La Sécurité dans les Réseaux Sans-Fil Ad Hoc

Valérie Gayraud

Loutfi Nuaymi Francis Dupont

Sylvain Gombault Bruno Tharon

SSTIC03 12 Juin 2003

Agenda

- Présentation des Réseaux Sans Fils Ad Hoc
- Analyse de Risque sur la Sécurité
- Travaux de Recherche - Solutions Proposées
- Démonstration / Conclusion

Les Réseaux Sans Fil Ad Hoc (1/2)

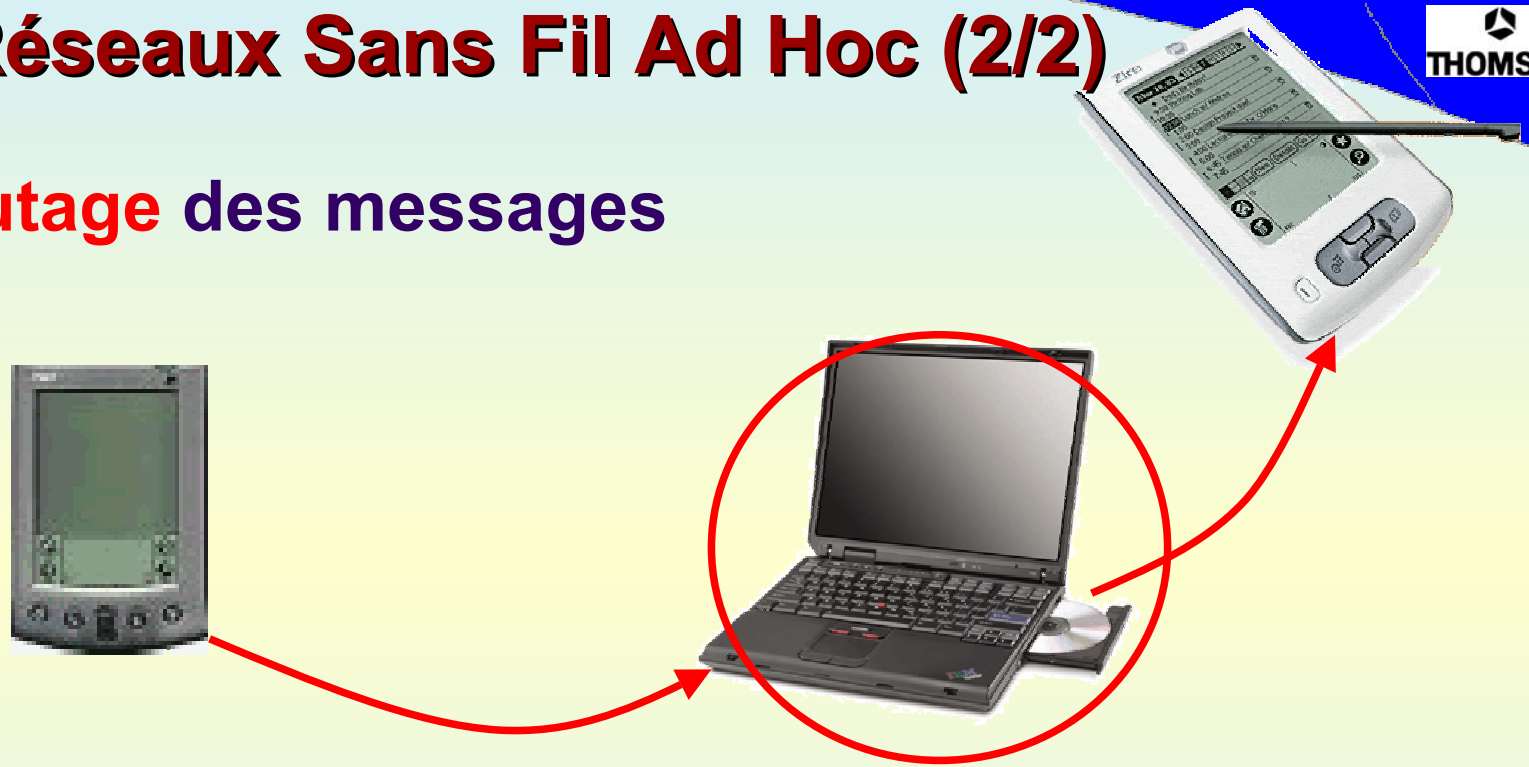
- Nœuds autonomes mobiles sans fil

- Pas d'infrastructure fixe

- Pas de contrôle central

Les Réseaux Sans Fil Ad Hoc (2/2)

- **Routage** des messages



- IETF : **MANET** *Mobile Ad Hoc NETwork*

Les Technologies Sans Fil

- IEEE 802.11b, 802.11g
- HomeRF
- Bluetooth

} Bande ISM 2,4 GHz

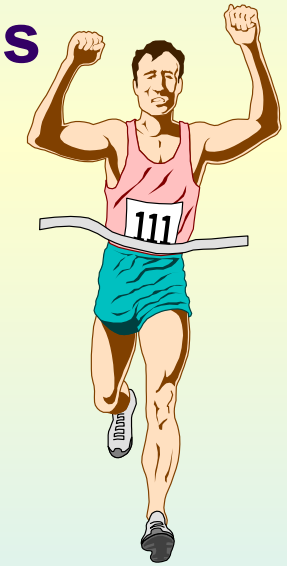
- IEEE 802.11a
- HiperLan/2

} Bande 5 GHz

- Infrarouge IrDA

Applications des Réseaux Sans Fil Ad Hoc

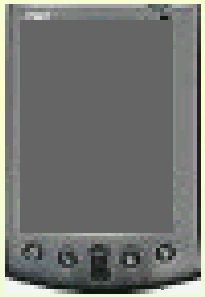
- *Personal Area Network* (PAN) / Réseaux domestiques
- Application militaire → Réseaux tactiques
- Couverture d'évènements exceptionnels
- Opérations de secours
- Applications industrielles : Capteurs



