

DETECTION D'INTRUSIONS DANS LES RESEAUX AD HOC

Jean-Marc PERCHER
Bernard JOUGA

SSTIC 03

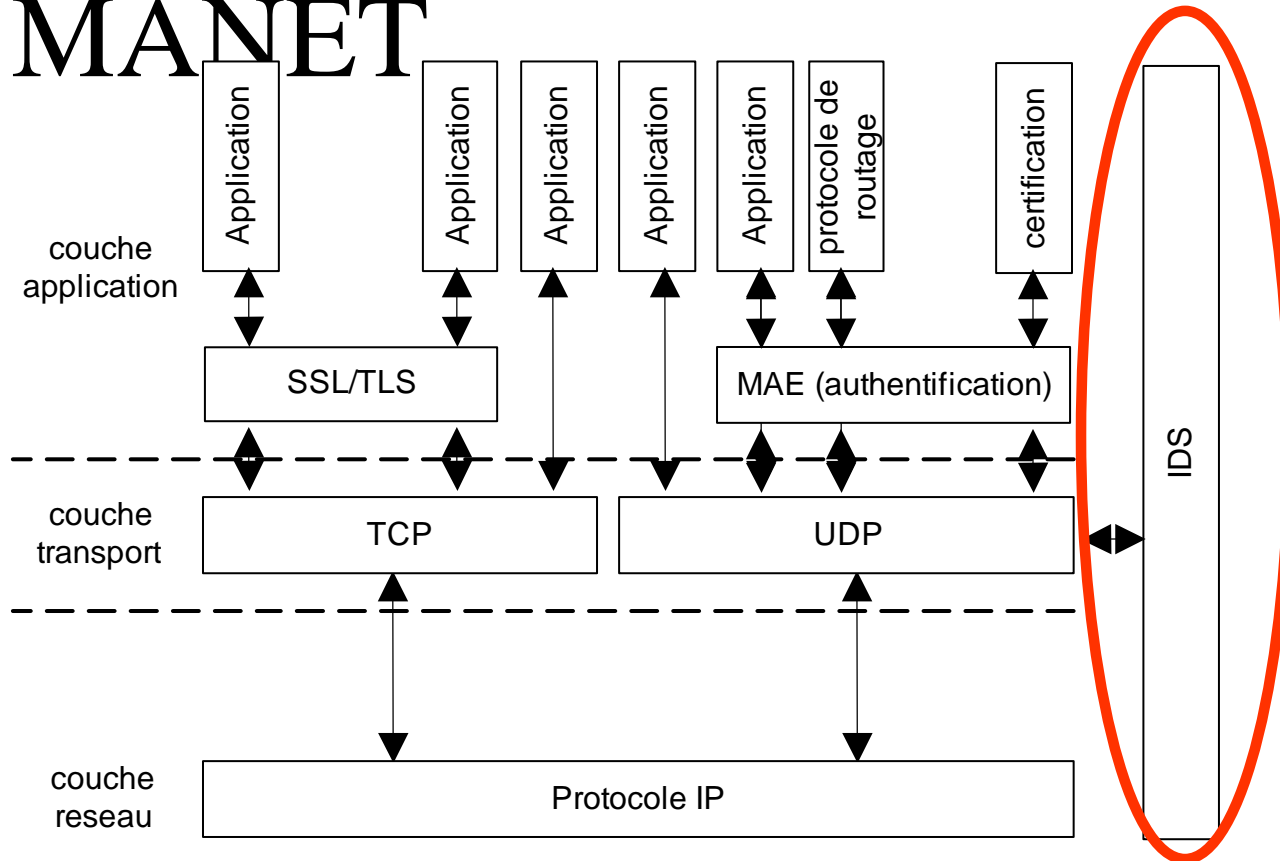
Le constat

- Réseaux sans fil plus sensibles aux problèmes de sécurité
 - Intrusion
 - Déni de service
- Failles de sécurité potentielles augmentées par le contexte ad hoc
 - Pas d'équipements dédiés de sécurité (pare feux, serveur d'authentification, etc.)
 - Vulnérabilités propres (protocole de routage, autoconfiguration, topologie dynamique)
 - Les services de sécurité doivent être distribués, coopératifs et compatibles avec la bande passante des réseaux sans fil

Agenda

- Le constat
- **Un modèle de sécurité pour les réseaux ad hoc**
- Motivation des travaux
- Modèle d'IDS distribué pour réseaux ad hoc
 - Spécifications
 - Architecture globale
 - Architecture interne d'un LIDS
- Validation fonctionnelle
- Conclusions et travaux futurs
- Démonstration

Modèle de sécurité pour les MANET



Agenda

- Le constat
- Un modèle de sécurité pour les réseaux ad hoc
- **Motivation des travaux**
- **Modèle d'IDS distribué pour réseaux ad hoc**
 - Spécifications
 - Architecture globale
 - Architecture interne d'un LIDS
- **Validation fonctionnelle**
- **Conclusions et travaux futurs**
- **Démonstration**

Motivation des travaux

- IDS pour réseaux filaires mal adaptés
 - Pas de points de concentration du trafic
 - Chaque noeud a une vision limitée de l'activité du réseau
- Nécessité de définir une architecture d'IDS spécifique
 - Modèle distribué et coopératif
 - LIDS, *Local Intrusion Detection System*, dans chaque noeud
 - Communication entre les LIDS

Analyse des IDS distribués existants

NOM	Année Publication	Type de détection	Pré traitement - des données	Analyse des Données (détection)	Type de réponse	Origine des données
AAFID	1998	scénarios	distribué	centralisée	passive	système
CSM	1996	comportementale	distribué	distribuée	active	système
DIDS	1992	hybride	distribué	centralisée	passive	système/réseau
DPEM	1994	comportementale	distribué	centralisée	passive	système
GrIDS	1996	hybride	distribué	centralisée	passive	système/réseau
IDA	1998	scénarios	agents mobiles	centralisée	passive	système
JiNao	1997	hybride	distribué	centralisée	passive	MIB/réseau
MICAEL	1999	scénarios	agents mobiles	distribuée	passive	MIB
SPARDA	2002	scénarios	agents mobiles	distribuée	passive	système/réseau

