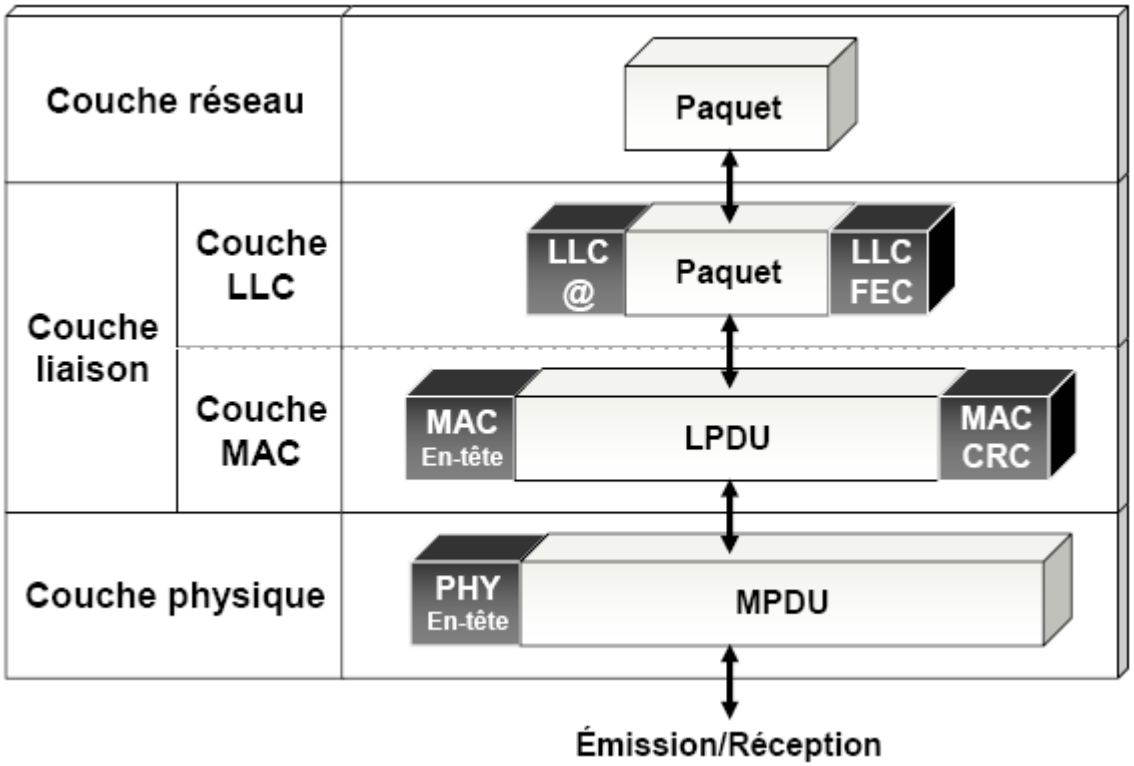


Couche Physique

- **Encodage des données et modulation**
  - Différentes techniques de modulation
  - Différentes bandes de fréquence
  - Différents débits
  - Différentes qualité de transmission
- **Écoute du support**

La couche liaison de données

- **Sous couche LLC**
  - Définie par IEEE 802.2
  - contrôle de flux
  - Reprise sur erre



La couche liaison de données

- **La sous couche MAC**
  - Fonctionnalités
    - ✓ Contrôle d'accès au support
    - ✓ Adressage et formatage des trames
    - ✓ Contrôle d'erreur par CRC
    - ✓ Fragmentation et réassemblage
    - ✓ Qualité de service
    - ✓ Gestion de l'énergie
    - ✓ Gestion de la mobilité
    - ✓ Sécurité
  - Deux méthodes d'accès
    - ✓ DCF (Distributed Coordination Function): avec contention, support de données asynchrones, chances égales d'accès au support, collisions
    - ✓ PCF (Point Coordination Function): sans contention, pas de collisions, transmission de données isochrones (applications temps-réel, voix, vidéo)

Problématique de l'accès au support radio

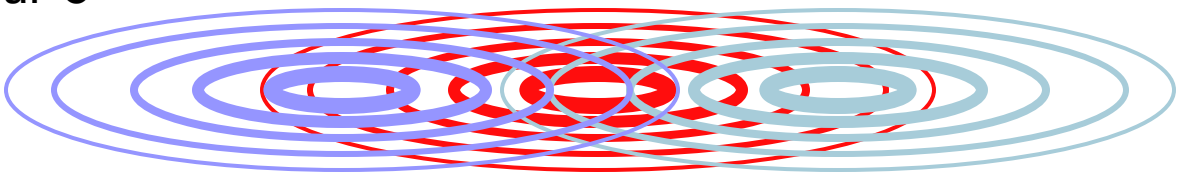
- **Est ce qu'on peut appliquer les méthodes d'accès des réseaux filaires?**

- **Exemple CSMA/CD**
  - **C**arrier **S**ense **M**ultiple **A**ccess with **C**ollision **D**etection
  - Envoyer dès que le support est libre, écouter pour détecter d'éventuelle collision (IEEE 802.3)

- **Problème d'accès au support dans les réseaux sans fils**
  - La force du signal décroit avec le carré de la distance
  - L'emetteur peut appliquer le CS et CD, mais les collisions ont lieu au niveau du récepteur
  - L'émetteur peut ne pas écouter la collision, i.e., CD ne fonctionne pas
  - Le CS peut ne pas fonctionner si un terminal est "caché"

Noeuds cachés et exposés

- **Terminaux cachés**
  - A envoie à B, C ne peut pas recevoir de A
  - C veut envoyer à B, C detecte que le support est libre (CS ne fonctionne pas)
  - collision au niveau de B, A ne peut recevoir la collision (CD ne fonctionne pas)
  - A est “caché” pour C



A B C

- **Terminaux exposés**
  - B envoie à A, C veut envoyer à une autre terminal (pas A ou B)
  - C écoute la porteuse, détecte que le support est occupé et attend
  - A étant en dehors de la portée radio de C, donc l’attente de C est inutile
  - C est “exposé” à B

Multiple Access with Collision Avoidance (MA/CA) [Karn90]

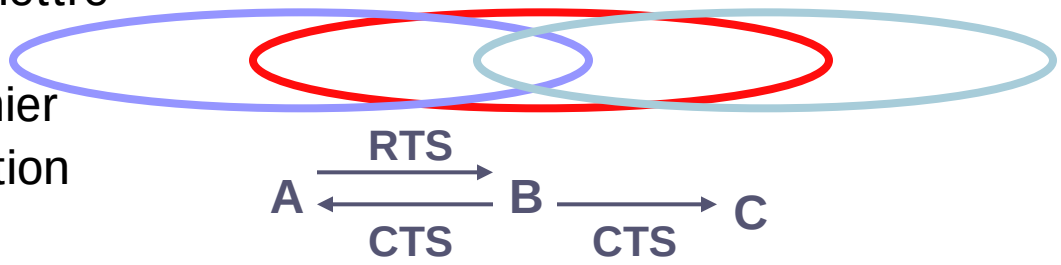
- **MACA utilise une signalisation pour éviter les collisions**
  - RTS (request to send)
    - ✓ L'émetteur demande le droit de transmettre avec un petit paquet RTS avant d'envoyer un paquet de données
  - CTS (clear to send)
    - ✓ Le récepteur donne le droit de transmettre dès qu'il peut recevoir

- **Le paquet de signalisation contient**
  - Adresse de l'émetteur
  - Adresse du récepteur
  - Taille du paquet

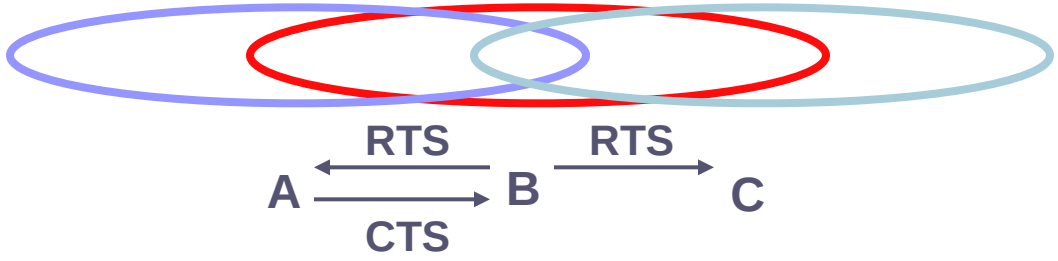
- **Variante de cette methode est utilisée dans IEEE 802.11 (CSMA/CA)**

MACA Solutions [Karn90]

- **MACA permet d'éviter le problème de la station cachée**
  - A et C veulent transmettre à B
  - A envoie RTS le premier
  - C attend après reception de CTS de B



- **MACA permet d'éviter le problème de la station exposée**
  - B veut transmettre à A, C à un autre terminal
  - C n'a pas à attendre il ne peut pas recevoir CTS de A



MAC: Fiabilité

- **Les liens sans fils sont victimes d'erreurs. Un taux élevé de perte de paquet dégrade les performances de la couche transport.**

- **Solution: Usage d'acquittement**
  - Quand B reçois un paquet de données de A, B renvoie un acquittement (Ack).
  - Si A ne reçois pas un Ack, il retransmet le paquet

Distributed Coordination Function

- **DCF**
  - Méthode d'accès générale pour le transfert de données asynchrones, sans gestion de priorité
  - Repose sur le CSMA/CA
- **CSMA/CA: Carrier Sense Multiple Access / Collisions Avoidance**
  - Accès aléatoire avec écoute de la porteuse: évite plusieurs transmissions simultanées, réduit le nombre de collisions
  - Impossible de détecter les collisions: il faut les éviter
    - ✓ Écoute du support
    - ✓ Back-off
    - ✓ Réservation
    - ✓ Trames d'acquittement positif

Distributed Coordination Function

- **L'écoute du support**
  - Couche physique
    - ✓ Détecte et analyse les trames
  - Couche MAC
    - ✓ Réserve le support
    - ✓ Deux types de mécanismes

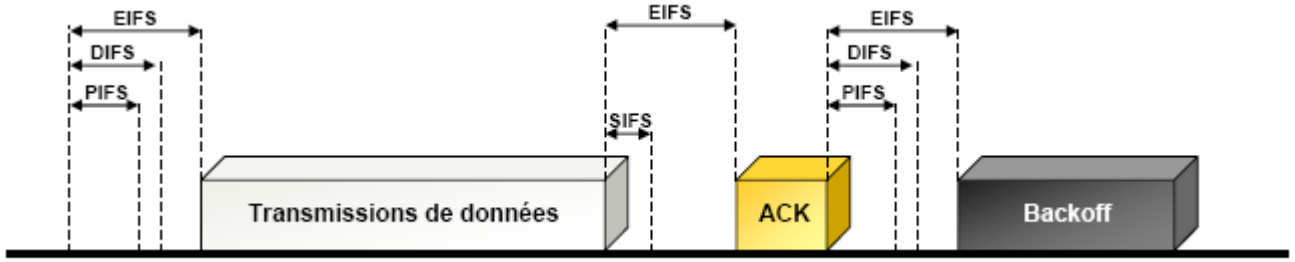
      Réservation par trames RTS/CTS

      - Optionnelle: trames RTC/CTS à 1 Mbps font chuter le débit moyen de 11Mbps à 6Mbps.

      Utilisation d'un timer (NAV: Network Allocation Vector) calculé par toutes les stations à l'écoute de la trame transmise par la source

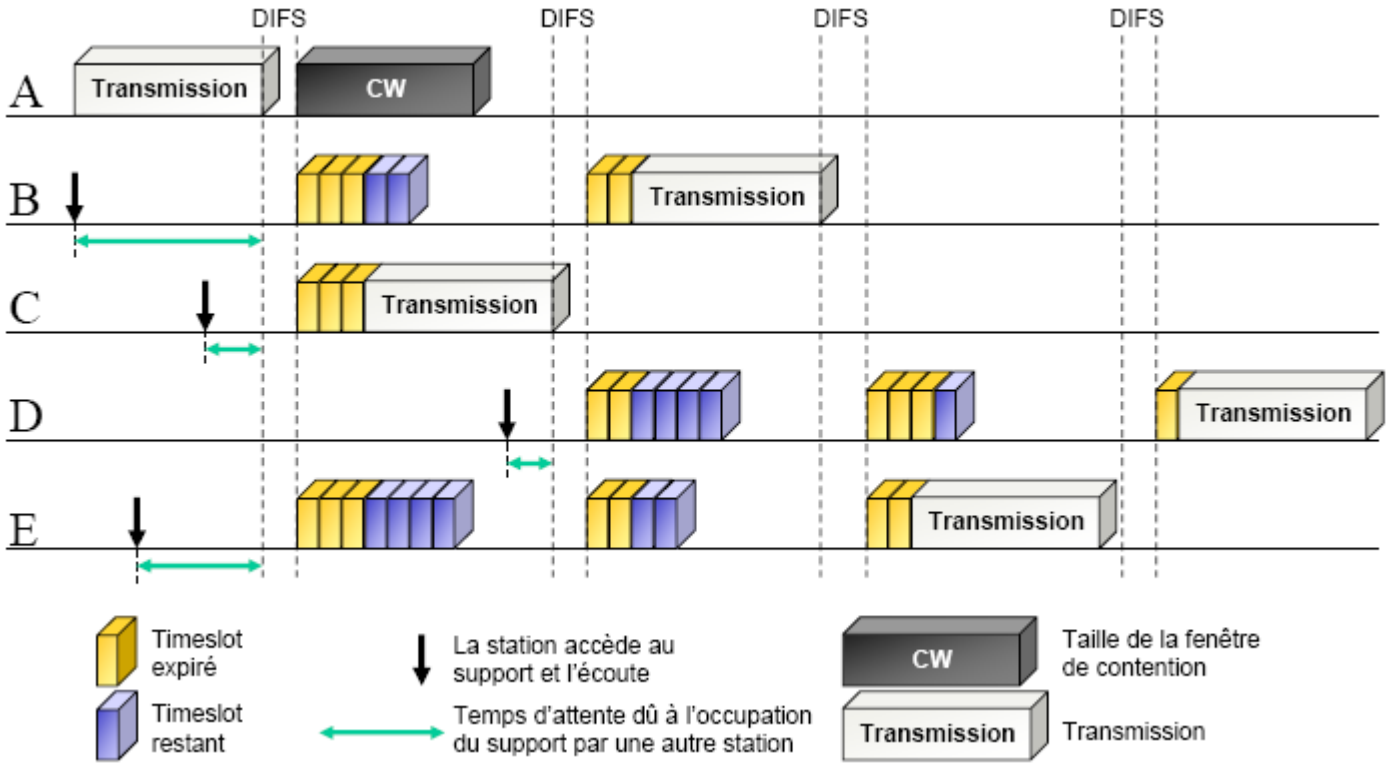
Distributed Coordination Function

- **L'accès au support**
  - Mécanisme d'éspacement entre deux trames: IFS
  - 4 types d'Inter-Frame Spacing
    - ✓ SIFS: Short IFS: sépare les différentes trames d'un même dialogue (données et ACK, RTS, CTS, différents fragments d'une trame segmentée, trame de polling en mode PCF)
    - ✓ PIFS: PCF IFS= SIFS + 1 timeslot: accès prioritaire, mode PCF
    - ✓ DIFS: DCF IFS=SIFS + 2 timeslots: mode DCF
    - ✓ EIFS: Extended IFS: le plus long, uniquement en mode DCF, lorsqu'une trame de données est erronée attente de l'acquittement



