Ecole Nationale Polytechnique d’Oran- Maurice AUDIN
Département de Génie des Systèmes Informatiques

Intitulé de la matière: **Technologies des Réseaux Sans Fil**

Chapitre 3: Les Réseaux Ad Hoc

Dr. Nawel BENDIMERAD

Année universitaire 2023/2024

Contenu du Chapitre 3

1/ Introduction

2/ Définition

3/ Caractéristiques

4/ Avantages et inconvénients

5/ Domaines d’application

6/ Routage

7/ Exemples de protocoles de routage

8/ Sécurité

1/ Introduction (1)

- L’introduction des réseaux ad-hoc est récente, bien que cette technique soit depuis longtemps testée par les fabricants d’équipements militaires.
- Le début des années 1970 voit, au sein du projet militaire Américain DARPA (The Defense Advanced Research Projects Agency), la naissance des premiers réseaux utilisant le médium radio. Ces réseaux disposaient déjà d’une architecture distribuée, partageaient le canal de diffusion en répétant des paquets pour élargir la zone de couverture globale.
- Par la suite, en 1983, *les Sur vivable Radio Networks* (SU RAN) furent développés par le DARPA. L’objectif était de dépasser les limitations (en particulier permettre le passage à des réseaux comportant énormément de nœuds, gérant la sécurité, l’énergie, etc.). Mais les recherches sur ces réseaux restaient exclusivement militaires.

1/ Introduction (2)

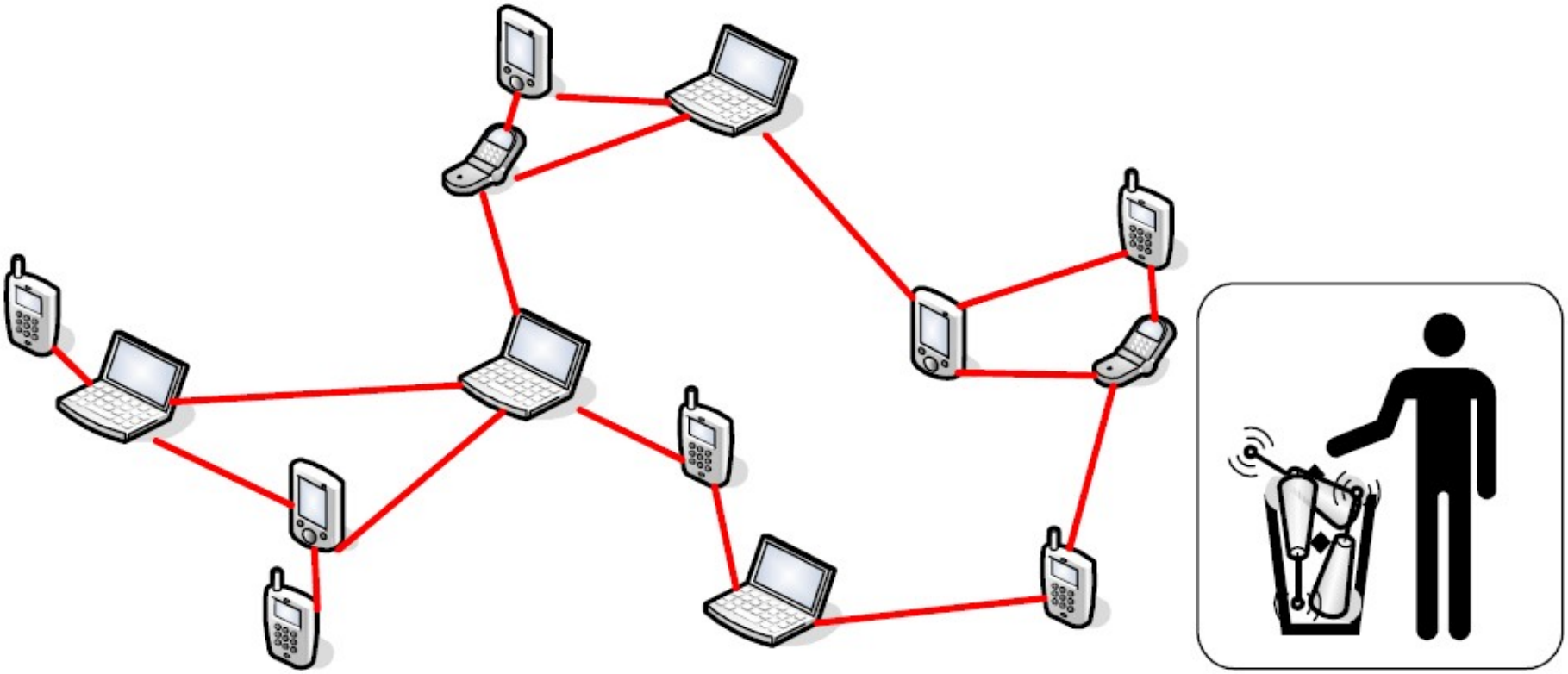
- Ce n'est qu'avec l'arrivée du protocole 802.11 de l'IEEE qui permet de bâtir des réseaux sans fil autour de bases fixes, que la recherche civile s'empare à la fin des années 90 des problématiques liées à ces réseaux.
- L'activité du groupe MANET (Mobile Ad hoc NETworks) de l'IETF (Internet Engineering Task Force) montre que le développement de ces réseaux sans fil et sans infrastructure est en plein essor. Cependant, cette absence d'infrastructure fixe pose un certain nombre de problèmes non triviaux.
- Les réseaux Ad Hoc sont idéals pour les applications caractérisées par une absence (ou la non-fiabilité) d'une infrastructure préexistante, tel que les applications militaires et les autres applications de tactique comme les opérations de secours (incendies, tremblement de terre..) et les missions d'exploration.

2/ Définition (1)

- Un réseau mobile Ad Hoc appelé généralement MANET, consiste en une grande population relativement dense d'unités mobiles qui se déplacent dans un territoire quelconque.
- Le seul moyen de communication est l'utilisation des «ondes radio» qui se propagent entre les différents nœuds mobiles sans l'aide d'une infrastructure préexistante ou administration centralisée.
- Dans un réseau Ad Hoc, un nœud peut communiquer directement (mode *point-à-point*) avec n'importe quel nœud s'il est situé dans sa zone de transmission, tandis que la communication avec un nœud situé en dehors de sa zone de transmission s'effectue via plusieurs nœuds intermédiaires (mode *multi-sauts*)

2/ Définition (2)

- Dans un réseau Ad Hoc, l'absence d'infrastructure ou d'un réseau filaire composé de station de base, oblige les unités mobiles à se comporter comme des routeurs qui participent à la découverte et à la maintenance des chemins pour les autres hôtes du réseau.



Exemple d'un réseau Ad Hoc

3/ Caractéristiques (1)

- Les principales caractéristiques des réseaux Ad Hoc sont les suivantes:

➢ **Mobilité (Une topologie dynamique) :**

- La mobilité des nœuds dans un réseau Ad Hoc est intrinsèque au fonctionnement du réseau.
- Dans un réseau Ad Hoc, la topologie du réseau peut changer rapidement, de façon aléatoire et non prédictible et les techniques de routage des réseaux classiques, basées sur des routes préétablies, ne peuvent plus fonctionner correctement.

➢ **Equivalence des nœuds du réseau :**

- Dans un réseau classique, il existe une distinction nette entre les nœuds terminaux (stations, hôtes) qui supportent les applications et les nœuds internes (routeurs par exemple) du réseau, en charge de l'acheminement des données.
- Cette différence n'existe pas dans les réseaux ad hoc car tous les nœuds peuvent être amenés à assurer des fonctions de routage.

3/ Caractéristiques (2)

- **Liaisons sans fil (Une bande passante limitée) :**

- Les technologies de communication sans fil sont indispensables à la mise en place d'un réseau Ad Hoc.
- Malgré des progrès très importants, leurs performances restent en dessous de celles des technologies des réseaux filaires.
- La bande passante est moins importante, alors que le routage et la gestion de la mobilité génèrent davantage de flux de contrôle et de signalisation que dans une architecture de réseau filaire.