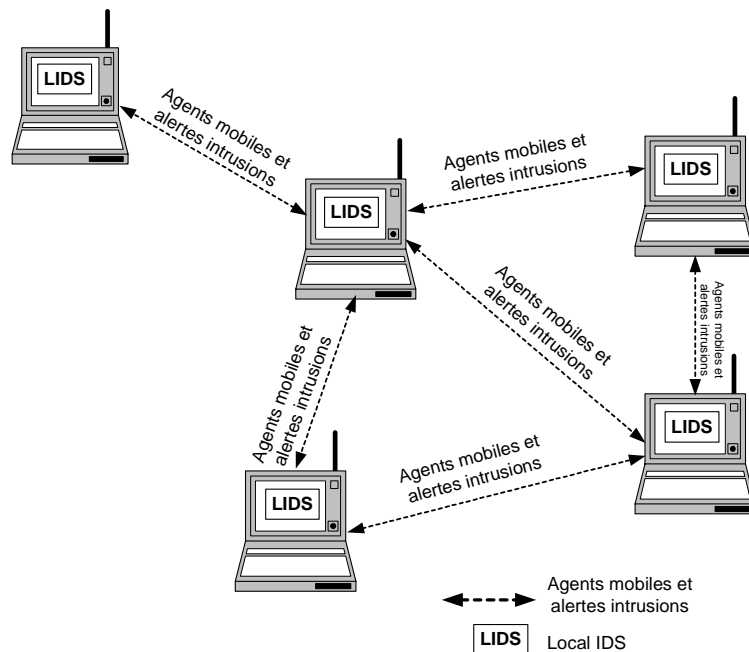
Agenda

- Le constat
- Un modèle de sécurité pour les réseaux ad hoc
- Motivation des travaux
- **Modèle d'IDS distribué pour réseaux ad hoc**
 - Spécifications
 - Architecture globale
 - Architecture interne d'un LIDS
- Validation fonctionnelle
- Conclusions et travaux futurs
- Démonstration

Spécifications de l'architecture

- Adaptée à plusieurs méthodes de détection
- Adaptée à l'exploitation de plusieurs sources de données
- Réalisant la détection en temps réel
- Réponse active en local et informative pour les autres nœuds du réseau
- Peu consommatrice en ressources réseau
- Respectant les normes et standards

Architecture globale



- LIDS : code portable (java)
- Collecte d'informations dans les MIB
- Technologies des Agents Mobiles pour la coopération des LIDS (plate-forme AGLET)

Agents Mobiles : coopération entre LIDS

- **Mobilité :**
 - Déplacement du code vers les données.
 - Exécution asynchrone de l'agent.
- **Autonomie des agents :**
 - Indépendants de la plate-forme origine.
- **Adaptabilité (intelligence) :**
 - Programmés pour s'adapter à différents contextes.
- Requêtes SNMP locales
- Diminution des échanges réseaux (Client/serveur)

