Diagnostic multi-sources adaptatif

Application à la détection d'intrusion dans des serveurs Web

Guyet Thomas, INRIA/IRISA

Wei Wang, INRIA/Sophia Antipolis

Quiniou René, INRIA/IRISA

Marie-Odile Cordier, Université Rennes 1/IRISA

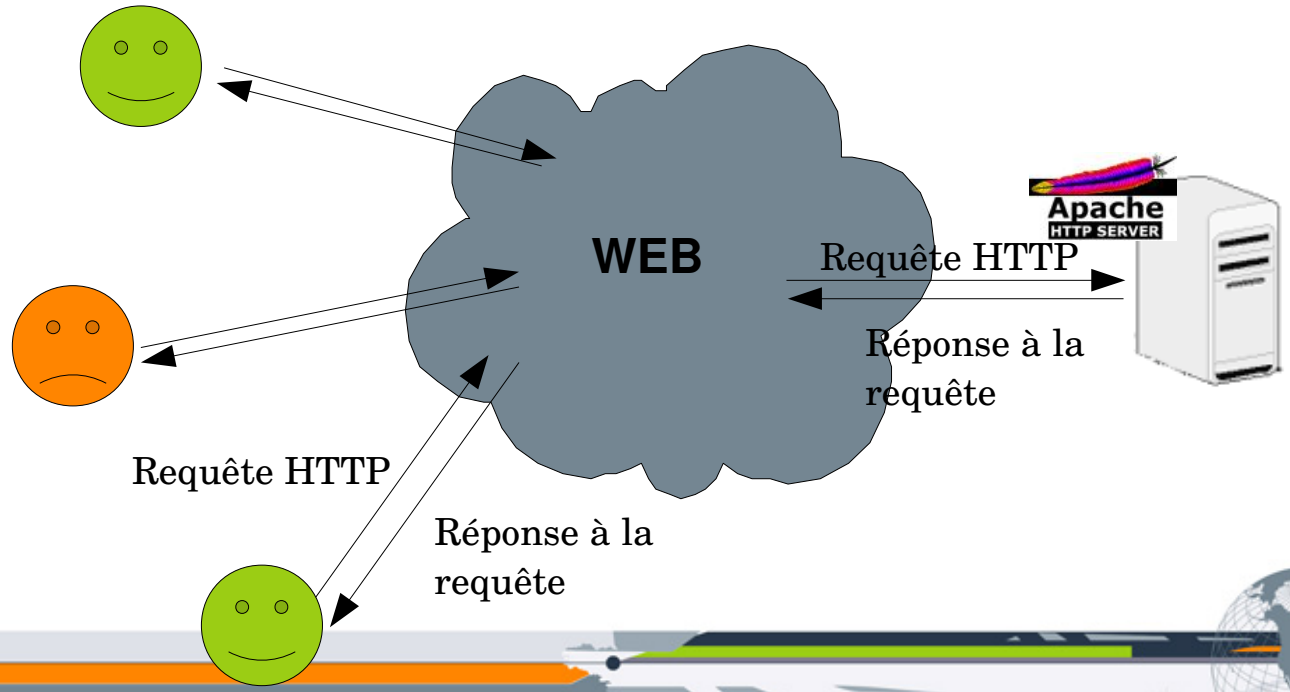
Conférence Extraction et Gestion des Connaissances,
Strasbourg, 28-30 jan 2009

Plan de présentation

1) Détection d'intrusion dans des serveurs Web
2) Problématique du diagnostic adaptatif
3) Diagnostic multi-source adaptatif
   - Principes
   - Réalisation
4) Expérimentations

Détection d'intrusion dans des serveurs Web

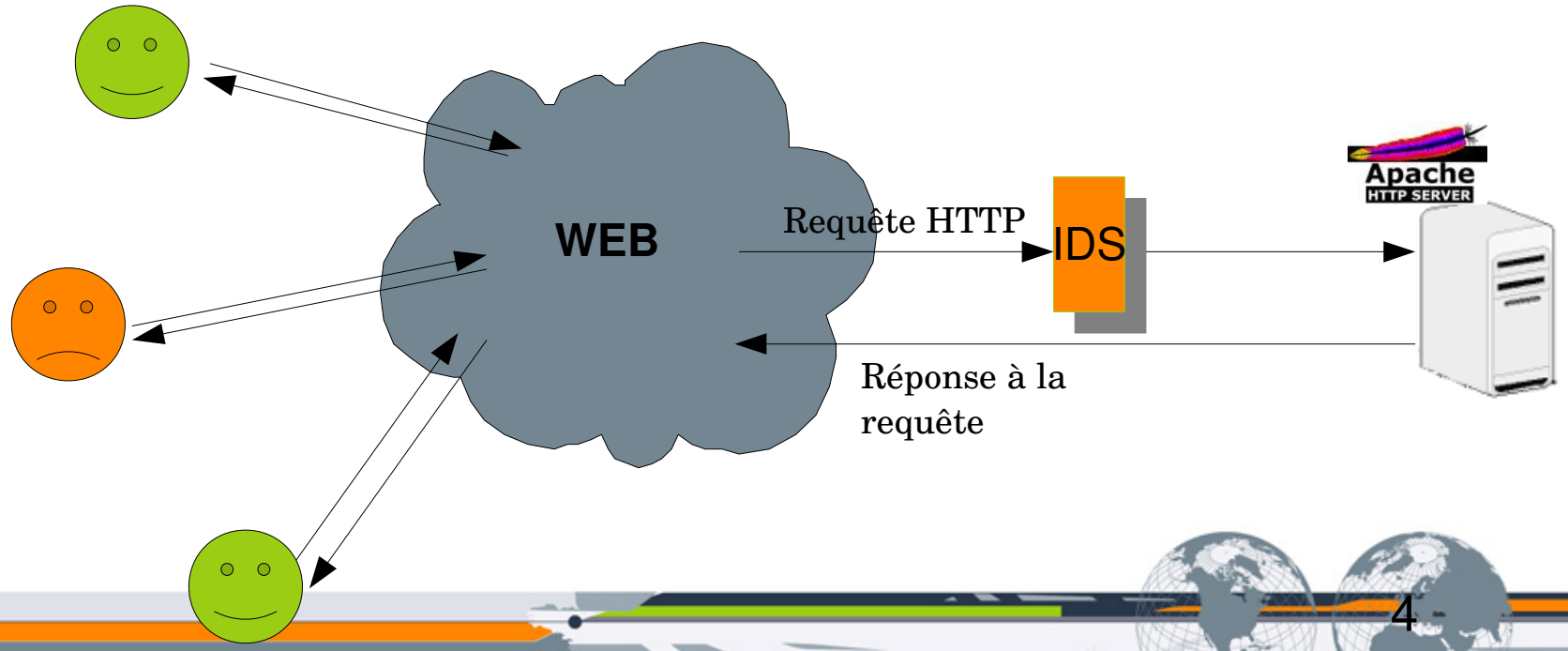
- Protection d'un serveur Web des intrusions
  - Assurer le service aux clients,
  - Protéger les données privées,
  - Prohiber les utilisations frauduleuses du serveur (diffusion illégales de pub, relais d'attaques DDOS, ...)