Contraintes (1/3)

NŒUDS

- Terminaux **hétérogènes**
- Terminaux **légers**
- Capacité d'**auto-configuration**



ÉNERGIE

- **Énergie limitée**
- Baisse de **réactivité**
  - Temps de réveil

Contraintes (2/3)

RÉSEAU

- Routage multi-sauts
- Opération distribuée
- Absence d'infrastructure centralisée

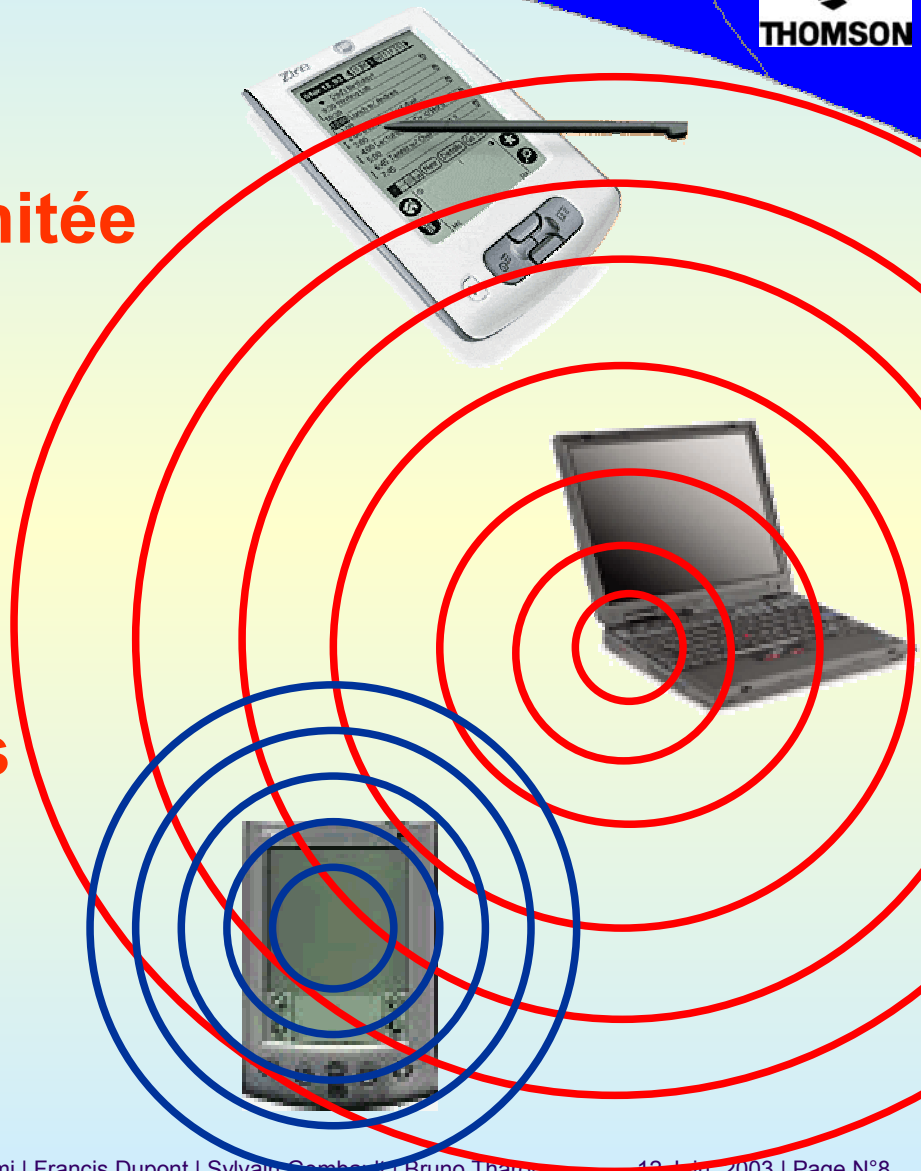
MOBILITÉ

- Topologie dynamique
- Peu ou pas de protection physique

Contraintes (3/3)