Distributed Coordination Function

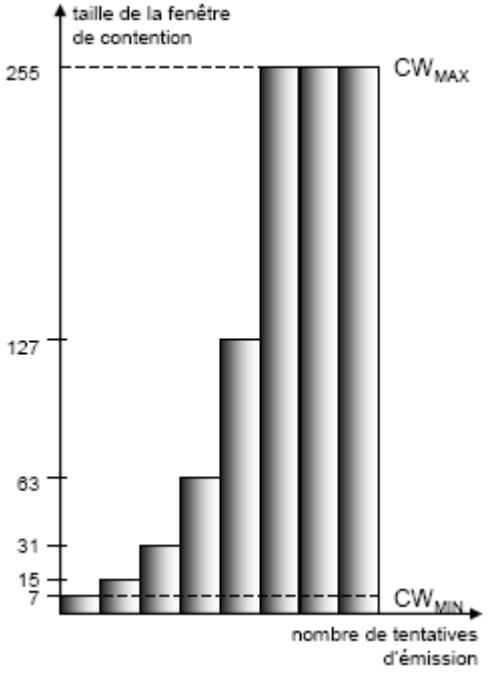
- **Le backoff**
  - Fenêtre de contention CW, et un timer Tbackoff=random(0, CW)xtimeslot



Distributed Coordination Function

La contention

- En cas de collision la fenêtre de contention CW est doublée
  - ✓ Le tirage au sort de la durée d'attente s'effectue sur un intervalle plus grand
  - ✓ Deux stations qui sont entrées en collision ont une probablité plus faible mais non nulle d'entrer à nouveau en collision
  - ✓ Ième tentative de transmission:

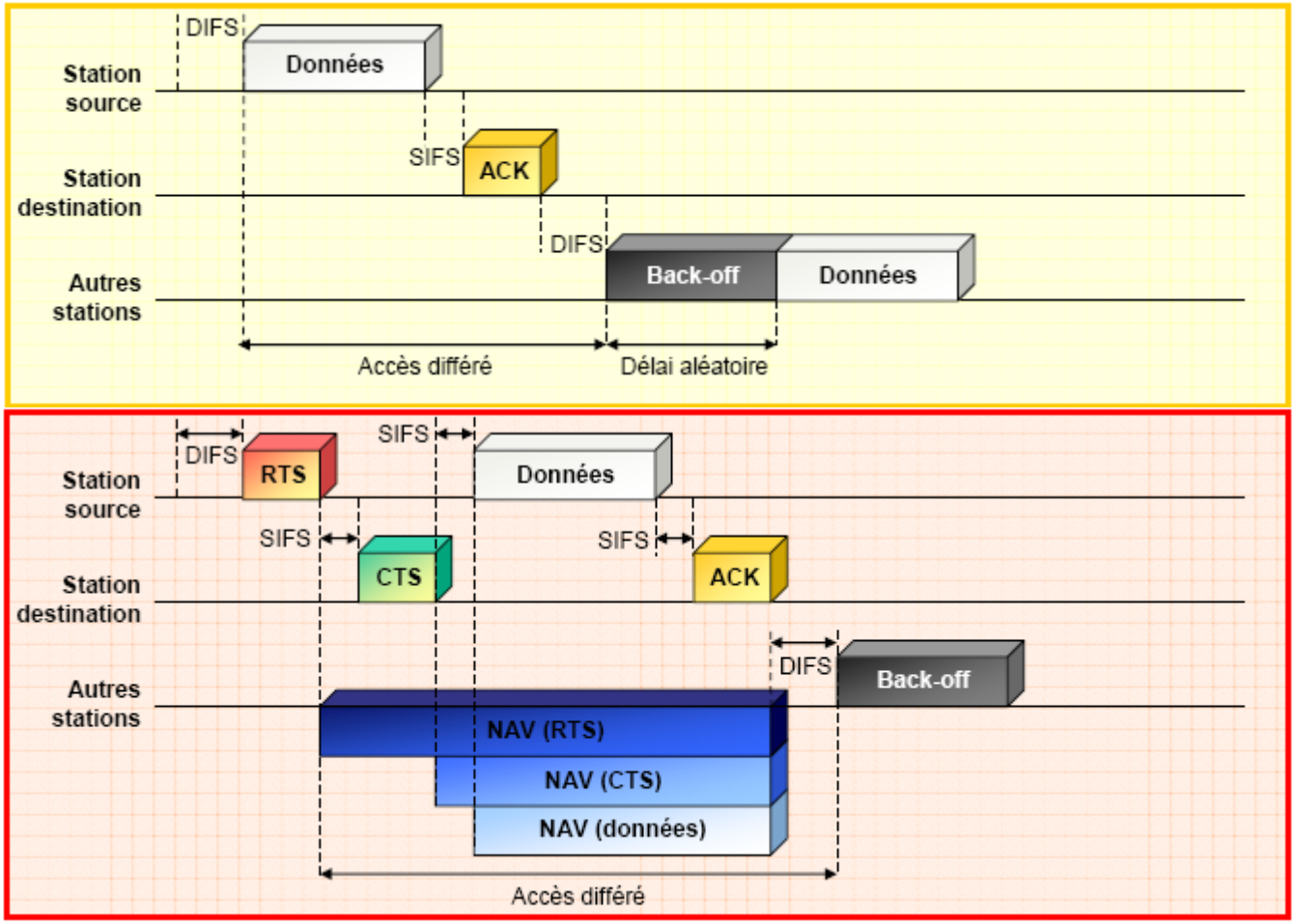


$$T_{backoff}(i) = random(0, CW_i) \times timeslot$$

$$CW_i = 2^{k+i} - 1$$

Distributed Coordination Function

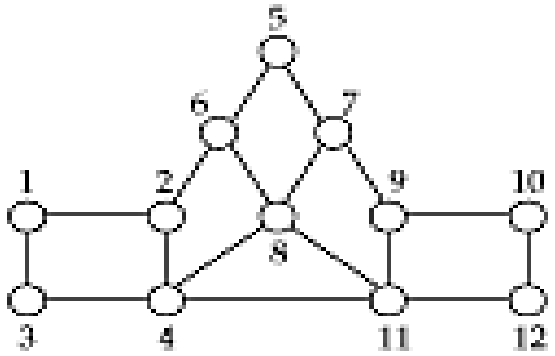
- **Exemples de transmissions**



PROTOCOLES DE ROUTAGE DANS MANET

Routage traditionnel

- **Un protocole de routage construit une table de routage dans chaque routeur**



ROUTING TABLE AT 1

Destination	Next hop	Destination	Next hop
1	—	7	2
2	2	8	2
3	3	9	2
4	3	10	2
5	2	11	3
6	2	12	3

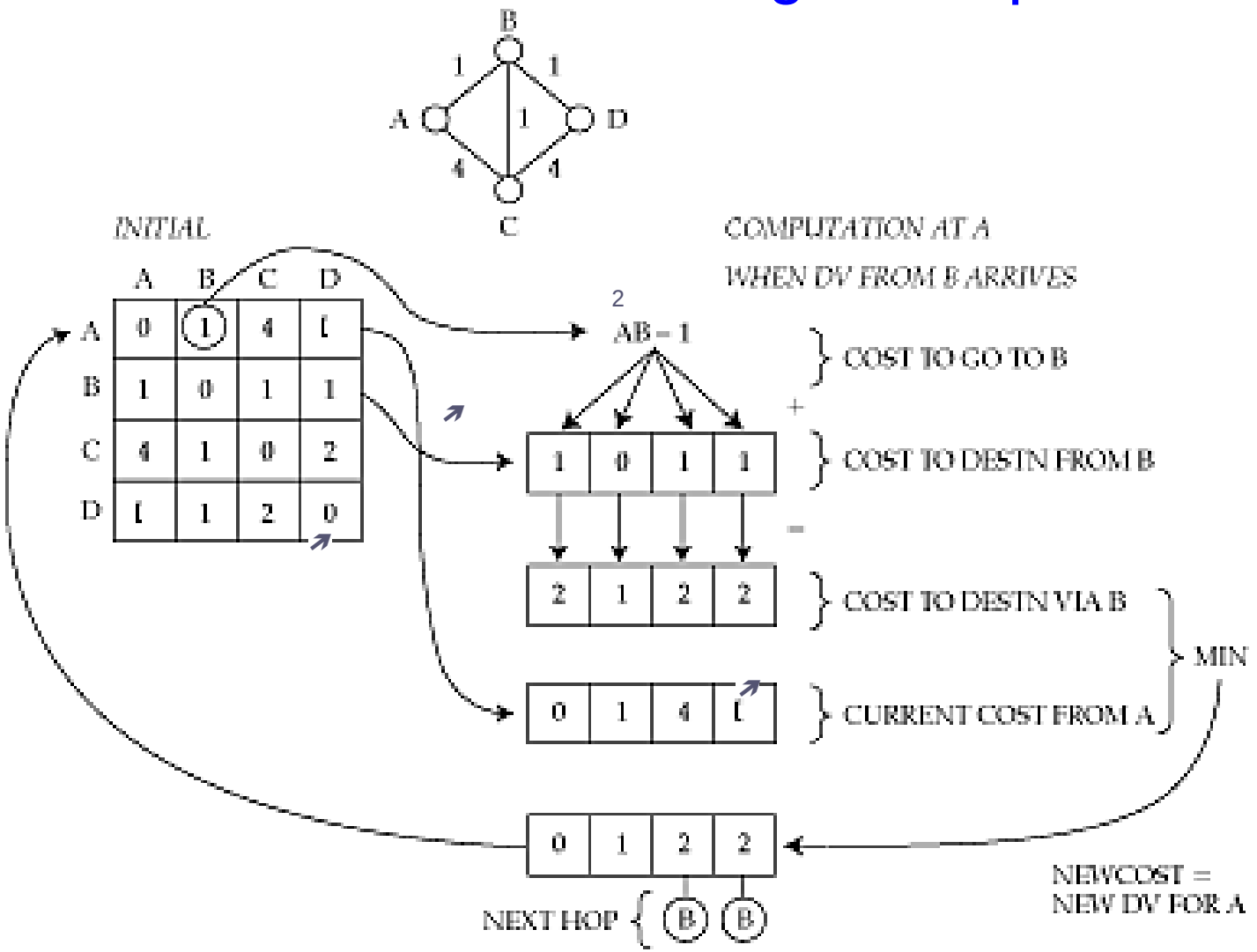
- **Un noeud fait un choix local selon une topologie globale**

Distance-vector & Link-state Routing

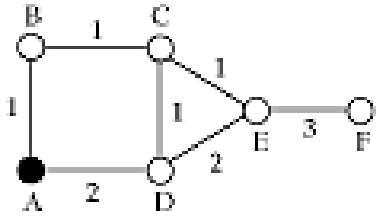
- **Les deux approches supposent qu'un noeud connaît:**
  - Adresse de chaque voisin
  - Le coût pour atteindre chaque voisin
- **Les deux approches permettent à un routeur de déterminer une information de routage global suite à des échanges avec les voisins**

- **Distance vector – un routeur connaît le coût pour atteindre chaque destination**
- **Link state – un routeur connaît toute la topologie du réseau et calcule les plus courts chemins**

Distance Vector Routing: Exemple

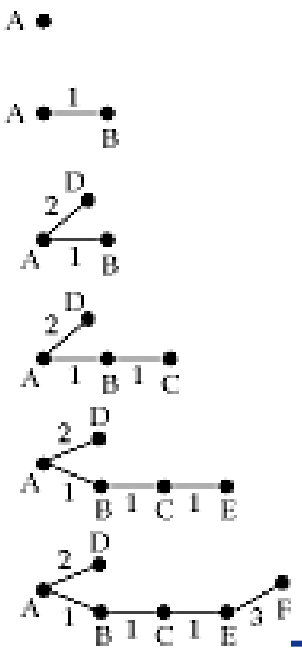


Link State Routing: Exemple



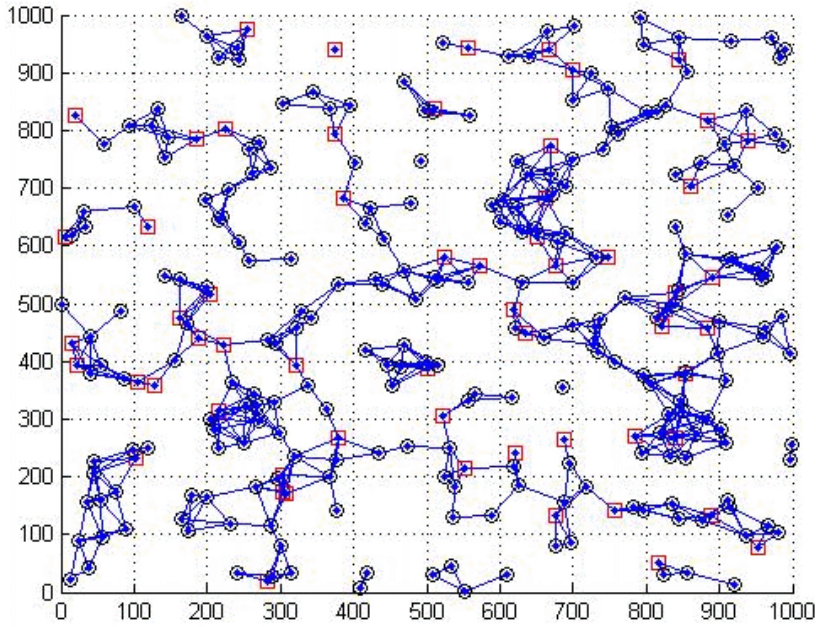
B(A,1) means B was reached by A, cost 1

PERMANENT	TEMPORARY	COMMENTS
A	B(A,1), D(A,2)	ROOT AND ITS NEIGHBORS
A, B(A,1)	D(A,2), C(B,2)	ADD C(B,2)
A, B(A,1) D(A,2)	E(D,4), C(B,2)	C(D,3) DIDN'T MAKE IT
A, B(A,1) D(A,2), C(B,2)	E(C,3)	E(D,4) TOO LONG
A, B(A,1) D(A,2), C(B,2) E(C,3)	F(E,6)	
A, B(A,1) C(B,2), D(A,2) E(C,3), F(E,6)	NULL	STOP