Diagnostic multi-source adaptatif, Guyet T., Wang W., Quiniou R. et Cordier M-O., *EGC*, 2009

Détection d'intrusion dans des serveurs Web

- Système de détection d'intrusion (IDS), agit comme un *firewall*
  - Détecte et bloque les tentatives d'intrusions (trafic entrant),
  - Autorise le trafic pour les requêtes non-intrusives ('normales'),
  - Informe les administrateurs des attaques.



Diagnostic multi-source adaptatif, Guyet T., Wang W., Quiniou R. et Cordier M-O., *EGC*, 2009

Détection d'intrusion dans des serveurs Web

- La détection d'une intrusion se fait à partir des logs de requête HTTP
  - Log d'une requête HTTP : enregistrement des informations relatives à la requête d'un client

client.remotehost.fr - - [09/May/2008:21:42:37 +0200] "GET /cgi-bin/fom.cgi?_insert=answer&cmd=addItem&file=1&keywords=%3f HTTP/1.1" 200 17 "-" "Mozilla2.4"

Détection d'intrusion dans des serveurs Web

- Utilisation d'une base de modèles d'intrusion
  - Modèle : abstraction caractérisant une requête comme intrusive *ou non* à partir de propriétés de son log.
  - Exemples de modèle à partir d'une requête
    - Tokens typiques d'une intrusion

client.remotehost.fr - - [09/May/2008:21:42:37 +0200] "GET /cgi-bin/db4web_c/dbdirname//etc/passwd HTTP/1.1" 302 17 "-" "Mozilla/4.75"

Détection d'intrusion dans des serveurs Web

- Utilisation d'une base de modèles d'intrusion
  - Modèle : abstraction caractérisant une requête comme intrusive *ou non* à partir de propriétés de son log.
  - Exemples de modèle à partir d'une requête
    - Tokens typiques d'une intrusion
    - Longueur typique de la requête d'une intrusion

client.remotehost.fr - - [09/May/2008:21:42:37 +0200] "GET /x/x/x/x/x/x/ ... /x/x/x/x/x/x/ HTTP/1.1" 302 17 "-" "Mozilla/4.75"

=> Peut provoquer des bugs dans les vieilles versions de serveurs Apache par dépassement de mémoire

Détection d'intrusion dans des serveurs Web

- Utilisation d'une base de modèles d'intrusion
  - Modèle : abstraction caractérisant une requête comme intrusive *ou non* à partir de propriétés de son log.
  - Exemples de modèle à partir d'une requête
    - Tokens typiques d'une intrusion
    - Longueur typique de la requête d'une intrusion
    - Client ayant soumis la requête connu comme malveillant

client.remotehost.fr - - [09/May/2008:21:42:37 +0200] "GET / HTTP/1.1" 302 17 "-" "Mozilla/4.75"

Détection d'intrusion dans des serveurs Web

- Utilisation d'une base de modèles d'intrusion
  - Modèle : abstraction caractérisant une requête comme intrusive *ou non* à partir de propriétés de son log.
  - Exemples de modèle à partir d'une requête
    - Tokens typiques d'une intrusion
    - Longueur typique de la requête d'une intrusion
    - Client ayant soumis la requête connu comme malveillant
    - Distribution typique de caractères d'une intrusion

client.remotehost.fr - - [09/May/2008:21:42:37 +0200] "GET /cgi-bin/alias=X%0acat%20/etc/passwd HTTP/1.1" 302 17 "-" "Mozilla/4.75"

=> Présence de caractères '%' en *proportion importante* laisse penser à une attaque

Détection d'intrusion dans des serveurs Web

- Utilisation d'une base de modèles d'intrusion
  - Modèle : abstraction caractérisant une requête comme intrusive *ou non* à partir de propriétés de son log.
  - Exemples de modèle à partir d'une requête
    - Tokens typiques d'une intrusion
    - Longueur typique de la requête d'une intrusion
    - Client ayant soumis la requête connu comme malveillant
    - Distribution typique de caractères d'une intrusion
    - ...
  - Typique = modèle appris à partir d'exemples de requêtes intrusives et normales *ou* fournis par un expert

Détection d'intrusion dans des serveurs Web

- Utilisation d'une base de modèles d'intrusion
  - Modèle : abstraction caractérisant une requête comme intrusive *ou non* à partir de propriétés de son log.
  - Exemples de modèle à partir d'une transaction
    - Transaction : ensemble des requêtes soumises par un client (identifié par son IP) dans un intervalle de temps prédéfini.

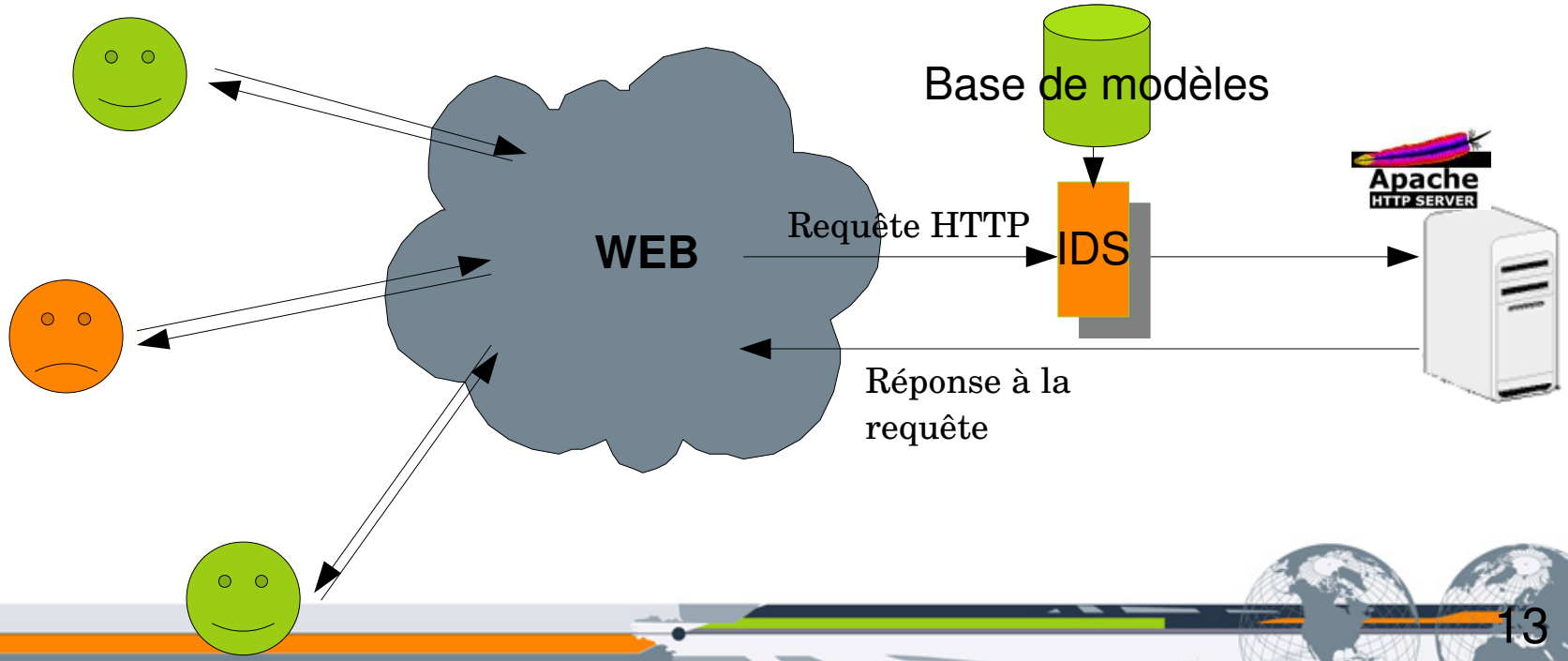
client.remotehost.fr - - [09/May/2008:21:42:37 +0200] "GET /cgi-bin/fom.cgi?_insert=answer&cmd=addItem&file=1&keywords=%3f HTTP/1.1" 404 17 "-" "Mozilla2.4"
client.remotehost.fr - - [09/May/2008:21:43:42 +0200] "GET /index.html HTTP/1.1" 200 1455 "-" "Mozilla2.4"
client.remotehost.fr - - [09/May/2008:21:44:13 +0200] "GET /images/puce.gif HTTP/1.1" 200 374 "-" "Mozilla2.4"