- **Vulnérabilité (Une sécurité physique limitée) :**

- Les réseaux sans fil sont par nature plus sensibles aux problèmes de sécurité.
- Pour les réseaux Ad Hoc, le principal problème réside dans le fait que tous les nœuds sont équivalents et potentiellement nécessaires au fonctionnement du réseau**.**

3/ Caractéristiques (3)

- **Interférences Radio :**

- Due à l'utilisation du médium radio dans les communications sans fil, les interférences et le taux de collision de paquets sont élevés.
- Le phénomène des nœuds caché est parmi les phénomènes très particuliers à l'environnement sans fil, où les nœuds voisins utilisent le support de communication simultanément

- **Autonomie des nœuds (Des contraintes d'énergie) :**

- La consommation d'énergie constitue un problème important pour des équipements fonctionnant grâce à une alimentation électrique autonome.
- Ces équipements intègrent des modes de gestion d'énergie et il est important que les protocoles mis en place dans les réseaux Ad Hoc prennent en compte ce problème**.**

4/ Avantages et inconvénients (1)

- Les avantages de cette technologie sont nombreux du fait qu'il n'y a pas besoin d'infrastructure préexistante :

- Les réseaux Ad Hoc peuvent être déployés dans un environnement quelconque.
- Le coût d'exploitation du réseau est faible : aucune infrastructure n'est à mettre en place initialement et surtout aucun entretien n'est à prévoir.
- Le déploiement d'un réseau Ad Hoc est simple et rapide : ne nécessite aucun prérequis puisqu'il suffit de disposer d'un certain nombre de terminaux dans un espace pour créer un réseau Ad Hoc.
- La souplesse d'utilisation : est un paramètre très important, puisque les seuls éléments pouvant tomber en panne sont les terminaux eux-mêmes (si une station qui sert au routage tombe en panne donc elle peut être remplacée par une autre).

4/ Avantages et inconvénients (2)

- Même si les perspectives pour les réseaux Ad Hoc sont prometteuses, plusieurs contraintes restent encore à traiter :

- La connectivité limite les possibilités de communication. Ainsi, deux stations ne sont joignables que s'il existe un ensemble de stations pouvant assumer la fonction de routage afin de faire suivre les paquets de données échangés entre les deux stations.
- Les liens entre les stations ne sont pas isolés les uns des autres et polluent le voisinage, par diffusion, lors de chaque émission ou réception des données. La diffusion est un facteur qui alourdit aussi d'autres paramètres tels que la bande passante et la consommation de la batterie.
- La sécurité dans les réseaux Ad Hoc est difficile à contrôler, car l'écoute clandestine est très simple à réaliser.
- La faible autonomie des batteries constitue un frein à une utilisation longue du terminal et à la mise en place de nouveaux services, du moment que les ressources énergétiques sont mises en commun même pour les besoins du routage.

5/ Domaines d’application

- Les applications tactiques comme les opérations de secours, militaires ou d’explorations trouvent en Ad Hoc, le réseau idéal.
- La technologie Ad Hoc intéresse également la recherche, ainsi que les applications civiles. Nous pouvons en distinguer:

- **Les services d’urgence** : opération de recherche et de secours des personnes (ex. tremblement de terre, incendie, etc.) dans le but de remplacer l’infrastructure filaire.
- **Le travail collaboratif et les communications dans des entreprises ou bâtiments** : dans le cadre d’une réunion ou d’une conférence par exemple.
- **Les applications commerciales** : pour un paiement électronique distant ou pour l’accès mobile à l’Internet, ou service de guide en fonction de la position de l’utilisateur.
- **Les réseaux de capteurs** : Les capteurs, chargés de mesurer les propriétés physiques des environnements (comme la température, la pression, etc.), sont dispersés (le plus souvent déployés à partir d’un avion ou d’un hélicoptère) par centaines, voire par milliers sur le site, effectuent leurs mesures et envoient les résultats à une station par l’intermédiaire d’un routage Ad Hoc à travers le réseau.

6/ Routage (1)

- Le Routage consiste à faire transiter une information depuis un émetteur vers une destination.
- Le rôle principal d'un protocole de routage consiste à établir des routes efficaces entre une paire de nœuds pour que les messages puissent être livrés au moment opportun.
- La construction des routes doit être faite avec un minimum de charge de contrôle et de consommation de bande passante.
- A cause de l'absence d'un contrôle centralisé, le routage dans un réseau Ad Hoc devient le problème principal et un challenge majeur car la topologie du réseau change constamment.
- Le problème qui se pose dans le contexte des réseaux Ad Hoc est l'adaptation de la méthode d'acheminement utilisée avec le grand nombre d'unités existant dans un environnement caractérisé par de modestes capacités de calcul et de sauvegarde.

6/ Routage (2)

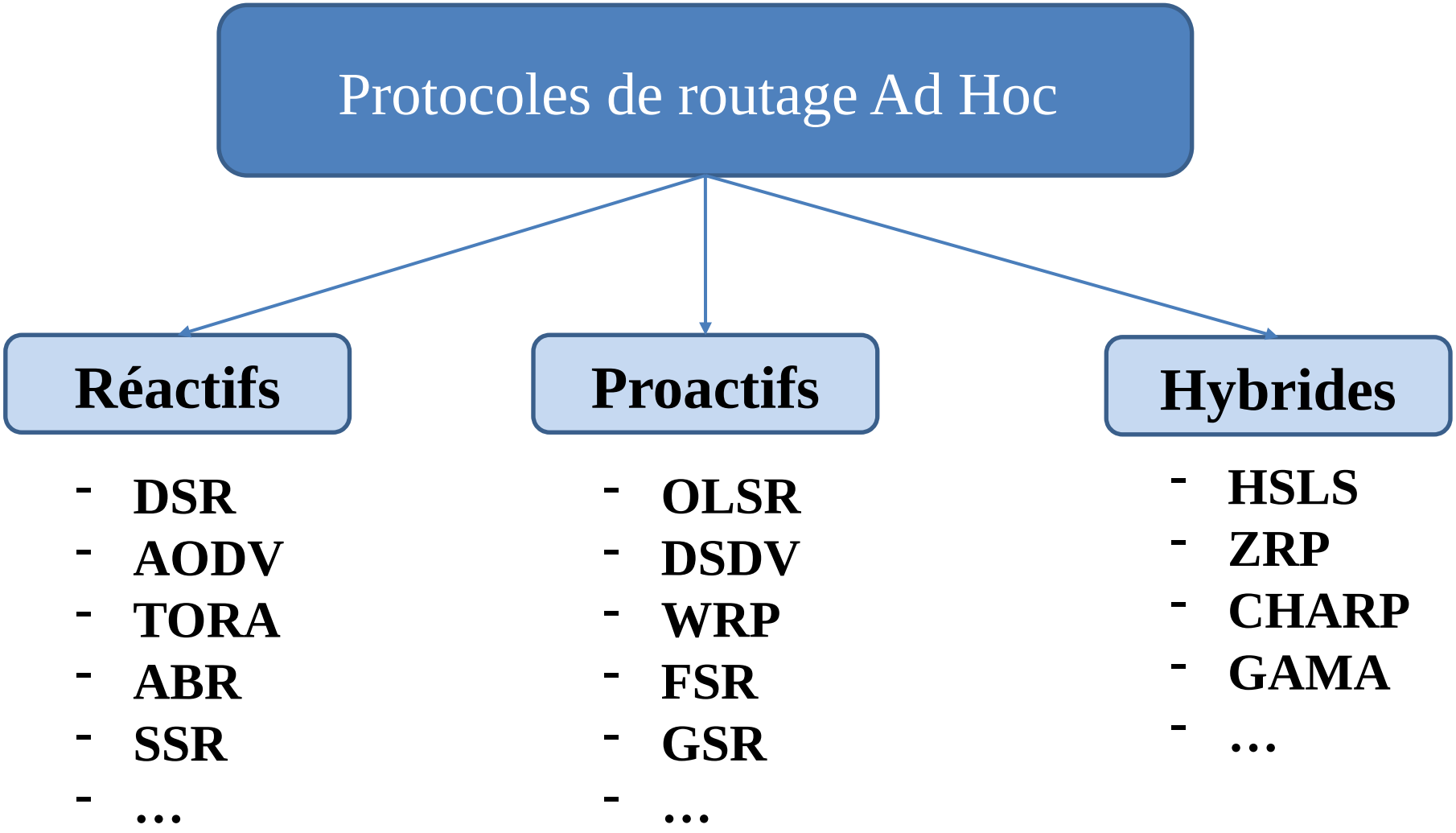
- Plusieurs protocoles de routage ont été proposés pour les réseaux Ad Hoc, qu'ils s'agissent d'adaptation des protocoles de routage existants au contexte Ad Hoc ou de nouveaux protocoles spécifiques aux réseaux MANET.
- Globalement, toutes stratégies de routage reposent sur des méthodes et des mécanismes que l'on peut regrouper en deux grandes classes :

➢ Les protocoles de routage proactifs qui anticipent la demande de routage de paquets.

