

Les attaques sur le routage dans les Réseaux Ad hoc

Alexandre POCQUET

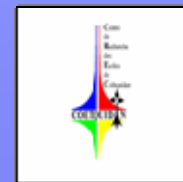
alexandre.pocquet@st-cyr.terre.defense.gouv.fr

CREC Saint-Cyr - Laboratoire MACCLIA

IRISA – Équipe ARMOR



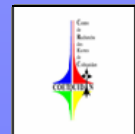
IRISA, Rennes, le vendredi 09 février 2007



- ❑ **Caractéristiques des réseaux Ad-Hoc**
 - **Définition et Contextes d'utilisation.**
 - **Analyse des contraintes et des besoins: le choix du routage**
 - **Techniques et objectifs du routage dans les réseaux Ad-Hoc**

- ❑ **Les attaques sur le routage**
 - **Les critères de classification des attaques.**
 - **Attaques du « trou de vers ».**
 - **Attaques du « trou noir ».**
 - **Attaques par usurpation d'identité(s)**
 - **Attaques par harcèlement**
 - **Attaques ciblant les protocoles réactifs et proactifs**
 - **Classification des attaques**

Conclusions



Définition et contextes d'utilisation

Introduction

Caractéristiques des réseaux Ad-Hoc

Les attaques sur le routage

Conclusion

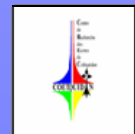
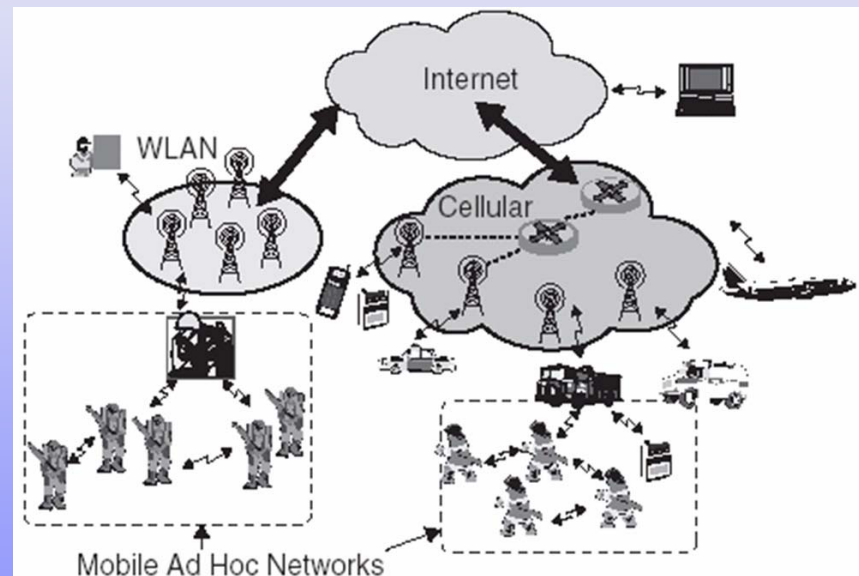
3

Définition:

«Réseaux sans fils et sans infrastructure dont les services à distance sont assurés en exploitant uniquement les capacités des équipements de ses utilisateurs.»

Contextes d'utilisation:

- Théâtres d'opérations
- Opérations de secours



Analyse des contraintes et des besoins: le choix du routage

Introduction

Caractéristiques des réseaux Ad-Hoc

Les attaques sur le routage

Conclusion

4

Contraintes:

- Autonomie
- Portées
- Bande passante
- Liens de nature différentes
- Absence d'infrastructure
- Topologie dynamique

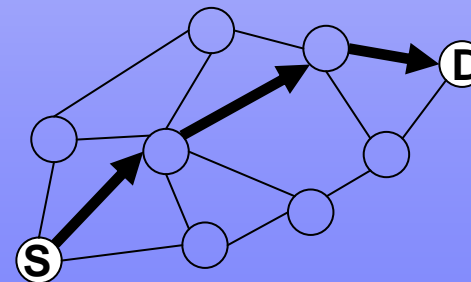
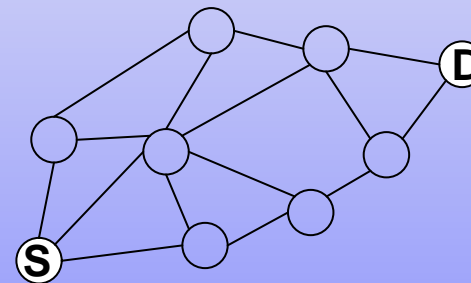
Besoins:

- Couverture
- Mobilité
- **Sécurité**

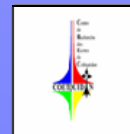
Choix:

- Coopération
- **Routage**

Topologie du réseau



- Ⓢ Nœud source
- ⓓ Nœud destinataire
- Nœud intermédiaire
- Lien symétrique
- ➔ Route entre la source et le destinataire



Techniques de routage et objectifs généraux

Introduction

Caractéristiques des réseaux Ad-Hoc

Les attaques sur le routage

Conclusion

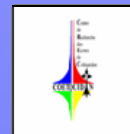
5

Techniques de routage

Routage proactif (OLSR,CGSR,DSDV)	Routage réactif (AODV,DSR)
Maintenance périodique des routes actives (OLSR,DSDV,CGSR)	Maintenance événementielle des routes actives (OLSR,DSDV,AODV,DSR)
Routage saut par saut (OLSR,DSDV,AODV,CGSR)	Routage par la source (DSR)
Distribution du calcul des routes (DSR,AODV,DSDV,CGSR)	Décentralisation du calculs des routes (OLSR)
Vision non uniforme de la topologie (OLSR,CGSR)	Vision uniforme de la topologie (DSDV,AODV,DSR)
Routage par état de lien (OLSR)	Routage par vecteur de distance (AODV,DSDV,CGSR)
Route unique (OLSR,DSDV,CGSR)	Routes multiples si possible (AODV,DSR)

Objectifs généraux du routage:

- Calcul et maintenance des meilleures routes dans un contexte de topologie dynamique
- Limiter les temps de latence
- Minimiser les coûts en temps de calcul et en mémoire
- Minimiser le trafic propre au routage (taille et nombre de messages)



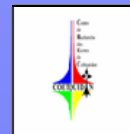
Critères de classifications des attaques sur le routage

Critères choisis :

1. Les pré requis, l'intégration dans le réseau
2. Les méthodes employées
3. Les objectifs
4. Les techniques de routage vulnérables

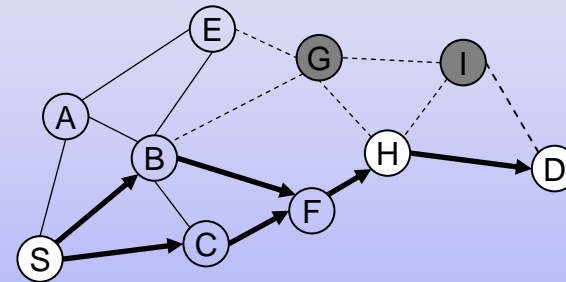
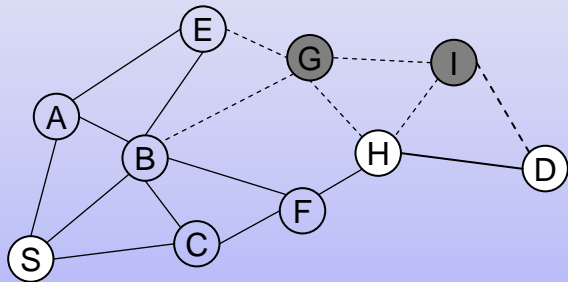
Autre critère:

- Discrétion de l'attaque

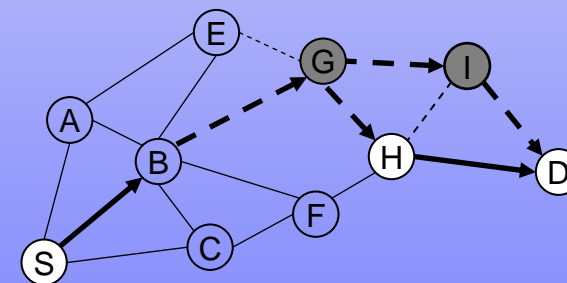


Attaques du « trou de vers »

1. Attaque externe
2. Diffusion sélective par un « réseau privé »
3. Détournement, absorption du trafic
4. Tous types de routage