Détection d'intrusion dans des serveurs Web

- Utilisation d'une base de modèles d'intrusion
  - Modèle : abstraction caractérisant une requête comme intrusive *ou non* à partir de propriétés de son log.
  - Exemples de modèle à partir d'une transaction
    - Transaction : ensemble des requêtes soumises par un client (identifié par son IP) dans un intervalle de temps prédéfini.
    - Exemple de modèles d'intrusion
      - Taille de la transaction
      - Distribution de caractères sur l'ensemble des requêtes
      - Proportion d'erreur 404 dans la transaction
      - ...

Détection d'intrusion dans des serveurs Web

- Base de modèles pour la détection d'intrusions
- L'IDS analyse les logs entrants avec la base de modèles pour construire un **diagnostic de la requête : intrusive** ou **non-intrusive**



Diagnostic multi-source adaptatif, Guyet T., Wang W., Quiniou R. et Cordier M-O., *EGC*, 2009

Détection d'intrusion dans des serveurs Web

- Base de modèles
  - Doit initialement correspondre aux besoins de protection et au contenu du serveur
  - **Doit être régulièrement adaptée** pour tenir compte
    - Des nouvelles intrusions qui peuvent survenir
    - Des modifications du contenu du serveur
- Les problèmes soulevés par la détection d'intrusions
  - Comment construire initialement la base de modèles ?
  - **Comment maintenir à jour la base de modèles ?**

Détection d'intrusion dans des serveurs Web

- Base de modèles
  - Doit initialement correspondre aux besoins de protection et au contenu du serveur
  - **Doit être régulièrement adaptée** pour tenir compte
    - Des nouvelles intrusions qui peuvent survenir
    - Des modifications du contenu du serveur
- Les problèmes soulevés par la détection d'intrusions

Apprentissage supervisé

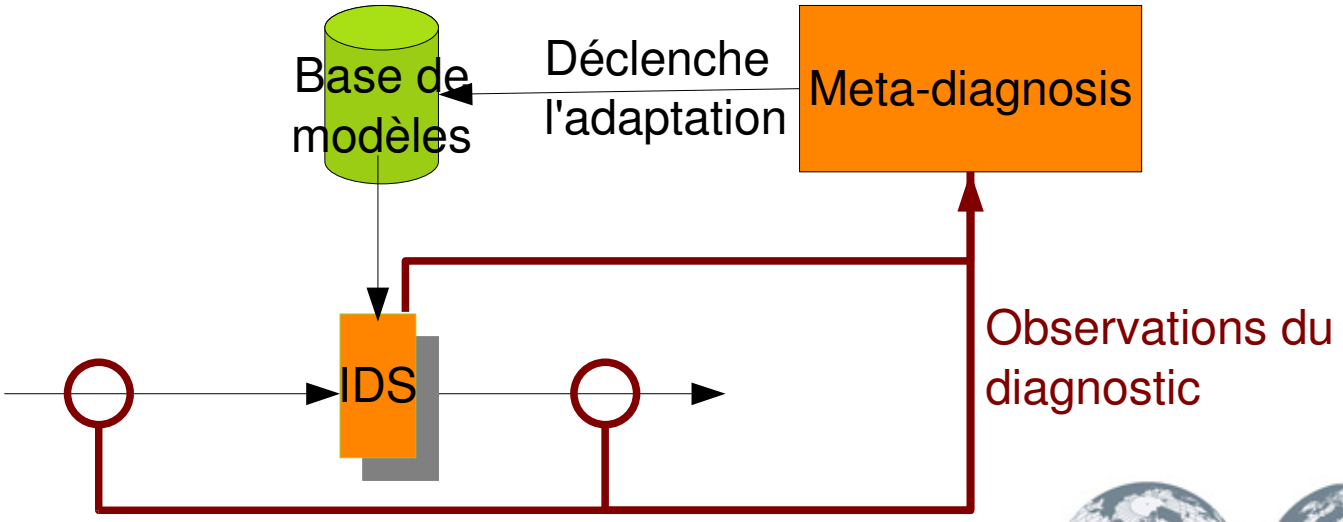
  - Comment construire initialement la base de modèles ?
  - **Comment maintenir à jour la base de modèles ?**

Diagnostic adaptatif

- Objectif : détecter les intrusions **et** maintenir à jour automatiquement la base de modèles
- Principe général
  - Tant que les modèles sont à jour, ils peuvent être utilisés pour détecter les intrusions
  - Lorsque les modèles ne sont plus à jour, il faut déclencher leur adaptation
- Problème : Comment déterminer s'il faut adapter les modèles ?

Diagnostic adaptatif

- Vers une méthode de diagnostic adaptatif
  - **Diagnostic** : Détecter les intrusions
  - **Méta-diagnostic** (diagnostic du diagnostiqueur) : Détecter les besoins d'adaptation des modèles



Diagnostic multi-source adaptatif, Guyet T., Wang W., Quiniou R. et Cordier M-O., *EGC*, 2009

Méta-diagnostic : principes

- Comment détecter le besoin d'une adaptation ? *ou*
- Comment détecter une erreur de diagnostic ?

  – Détecter les augmentations de faux positifs et/ou de faux négatifs ?