Routage et mobilité

- **Trouver un chemin d'une source à une destination**
- **Problèmes**
  - Changement de routes fréquents dûs aux mouvements de noeuds
  - Faible bande passante
- **Objectifs des protocoles de routage**
  - Réduire l'overhead dû au routage
  - Construire des routes courtes
  - Construire des routes stables malgrè la mobilité



Unicast Routing Protocols for MANET

- **Plusieurs protocoles proposés dans la littérature**

- **Certains conçus spécialement pour les MANET**
- **D'autres adaptés des réseaux filaires**

- **Pas un protocole qui fonctionne bien dans tous les environnements**

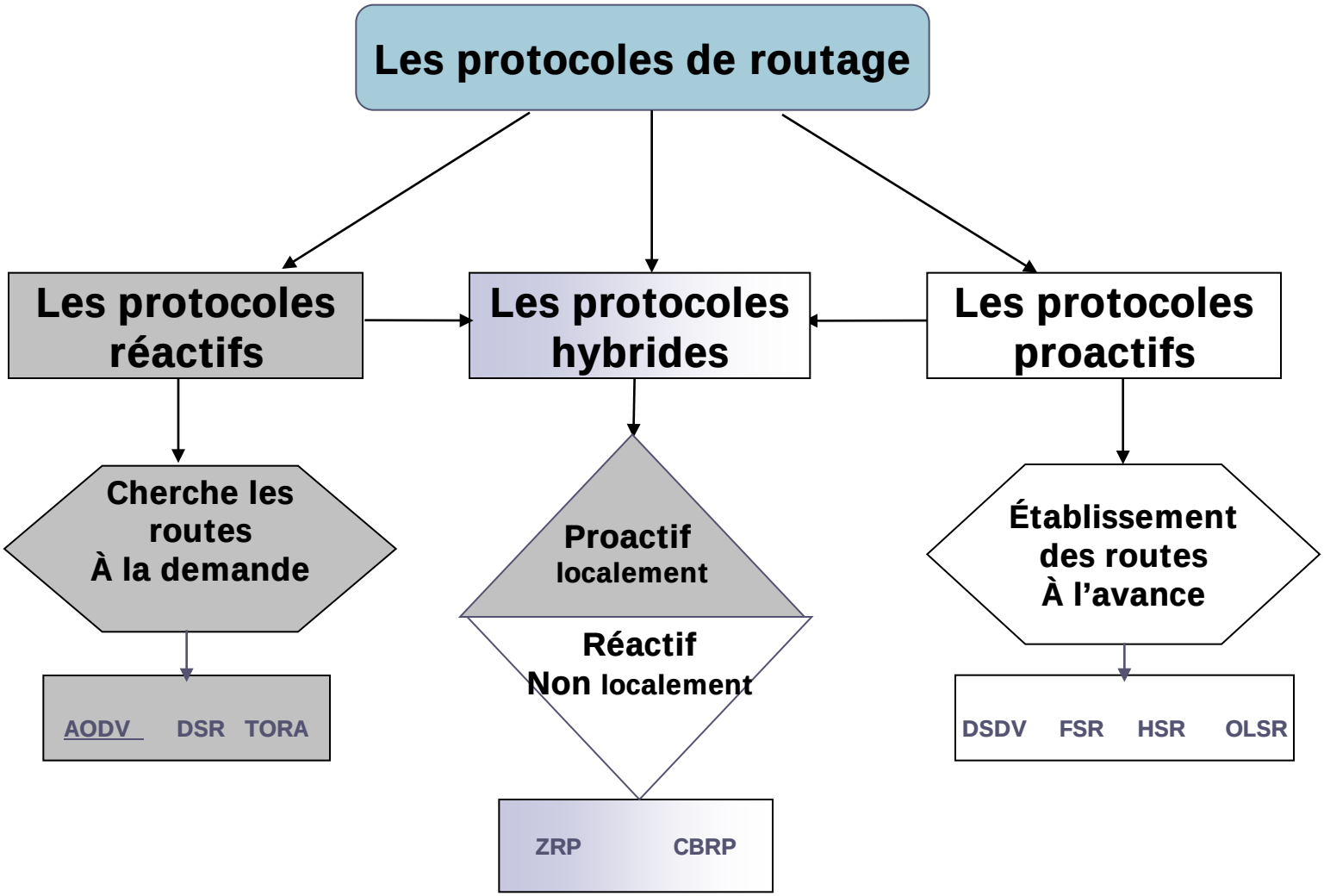
- **Standardisation à IETF**
  - MANET working group
  - **http://www.ietf.org**

Routing Protocols for MANET

- **Proactive protocols**
  - Maintien de routes tout le temps entre toutes les paires
  - Basée sur la mise-à-jours périodique; Overhead important
  - Example: DSDV (destination sequenced distance vector)

- **Reactive protocols**
  - Determiner des routes quand c'est nécessaire
  - La Source initie la découverte de route
  - Exemple: DSR (dynamic source routing)

- **Hybrid protocols**
  - Combinaison des approches proactive and reactive
  - Exemple : ZRP (zone routing protocol)


Les protocoles de routage
Les protocoles réactifs
Les protocoles hybrides
Les protocoles proactifs
Cherche les routes À la demande
Proactif localement
Réactif Non localement
Établissement des routes À l'avance
AODV DSR TORA
ZRP CBRP
DSDV FSR HSR OLSR

Protocol Trade-offs

- **Proactive protocols**
  - Maintenance continue des routes
  - Peu ou pas de délai pour déterminer une route
  - Consommation de bande passante pour mettre à jour les routes
  - Maintien de routes qui ne seraient jamais utilisées

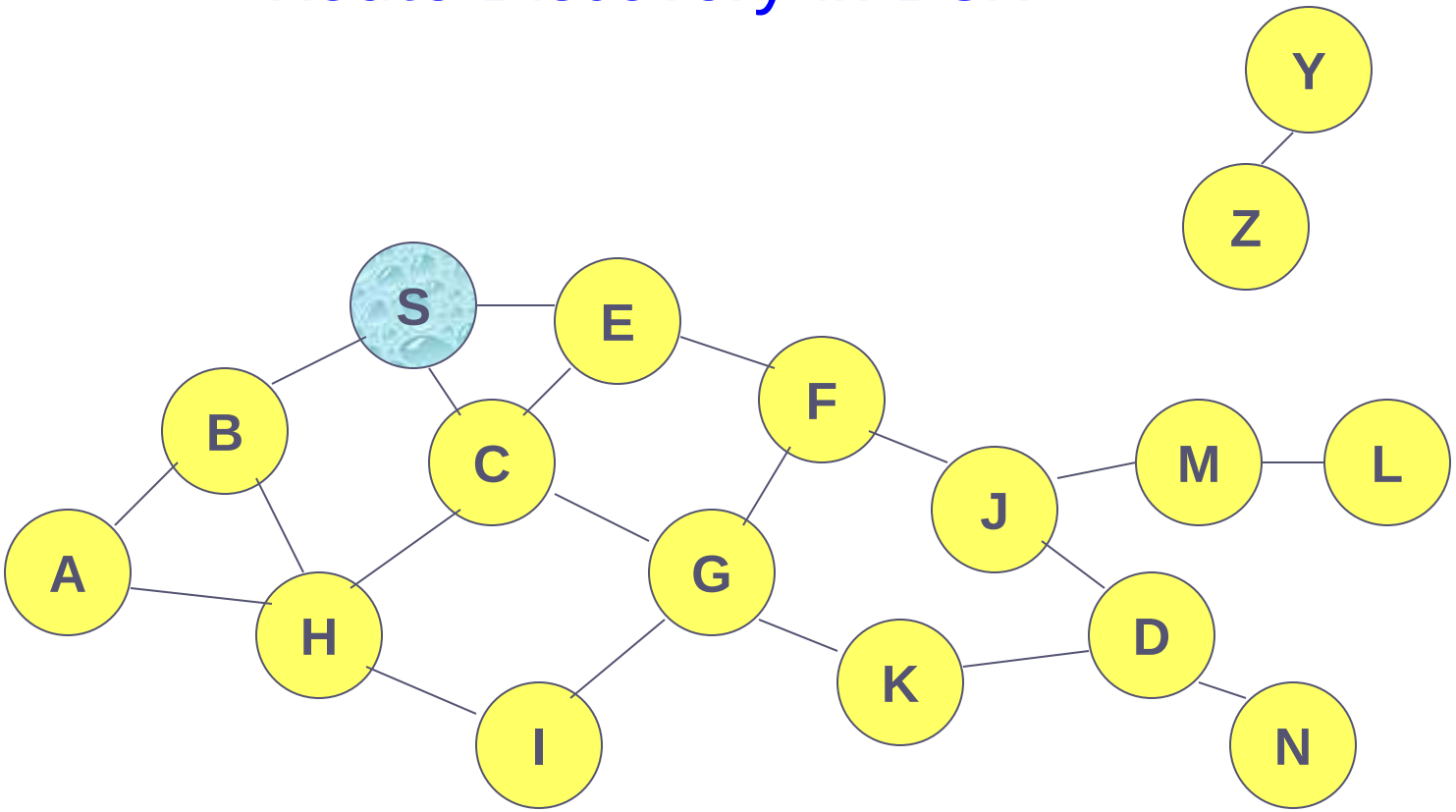
- **Reactive protocols**
  - Faible overhead puisque les routes sont déterminées à la demande
  - Délai important pour la détermination d'une route
  - Usage de l'inondation (recherche globale)

REACTIVE ROUTING PROTOCOLS

Dynamic Source Routing (DSR) [Johnson96]

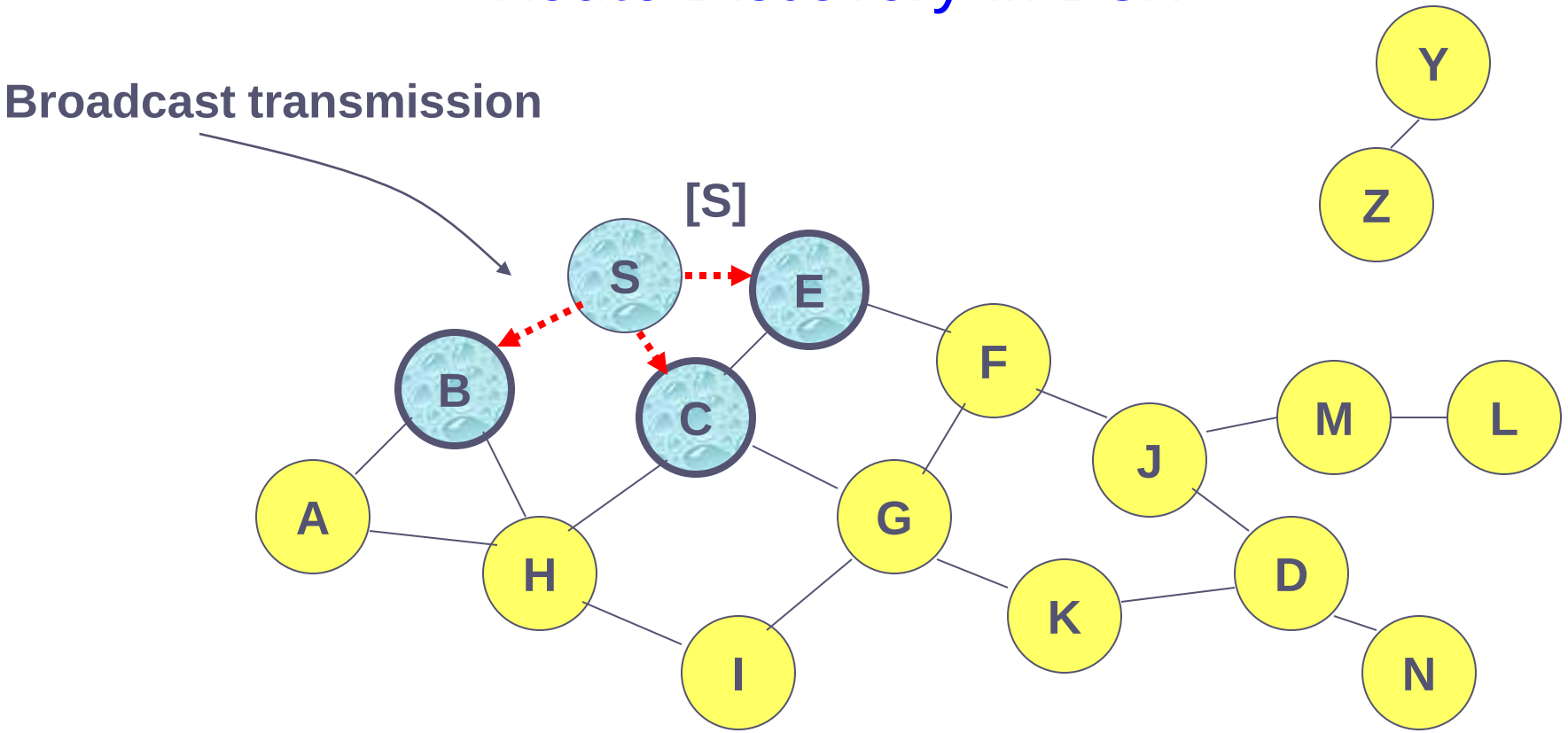
- **Quand S veut envoyer un paquet à D, mais ne connaîs pas de route vers D, S initie un route discovery**
- **Le noeud Source S diffuse Route Request (RREQ)**
- **Chaque noeud rajoute son identifiant avant de relayer RREQ**