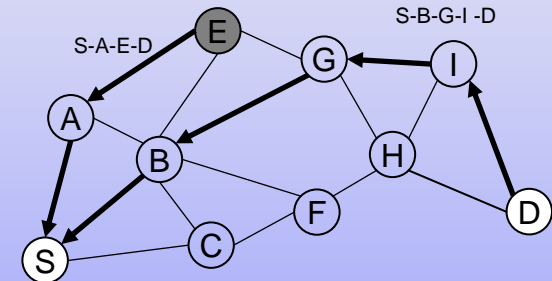
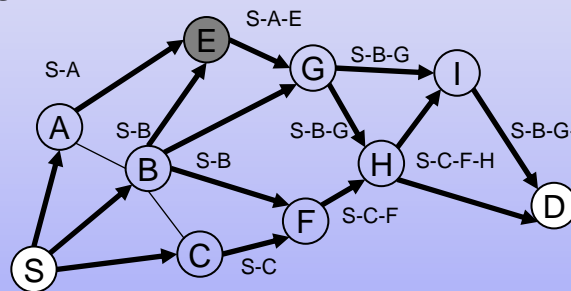
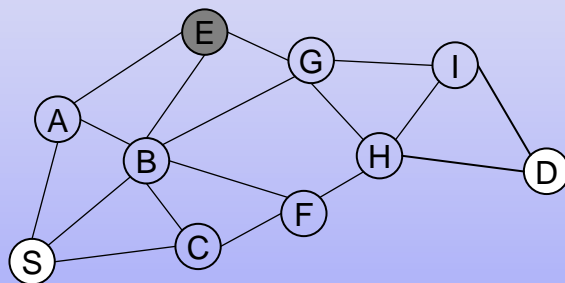
- Ⓢ Nœud source
- ⓧ Nœud(s) destinataire(s)
- ⓧ Nœud(s) attaquants
- Lien symétrique
- Lien asymétrique
- Route entre la source et le destinataire



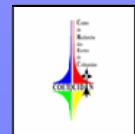
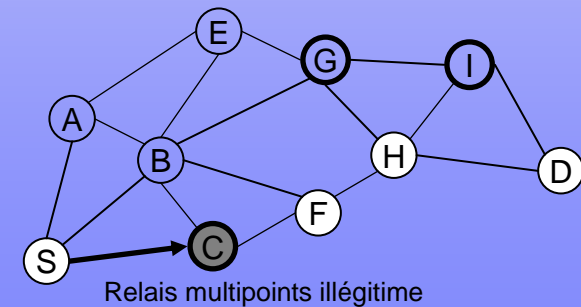
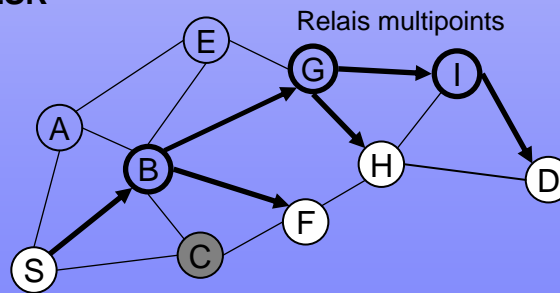
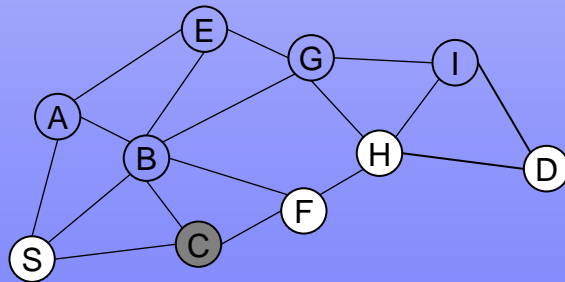
Attaques du « trou noir »

1. Attaque interne
2. Falsification des informations (vecteurs de distance, liens, routes)
3. Détournement, absorption du trafic.
4. Tous type de routage et, **calcul distribué**, routage non uniforme en particulier.

Attaque sur le protocole de routage DSR



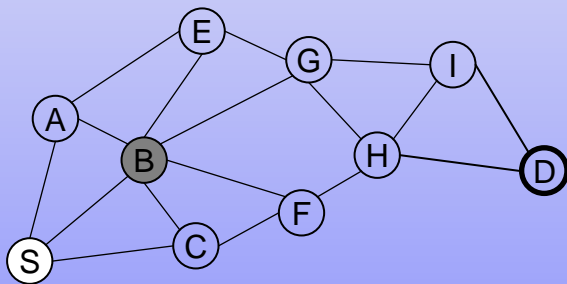
Attaque sur le protocole de routage OLSR