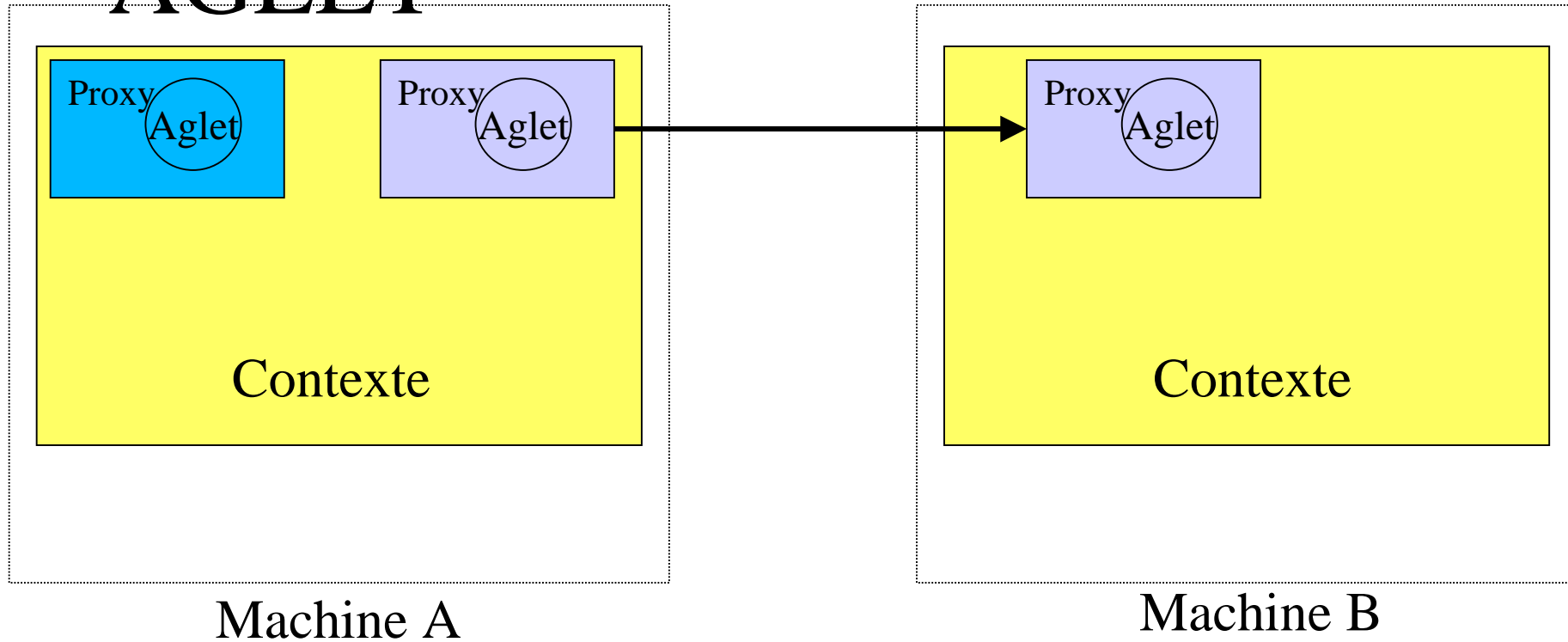
Agents Mobiles : plate-forme

AGLET

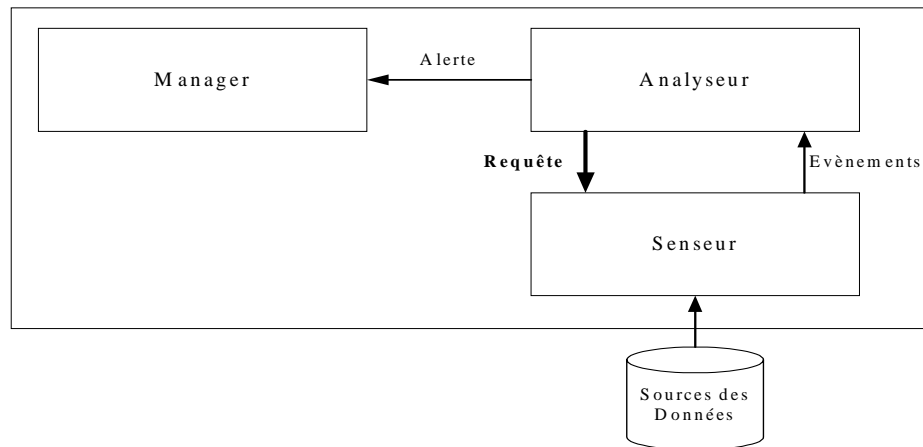
- IDS dans réseaux ad hoc : mobilité faible
- Architecture de sécurité des Aglets
 - Aglet : objet Java (*Bac à sable – Sérialisation....*)
 - Aglet exécutée dans un *contexte*
 - Dialogue entre Aglets par messages
 - Accès Aglet par un *proxy*
 - Authentification et confidentialité (SSL) de l'Aglet
 - Politique de sécurité propre au *contexte*

Agents Mobiles : plate-forme

AGLET

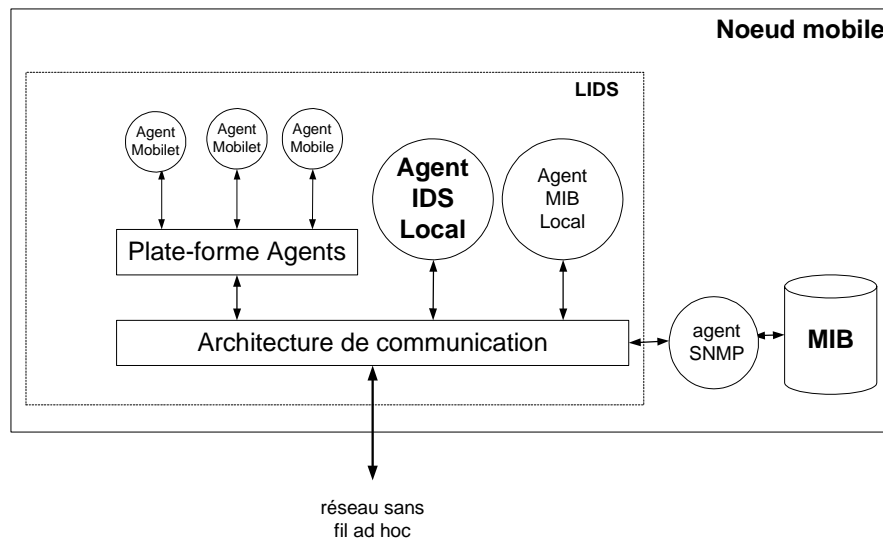


Extension du modèle de l'IDWG (IETF)



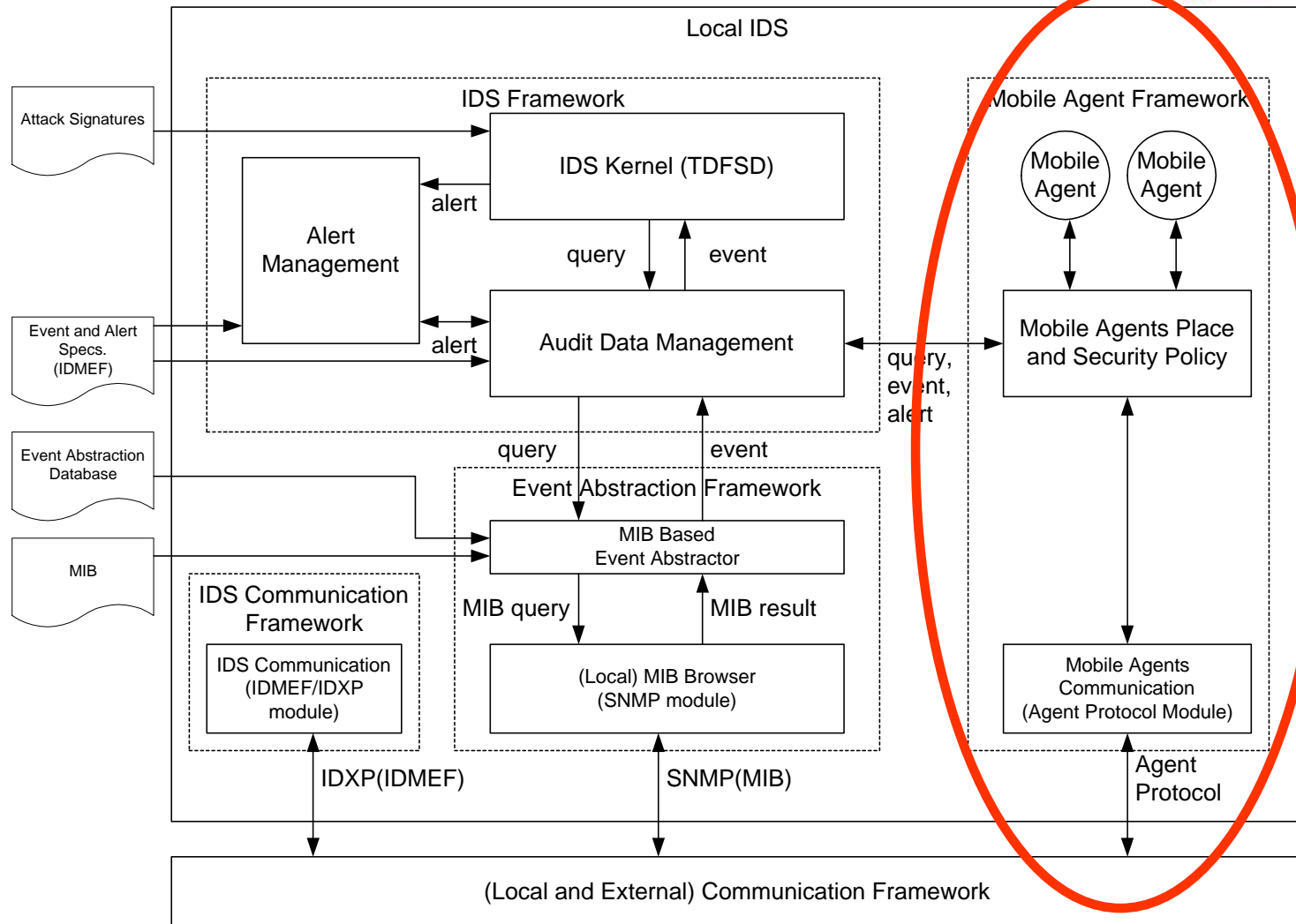
- Ajout du message requête
 - Permet à l'analyseur de collecter si besoin des données complémentaires