➢ Les protocoles de routage réactifs qui réagissent à la demande.

- Nous pouvons trouver également les protocoles de routage hybrides qui représente une combinaison entre les deux classes précédentes.

6/ Routage (3)



Classes de protocoles de routage Ad Hoc

6/ Routage (4)
Les protocoles de routage réactifs

- Les protocoles de routage réactifs (ou protocoles de routage à la demande) représentent les protocoles les plus récents, proposés dans le but d'assurer le service du routage dans les réseaux sans fil Ad Hoc.
- La majorité des solutions proposées pour résoudre le problème de routage dans les réseaux Ad Hoc, et qui sont évaluées par le groupe de travail MANET de l'IETF, appartiennent à cette classe de protocoles de routage.
- Les protocoles de routage appartenant à cette catégorie, créent et maintiennent les routes selon les besoins. Lorsque le réseau a besoin d'une route, une procédure de découverte de routes est lancée.
- Actuellement, les plus connus de ces protocoles est AODV (Ad hoc On Demande Distance Vector) et DSR (Dynamic Source Routing Protocol).

6/ Routage (5)
Les protocoles de routage réactifs

- Dans le routage réactif *(reactive routing* ou *on-demand routing)*, les tables de routage ne sont mises à jour que lorsque le besoin s'en fait sentir. L'approche générale est la suivante:

➢ Si le nœud qui désire acheminer un paquet de données vers une certaine direction constate que sa table de routage ne contient aucune indication pour atteindre cette destination, il diffuse alors dans l'ensemble du réseau un message de contrôle *(RREQ: Route REQuest)* invitant tous les nœuds du réseau à mettre à jour leur table de routage vis-à-vis de la destination visée.

➢ Cette mise à jour s'effectue aussi grâce à un second message de contrôle (*RREP: Route REPly*) initié par le nœud destinataire lui-même. Ce message est remonté (en *source-routing*) vers le nœud source.

6/ Routage (6)
Les protocoles de routage réactifs

- Dans le mécanisme de routage des protocoles reposant sur une approche réactive aucun message de contrôle ne charge le réseau pour des routes inutilisées ce qui permet de ne pas gaspiller les ressources du réseau.
- Les principaux inconvénients sont les suivants:

➢ La mise en place d'une route par inondation peut être coûteuse et provoquer des délais importants avant qu'une route vers une certaine destination puisse être exploitée pour la première fois.

➢ En cas de changements de topologie fréquents, une réactualisation fréquente des routes dans le réseau est nécessaire.

6/ Routage (7)
Les protocoles de routage proactifs

- Dans le routage proactif *(proactive routing* ou *table-driven routing)*, chaque nœud s'efforce de maintenir constamment à jour sa propre table de routage, de sorte que lorsqu'un paquet de données doit être émis (ou routé) par ce nœud, la route que ce paquet doit suivre soit d'ores et déjà connue, et donc immédiatement exploitable.
- L'approche communément adoptée pour réaliser ce type de routage consiste à faire en sorte que chaque nœud diffuse périodiquement sa propre table de routage, et la mette par ailleurs à jour en fonction d'informations similaires reçues de tous ses voisins.
- Dans ce type de routage les routes sont sauvegardées même si elles ne sont pas utilisées.
- Les plus aboutis de ces protocoles est OLSR (Optimized Link State Routing Protocol) et DSDV (Destination Sequenced Distance Vector).

6/ Routage (8)
Les protocoles de routage proactifs

- Avec un protocole proactif, les routes sont disponibles immédiatement ; ainsi, l'avantage d'un tel protocole est le gain de temps lors d'une demande de route.
- Les inconvénients majeurs sont les suivants:

➢ Le surcoût important occasionné par le trafic induit par les messages de contrôle et de mise à jour des tables de routage.

➢ Le temps de réaction souvent assez long lorsque des changements dans la topologie du réseau obligent l'ensemble des nœuds à corriger leurs tables de routage en conséquence, ce qui gaspille la capacité du réseau sans fil.

➢ La taille des tables de routage croit linéairement en fonction du nombre de nœud.

6/ Routage (9)
Les protocoles de routage hybrides

- Les protocoles de routage dits « hybrides » (par exemple HSLS (Hazy Sighted Link State) et ZRP (Zone Routing Protocol)) sont des protocoles qui combinent les approches proactives et réactives afin de bénéficier du meilleur de ces deux techniques.
- Ils utilisent un protocole proactif, pour apprendre à chaque nœud son voisinage à un, deux ou trois sauts, etc. Ainsi, ces protocoles disposent des routes immédiatement dans le voisinage. Au delà de cette zone prédéfinie, le protocole hybride fait appel aux techniques des protocoles réactifs pour chercher des routes.

6/ Routage (10)
Les protocoles de routage hybrides

- Avec ce découpage, le réseau est partagé en plusieurs zones, et la recherche de route en mode réactif peut être améliorée.
- A la réception d'une requête de recherche réactive, un nœud peut indiquer immédiatement si la destination est dans le voisinage ou non, et par conséquent savoir s'il faut aiguiller la dite requête vers les autres zones sans déranger le reste de sa zone.
- Ce type de protocole s'adapte bien aux grands réseaux, cependant, il cumule aussi les inconvénients des protocoles réactifs.

7/ Exemples de protocoles de routage (1)
Le protocole DSR

- *DSR* (*Dynamic Source Routing*) est l'un des premiers protocoles de routage qui a été proposé pour les réseaux *Ad Hoc*. Après de nombreuses années, il a été normalisé sous la forme de la *RFC* 4728.
- Il s'agit d'un protocole réactif qui a la particularité de s'appuyer sur un routage par la source.
- Lorsqu'un paquet est émis, celui-ci contiendra toutes les informations (la liste des nœuds par lesquels doit passer le paquet) qui sont nécessaires à son acheminement jusqu'à la destination.
- Le protocole se décompose en deux grandes phases : la découverte et la maintenance de route.

7/ Exemples de protocoles de routage (2)

Le protocole DSR

Procédure de découverte de route

- Lorsqu'un nœud cherche à émettre un paquet vers une destination pour laquelle il n'a pas de route en cache, le nœud initie une découverte de route vers la destination, appelée alors la cible, et met le paquet dans un tampon.
- Un message *RREQ* est envoyé en diffusion à l'aide d'un mécanisme d'inondation. Ce message contient les informations nécessaires au bon fonctionnement de la découverte de route, à savoir : l'adresse du nœud initiateur, l'adresse de la cible, un identifiant unique de la requête, ainsi qu'une liste de tous les nœuds parcourus par le message. Cette liste est évidemment différente pour chaque instance du message.