Route Discovery in DSR



Représente un noeud qui a reçus RREQ pour D de S

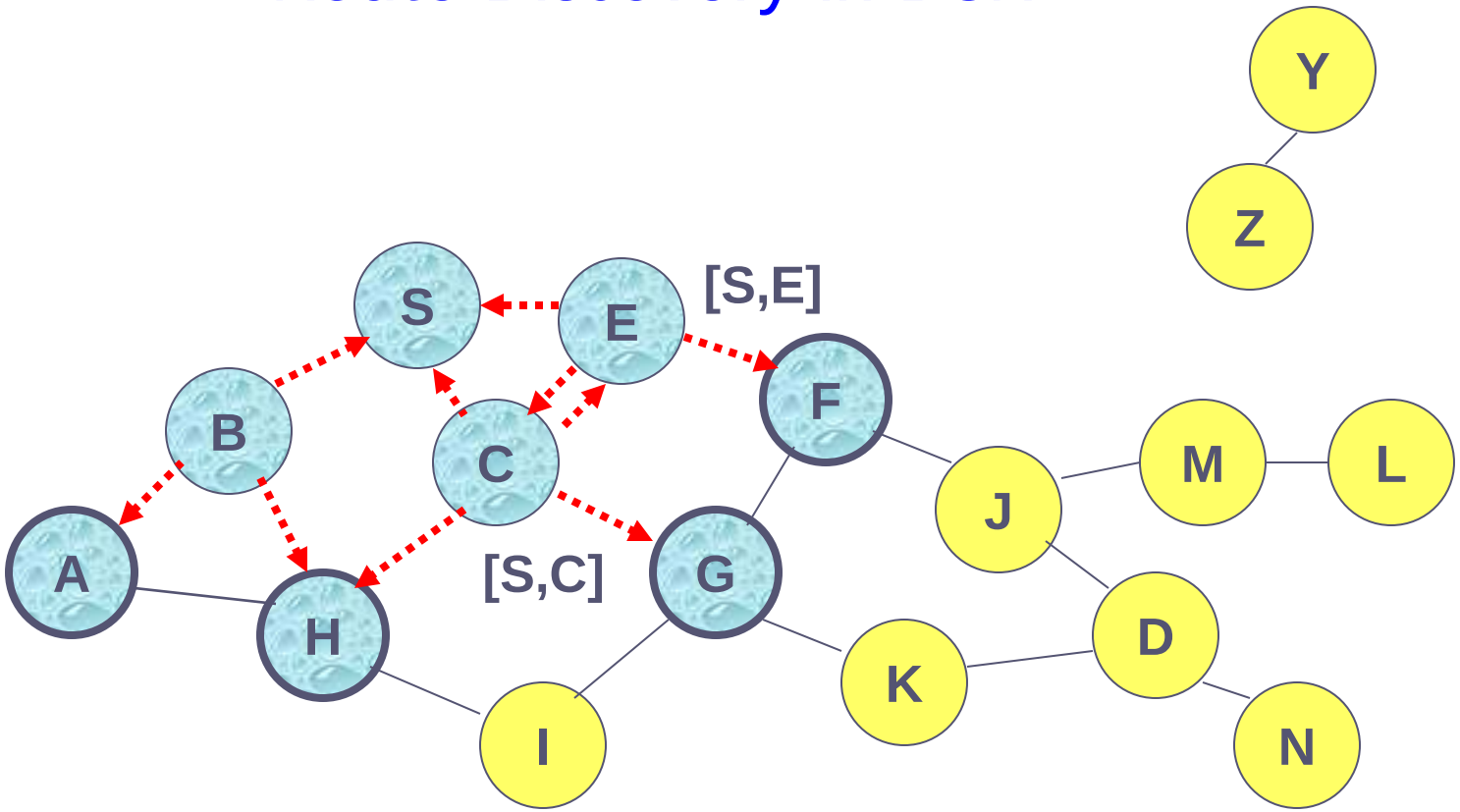
Route Discovery in DSR



Represents transmission of RREQ

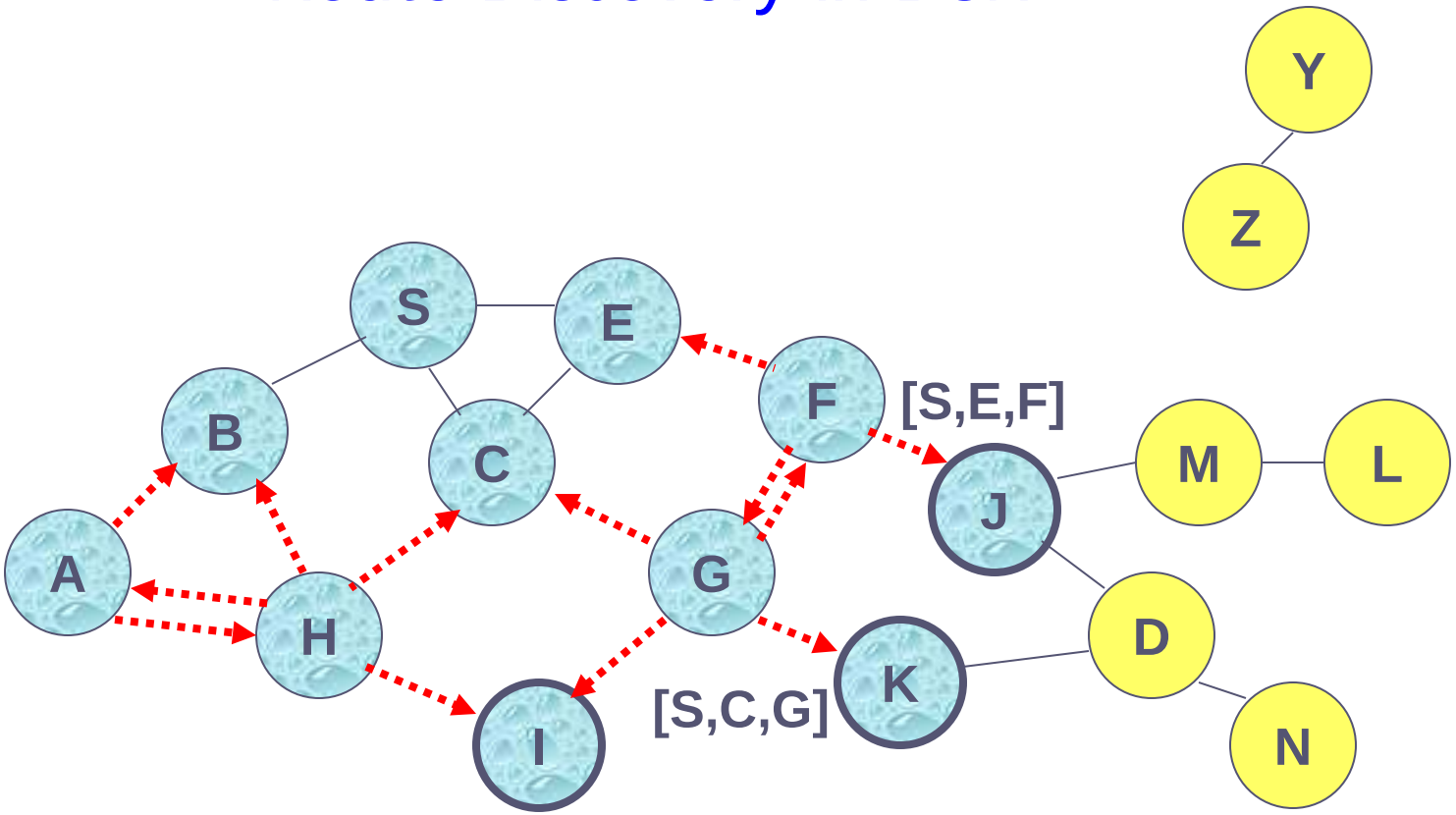
[X,Y] Represents list of identifiers appended to RREQ

Route Discovery in DSR



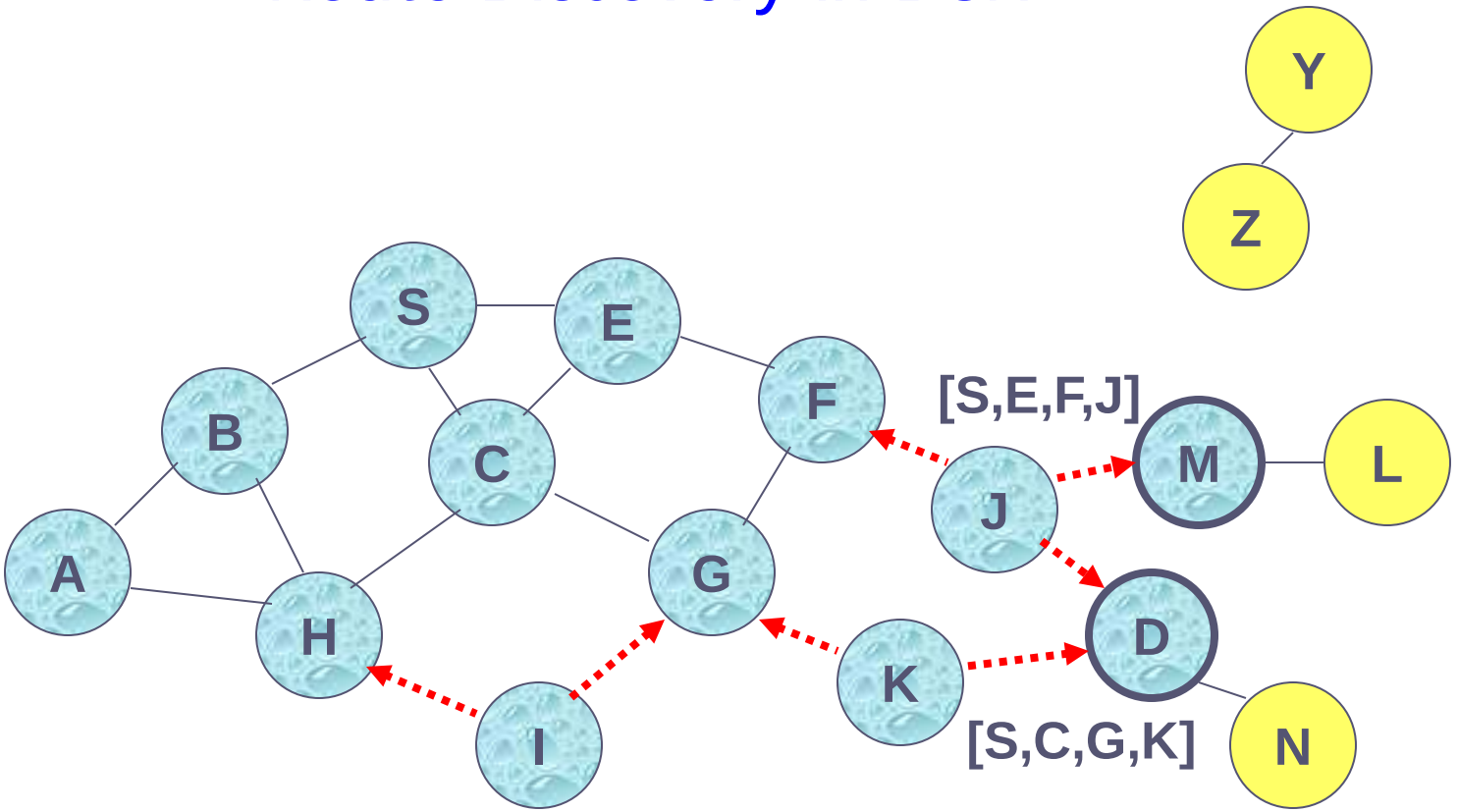
- **Node H receives packet RREQ from two neighbors: potential for collision**

Route Discovery in DSR



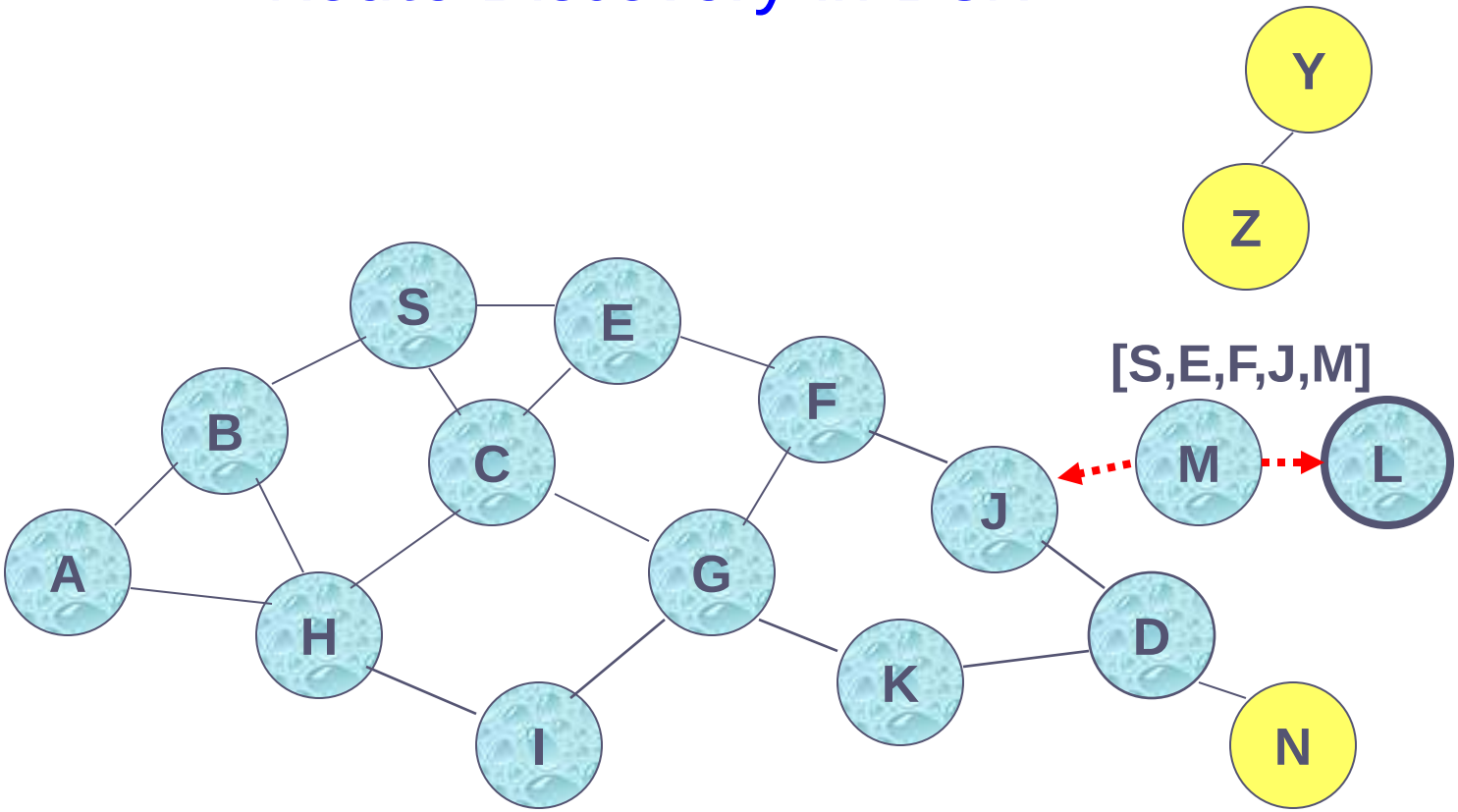
- **Node C receives RREQ from G and H, but does not forward it again, because node C has already forwarded RREQ once**