SANS FIL

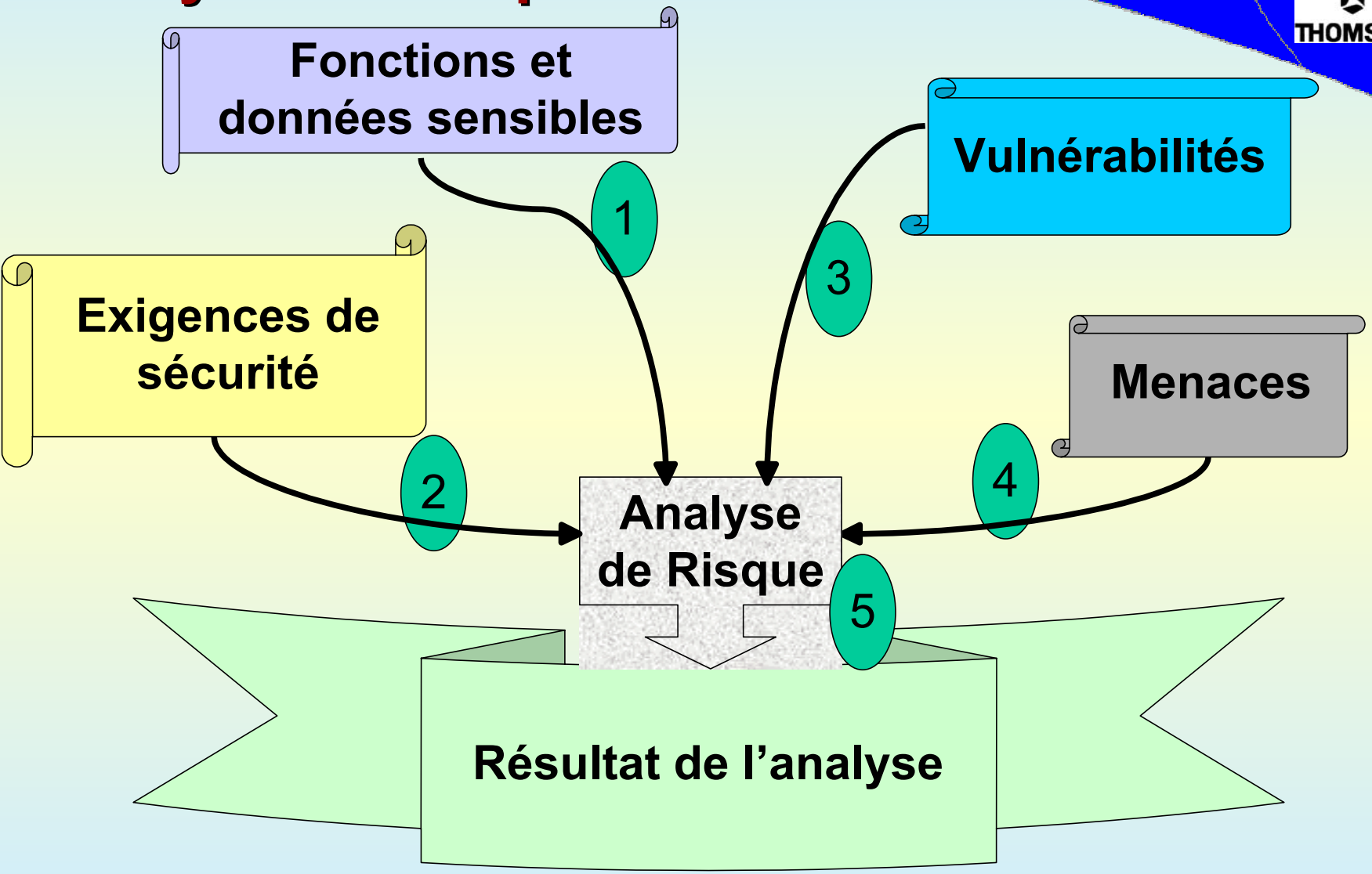
- Bande passante limitée
- Liens à capacités variables
- Liens asymétriques



Analyse de Risque

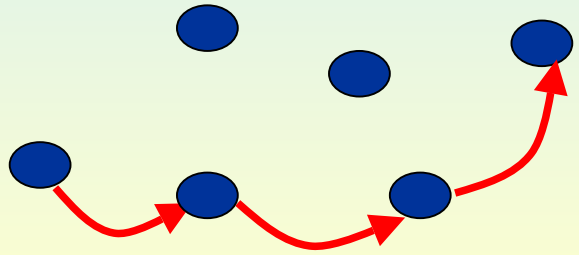
- Démarche
- Résultats

Analyse de Risque EBIOS



Analyse de Risque / Étape 1
Fonctions et Données à protéger

- Routage



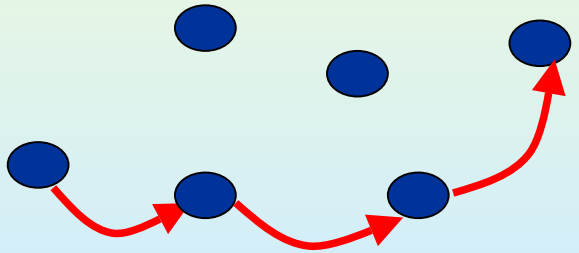
- (Auto)Configuration
- Gestion d'énergie
- Mécanismes de sécurité