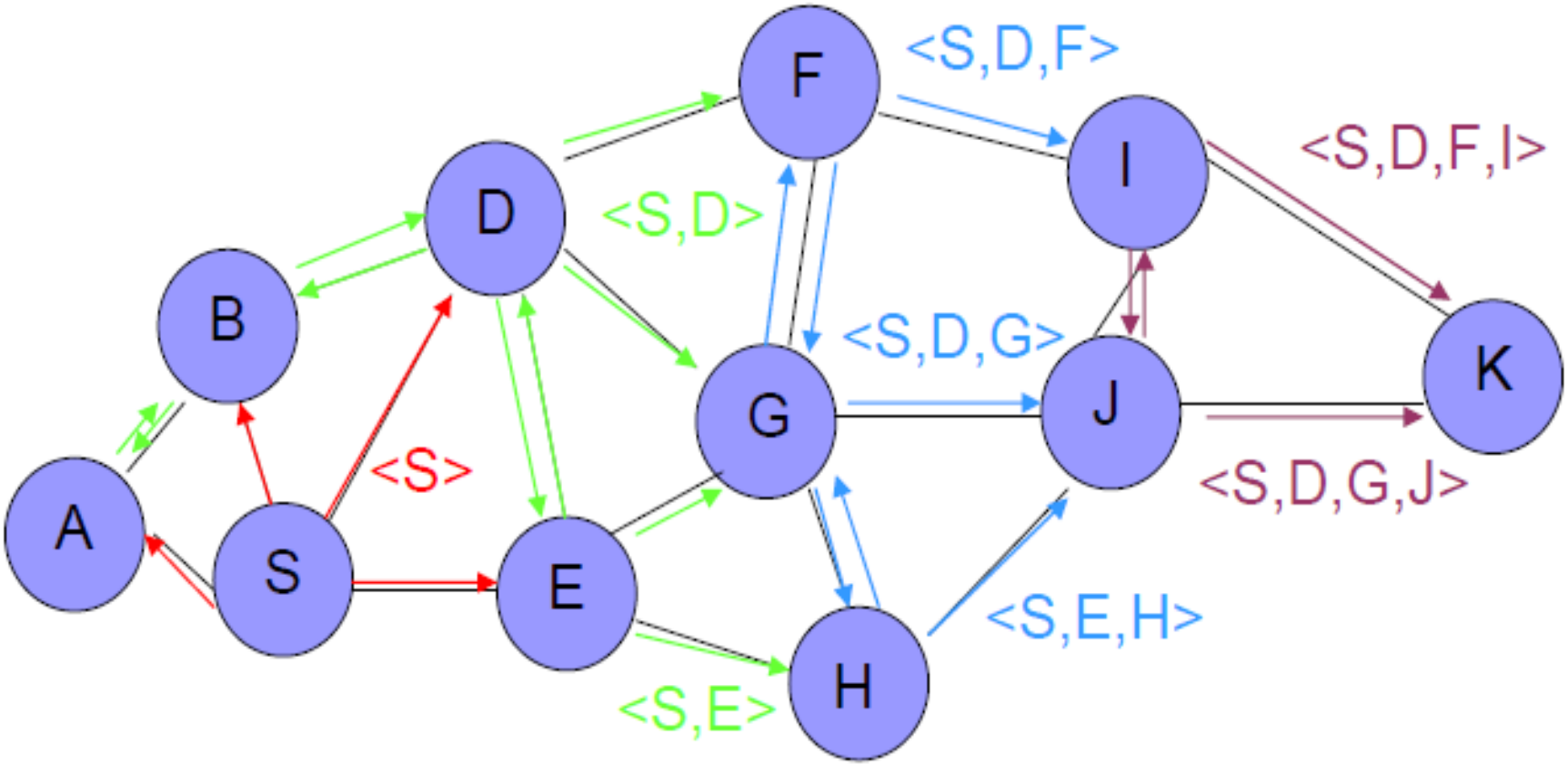
7/ Exemples de protocoles de routage (3)

Le protocole DSR

Procédure de découverte de route

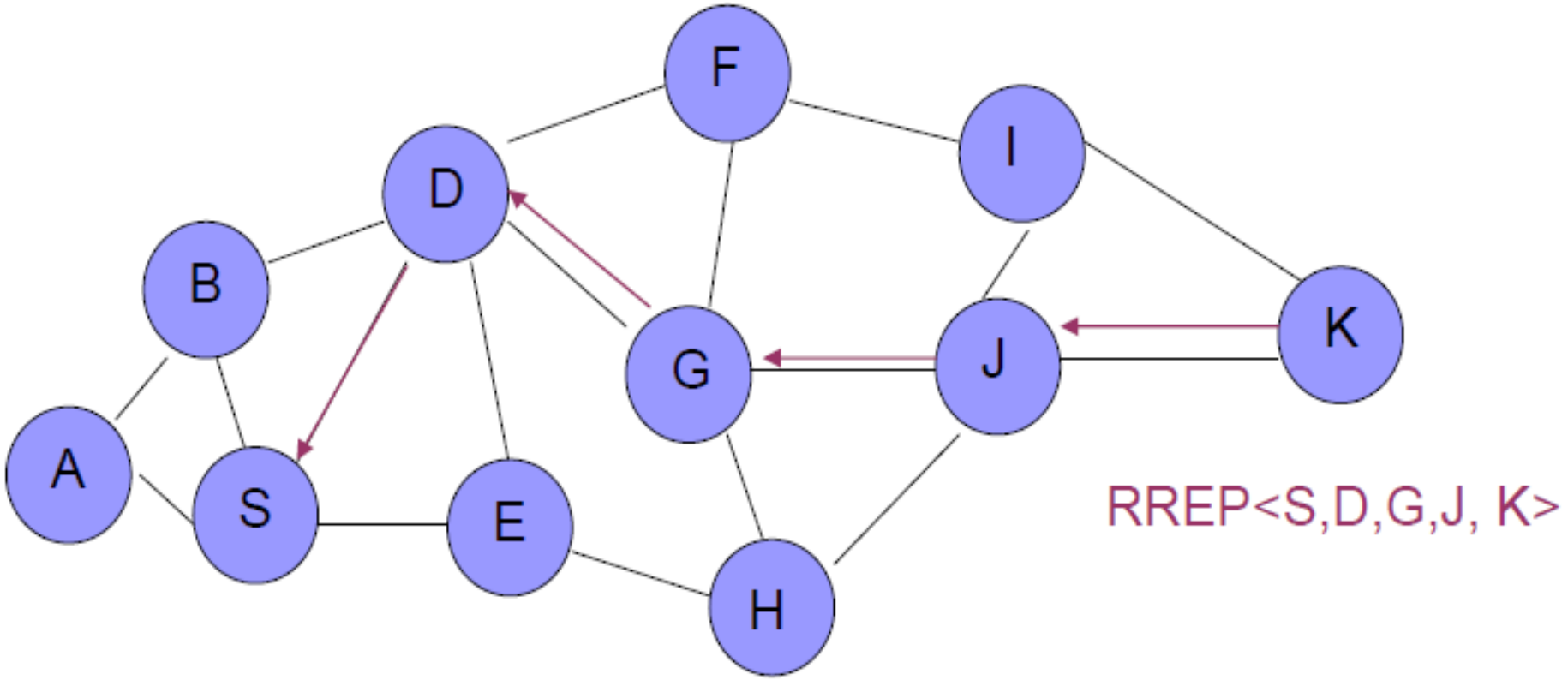
- Lorsqu'un nœud reçoit un message *RREQ*, s'il n'est pas la cible de cette requête, alors il détermine s'il doit retransmettre la requête. Celle-ci ne sera retransmise que si aucune requête du même nœud initiateur avec le même identifiant n'a été reçue et si le nœud n'apparait pas à la liste des nœuds parcourus par le message. Avant l'éventuelle retransmission, le nœud s'ajoute à la liste des nœuds parcourus.
- Si le nœud recevant le message *RREQ* est la cible de la requête, alors une réponse *RREP* est envoyée au nœud initiateur. Cette réponse contient la liste des nœuds parcourus par le message *RREQ* reçu.
- Lorsque le nœud initiateur reçoit une réponse *RREP*, la route fournie est mise en cache afin de pouvoir être réutilisée ultérieurement. Les paquets mis en tampon pour la cible sont finalement émis.