  – **Pb :** Le système n'a pas accès à une ***référence absolue*** du diagnostic

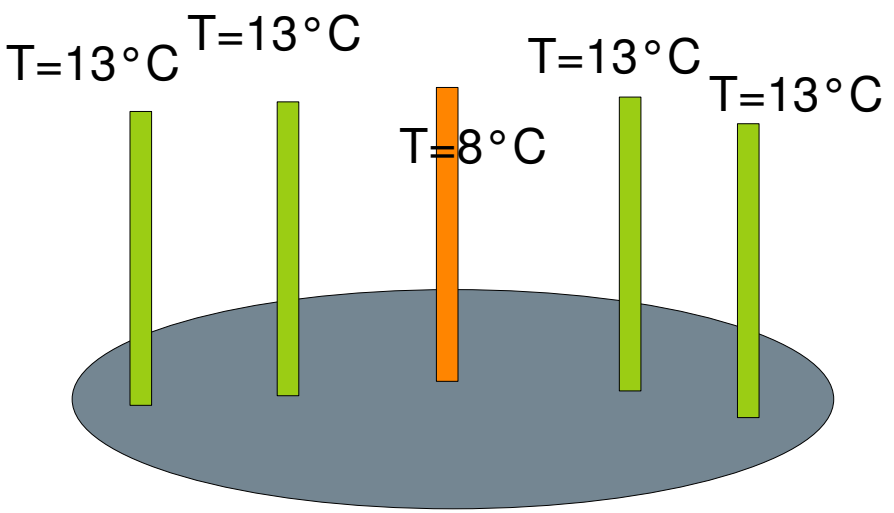
Méta-diagnostic : principes

- Comment détecter le besoin d'une adaptation ? *ou*
- Comment détecter une erreur de diagnostic ?

  – Le meta-diagnostic utilise des ***différences relatives*** entre diagnostics pour détecter les manquements du diagnostic

Méta-diagnostic : principes

- Exemple d'utilisation de différences relatives entre diagnostics
  - 5 thermomètres identiques plongés dans la même eau
  - Le thermomètre donnant une température différente des autres est suspect d'être cassé et doit être réparé



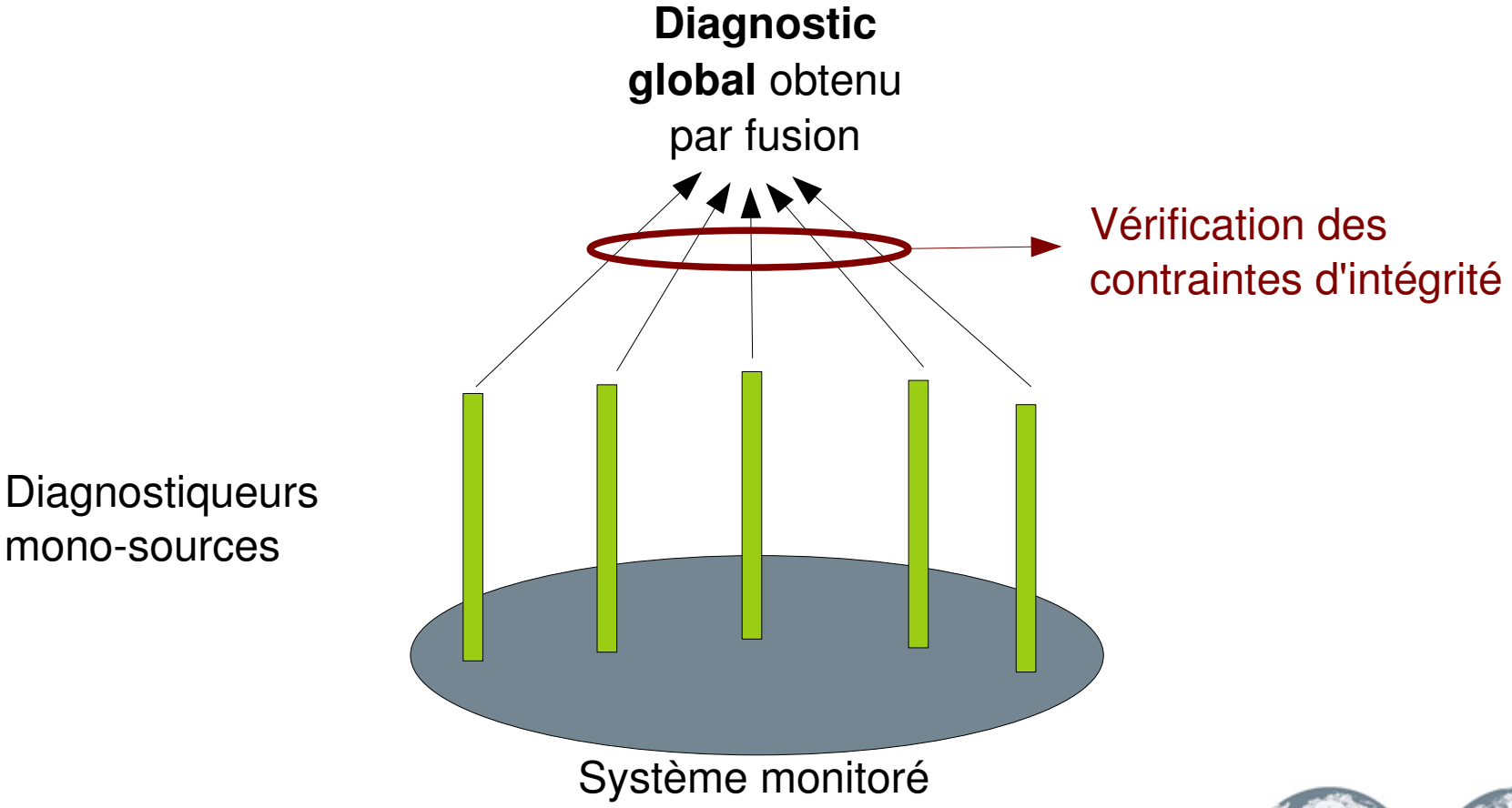
Diagnostic multi-source adaptatif, Guyet T., Wang W., Quiniou R. et Cordier M-O., *EGC*, 2009

Méta-diagnostic : principes

- Comment détecter le besoin d'une adaptation?
  - Diagnostic ***multi-sources*** : construire un diagnostic à partir de plusieurs sources d'informations
  - Méta-diagnostic : Vérifier des ***contraintes d'intégrité*** entre plusieurs diagnostics
    - Utiliser des connaissances expertes sur la redondances des informations entre les sources pour définir ces contraintes d'intégrité
      - Redondances temporelles, spatiales et structurelles

Diagnostic multi-sources adaptatif

- Architecture générale proposée



Diagnostic multi-source adaptatif, Guyet T., Wang W., Quiniou R. et Cordier M-O., *EGC*, 2009

Diagnostic multi-sources adaptatif

- Diagnostiqueur mono-source (DMoS)
  - Construit un diagnostic à partir d'observations du système diagnostiqué
  - Chaque diagnostiqueur apporte son propre point de vue sur le système
  - *Pour l'analyse de log HTTP, un DMoS est associé à un type de modèle d'intrusion*
    - *Distribution de caractères dans la requête*
    - *Présence de tokens significatifs dans la requête*
    - *Valeur du status code*
    - *Distribution de caractères dans la transaction*
    - *Taille de la transaction*