Route Discovery in DSR



- Nodes J and K both broadcast RREQ to node D
- Since nodes J and K are **hidden** from each other, their transmissions may collide

Route Discovery in DSR

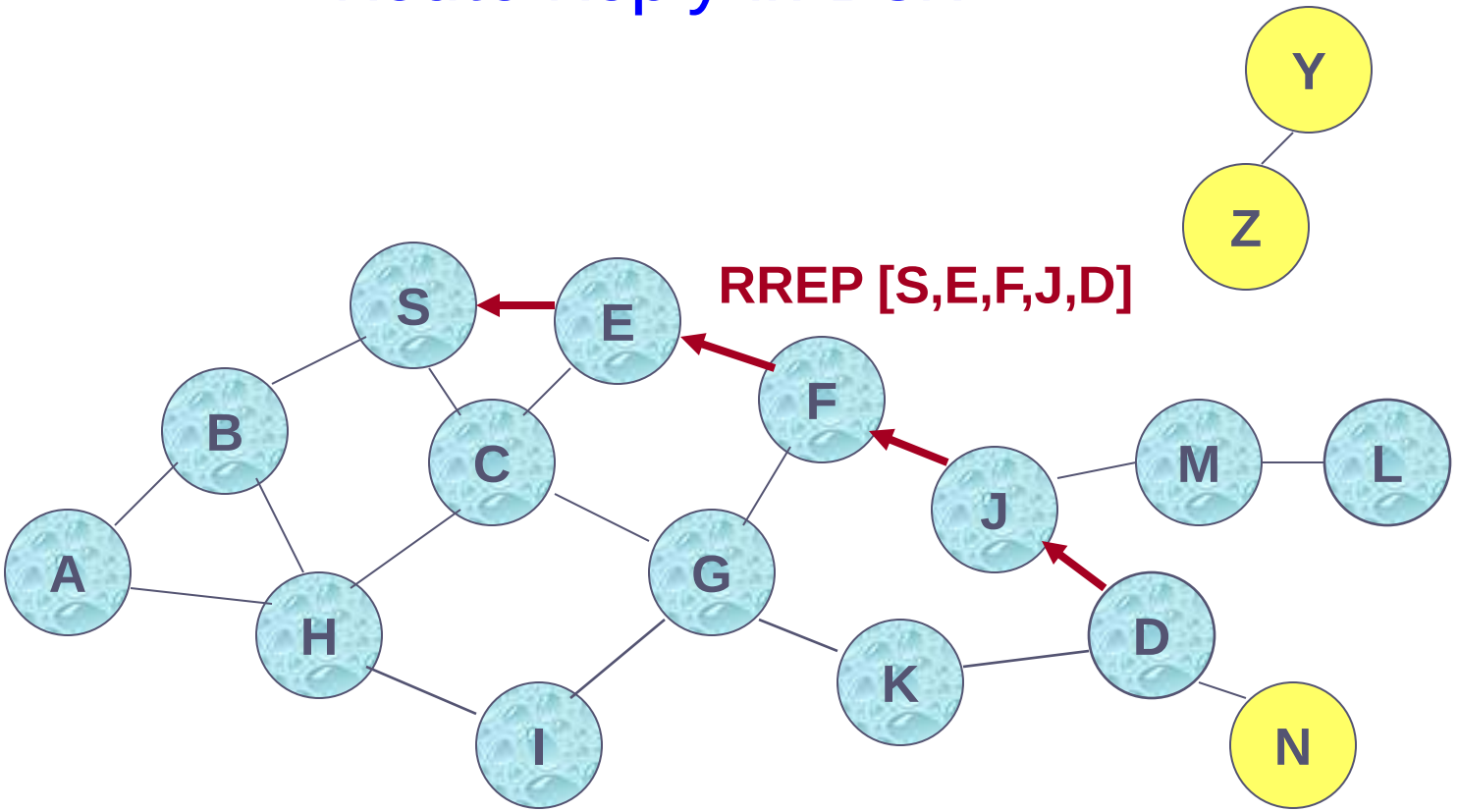


- Node D **does not forward** RREQ, because node D is the **intended target** of the route discovery

Route Discovery in DSR

- **La destination D répond par un Route Reply (RREP) après réception du premier RREQ**
- **RREP est envoyé par la route inverse attachée à RREQ**
- **RREP porte la route de S vers D construite grâce à la propagation de RREQ de S vers D**

Route Reply in DSR



Represents RREP control message

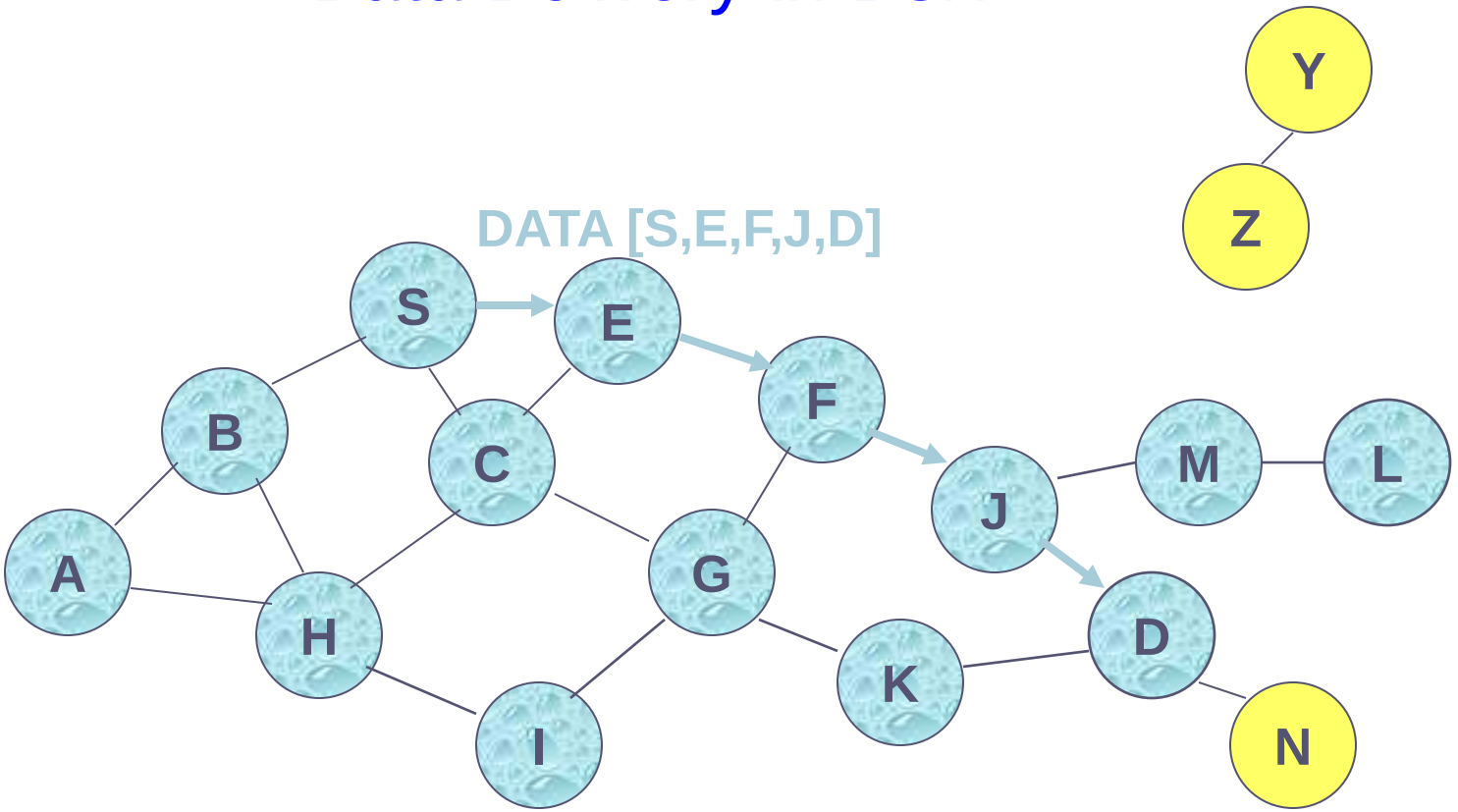
Dynamic Source Routing (DSR)

- **Quand S reçoit RREP, il met la route construite dans son cache**

- **Lorsque S envoie un paquet de données à D, la route entière est incluse dans l'entête du paquet**
  - D'où le nom source routing

- **Les noeuds intermédiaires utilisent la route incluse dans l'entête du paquet pour déterminer à qui relayer le paquet.**

Data Delivery in DSR



La taille de l'entête d'un paquet est proportionnelle à la longueur de la route

DSR Optimization: Route Caching

- **Chaque noeud enrichie son cache par tous les myens**
- **Quand S trouve la route [S,E,F,J,D] vers D, S apprend aussi la route [S,E,F] vers F**
- **Quand K reçois Route Request [S,C,G] destiné à qulequ'un, K apprend la route [K,G,C,S] vers S**
- **Quand F relai Route Reply RREP [S,E,F,J,D], F apprend la route [F,J,D] vers D**
- **Quand E relai Data [S,E,F,J,D] il apprend la route [E,F,J,D] vers D**
- **Un noeud peut aussi apprendre une route quand il écoute Data**

Dynamic Source Routing: Avantages

- **Routes maintenues uniquement entre des noeuds qui désirent communiquer**
  - Réduire l'overhead de la maintenance des routes
- **La mise en cache des Route réduit d'avantage l'overhead de découverte**
- **Un seul Route Discovery peut entraîner la construction de plusieurs routes vers la destination (fiabilité)**

Dynamic Source Routing: Inconvénients

- **Taille de l'entête grandit avec la longueur de route**
- **Inondation du réseau par les route request**
- **Collisions potentielles dûes à la propagation de RREQ de voisins**
  - insertion de délais aléatoires avant de relayer RREQ

Ad Hoc On-Demand Distance Vector Routing (AODV) [Perkins99Wmcsa]

- **DSR inclut les routes dans l'entête des paquets**
- **Les grandes entêtes résultants peuvent dégrader les performances**
  - Surtout lorsque la données transportées est petite en taille (rendement)

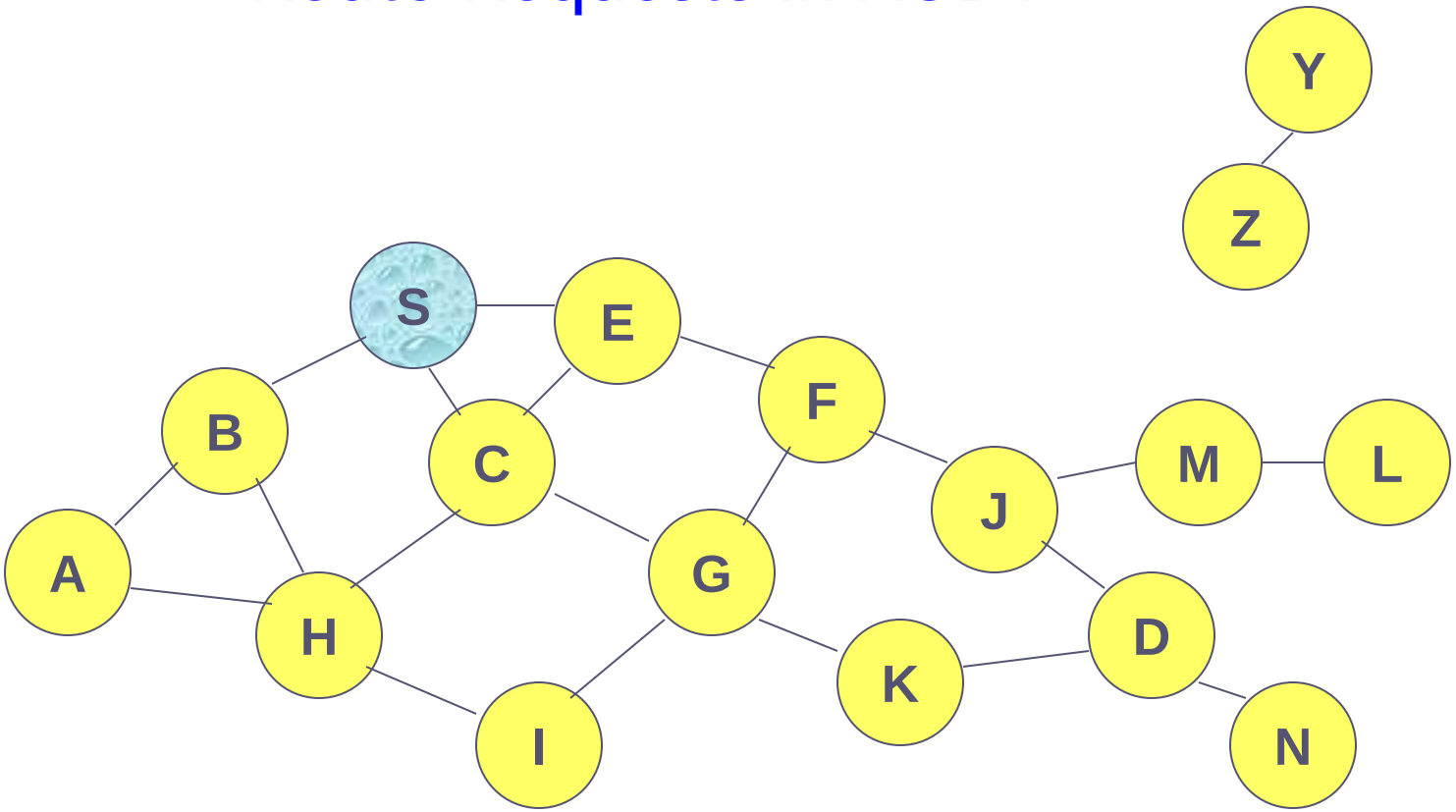
- **AODV tente d'améliorer DSR par la construction de tables de routage au niveau des noeuds, de telle sorte que les paquets de données ne transportent pas les routes**