7/ Exemples de protocoles de routage (4)
Le protocole DSR



Le nœud source S désire communiquer avec le nœud K: Emission d'un message RREQ

7/ Exemples de protocoles de routage (5)
Le protocole DSR



Envoi d'un message RREP de K à S par chemin inverse

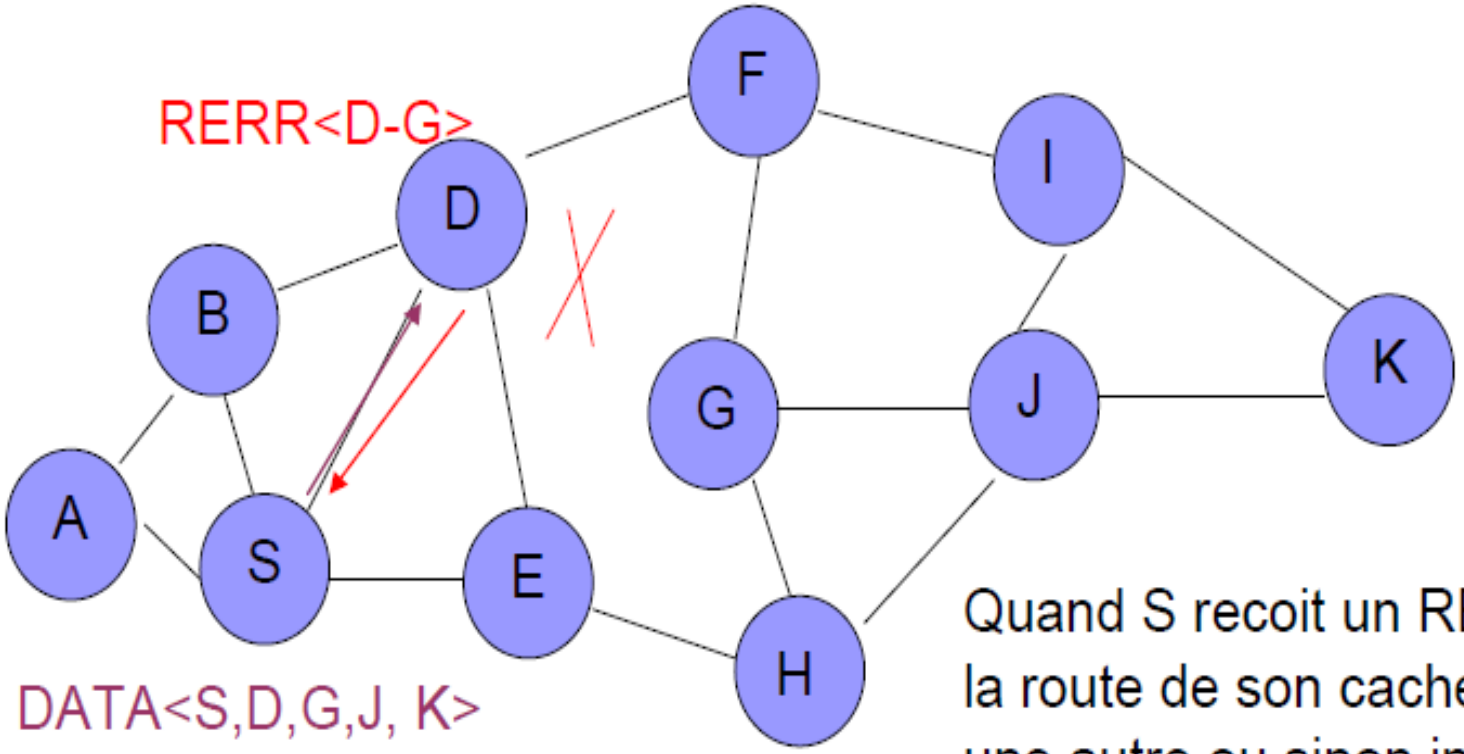
7/ Exemples de protocoles de routage (6)

Le protocole DSR

Procédure de maintenance de route

- Quand un nœud détecte un problème fatal de transmission, à l'aide de sa couche liaison, un message *RERR (Route ERRor)* est envoyé à l'émetteur original du paquet.
- Le message d'erreur contient l'adresse du nœud qui a détecté l'erreur et celle du nœud qui le suit dans le chemin.
- Lors de la réception du paquet *RERR* par le nœud source, le nœud concerné par l'erreur est supprimé du chemin sauvegardé, et tous les chemins qui contiennent ce nœud sont tronqués à ce point-là.
- Si aucun autre chemin n'existe vers la destination, une nouvelle opération de découverte de route est initiée par l'émetteur.

7/ Exemples de protocoles de routage (7)
Le protocole DSR



Quand S recoit un RERR, il retire la route de son cache, en essaye une autre ou sinon initialise une nouvelle ROUTE DISCOVERY.

Envoi d'un message RREP de K à S par chemin inverse

7/ Exemples de protocoles de routage (8)

Le protocole DSR

Avantages et inconvénients

- Parmi les avantages du protocole *DSR* utilisant la technique « routage à la source », on peut citer le fait que les nœuds de transit n'aient pas besoin de maintenir les informations de mise à jour pour envoyer les paquets de données, puisque ces derniers contiennent toutes les décisions de routage.
- En outre, dans ce protocole, il y a une absence totale de boucle de routage, car le chemin source destination fait partie des paquets de données envoyés.
- Dans le cas ou les chemins reliant deux nœuds deviennent longs, l'ajout de l'ensemble des nœuds permettant d'atteindre une destination dans les paquets influence négativement sur la bande passante.

7/ Exemples de protocoles de routage (9)

Le protocole AODV

Principe

- Le protocole *AODV* (*Ad hoc On-demand Distance Vector*) est un protocole de routage réactif ce qui signifie qu'une route vers une certaine destination n'est construite que lorsqu'elle est nécessaire.
- *AODV* emprunte l'utilisation des numéros de séquence de *DSDV* pour actualiser ses informations de routage et se prémunir des boucles, tandis que sa procédure de découverte de route est dérivée de celle adoptée par *DSR*.
- La principale différence avec *DSR* est que la route découverte est stockée au niveau de chaque nœud plutôt que dans l'entête du paquet.
- Ce protocole fonctionne également à partir de trois types de messages : RREQ, RREP et RERR.

7/ Exemples de protocoles de routage (10)

Le protocole AODV

Gestion de la table de routage (1)

- Le protocole *AODV* maintient les chemins d'une façon distribuée en gardant une table de routage, au niveau de chaque nœud de transit appartenant au chemin cherché.
- Une entrée de la table de routage contient essentiellement :

➢ L'adresse *IP* de la destination,

➢ L'adresse *IP* du nœud suivant,

➢ Le nombre de sauts nécessaire pour atteindre la destination,

➢ Le numéro de séquence de la destination,

➢ La liste des voisins actifs,

➢ Le temps d'expiration de l'entrée de la table (temps au bout duquel l'entrée est invalidée),

➢ L'état de la route et autres avertissements (valide, invalide, à réparer, en cours de réparation).

7/ Exemples de protocoles de routage (11)

Le protocole AODV

Gestion de la table de routage (2)

- De plus chaque nœud utilise une table *source-broadcast_id* qui contient le dernier *broadcast_id* de chaque source qui a diffusé un *RREQ*. Cette table est utilisée pour faire la différence entre les nouvelles demandes de route et les anciennes.
- Pour éviter le problème du comptage à l'infini de *Bellman-Ford*, on a recours à l'utilisation de numéros de séquence dans les tables de routage en plus de la distance.
- Le numéro de séquence accompagne son adresse dans les messages de contrôle et permet aux autres nœuds de distinguer les messages importants des messages redondants.

7/ Exemples de protocoles de routage (12)

Le protocole AODV

Gestion de la table de routage (3)

- Une mise à jour de la table de routage ne s'effectue que si l'une des conditions suivantes est vérifiée :

➢ Le numéro de séquence du paquet de contrôle est strictement supérieur au numéro de séquence contenu dans la table de routage.

➢ Les numéros de séquence (de la table et du paquet) sont égaux mais la distance en nombre de sauts du paquet plus *«1»* est inférieure à la distance actuelle dans la table de routage.

➢ Le numéro de séquence pour cette destination est inconnu.