Diagnostic multi-source adaptatif, Guyet T., Wang W., Quiniou R. et Cordier M-O., *EGC*, 2009

Diagnostic multi-sources adaptatif

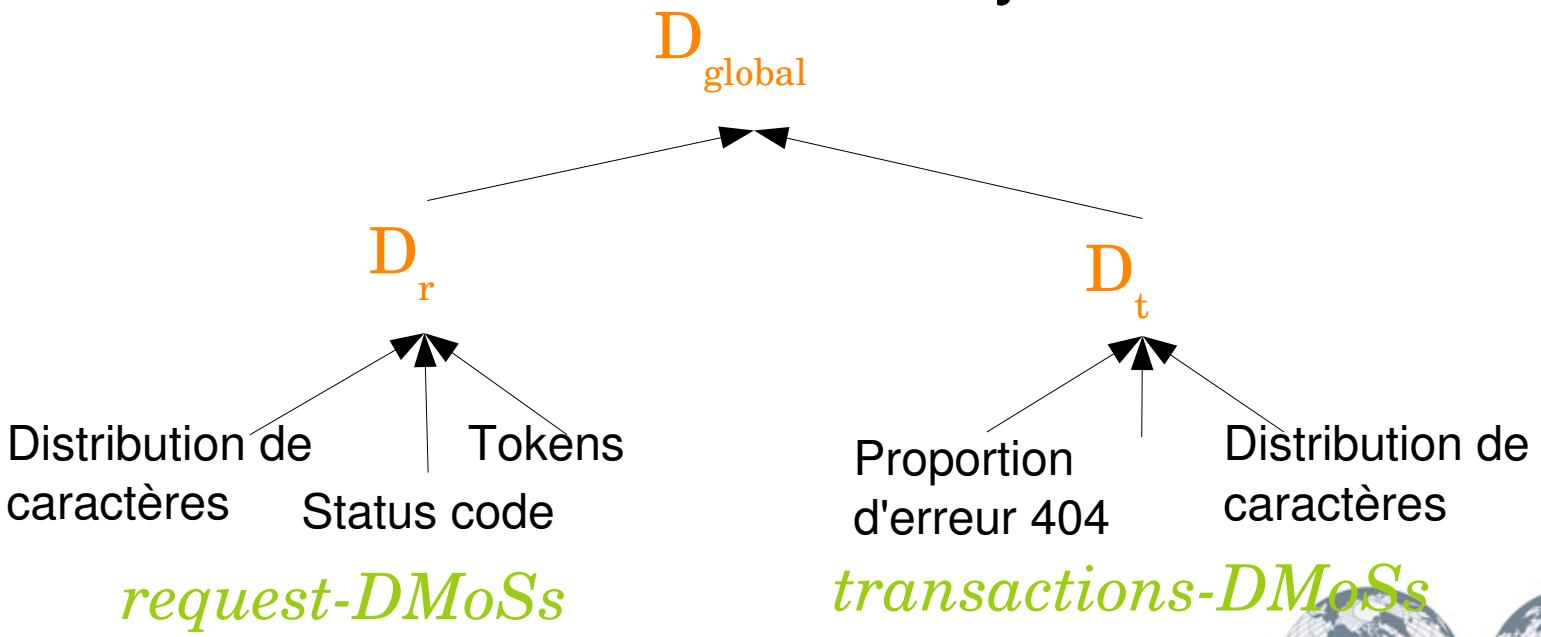
- Pour obtenir le diagnostic global, les diagnostics sont fusionnés
- Cadre de la fusion de Dempster-Shafer
  - Un diagnostic = un distribution normalisée de masses sur un espace de discernement Ω.
    - *Pour la détection d'intrusion, Ω* = {I, N, U}
  - Combinaison de 2 diagnostics

$$\forall A \in \Omega,\ (m_1 \oplus m_2)(A) = \frac{m_1(A)m_2(A)}{1 - \sum_{B \cap C = \emptyset} m_1(B)m_2(C)},$$

$$\sum_{B \cap C = \emptyset} m_1(B)m_2(C) = m_1(N)m_2(I) + m_1(N)m_2(U) + m_1(U)m_2(I) + m_1(U)m_2(N) + m_1(I)m_2(N) + m_1(I)m_2(U)$$

Diagnostic multi-sources adaptatif

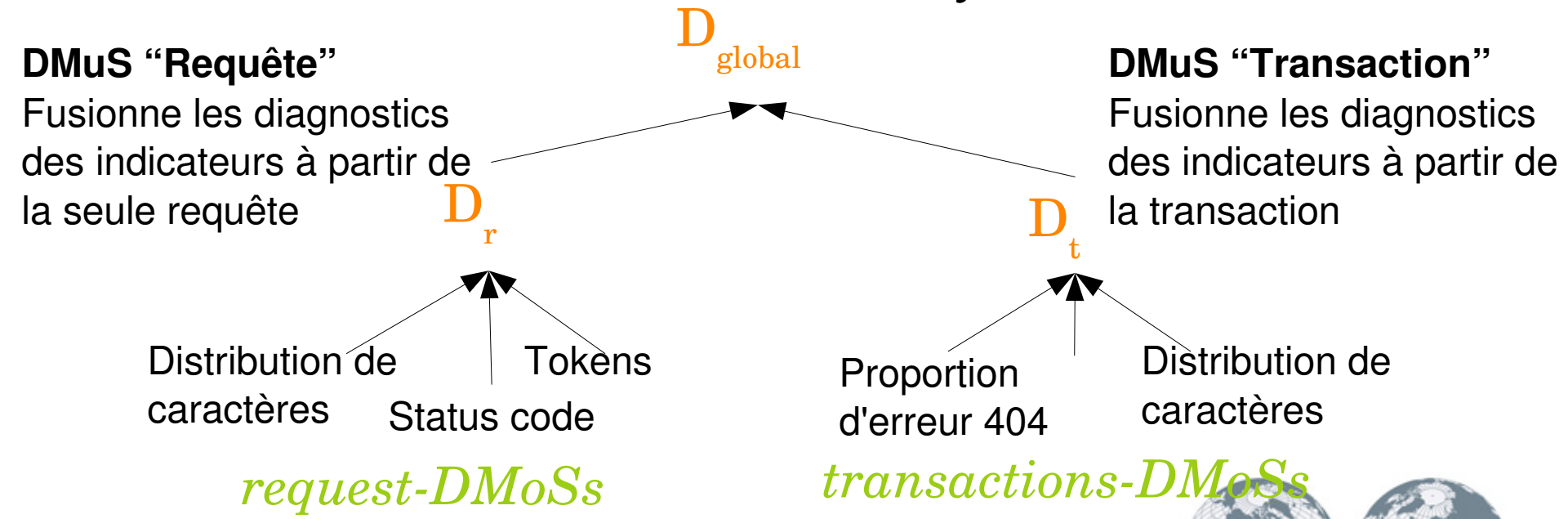
- La fusion est réalisée par des diagnostiqueurs multi-sources (DMuS)
  - Diagnostics intermédiaires (utiles au méta-diagnostic)
  - Points de vue *virtuels* sur le système