Architecture interne d'un LIDS



- Agent IDS Local
 - Analyse des données locales (MIB II)
- Agent MIB local
 - Gestion extensions MIB (routage ad hoc)

LID S



Agenda

- Le constat
- Un modèle de sécurité pour les réseaux ad hoc
- Motivation des travaux
- Modèle d'IDS distribué pour réseaux ad hoc
 - Spécifications
 - Architecture globale
 - Architecture interne d'un LIDS
- **Validation fonctionnelle**
- Conclusions et travaux futurs
- Démonstration

Attaques mises en œuvre et détectées

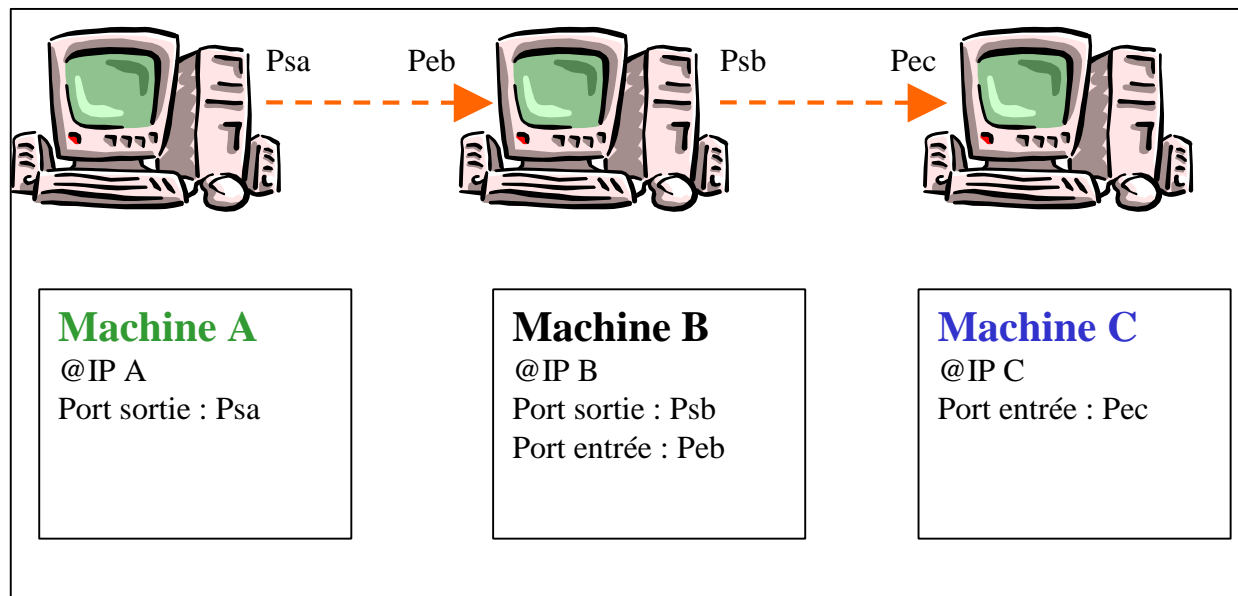
Attaques sur le routage OLSR

- Résultat d'une étude sur la vulnérabilité d'OLSR
- Définition d'une extension MIB spécifique
- Déni de service N sauts
 - Isolation d'une station
- Déni de service 1+N sauts
 - Détournement de trafic vers un nœud malicieux