Analyse de Risque / Étape 2
Exigences de sécurité

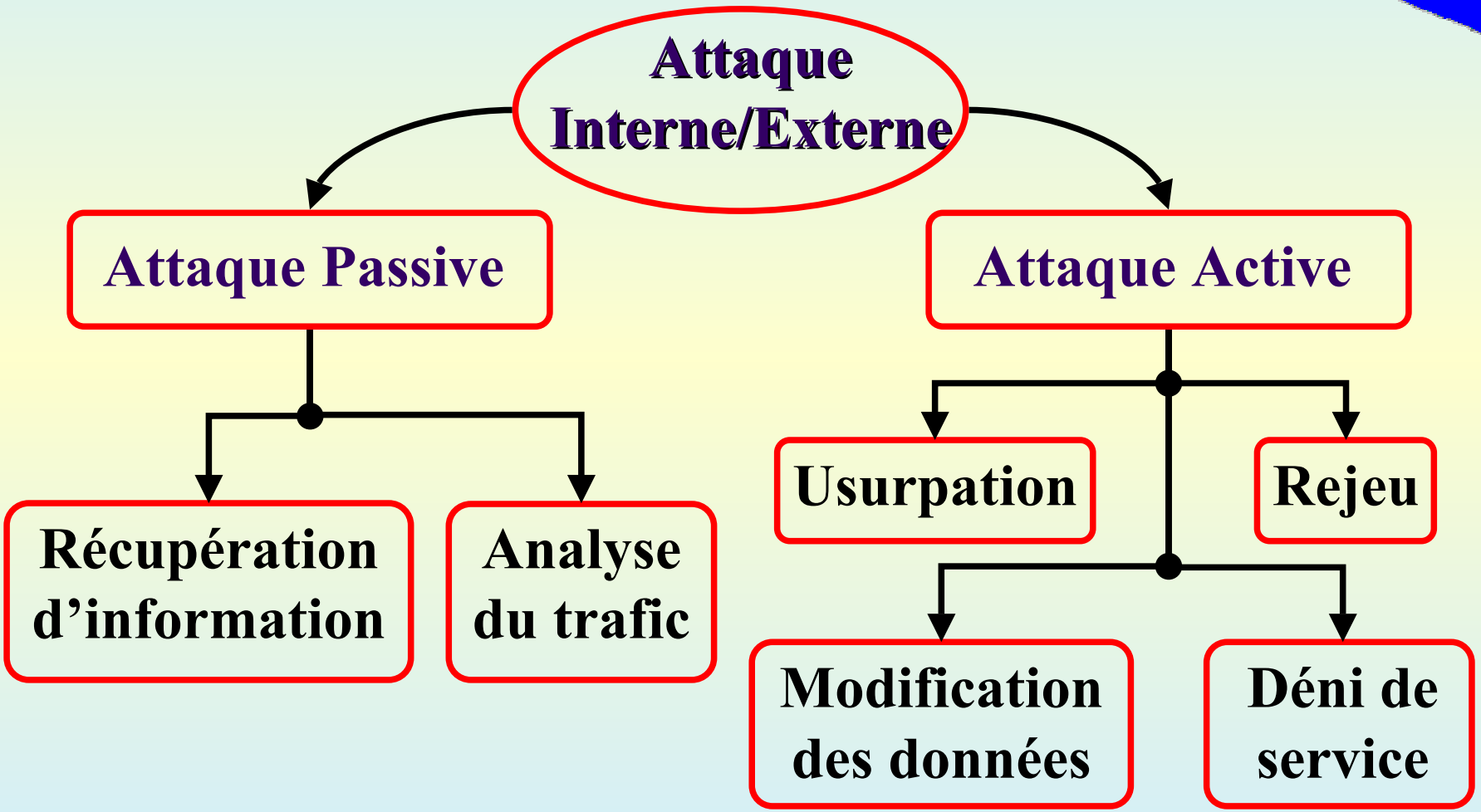
- **Authentification**
  - Liée aux fonctions sensibles : routage, configuration, gestion d'énergie
- **Intégrité**
  - Messages de gestion et données
- **Confidentialité**
  - Protection de la vie privée

Analyse de Risque / Étape 3
Vulnérabilités

- Vulnérabilités des technologies sans fil
- Canal radio
- Nœuds
  - Système d'exploitation et matériel
- Mécanisme de routage



Analyse de Risque / Étape 4
Les Menaces



Analyse de Risque

- Démarche
- **Résultats**

Résultats de l'Analyse de Risque

Attaques sur les mécanismes de base

Routage et configuration

Attaques sur les mécanismes de sécurité

Analyse de Risque : Scénarii Potentiels (1/2)

- Écoute / Analyse
- Usurpation
- Attaques physiques

Analyse de Risque
Scénarii Potentiels (2/2)

- **Dénis de service**

- **Brouillage du canal radio**
- **Exhaustion de batterie**
- **Détournement de trafic**
- **Perversion des mécanismes de sécurité**

Travaux de Recherche

- Modèles proposés dans la littérature
- Le routage en question
- Une solution spécifique : Ariadne

Exemple de Protocole de Routage pour les Réseaux Ad Hoc

DSR Dynamic Source Routing

- **Découverte de route :**
  - ***Route Request***
  - ***Route Reply***

- **Maintenance de route :**
  - ***Route Error***

Solutions de la littérature

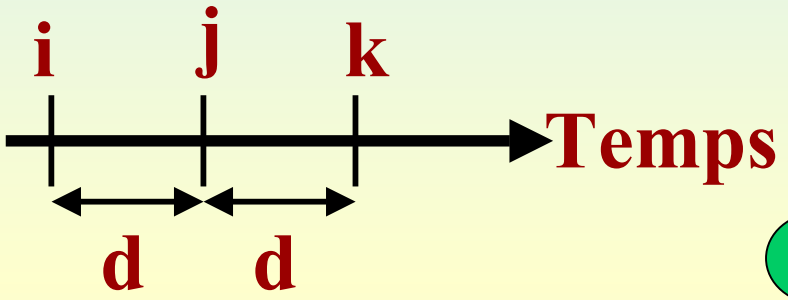
- **Authentification**
  - ⇨**Trois grands courants** :
    - –***Key agreement* - Partage/Échange de clés**
      - Contribution
      - Distribution
    - –**Modèle de sécurité du *Resurrecting Duckling***
      - *Empreinte*: Association temporaire de type maître/esclave → Contact physique
    - –**Infrastructure à clé publique auto-organisée**
      - Les certificats sont créés, stockés et distribués par les nœuds