Diagnostic multi-source adaptatif, Guyet T., Wang W., Quiniou R. et Cordier M-O., *EGC*, 2009

Diagnostic multi-sources adaptatif

- La fusion est réalisée par des diagnostiqueurs multi-sources (DMuS)
  - Diagnostics intermédiaires (utiles au méta-diagnostic)
  - Points de vue *virtuels* sur le système



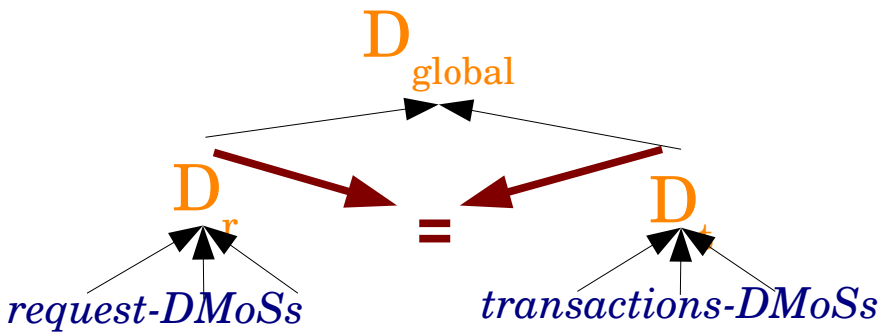
Diagnostic multi-source adaptatif, Guyet T., Wang W., Quiniou R. et Cordier M-O., *EGC*, 2009

Diagnostic multi-sources adaptatif

- Contrainte d'intégrité entre diagnostics
  - Définit une **relation** systématiquement attendue entre les diagnostics fournis par des diagnostiqueurs
  - Exprime des connaissances *a priori* du concepteur
- Si une contrainte d'intégrité n'est pas respectée, l'un au-moins des diagnostiqueurs impliqué dans la contrainte doit être adapté
  - Lequel ?

Diagnostic multi-sources adaptatif

- *Contraintes d'intégrité pour l'analyse de logs HTTP*
  - *Hypothèse : toutes les requêtes d'une transaction sont toutes intrusives ou toutes normales*
  - *Contrainte d'intégrité : le diagnostic fournis par Dr doit être le même que celui de Dt*

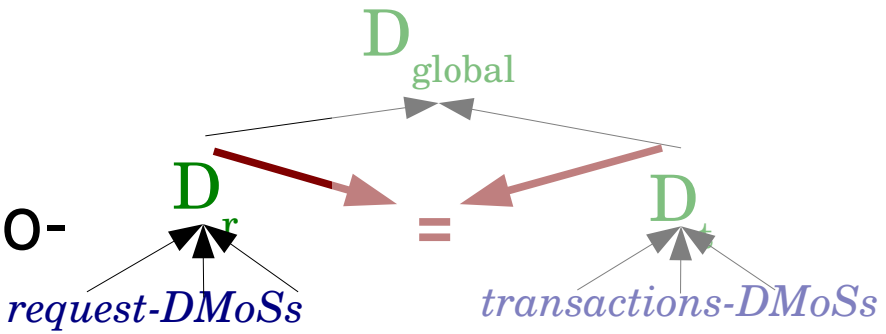


Diagnostic multi-sources adaptatif

- *Contraintes d'intégrité pour l'analyse de logs HTTP*
  - *Si la contrainte n'est pas vérifiée, il faut savoir si la faute vient des transactions ou des requêtes*
  - *Heuristique: On fait confiance au diagnostiqueur qui est le plus sûr de son diagnostic*
    - *Le système détecte un besoin d'adaptation des diagnostiqueurs à partir de la transaction si le diagnostic à partir de la requête est sûr et celui à partir de la transaction est peu sûr.*

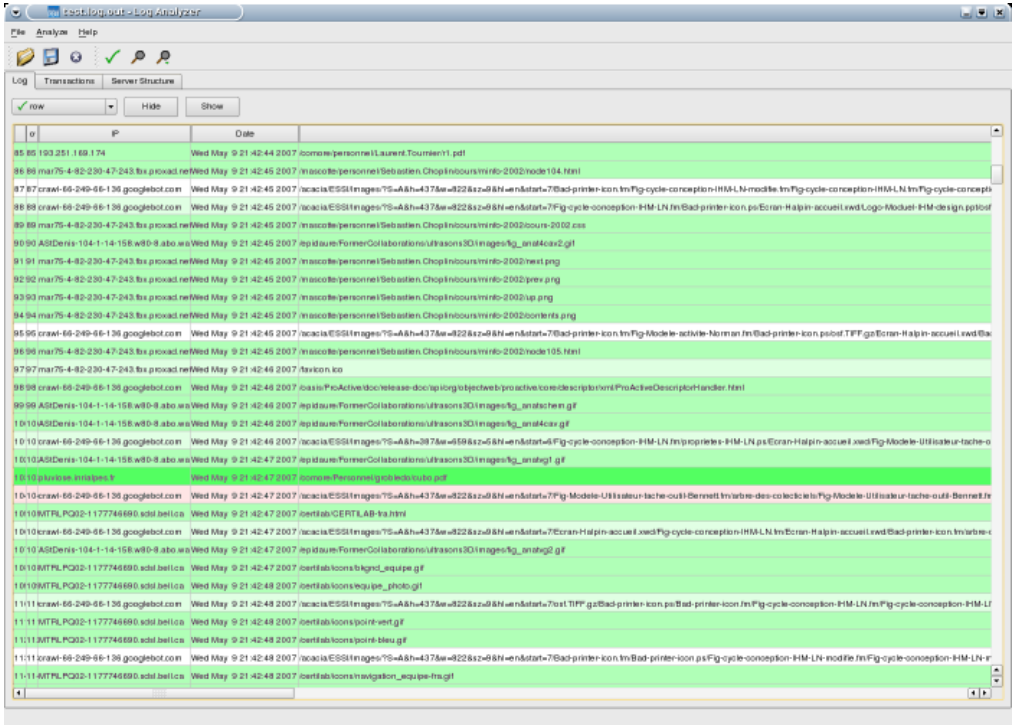
Diagnostic multi-sources adaptatif

- Diagnostiqueurs adaptés
  - Tous les diagnostiqueurs mono-sources **aux feuilles** d'une contrainte non-satisfaite sont adaptés
- Adaptation effective
  - Les diagnostiqueurs mono-sources disposent des mécanismes d'adaptation de leurs modèles
  - *Exemple : adaptation de la distribution de caractères*