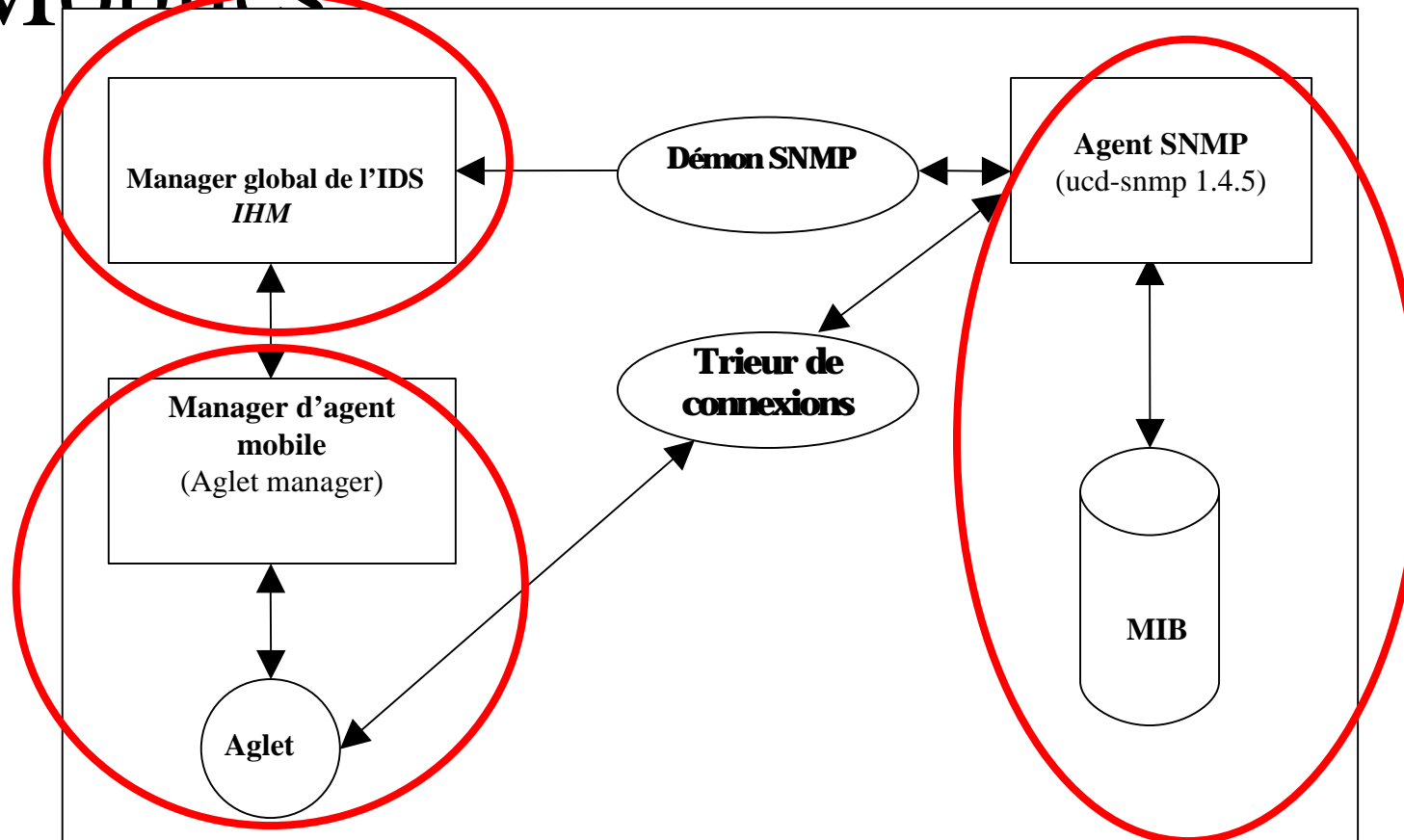
Attaque *Stepstone*

- Cascade de connexions Telnet
- Pas spécifique aux réseaux ad hoc
- Démontre l'intérêt de la mise en œuvre d'agents mobiles

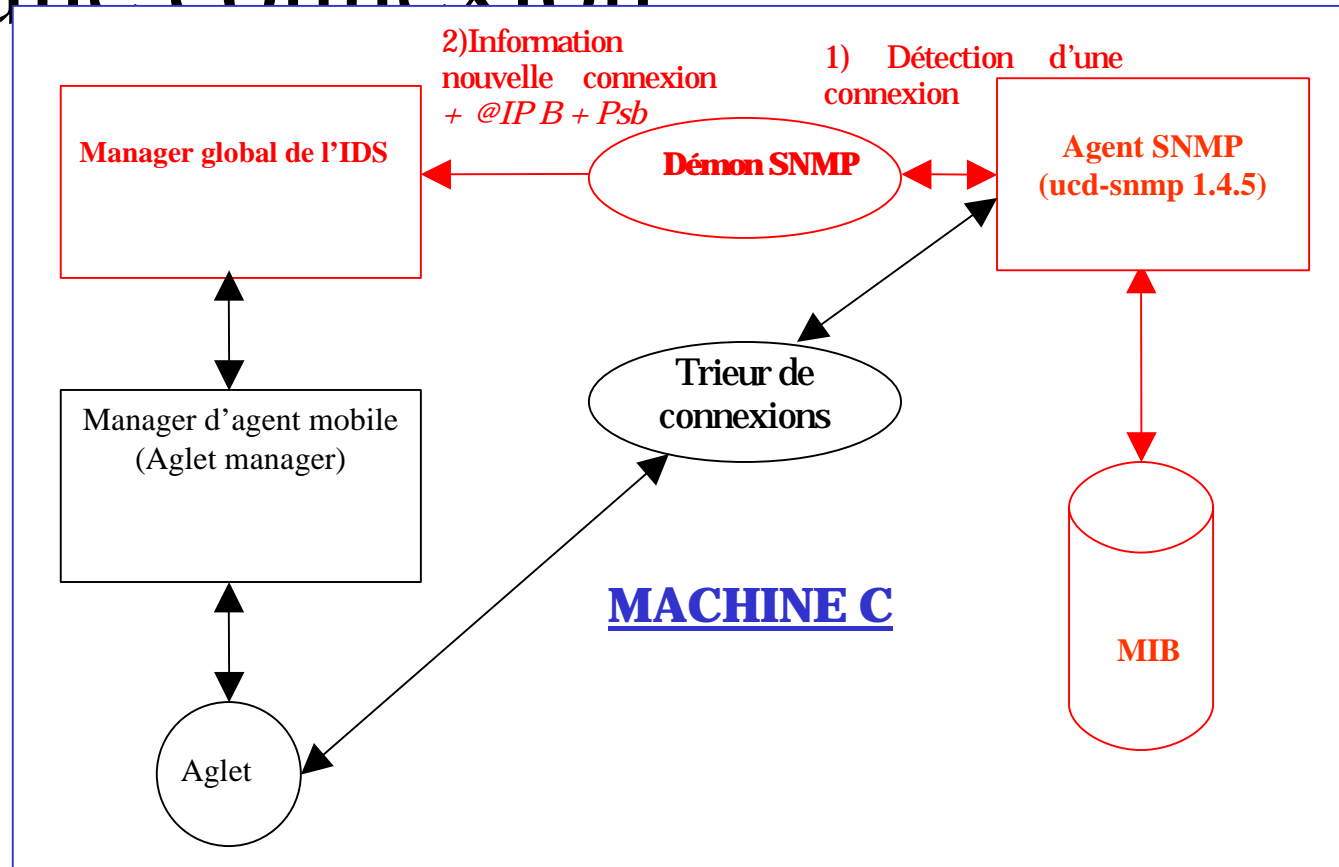
Détection d'une attaque par rebonds *Telnet*