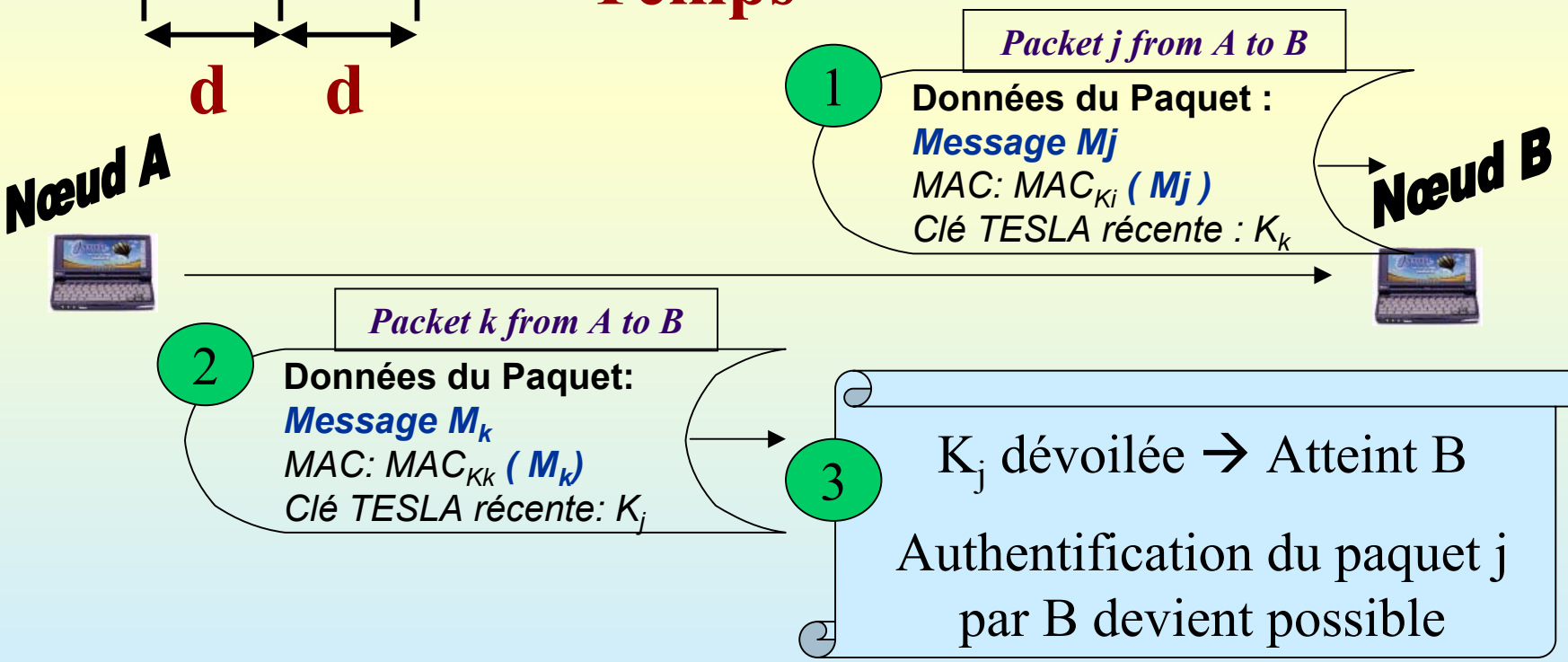
Solutions de la littérature 2/2

- **Intégrité des messages échangés**
  - **Signature numérique à clé publique**
    - **Très calculatoire**
  - **TESLA**
    - **Extension du protocole de « *Guy Fawkes* »**

TESLA

- **Authentification / Intégrité des messages par MAC**
- **Kn nombre aléatoire généré par le nœud A, $K_i = h(K_{i+1})$ → Clés**
- **"d": Temps au bout du quel une clé peut être dévoilée, dépend de :**
  - Délai de transmission et tolérance sur la synchronisation entre nœuds





TESLA

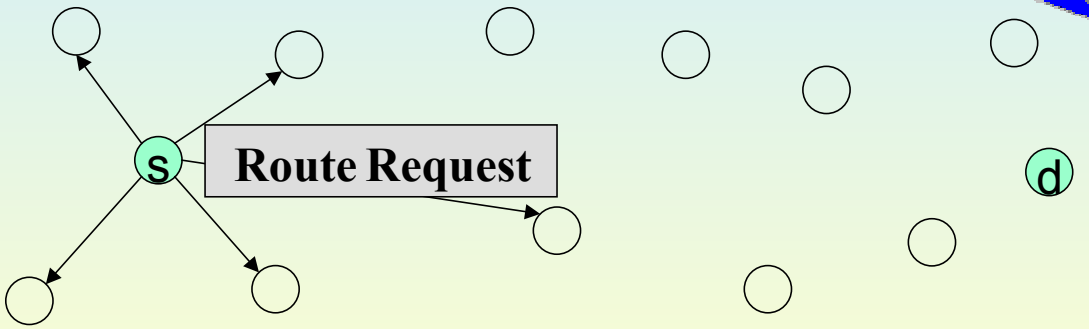
- **Intégrité des messages**
  - **MAC ⇨ Clé dévoilée après réception du paquet**
- **Authentification de la source**
  - **Initialisation par authentification du premier message avec un protocole à clé publique**
  - **Chaîne de clés**
- **Pas de confidentialité**

Travaux de Recherche

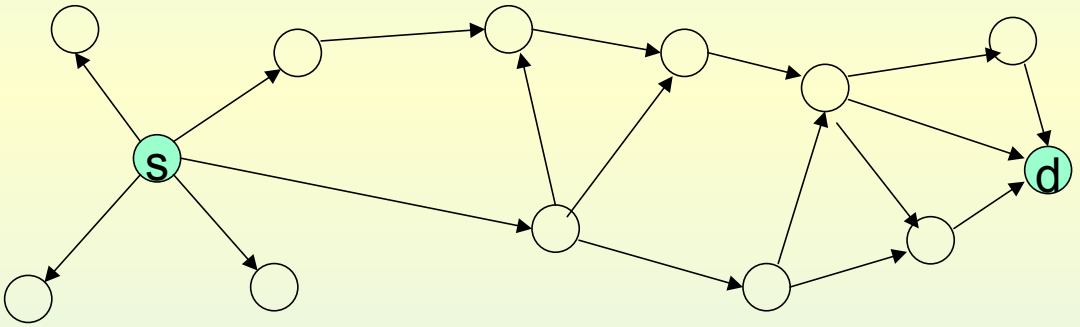
- Modèles proposés dans la littérature
- Le routage en question
- Une solution spécifique : Ariadne