Implémentation

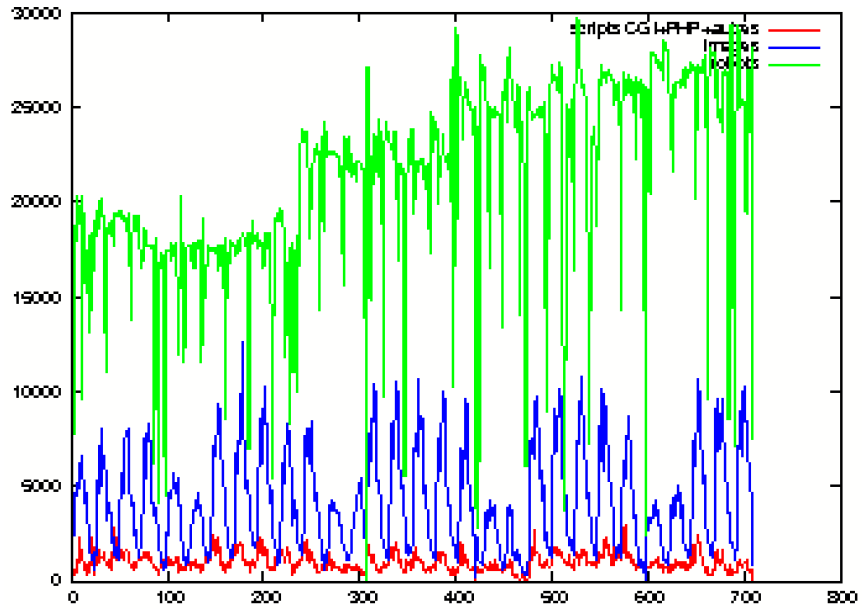
- LogAnalyzer (C++)
  - Outil d'analyse interactif
  - Permet de traiter les logs en flux
- Fonctionnalités
  - Visualisation, filtrage, statistiques, ...

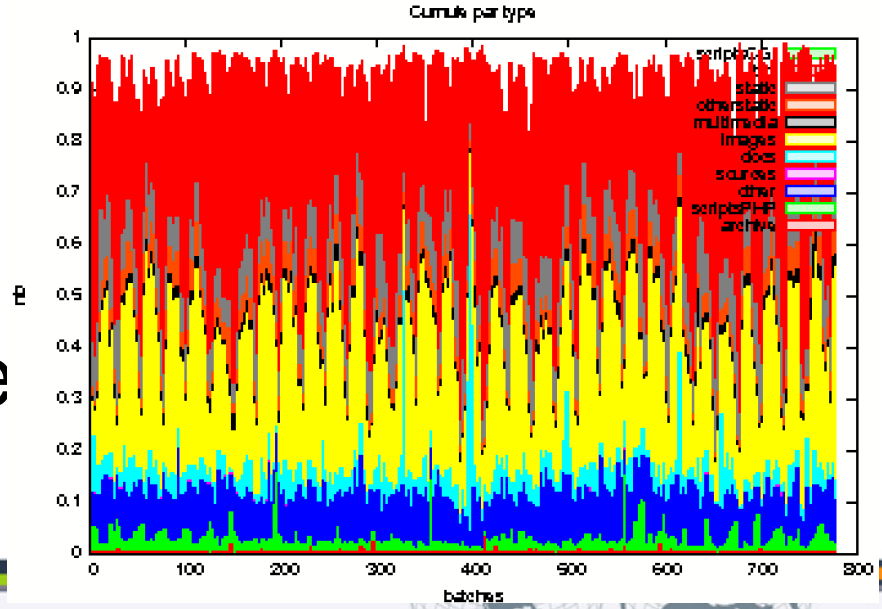


http://www.irisa.fr/dream/LogAnalyzer/

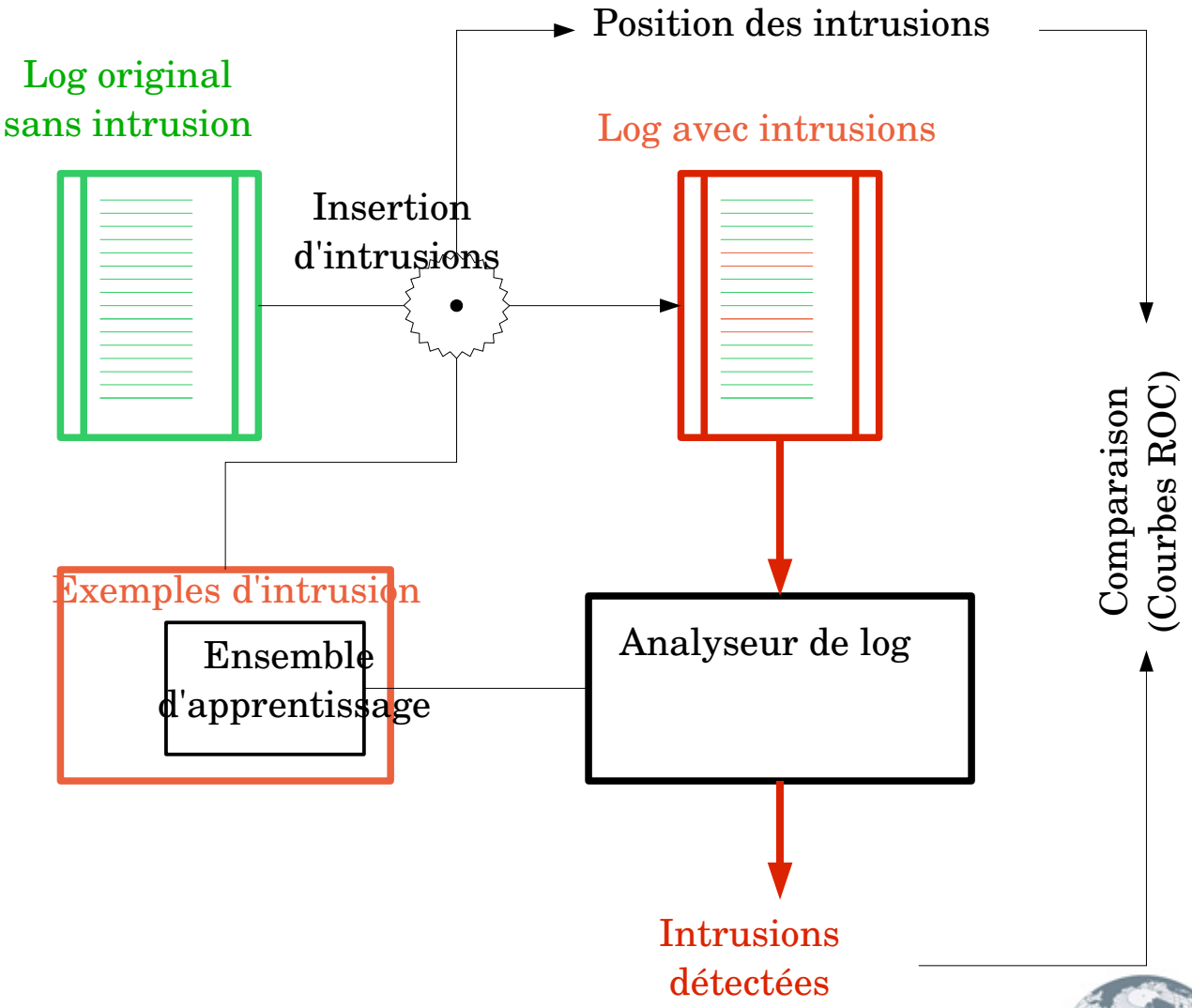
Données

- Logs des serveurs web
  - INRIA/Sophia-Antipolis (juillet 2007), ~1.5 M de requêtes
  - IRISA (juin 2008), ~10M de requêtes
- Données prétraitées et filtrées pour permettre une vérification manuelle de l'absence d'intrusion