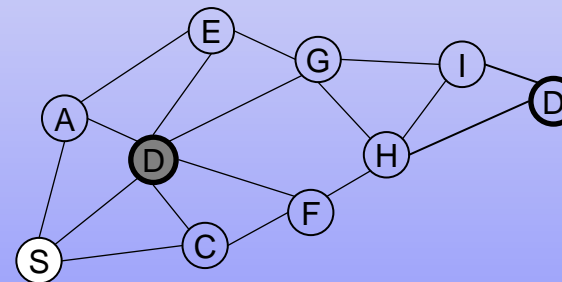
Attaques par usurpation d'identité(s)

1. Attaque interne
2. Falsification des informations relatives aux identités
3. Isolement de nœud, vision fautive de la topologie.
4. Tous type de routage en général, et calcul distribué et non uniforme en particulier

Topologie du réseau



Topologie vue par le nœud D sous l'influence du nœud B



Attaques par harcèlement

Introduction

Caractéristiques des réseaux Ad-Hoc

Les attaques sur le routage

Conclusion

10

1. Attaque externe
2. Émission régulières et inutiles de paquets
3. Augmentation de la charge du réseau, consommation excessives des ressources, vision fausse de la topologie.
4. Maintenance événementielle de route actives et/ou de la topologie, découvertes de routes

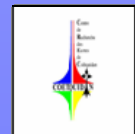
Exemples:

- Demandes incessantes de découvertes de routes (RREQ) et/ou de maintenance de route (RERR)
- Émissions de messages de modification de la topologie
- Rejeu



IRISA

Les attaques sur le routage dans les réseaux Ad hoc
Alexandre Pocquet - CREC Saint-Cyr - Laboratoire MACCLIA



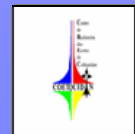
Attaques ciblant les protocoles réactifs et proactifs

Attaques ciblant les protocoles réactifs:

- Attaque par précipitation
- Attaque par falsification des paquets Route Reply
- Attaque par falsification des paquets Route Request (numéro de séquence, destination, nombre de saut..)
- Attaque par non diffusion des paquets Route Error

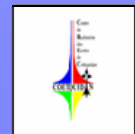
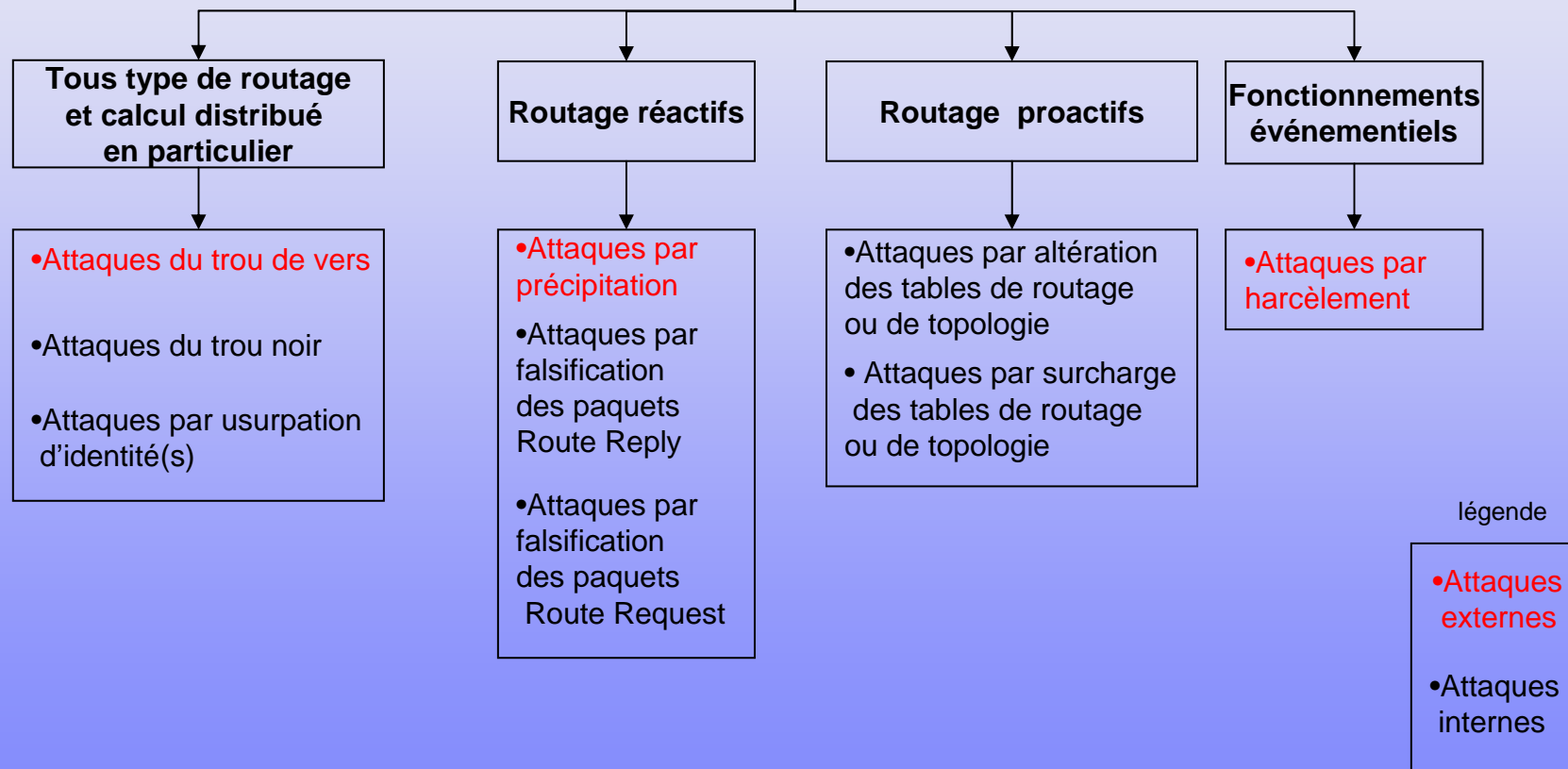
Attaques ciblant les protocoles proactifs:

- Attaque par altération des tables de routage ou de la topologie
- Attaque par surcharge des tables de routage ou de la topologie



Classification des attaques

Classification des attaques selon les techniques de routage particulièrement sensibles



Conclusions

Coût des techniques de routage/vulnérabilités

Facteurs aggravants:

- Attaques cohérentes menées par plusieurs attaquants
- Combinaison de différents types d'attaques
- Isolement des victimes sur le plan de la topologie
- Comportement égoïste de certains nœuds

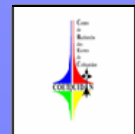
Actions de prévention:

- Authentification des nœuds, gestion de clefs.
- Protocoles de routage sécurisés (marquage de paquets, authentification point à point, métriques intégrant des aspects de la sécurité)
- Techniques de routage hybrides

Action de détection:

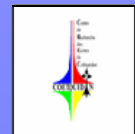
- Systèmes anti-intrusion (IDS)

Coût global??



Bibliographie (1)

- C.E.Perkins and E.M.Royer. Ad-hoc on-demand distance vector routing. Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications
- C.E.Perkins and P.Bhagwat. Highly dynamic destination-sequenced distance-vector routing (dsv) for mobile computers. ACM SIGCOM
- D.B.Johnson, D.A.Maltz, and J.A.Broch. Dsr : The dynamic source routing protocol for multi-hop wireless ad hoc networks. 2001.
- P.Jacquet, P.Mühlethaler, T.Clausen, A.Laouiti, A.Qayyum, and L.Viennot. Optimized link state routing protocol for ad hoc networks. 5th IEEE Multi Topic Conference, 2002.
- S.E.Vertanen and P.Nikander. Local clustering for hierarchical ad hoc networks.
- X.Zou, B.Ramamurthy, and S.Magliveras. Routing techniques in wireless ad-hoc networks - classification and comparison.



Bibliographie (2)

- C.Siva Ram Murthy and B.S.Manoj. Ad Hoc Wireless Networks Architectures and Protocols. Prentice Hall Communications Engineering and Emerging Technologies. Pearson Education, fourth edition, 2004. V.
- M.Ilyas. The Handbook of Ad-Hoc Wireless Networks. Electrical Engineering Handbook. CRC PRESS, 2003.
- S.Basagni, M.Conti, S.Giordano, and I.Stojmenovic. Mobile Ad Hoc Networking. IEEE, 2004.
- Y.C.Hu, A.Perrig, and D.B.Johnson. Packet leases : A defense against wormhole attacks in wireless ad hoc networks. 2001.
- Praphul Chandra. Bulletproof Wireless Security, GSM, UMTS, 802.11, and Ad Hoc Security. Elsevier, Communications Engineering series.2005
- Prasant Mohapatra, Srikanth Krishnamurthy. Ad Hoc Networks, Technologies and Protocols. Springer 2005.