Découverte de route

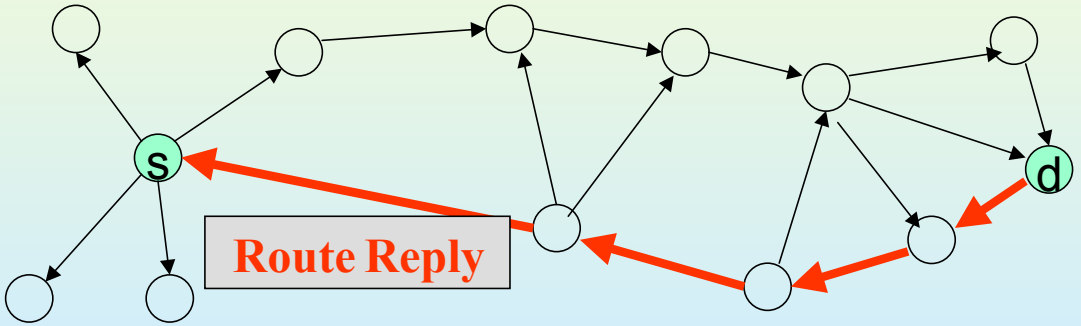
Route Request
nœud *s* vers *d*



Rediffusion de nœud en nœud



Route Reply
nœud *d* vers *s*

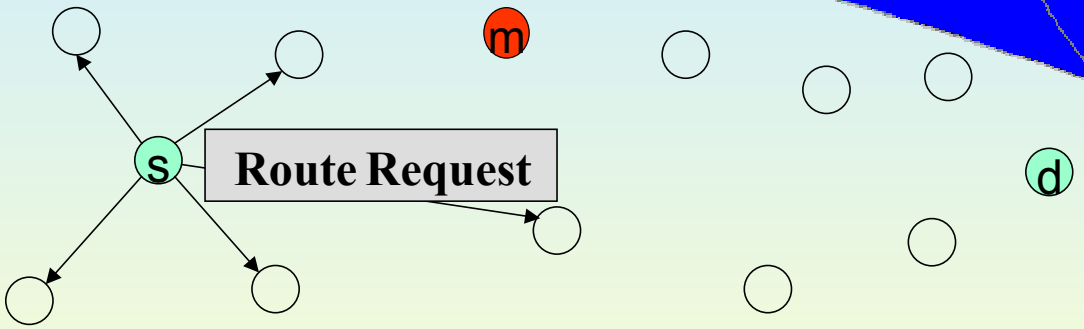


Attaques Liées aux Protocoles de Routage

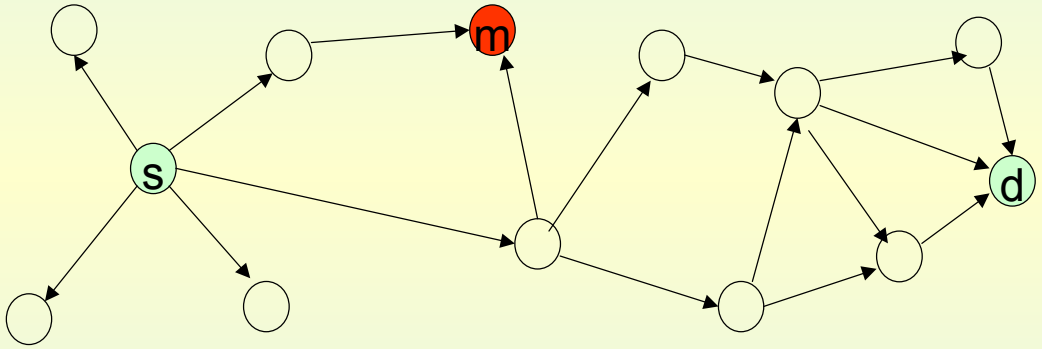
- Injection de faux messages de routage
  - Boucles
  - *Black hole*
  - Détours

Attaque Black Hole

Route Request
nœud *s* vers *d*

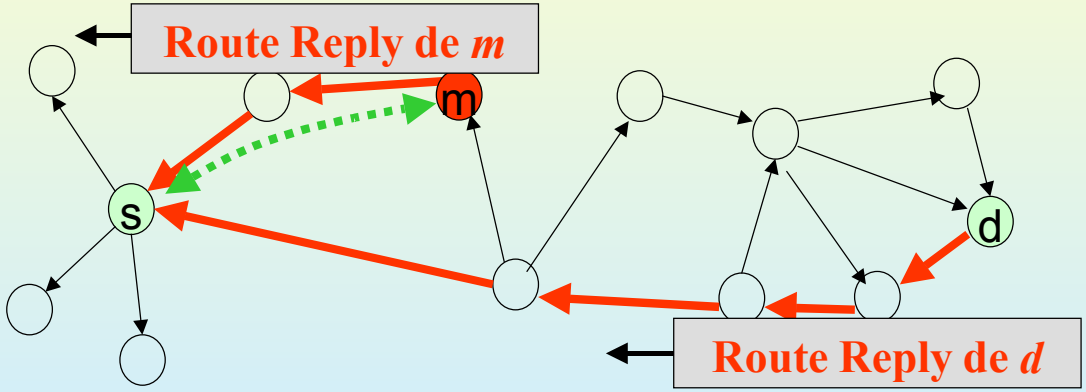


Rediffusion de nœuds en nœuds



Route Reply
nœud *m* vers *s*

Cette route est choisie par s



Protocole de Routage Sécurisé Ariadne

- **Protocole de type réactif sécurisé basé sur DSR**

- **Prévention des attaques actives**
  - Boucles de routage
  - *Black hole*
  - Détours
  - Dénis de service