- **AODV maintient l'avantage de DSR qui consiste à construire des routes à la demande**

AODV

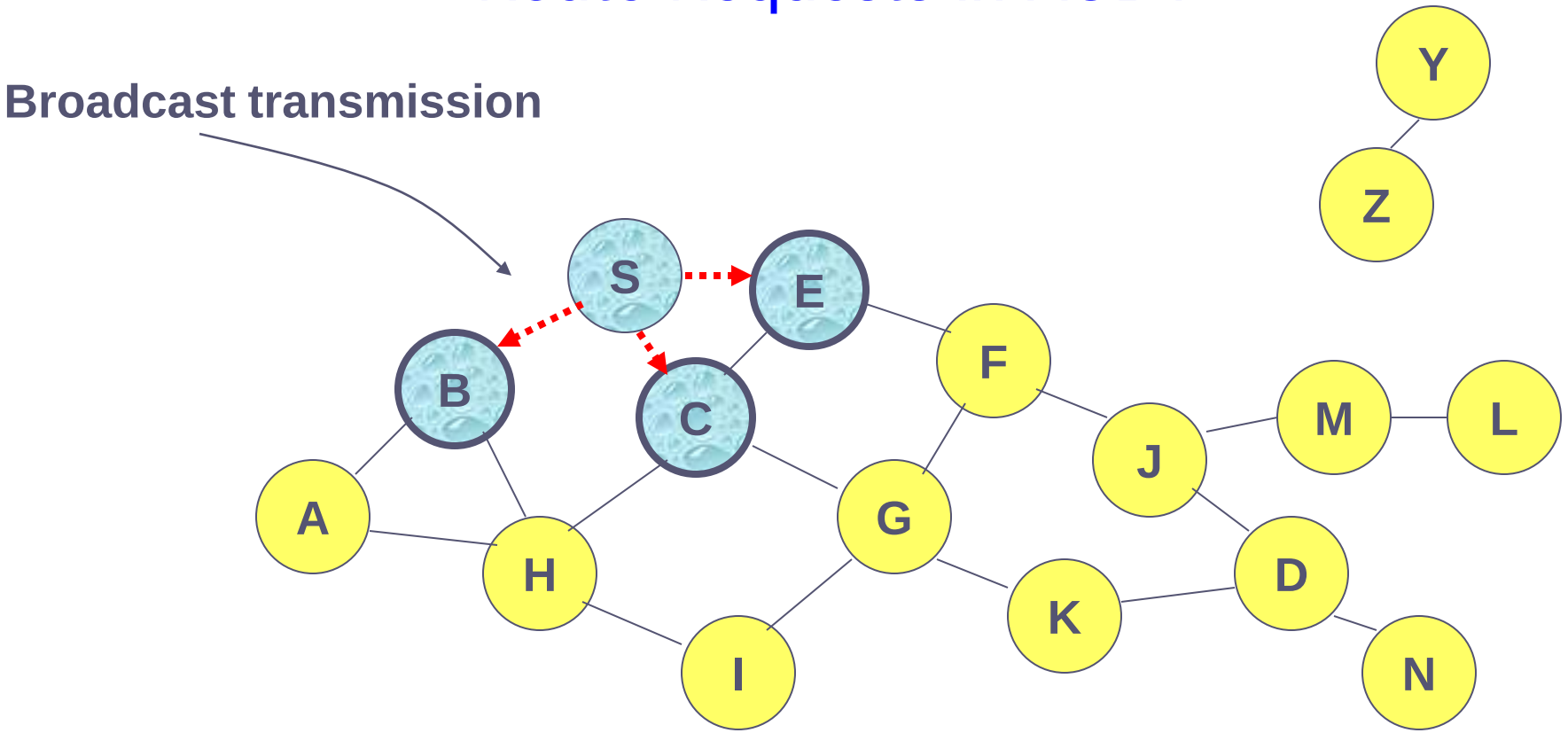
- **Route Requests (RREQ) sont relayés de la même façon que DSR**
- **Quand un noeud “re-broadcast” un Route Request, il établie un chemin inverse pointant vers la source**
  - AODV suppose des liens symmetriques (bi-directionnel)
- **Quand la destination reçois le Route Request, elle répond en renvoyant un Route Reply (RREP)**
- **Route Reply traverse le chemin inverse construit lors de la propagation de Route Request**