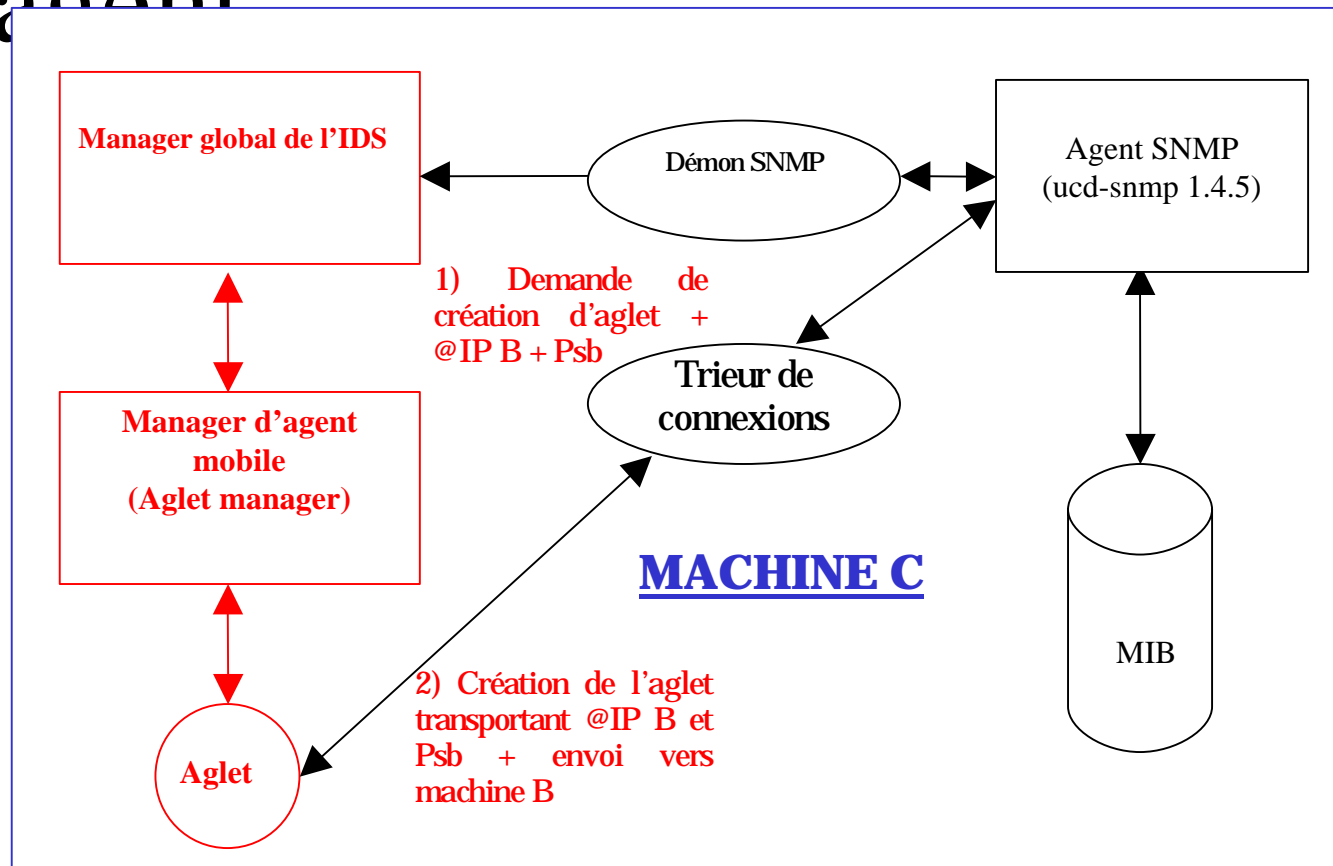
Composants de l'IDS à Agents Mobiles



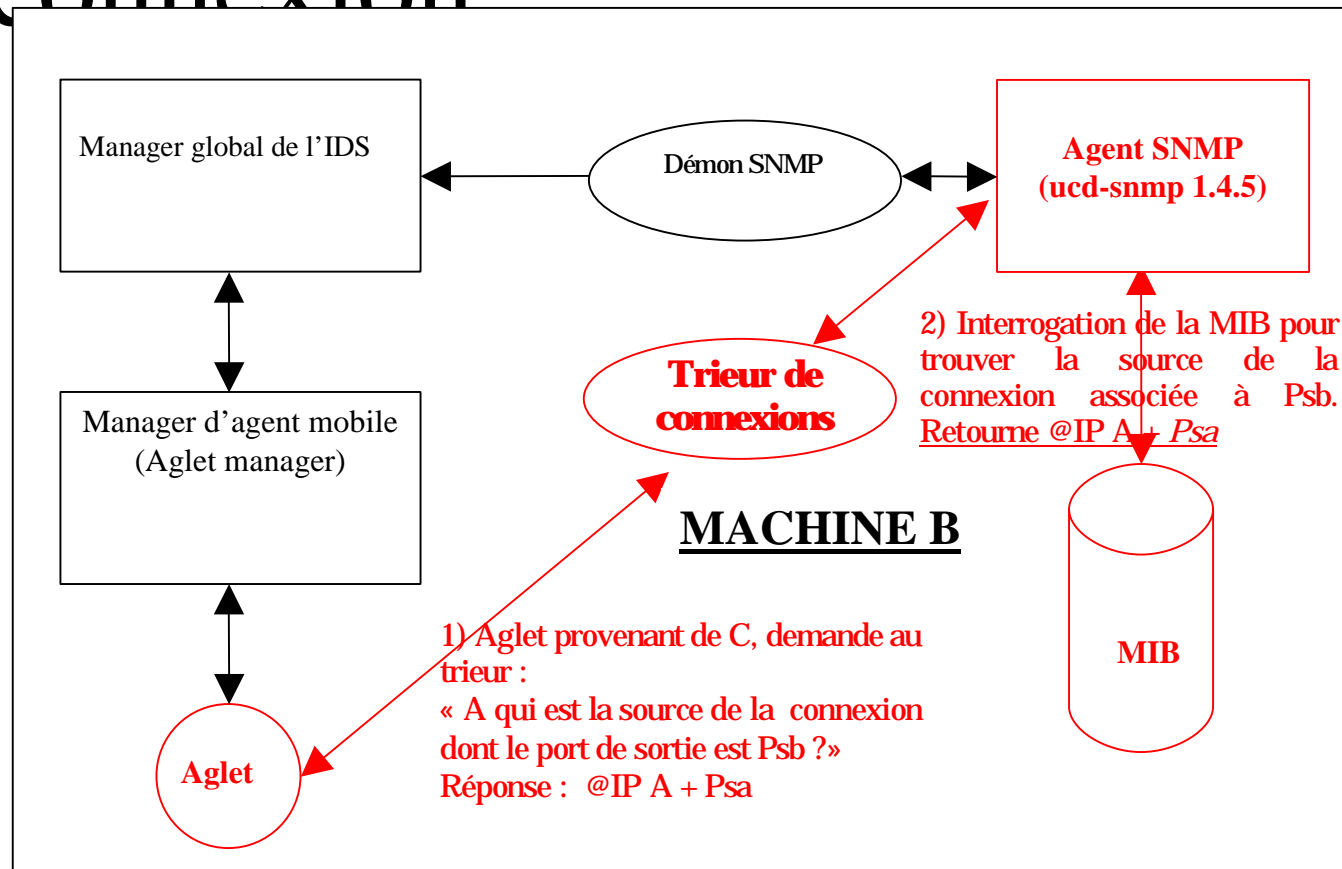
IDS sur la machine C : arrivée d'une connexion