Expérimentations



Diagnostic multi-source adaptatif, Guyet T., Wang W., Quiniou R. et Cordier M-O., *EGC*, 2009

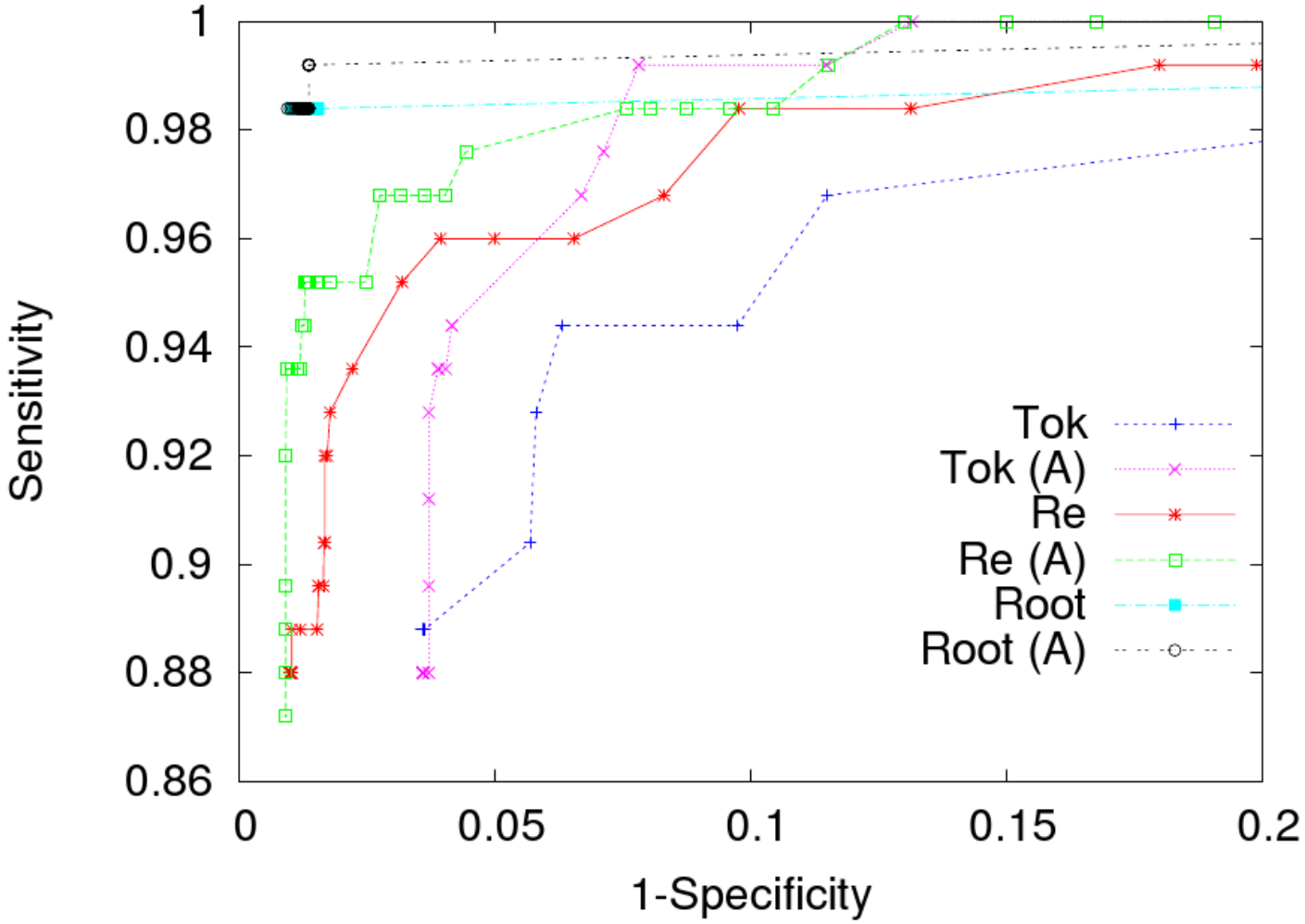
Résultats

	Shafer	Moyenne
Nb d'adaptation	121.04 ($\pm$ 97.94)	139.19 ($\pm$44.36)
Adaptations correctes	**0.95** ($\pm$0.02)	0.93 ($\pm$0.03)
Expérimentations détectant la nouvelle intrusion	**0.35**	0.27

	Shafer		Moyenne	
	Avec adaptation	Sans adaptation	Avec adaptation	Sans adaptation
Temps (s.)	12.68 ($\pm$ 0.46)	**11.83** ($\pm$ 0.38)	10.12 ($\pm$ 0.22)	**9.58** ($\pm$ 0.19)
Rappel	**0.94** ($\pm$ 0.03)	0.93 ($\pm$ 0.04)	**0.50** ($\pm$ 0.26)	0.49 ($\pm$ 0.33)
Precision	**0.81** ($\pm$ 0,25)	0.78 ($\pm$ 0.31)	**0.93** ($\pm$ 0,09)	0.91 ($\pm$ 0.09)
F-mesure	**0.85** ($\pm$ 0.18)	0.81 ($\pm$ 0.22)	**0.61** ($\pm$ 0.28)	0.55 ($\pm$ 0.35)

Traitements d'extraits de logs de 10000 requêtes

Résultats



Diagnostic multi-source adaptatif, Guyet T., Wang W., Quiniou R. et Cordier M-O., *EGC*, 2009

Conclusions

- Une méthode de diagnostic adaptatif *(en contexte changeant)*
  - Diagnostic multi-sources
  - Méta-diagnostic à partir de contraintes d'intégrités

- Application à la détection d'intrusions dans des serveurs Web
  - Les adaptations proposées sont très pertinentes
  - Les performances sont améliorées par l'adaptation

Diagnostic multi-source adaptatif, Guyet T., Wang W., Quiniou R. et Cordier M-O., *EGC*, 2009

Perspectives

- Développer d'autres modèles d'intrusion pour rendre les décisions plus robustes
- Évaluer le système sur des intrusions réelles
  - Évaluation de la pertinence réelle de la contrainte d'intégrité utilisée
  - Essai de nouvelles contraintes d'intégrités
- Tirer partie de la fusion de données dans un contexte de flux de données
  - Réduire le nombre de sources pour accélérer le traitement
  - Ouvre le problème du choix dynamique des sources les plus pertinentes

Merci ...

Questions ?