Route Requests in AODV

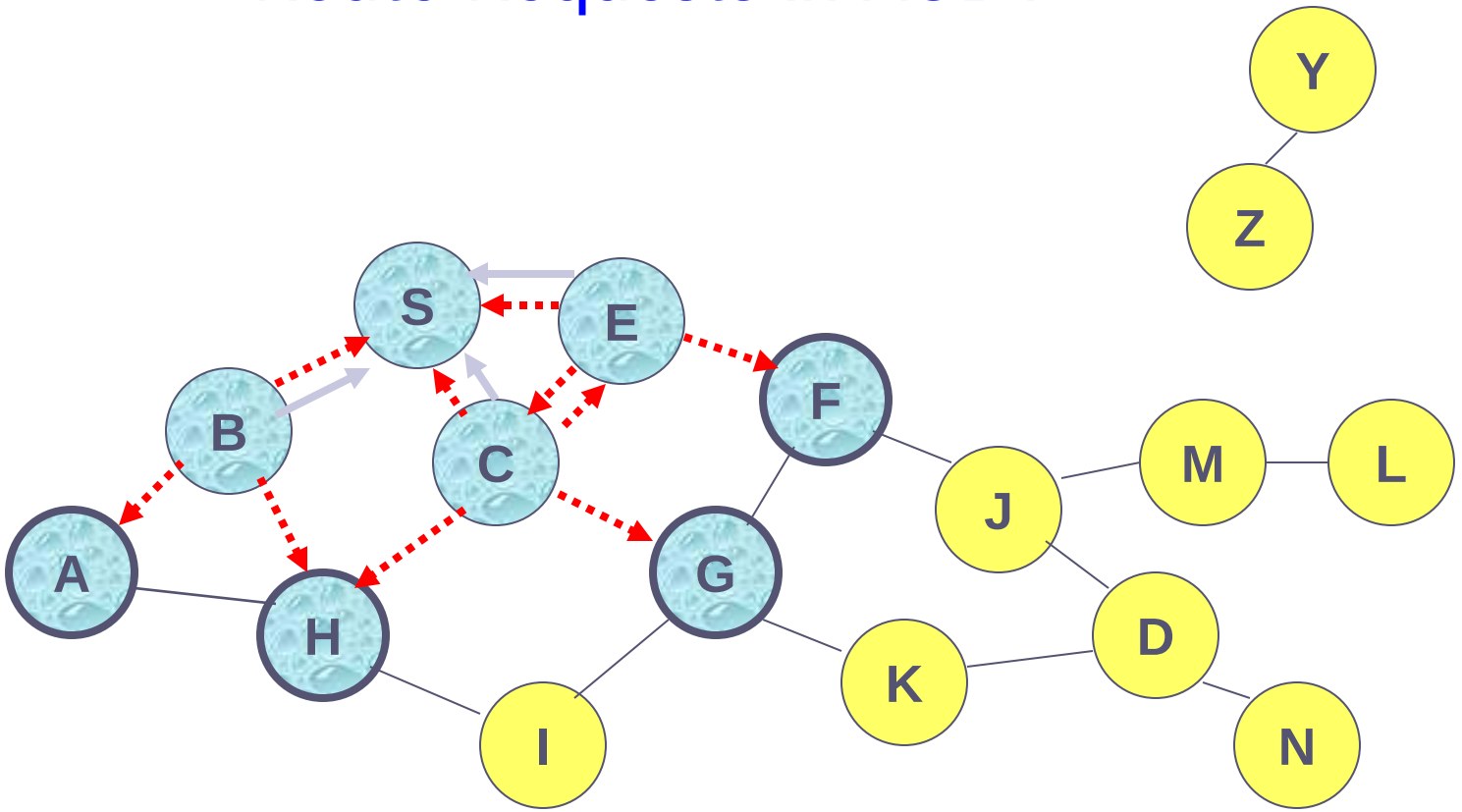


Represents a node that has received RREQ for D from S

Route Requests in AODV

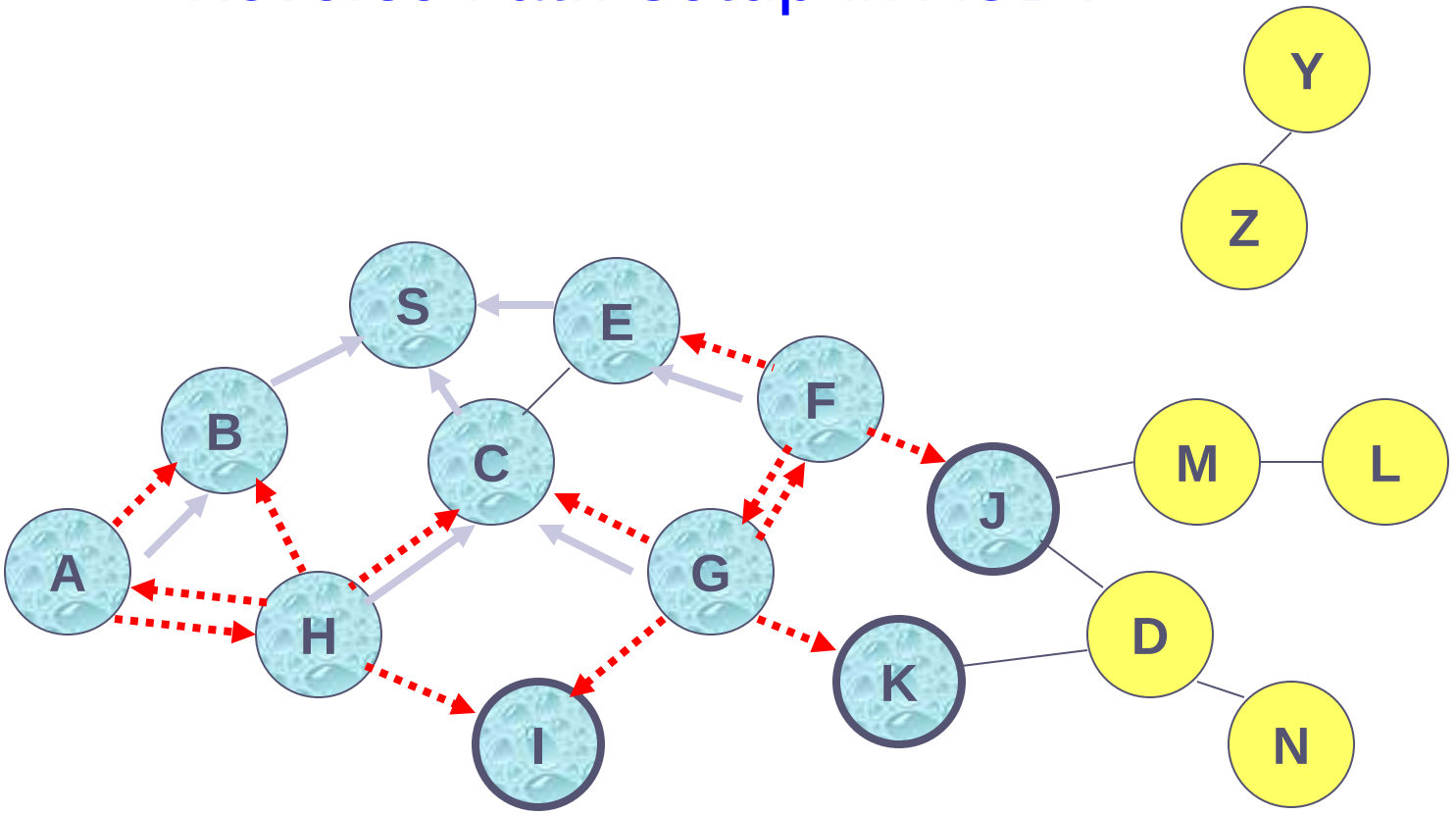


Route Requests in AODV



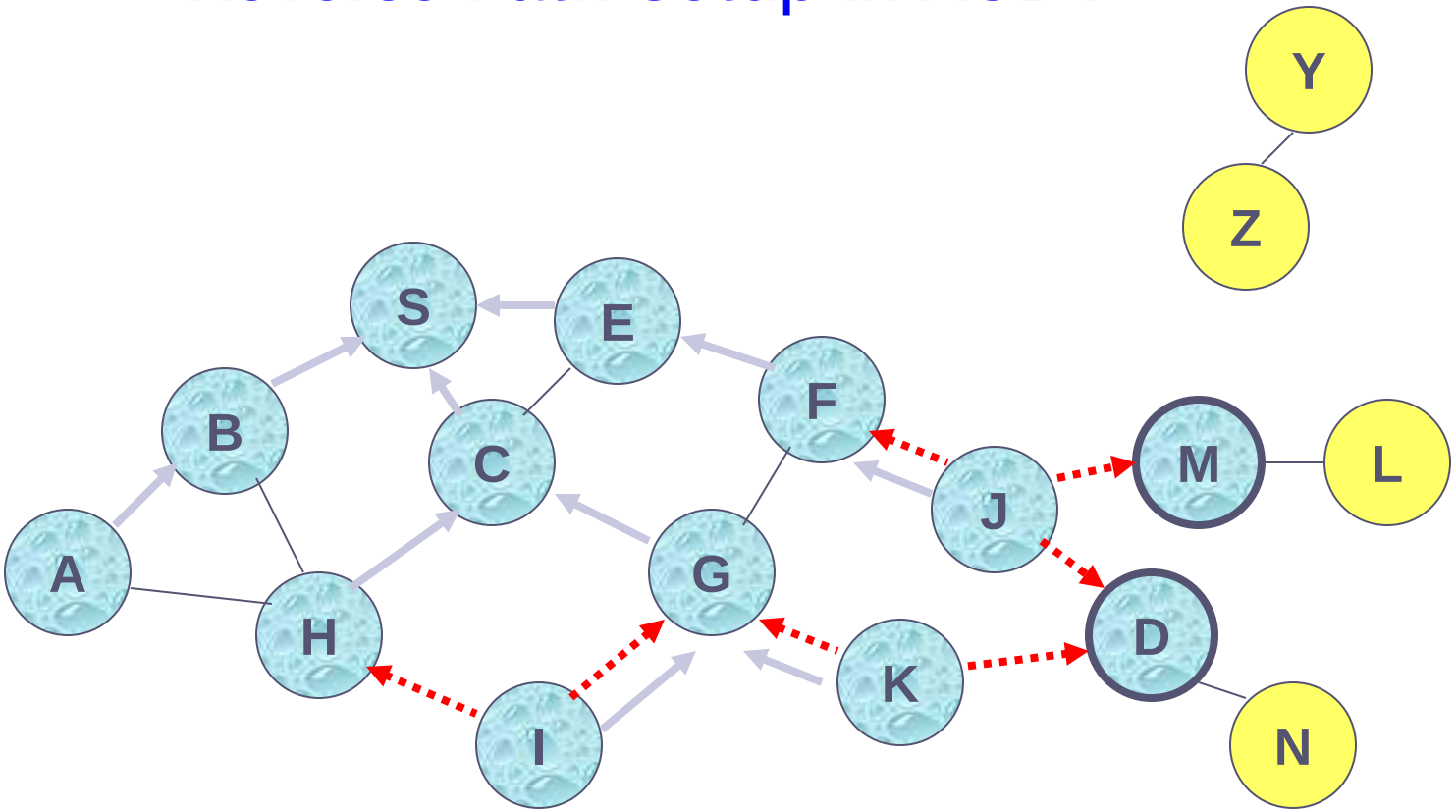
Represents links on Reverse Path

Reverse Path Setup in AODV

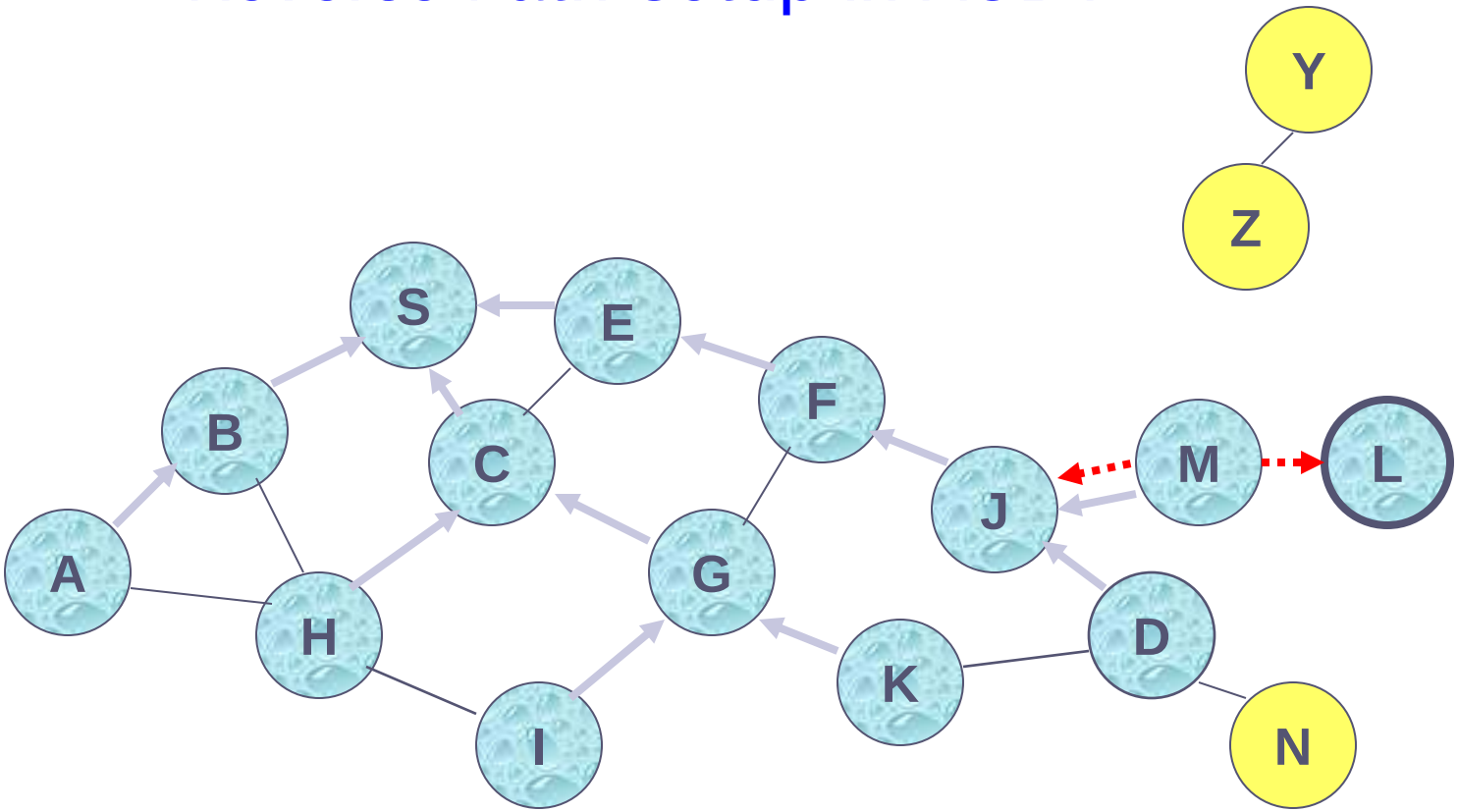


- **Node C receives RREQ from G and H, but does not forward it again, because node C has already forwarded RREQ once**

Reverse Path Setup in AODV

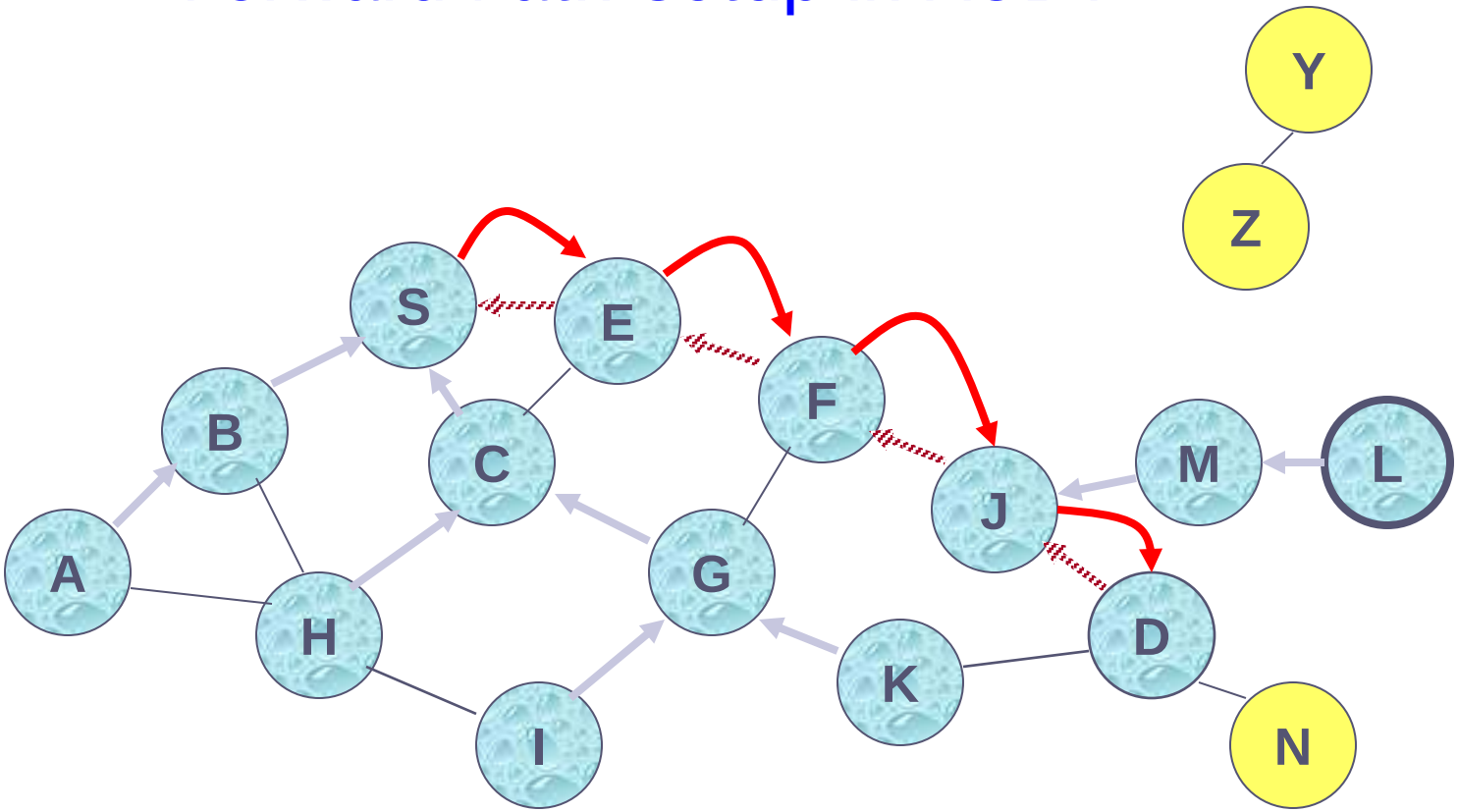


Reverse Path Setup in AODV



- 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

Route Request et Route Reply

- **Route Request (RREQ) inclut le dernier sequence number pour la destination**

- **Un noeud intermédiaire peut aussi envoyer un Route Reply (RREP) s'il connaît un chemin plus récent que celui recherché par la source**
- **Lorsque un noeud intermédiaire retransmet un RREP, il enregistre le next hop vers la destination (construction du chemin direct)**
- **Une entrée de la table de routage qui contient un chemin inverse est purgée après un timeout**
- **Une entrée de la table de routage qui contient un chemin dircet est purgée après un *active_route_timeout* interval**

Link Failure

- **Un noeud voisin X est considéré actif pour une entrée de la table de routage si le voisin a envoyé un paquet dans l'intervalle *active_route_timeout* et retransmis en utilisant cette entrée**
- **Les noeuds voisins échangent un hello message périodiquement**
- **Quand le next hop link d'une entrée de la table de routage est rompus, les voisins actifs sont informés**
- **Les pannes de liens sont propagées par le moyen de messages Route Error (RERR)**

Route Error

- **Quand un noeud X est incapable de router un paquet P (de S vers D) sur le lien (X,Y), il génère un message RERR**
- **Le noeud X incremente le “destination sequence number” pour D dans son cache**
- **Le sequence number *N* (incrémenté) est inclut dans le RERR**
- **Quand S reçoit le RERR, elle initie un nouveau Route Request pour D avec un “destination sequence number” au moins égal à *N***
- **Quand D reçois le route request avec “destination sequence number” N, le noeud D met son “sequence number” à N, à moins qu’il est déjà supérieur à N**

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 maintenire 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**

PROACTIVE ROUTING PROTOCOLS

Destination-Sequenced Distance-Vector (DSDV) [Perkins94Sigcomm]

- **Chaque noeud maintient une table de routage qui stocke**
  - next hop, cost metric vers chaque destination
  - un “sequence number” créé par la destination
- **Périodiquement, chaque noeud envoie la table de routage à ses voisins**
  - Chaque noeud incrémente et rajoute son sequence number en envoyant sa table de routage
- **Chaque route est étiquetée par un sequence number; les routes avec un plus grand sequence numbers sont préférées**

- **Chaque noeud annonce un sequence number pair d’une manière monotone**
- **Quand un noeud décide qu’une route est rompue, il incrémente le sequence number (impair) de la route et l’annonce avec une métrique infinie**

Destination-Sequenced Distance-Vector (DSDV)

- **Quand X reçoie une information de Y à propos d'une route vers Z**
  - Soit S(X) le sequence number de Z chez X, S(Y) est envoyé par Y

  - If S(X) > S(Y), then X ignore l'information reçue de Y
  - If S(X) = S(Y), ET coût via Y < coût route connue par X, then X met Y comme next hop vers Z
  - If S(X) < S(Y), then X met Y comme next hop vers Z, ET S(X) := S(Y)

Optimized Link State Routing (OLSR)

Optimized Link State Routing

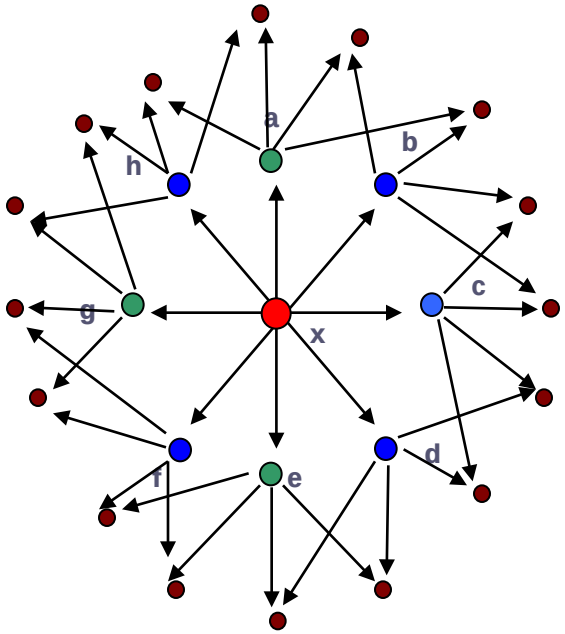
- Des paquets de contrôle sont périodiquement diffusés dans le réseau
- Les routes sont optimales
- Les routes sont immédiatement disponibles

Optimized Link State Routing (OLSR)

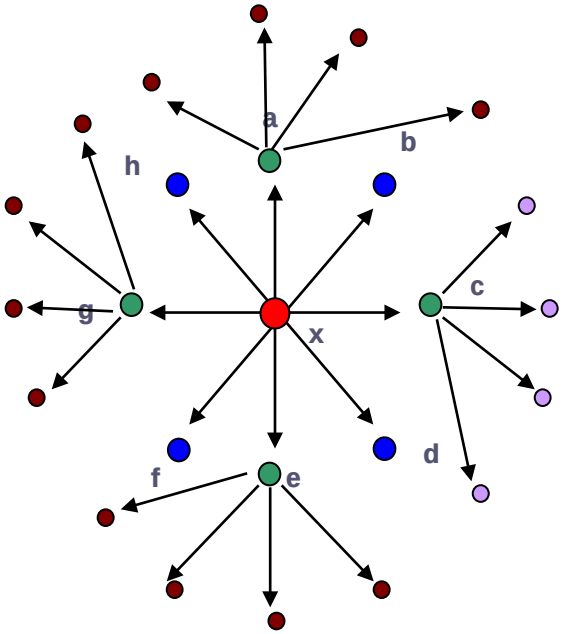
- **Optimisations par rapport à « link state »:**
  - Un paquet de contrôle d'un noeud ne contient une liste de voisins MPR (au lieu de tous les voisins)
  - La diffusion des paquets de contrôle ne passe que par les MPR (au lieu de l 'inondation complète)
  - Un MPR ne retransmet que si il reçoit le paquet en premier par le nœud dont il est MPR.
  - Les nœuds connaissent une topologie partielle constituée des voisins directs et des MPR des autres nœuds.
  - Néanmoins, les routes calculée sont optimales par rapport à la topologie complète.