7/ Exemples de protocoles de routage (13)

Le protocole AODV

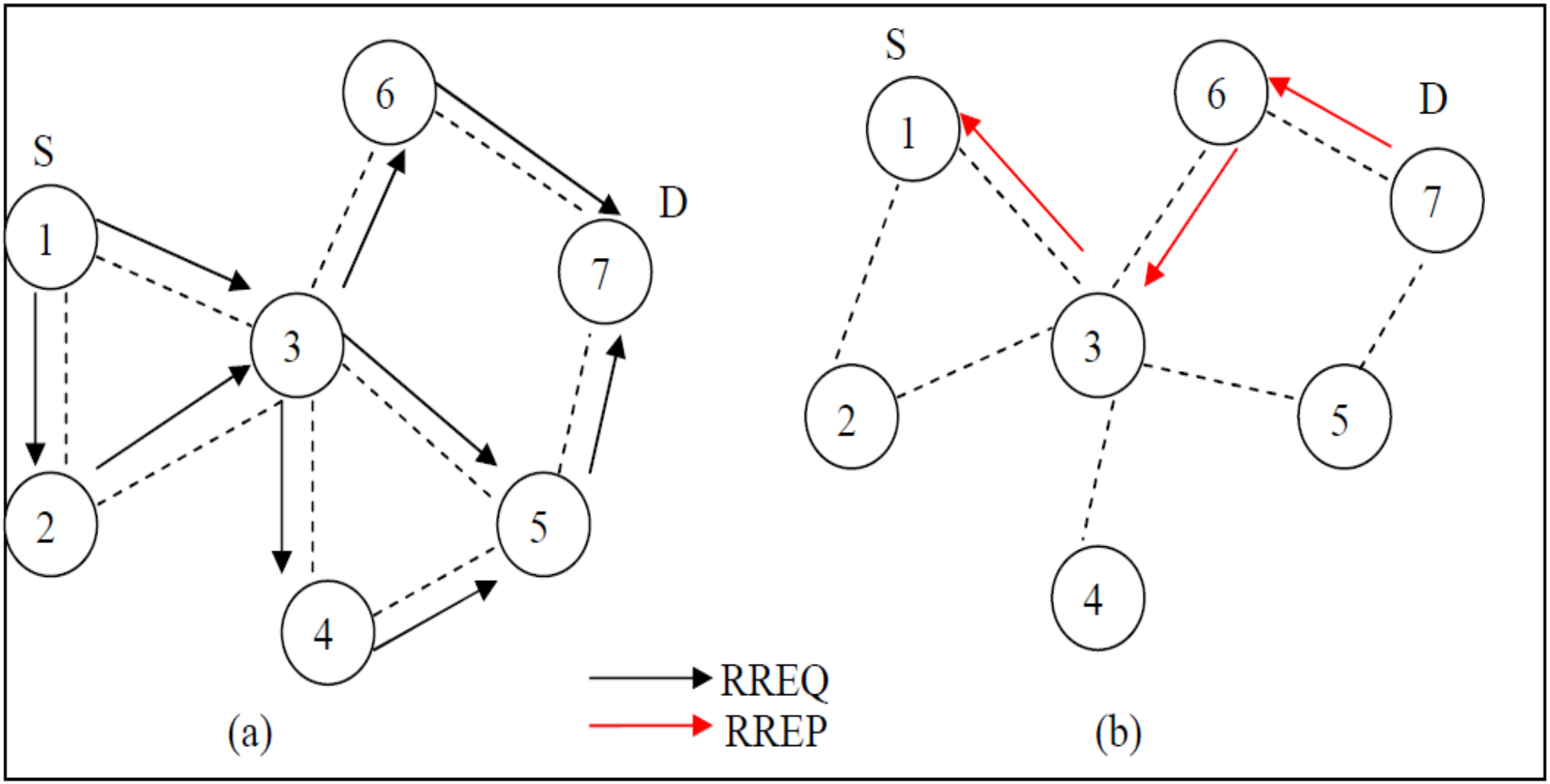
Découverte de route (1)

- Un nœud source souhaitant communiquer avec un nœud destinataire doit d'abord consulter sa table de routage. S'il ne trouve pas localement toutes les informations sur la route à suivre ; il diffusera un message de demande de route (*RREQ*) aux nœuds voisins.
- Avant de faire suivre le paquet *RREQ* à ses voisins, un nœud intermédiaire sauvegarde aussi l'identificateur du nœud à partir duquel la première copie de la requête a été reçue. Cette information est utilisée pour construire le chemin inverse, qui sera ensuite emprunté par le paquet *RREP* de manière unicast.
- A la réception d'un message *RREQ*, la destination envoie un *RREP*, ce message peut donc être acheminé vers la source et les nœuds intermédiaires vont également modifier leur table de routage suivant les champs contenus dans le paquet *RREP*.

7/ Exemples de protocoles de routage (14)

Le protocole AODV

Découverte de route (2)



Etablissement d'une route entre S et D

7/ Exemples de protocoles de routage (15)

Le protocole AODV

Format d'un paquet RREQ (1)

- Le format général d'un paquet *RREQ* est le suivant :

type	*Nbr_saut*	*Brcst_id*	*Dst_id*	*Dst_ns*	*Src_id*	*Src_ns*	*TTL*

- *Type :* indique le type du message,
- *Nbr_saut* : ce champ est incrémenté à chaque saut, il détermine le nombre de sauts vers la source du *RREQ*,
- *Brcst_id* : représente la combinaison de l'identificateur de la source avec son numéro de séquence,
- *Dst_id* : indique l'identificateur de la destination désirée,
- *Dst_ns* : correspond au numéro de séquence de la destination désirée,
- *Src_id* : indique l'identificateur de la source du *RREQ*,
- *Src_ns* : correspond au numéro de séquence de la source du *RREQ*,
- *TTL* : désigne la durée de vie du paquet *RREQ*.

7/ Exemples de protocoles de routage (16)

Le protocole AODV

Format d'un paquet RREQ (2)

- Le champ *Dst_ns* du paquet *RREQ* recevra la dernière valeur connue du numéro de séquence associé au nœud destinataire qui est recopiée de la table de routage. Si le numéro de séquence n'est pas connu, la valeur nulle sera prise par défaut. Le champ *Src_ns* du paquet *RREQ* recevra la valeur du numéro de séquence du nœud source.
- Si aucun *RREP* n'est reçu durant une certaine période (appelée *RREP_WAIT_TIME*), la source peut rediffuser une nouvelle requête *RREQ*.
- A chaque nouvelle diffusion, le champ *Brcst_id* du paquet *RREQ* est incrémenté pour identifier une requête de route particulière associée à une adresse source.
- Si la requête *RREQ* est rediffusée un certain nombre de fois (*RREQ_RETRIES*) sans la réception de réponse, un message d'erreur doit être délivré à l'application.

7/ Exemples de protocoles de routage (17)

Le protocole AODV

Format d'un paquet RREP

- Le format général d'un paquet *RREP* est le suivant :

Type	*Nbr_saut*	*Dst_id*	*Dst_ns*	*Src_id*	*TTL*

- *Type* : indique le type du message,
- *Nbr_saut* : ce champ est incrémenté à chaque saut, il détermine le nombre de sauts vers la source du *RREP*,
- *Dst_id* : indique l'identificateur de la destination du *RREP*,
- *Dst_ns* : correspond au numéro de séquence de la destination du *RREP*,
- *Scr_id* : indique l'identificateur de la source du *RREP*,
- *TTL* : désigne la durée de vie du paquet *RREP*.

Note: Une réponse adéquate qu'on appelle *RREP* gratuit « *Gratuitous RREP* » peut être générée par un nœud intermédiaire si celui-ci possède une route fraîche vers la destination. Un *RREP* sera alors envoyé vers la destination par le nœud intermédiaire.