- **Authentification des messages de routage**
  - Partage de clé secrète
  - TESLA
  - Signature numérique

} **MAC**

Un Protocole de Routage Sécurisé Ariadne → Évaluation avec TESLA

- **Découverte de route plus lente avec TESLA**
  - Retard dû au temps pendant le quel la clé n'est pas dévoilée
- **Traitement de messages d'erreur ralenti**
- **Utilisation de la bande passante**
- **26 % d'entête en plus que pour une version DSR non optimisée**

Conclusion

- Les challenges
- Les travaux de recherche
- Démonstration

Conclusion

- **Un Challenge pour la sécurité**
  - **Authentification des nœuds**
  - **Authentification des messages de gestion**
  - **Beaucoup de modèles théoriques, peu d'applications**

- **Mécanismes de routage**
  - **Conception de nouveaux protocoles de routage**
    - Orienté efficacité
    - Sécurité non prise en compte
  - **Immaturité du domaine**

- **Compromis entre sécurité et autonomie/efficacité**

Axes de Recherche pour les Réseaux Sans Fil Ad Hoc

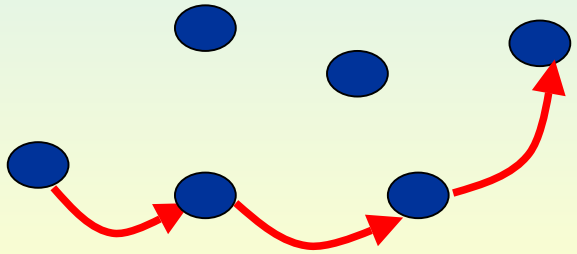
- Authentification, modèles de confiance
- Protocoles de routage sécurisé et efficace
- Utilisation de réseaux privés virtuels
- Détection d'intrusion

Démonstration

Démonstration

Rappel : Fonctions et données à protéger

- Routage



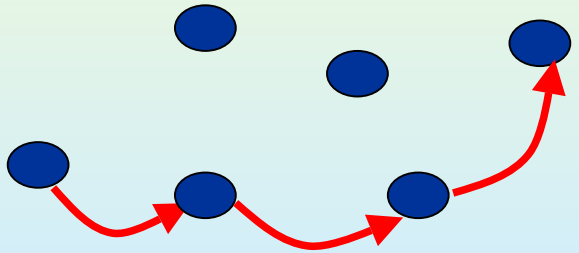
- (Auto)Configuration
- Gestion d'énergie
- Mécanismes de sécurité

Démonstration

Rappel : Vulnérabilités

- **Vulnérabilités des technologies sans fil**
- **Canal radio**
- **Nœuds**
  - **Système d'exploitation et matériel**

- **Mécanisme de routage**



Démonstration

Rappel : Résultat de l'Analyse de Risque

Attaques sur les mécanismes de base

Routage et configuration

Attaques sur les mécanismes de sécurité

Démonstration

Rappel : Analyse de Risque → Scénarii (1/2)

- Écoute / Analyse
- Usurpation
- Attaques physiques

Démonstration

Rappel : Analyse de Risque → Scénarii (2/2)

- **Dénis de service**
- **Brouillage du canal radio**
- **Exhaustion de batterie**
- **Dispersion du trafic**
- **Perversion des mécanismes de sécurité**

Démonstration

- Vulnérabilités d'une technologie sans fil

  ⇨ **802.11 : Messages de gestion non authentifiés**

- Attaques sur les mécanismes de sécurité

  ⇨ **Perversion du mécanisme d 'authentification**

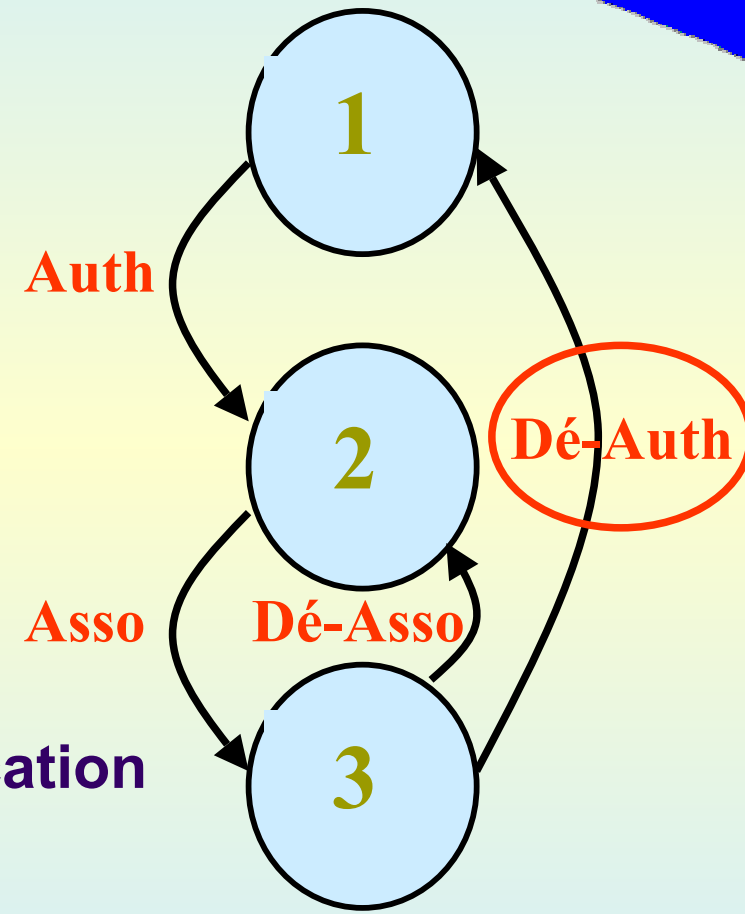
- Scénario

  ⇨ **Déni de service / Usurpation**

Déni de Service en IEEE 802.11

802.11 États

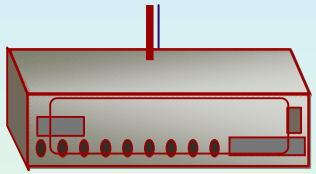
1. Non authentifié, non associé
2. Authentifié, non-associé
3. Authentifié, associé