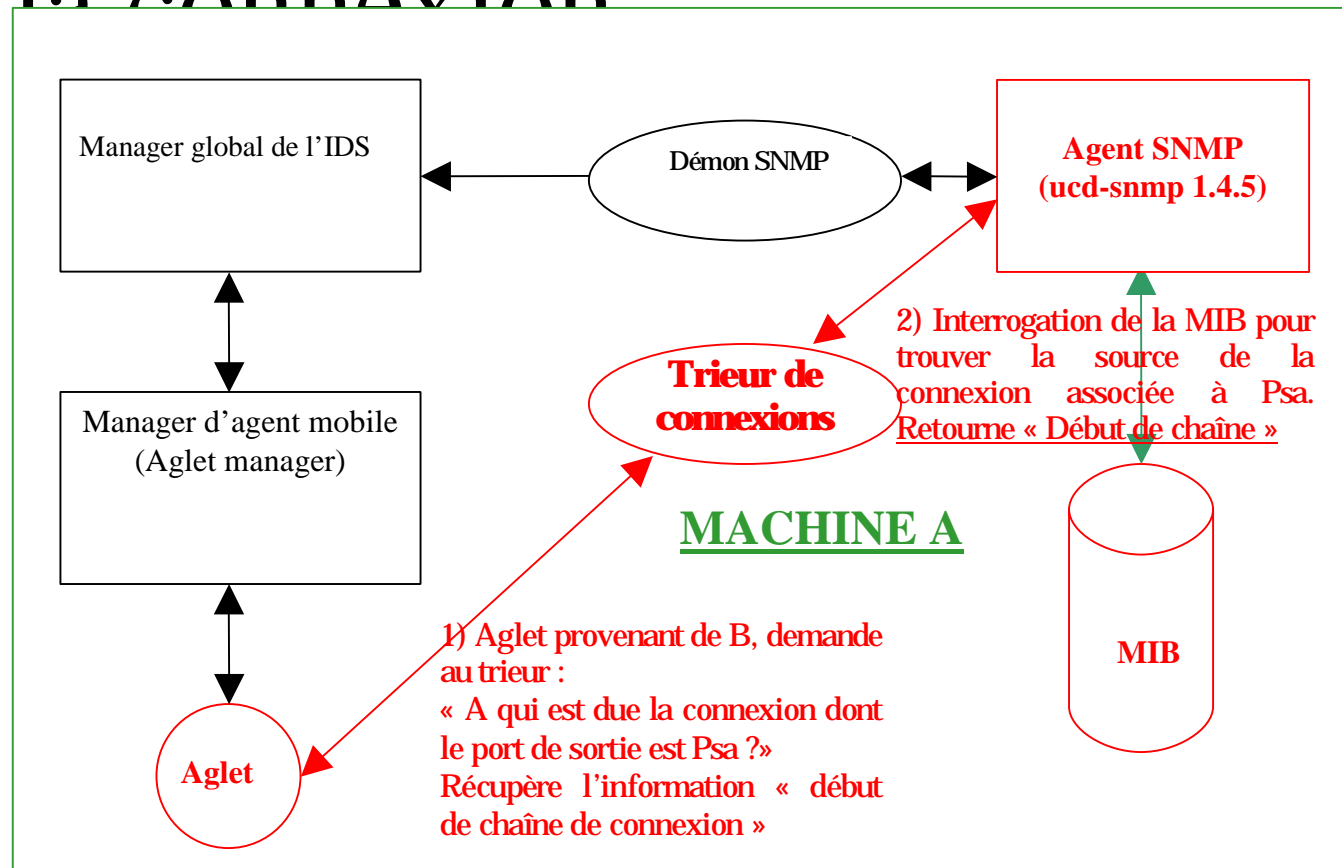
IDS sur la machine C : création de l'agent



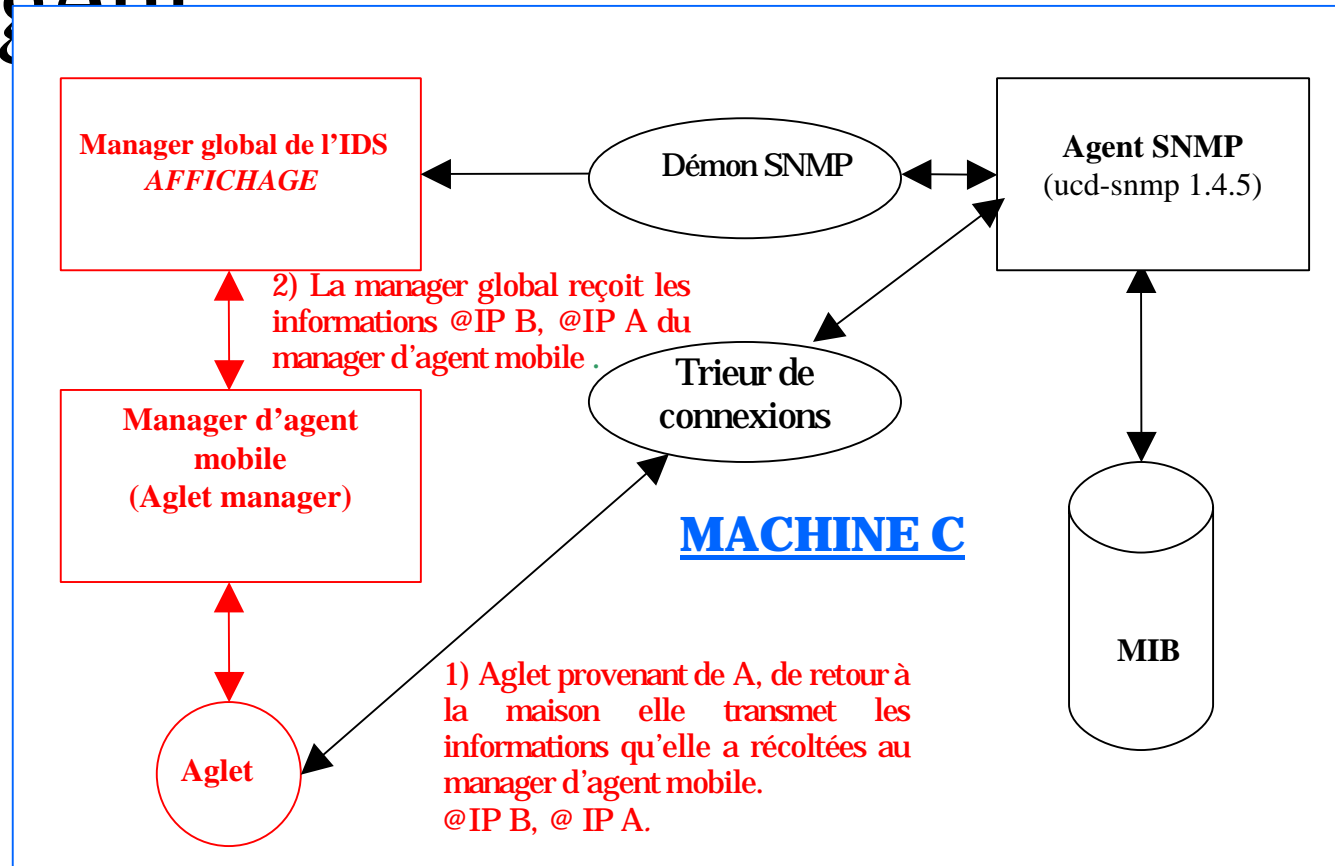
Aglet sur la machine B : source de la connexion