7/ Exemples de protocoles de routage (18)

Le protocole AODV

Maintenance de route (1)

- *AODV* propose deux méthodes pour détecter la présence des nœuds voisins et donc pour détecter la rupture d'un lien de communication.
  - La première est basée sur l'envoi de messages *HELLO* (qui est un *RREP* avec un *TTL* égale à *«1»*) à intervalle régulier,
  - tandis que la seconde repose sur les informations émanant directement de la sous couche *MAC*.
- Si un lien se brise le long d'une route active. Le nœud précédant la cassure peut choisir d'effectuer une réparation locale ou bien délivrer un message d'erreur listant l'ensemble des destinations injoignables. Par conséquent, Une nouvelle phase de demande de route devra être établie par le nœud d'origine.

7/ Exemples de protocoles de routage (19)

Le protocole AODV

Maintenance de route (2)

- En règle générale, les erreurs de routes et les liens brisés requièrent un traitement en quatre étapes:
  - rendre invalides des routes existantes,
  - lister les nœuds destinataires affectés par ces erreurs,
  - déterminer les éventuels voisins affectés par ces erreurs,
  - envoyer le message d'erreur *RERR* approprié à ces voisins.

7/ Exemples de protocoles de routage (20)

Le protocole AODV

Maintenance de route (3)

- Le format des messages d'erreur de route (*RERR*) se distingue des autres messages par les informations suivantes :

➢ *N* (*No Delete Flag)* : ce drapeau est utilisé si un nœud vient de réparer un lien local. Il indique aux autres nœuds de ne pas supprimer la route de leur table de routage.

➢ *DestCount* : ce champ indique le nombre de destinations inaccessibles annoncées dans le message. Du fait de la nature des messages *RERR*, ce champ doit valoir au moins *«1»*.

➢ *Unreachable Destination IP Address* : dans ces champs, il est indiqué la liste des adresses *IP* des différentes destinations inaccessibles concernées par ce message.

➢ *Unreachable Destination Sequence Number* : dans ces champs, il est indiqué la liste des numéros de séquence des différentes destinations inaccessibles concernées par ce message.

7/ Exemples de protocoles de routage (21)

Le protocole OLSR

Principe

- OLSR (Optimized Link State Routing) est un protocole de routage proactif, utilisé dans les réseaux Ad Hoc denses et peu mobiles.
- Il représente une adaptation et une optimisation du principe de routage à état de lien OSPF (Open Shortest Path First) pour les réseaux ad hoc.
- Il permet d'obtenir les routes de plus court chemin. L'optimisation tient au fait que dans un protocole à état de lien, chaque nœud déclare ses liens directs avec tous ses voisins à tout le réseau. Dans le cas d'OLSR, les nœuds ne vont déclarer qu'une sous partie de leur voisinage par l'utilisation de relais multipoints MPR (Multipoint Relay).
- Les MPR sont utilisés pour minimiser le trafic dû à la diffusion des messages de contrôle dans le réseau.

7/ Exemples de protocoles de routage (22)

Le protocole OLSR

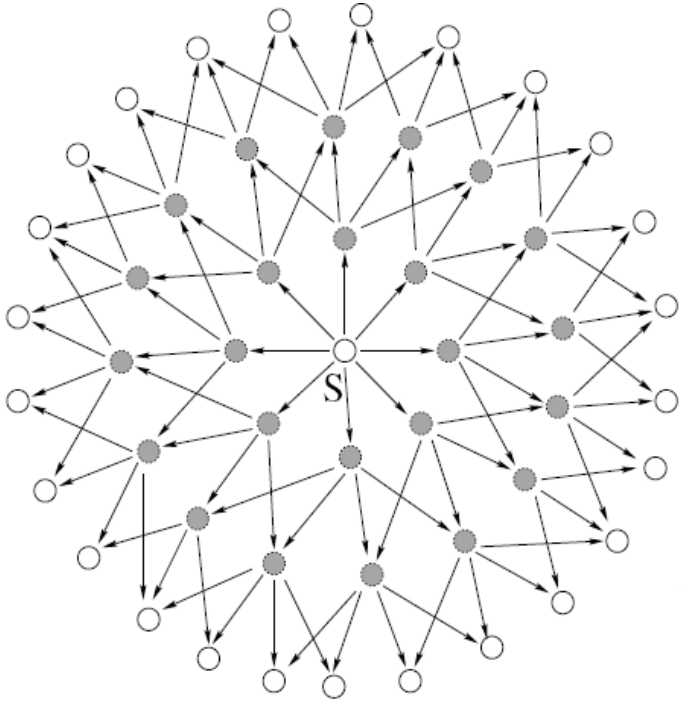
Principe

- Un MPR est un nœud sélectionné par un de ses voisins immédiats (appelé MS, MPR Selector) pour retransmettre ses messages de mise à jour.
- L'ensemble des MPR d'un nœud est choisi parmi les voisins immédiats, de manière à permettre d'atteindre tous les nœuds situés exactement à 2 sauts.
- OLSR utilise un seul format de message. L'entête précise si le message doit être seulement transmis au voisinage immédiat ou bien à l'ensemble du réseau.
- Le routage vers les stations éloignées de plus d'un saut (1+N sauts) se fait grâce aux MPR, qui diffusent périodiquement des messages TC (Topology Control) contenant la liste de leurs MS.

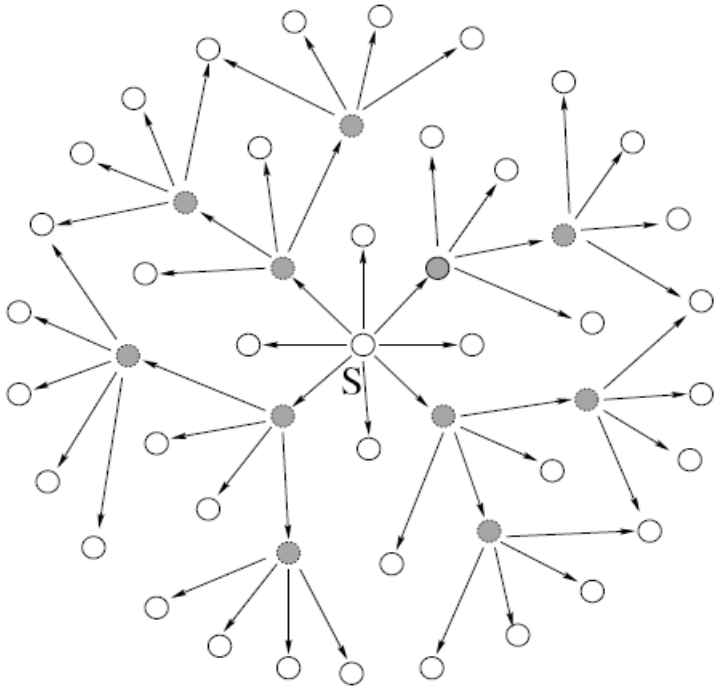
7/ Exemples de protocoles de routage (23)

Le protocole OLSR

Exemple: Nœuds à 3 sauts



Nœud retransmettant



Inondation classique: tous les nœuds retransmettent le message (24 retransmissions)

Inondation avec MPR: Seuls quelques nœuds MPR retransmettent le message (11 retransmissions)

7/ Exemples de protocoles de routage (24)
Le protocole DSDV

- Le protocole *DSDV* (Destination Sequence-Distance Vector) est un protocole de routage proactif orienté destination.
- Il est dérivé d'un algorithme classique de vecteur de distance, l'algorithme distribué de Bellman-Ford (DBF). Des perfectionnements sont faits afin d'éviter le problème des boucles présentes dans DBF. Ceci est évité en étiquetant chaque entrée de la table de routage avec un numéro de séquence pour commander l'information de routage.
- Dans DSDV, chaque nœud maintient une table de routage qui a une entrée pour chaque destination dans le réseau.
- Les principaux attributs pour chaque destination sont le prochain saut, le nombre de sauts, et un numéro de séquence.