Optimized Link State Routing (OLSR)

- Protocole proactif basé sur l'état de lien
- Éviter l'inondation: MPR(MultiPoint Relay)



Inondation

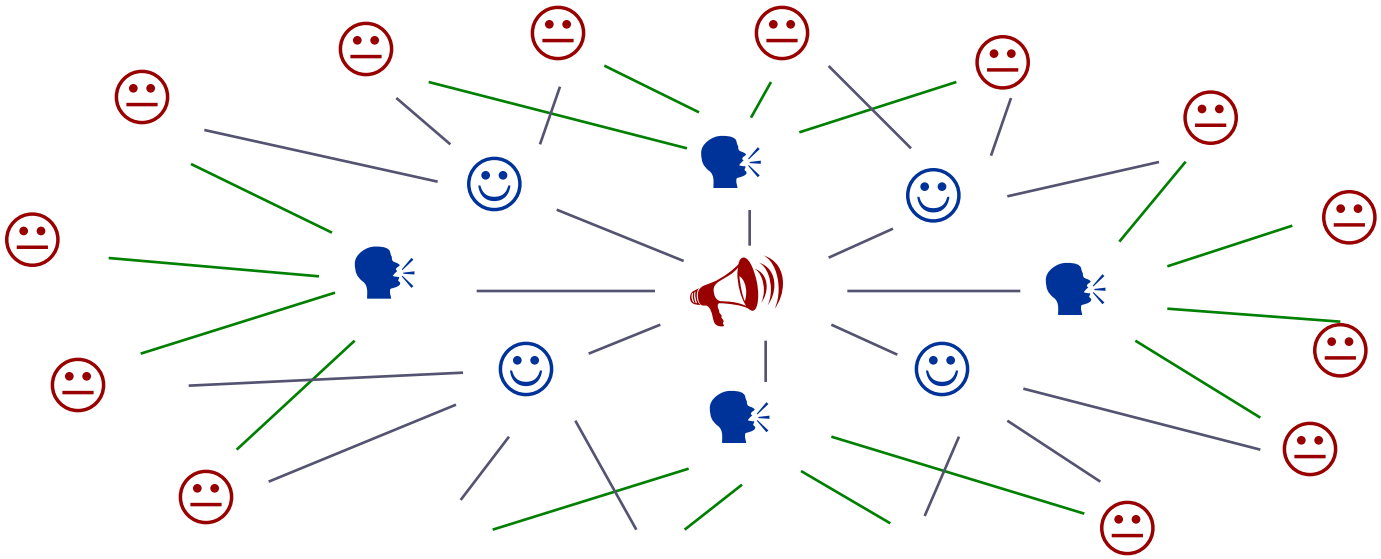


Diffusion à travers les MPR

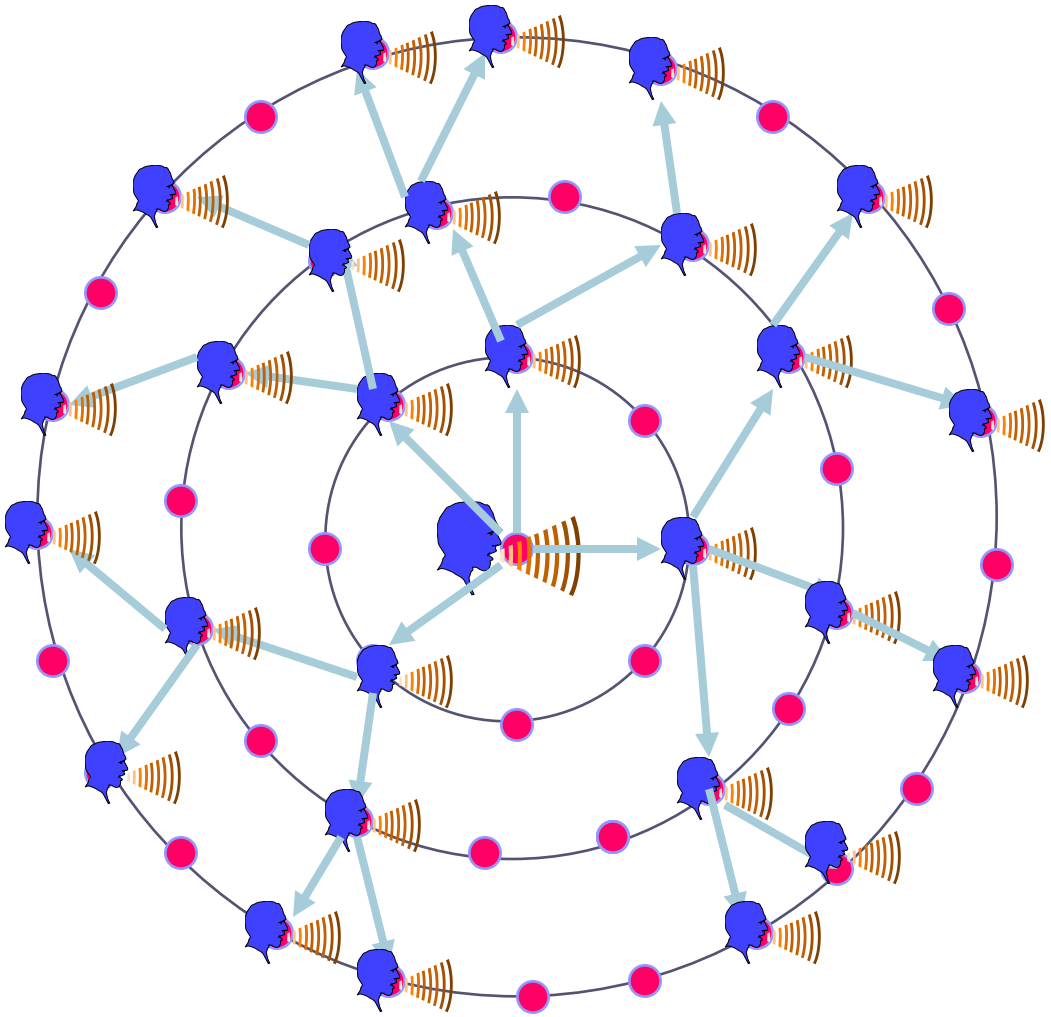
- Utilisation de messages de contrôle:
  - HELLO : Découverte du voisinage.
  - TC (Topology Control) : mise à jour de la topologie.

Les relais multipoints

- **Chaque nœud détermine son groupe MPR:**
  - Couverture minimale des nœuds à deux sauts
- **Les MPR relayent les paquets à diffusions**
  - réduction des répétitions inutiles dans les diffusions

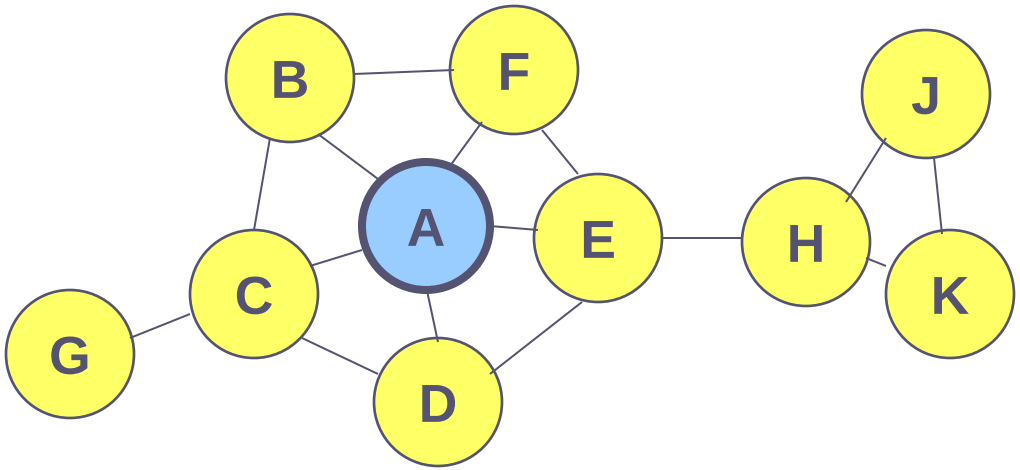


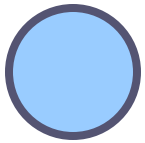
Les relais multipoints



Optimized Link State Routing (OLSR)[Jacquet00ietf]

- **C et E sont des Relais Multi-point de A**
  - Multipoint relays de A sont ses voisins qui lui permettent d'atteindre tous ses voisins à 2 sauts
  - Les noeuds échangent leurs listes de voisinspour connaître leurs voisins à 2 sauts et choisir leurs multipoint relays

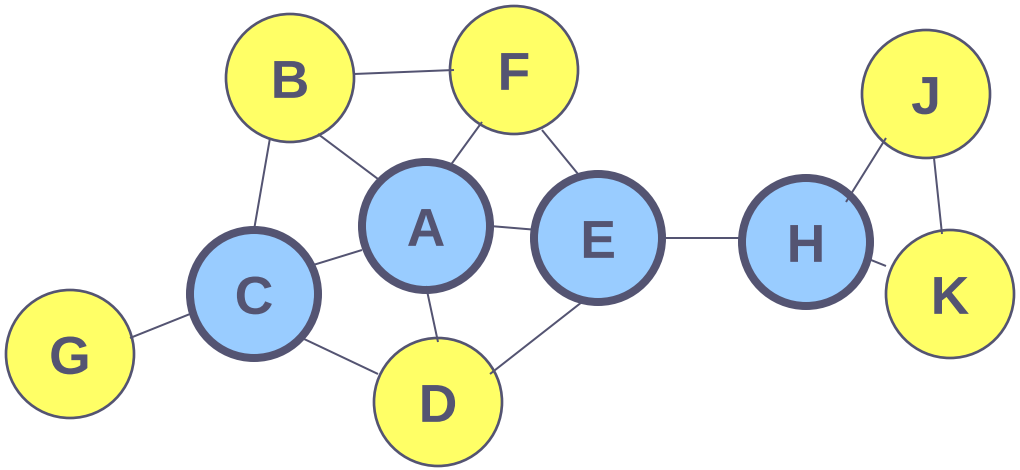




Node that has broadcast state information from A

Optimized Link State Routing (OLSR)

- **C et E retransmettent l'information reçue de A**
- **E et K sont des multipoint relays pour H**
- **K retransmet l'information reçue de H**



Node that has broadcast state information from A

HYBRID ROUTING PROTOCOLS

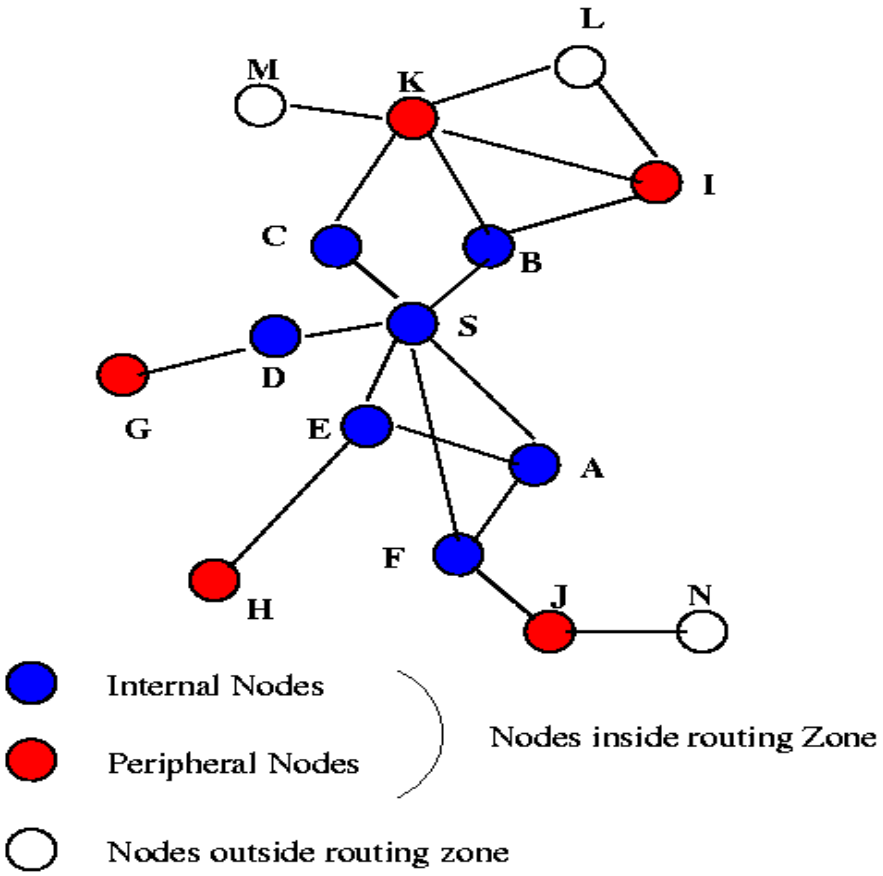
Zone Routing Protocol (ZRP) [Haas98]

- **ZRP combines les approches proactives et réactives**

- **Tous les noeuds à d sauts sont considérés dans la zone de routage du noeud X**
- **Tous les noeuds à éxactement d sauts sont dits périphériques du noeud X**

- **Intra-zone routing: Maintenire les routes d'une façon proactive à tous les noeuds dans la zone de routage de la source.**
- **Inter-zone routing: Utiliser un protocole à la demande similaire à DSR ou AODV pour déterminer les routes outside zone.**

Zone Routing Protocol (ZRP)



Radius of routing zone = 2

Conclusions

- **Protocoles**
  - Proactifs, réactifs, hybrides
  - Il existe beaucoup de protocoles de routage dans la littérature

- **Performances**
  - Généralement étudiée par simulation avec NS2
  - Nodes (10-30) restent stationnaires pour une pause (0-900s) puis bougent à une destination aléatoire (1500m X300m space) à une vitesse uniforme (0-20m/s). CBR traffic sources (4-30 packets/sec, 64-1024 bytes/packet)
  - Estimer la latence de route discovery, routing overhead, etc.

- **Trade-off depend beaucoup des patterns de trafic et mobilité**
  - Grande diversité du trafic (plus de paires source-destination) augmente overhead dans on-demand protocols
  - Grande mobilité augmente overhead dans tous les protocoles