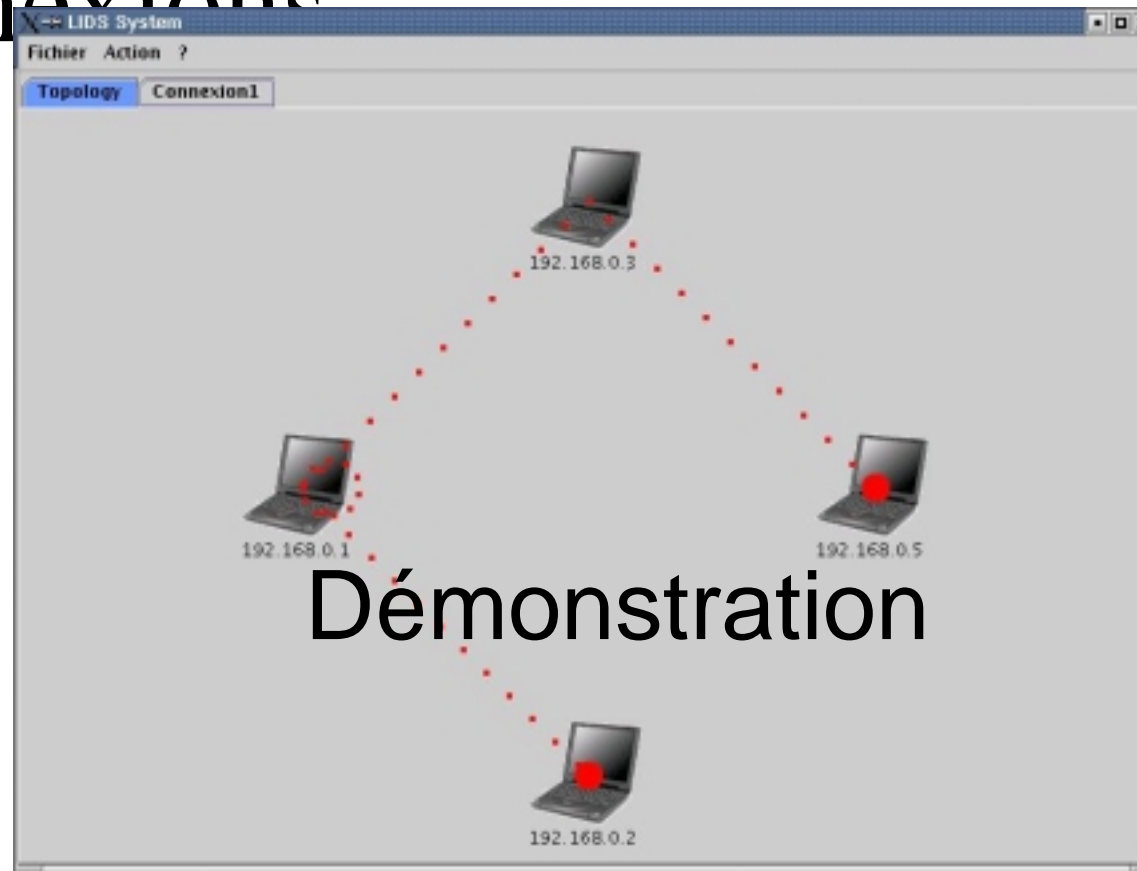
Aglet sur la machine A : origine de la connexion



IDS sur la machine C : retour de l'agent



Interface graphique de suivi des connexions



Agenda

- Le constat
- Un modèle de sécurité pour les réseaux ad hoc
- Motivation des travaux
- Modèle d'IDS distribué pour réseaux ad hoc
 - Spécifications
 - Architecture globale
 - Architecture interne d'un LIDS
- Résultats expérimentaux
- **Conclusions et travaux futurs**
- **Démonstration**



RAHMS

Réseaux Ad Hoc Multiservices Sécurisés



Les résultats du projet RAHMS :

- Conception et validation d'un IDS distribué à base d'agents mobiles pour MANET
 - Détection attaques sur le routage OLSR
 - Détection attaques rebonds Telnet
- Conception d'une plate-forme évolutive
 - Architecture modulaire et portable des LIDS
 - Collecte d'informations dans les MIB

Conclusions et futurs travaux

- **Mesures en cours** : performance Agents Mobiles / Client- Serveur dans les MANET.
 - Charge réseau induite,
 - Temps de réponse pour la collecte de données.
- Validation de la détection comportementale dans un contexte ad hoc.
- Plate-forme *agents mobiles*, optimisée IDS
- Définition/Gestion des politiques de sécurité dans les réseaux ad hoc.
- Deux thèses (2003) : détection des intrusions dans les réseaux ad hoc.
- Projet RNRT 2002 : everywhere (Supélec et ESEO)



Questions ????