7/ Exemples de protocoles de routage (25)
Le protocole DSDV

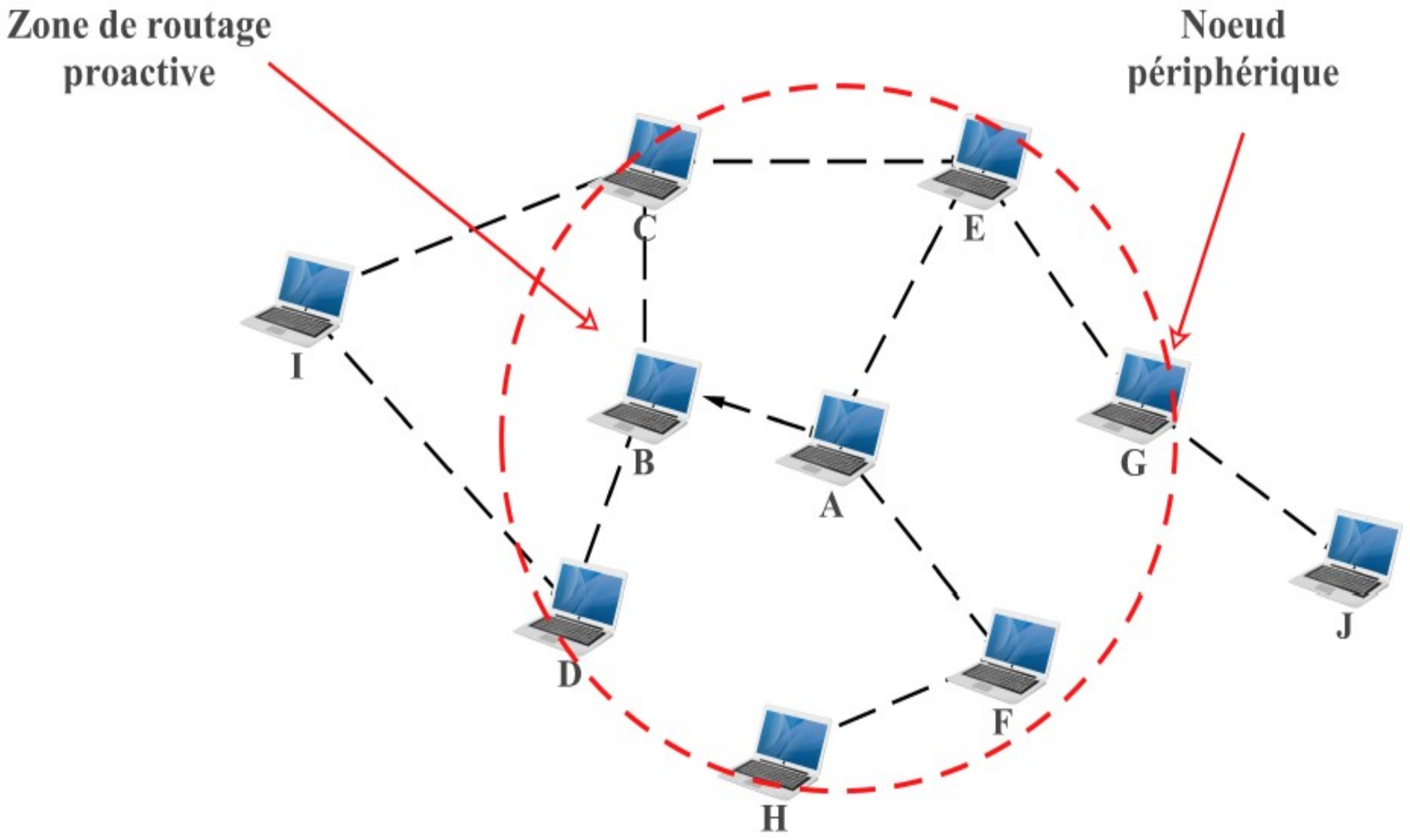
- DSDV utilise deux types de mises à jour: des mises à jour périodiques et d'autres basées sur les évènements afin de propager l'information de routage aussi rapidement que possible quand il y a n'importe quel changement topologique.
- Les paquets de mise à jour incluent les destinations accessibles de chaque nœud et le nombre de sauts exigés pour atteindre chaque destination avec le numéro de séquence lié à chaque route.
- Lors de la réception d'un paquet de mise à jour, chaque nœud le compare avec l'information existante concernant la route. Des routes avec des anciens numéros de séquence sont simplement ignorées.
- En cas de route avec le numéro de séquence égal au numéro de séquence de la route annoncée, on remplace l'ancienne si elle a une meilleure métrique. Les routes nouvellement enregistrées sont immédiatement annoncées à ses voisins.

7/ Exemples de protocoles de routage (26)
Le protocole ZRP

- Le protocole ZRP (Zone Routing Protocol) est parmi les protocoles hybrides les plus cités dans la littérature, à mi-chemin entre les deux familles de protocoles (proactifs et réactifs).
- Chaque nœud doit maintenir une table de routage, dont les données sont régulièrement émises en diffusion pour tous les nœuds qui lui sont distants de moins d'une valeur *d* prédéfinie (routage proactif dans cette zone).
- Pour atteindre tout autre nœud qui n'apparaît pas dans sa table de routage (une distance supérieure à *d*), un nœud a recours à un routage réactif.
- Ce type de protocole fournit un assez bon compromis en termes de diffusion pour les mises à jour. Cependant, en forte mobilité ou avec un nombre important de nœuds, cette solution devient moins efficace.

7/ Exemples de protocoles de routage (27)

Le protocole ZRP



Zone de routage du nœud A avec d=2

8/ Sécurité (1)

- Le protocole de routage utilisé dans un réseau Ad Hoc doit intégrer dans son système un mécanisme de sécurité qui dépendra de plusieurs facteurs (authentification, intégrité, confidentialité et disponibilité) et qui concerne deux aspects :
  - la sécurité du routage et
  - la sécurité des données.
- Ces deux aspects comportent certaines vulnérabilités et sont exposés à plusieurs attaques.
- Selon le niveau d'intrusion et les actions menées par un attaquant, on distingue généralement deux catégories d'attaques :
  - les attaques passives et
  - les attaques actives.

8/ Sécurité (2)
Les attaques passives

- Ce type d’attaque se limite à l’écoute non autorisée des flux et la surveillance des canaux de communication.
- Une écoute se produit lorsqu’un attaquant capture un nœud et étudie le trafic qui le traverse sans altérer le fonctionnement.
- L’intrus essaye uniquement par ces écoutes d’obtenir et de stocker des informations qu’il n’est pas sensé connaitre ou garder dans le but de découvrir des informations de base tel que le protocole de routage et les systèmes de sécurité pour obtenir des données privées d’un nœud ou d’un ensemble de nœuds sans affecter le déroulement du routage.
- Les données analysées aident l’intrus à agir plus tard.
- Un adversaire passif ne fait que menacer la confidentialité des données.

8/ Sécurité (3)
Les attaques actives

- Une attaque est active lorsqu'un nœud non autorisé altère des informations en transit par des actions de modification, suppression, ou fabrication, ce qui conduit à des perturbations du fonctionnement du réseau.
- D'une façon générale, ce type d'attaque modifie le comportement du réseau de façon arbitraire par rapport au comportement normal.
- Un attaquant actif pourra non seulement obtenir plus d'informations qu'un attaquant passif, mais aussi modifier significativement le fonctionnement d'un protocole ou d'empêcher le bon déroulement de son exécution.

8/ Sécurité (4)
Les attaques actives

Les attaques actives sont classifiées en quatre groupes :

- **Par suppression (Packet Dropping Attack)** : le nœud malveillant supprime tous les paquets qui ne sont pas destinés à lui.
- **Par modification (Modification Attack)** : le nœud malveillant capture les informations importantes et essaye de modifier l'un des paramètres du protocole, par exemple les informations de routage, tel que le fait de posséder le plus court chemin vers une destination.
- **Par fabrication (Fabrication Attack)** : l'attaquant envoie de faux messages aux nœuds voisins sans recevoir des messages relatifs, par exemple l'attaquant envoie un paquet de réponse de route sans qu'il ait reçu la requête de demande de route.
- **Timing Attack** : l'attaquant garde le paquet qu'il a reçu alors qu'il n'est pas le destinataire et fait un retard pour le retransmettre après un certain temps, ce qui provoque une perturbation dans l'échange des informations.

8/ Sécurité (5)
Classification détaillée