802.11 Messages

- Contrôle
- Management
  - Authentification / Dé-authentification
  - Association / Dé-association
- Data

Démonstration



Base 802.11

Client

Dé-authentification
@ MAC de la base

Serveur vidéo

Attaquant

Questions ?

Remerciements

Jean-Marie Bonnin	***ENST Bretagne***
Bruno Stevant	***ENST Bretagne***
Eric Diehl	***Security Lab de Thomson***
Olivier Heen	***Security Lab de Thomson***
Nicolas Prigent	***Security Lab de Thomson***

Bibliographie

MANET http://www.ietf.org/html.charters/manet-charter.html

BSD-AirTools http://dachb0den.com/projects/bsd-airtools.html

Air-Jack http://802.11ninja.net/

R. Anderson, F. Bergadano, B. Crispo, J.-H. Lee, C. Manifavas, and R. Needham, A new family of authentication protocols

Y. C. Hu, A. Perrig, and D. B. Johnson, Ariadne : A secure on-demand routing protocol for ad hoc networks

J. P. Hubaux, L. Buttyan, and S. Capkun, The quest for security in mobile ad hoc networks

A.Perrig, R. Canetti, J. Tygar, and D. Song, Efficient authentication and signing multicasts streams over lossy channels8. F. Stajano

B.F. Stajano and R. Anderson, The resurrecting duckling : Security issues for adhoc wireless networks

Glossaire

AP	**A**ccess **P**oint
AODV	**A**d hoc **O**n-demand **D**istance **V**ector
ART	**A**utorité de **R**égulation des **T**élécommunications
AT-GDH	**A**rbitrary **T**opology **G**eneralization of **D**iffie-**H**ellman
BD-ADDR	**B**luetooth **D**evice **ADDR**ess
BER	**B**it **E**rror **R**ate
BRAN	**B**roadband **R**adio **A**ccess **N**etworks (Groupe de travail de l'ETSI)
CRC	**C**yclic **R**edundancy **C**heck
CSMA/CA	**C**arrier **S**ense **M**ultiple **A**ccess / **Ca**rrier **A**voidance
DSR	**D**ynamic **S**ource **R**outing
DVMRP	**D**istance **V**ector **M**ulticast **R**outing **P**rotocol
EAP	**E**xtensible **A**uthentication **P**rotocol
ETSI	**E**uropean **T**elecommunications **S**tandards **I**nstitute
FCC	**F**ederal **C**ommunications **C**ommission
FSK	**F**requency-**S**hift **K**eying
GDH	**G**eneralization of **D**iffie-**H**ellman
GMSK	**G**aussian **M**inimum **S**hift **K**eying
GPRS	**G**eneral **P**acket **R**adio **S**ervice
HiperLAN	**Hi**gh **Per**formance **L**ocal **A**rea **N**etwork
IDS	**I**ntrusion **D**etection **S**ystem
IEEE	**I**nstitute of **E**lectrical and **E**lectronics **E**ngineers
IETF	**I**nternet **E**ngineering **T**ask **F**orce
IrDA	**I**nfrared **D**ata **A**ssociation
ISM	**I**ndustrial, **S**cientific and **M**edical
IV	**I**nit **V**ector
MAC	**M**edium **A**ccess **C**ontrol
MANET	**M**obile **A**d hoc **NET**work
MAODV	**M**ulticast **A**d hoc **O**n-demand **D**istance **V**ector
MPR	**M**ulti **P**oint **R**elay
NSA	**N**ational **S**ecurity **A**gency
OLSR	**O**ptimized **L**ink **S**tate **R**outing
PAN	**P**ersonal **A**rea **N**etwork
PDA	**P**ersonal **D**igital **A**ssistant
PGP	**P**retty **G**ood **P**rivacy
PRNG	**P**seudo **RaN**dom **G**enerator
RIP	**R**outing **I**nternet **P**rotocol
RREQ	**R**oute **REQ**uest
RREP	**R**oute **REP**ly
RERR	**R**oute **ERR**or
RSN	**R**obust **S**ecurity **N**etworks
SAR	**S**ecurity-**A**ware ad hoc **R**outing
SIG	**S**pecial **I**nterest **G**roup
SNMP	**S**imple **N**etwork **M**anagement **P**rotocol
SRR	**S**end **R**oute **R**equest
SWAP	**S**hared **W**ireless **A**ccess **P**rotocol
TDMA	**T**ime **D**ivision **M**ultiple **A**ccess
TESLA	**T**ime **E**fficient **S**tream **L**oss-tolerant **A**uthentication
UMTS	**U**niversal **M**obile **T**elecommunications
WECA	**W**ireless **E**thernet **C**ompatibility **A**lliance
WEP	**W**ired **E**quivalent **P**rivacy Protocole
Wi-Fi	**Wi**reless **Fi**delity
WLAN	**W**ireless **L**ocal **A**rea **N**etwork
WPAN	**W**ireless **P**ersonal **A**rea **N**etwork