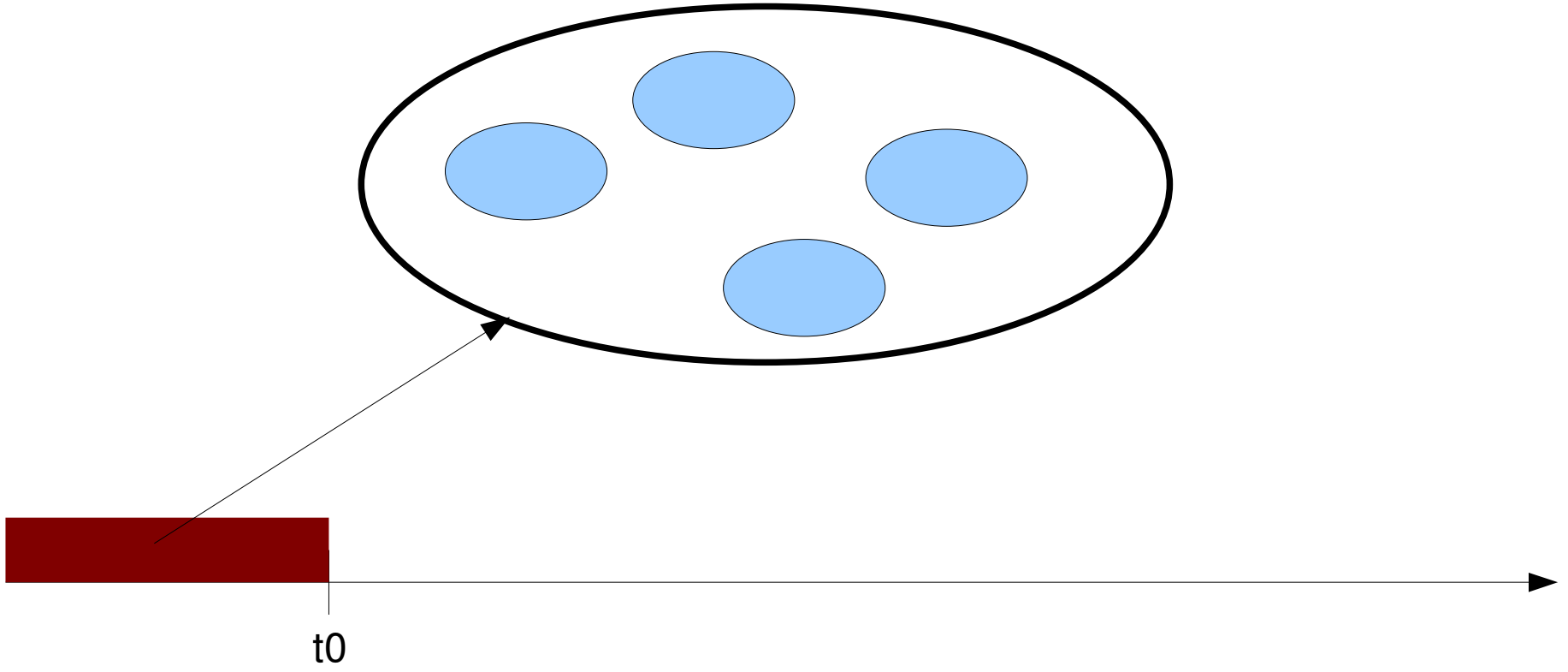
Online and adaptive anomaly detection: detecting intrusions in unlabelled audit data streams

Wei Wang, *INRIA/Sophia Antipolis*
Thomas Guyet, *INRIA/IRISA*
René Quiniou, *INRIA/IRISA*
Marie-Odile Cordier, *Université Rennes 1/IRISA*
Florent Masseglia, *INRIA/Sophia Antipolis*

Conférence EGC, Strasbourg, 28-30 Jan. 2009

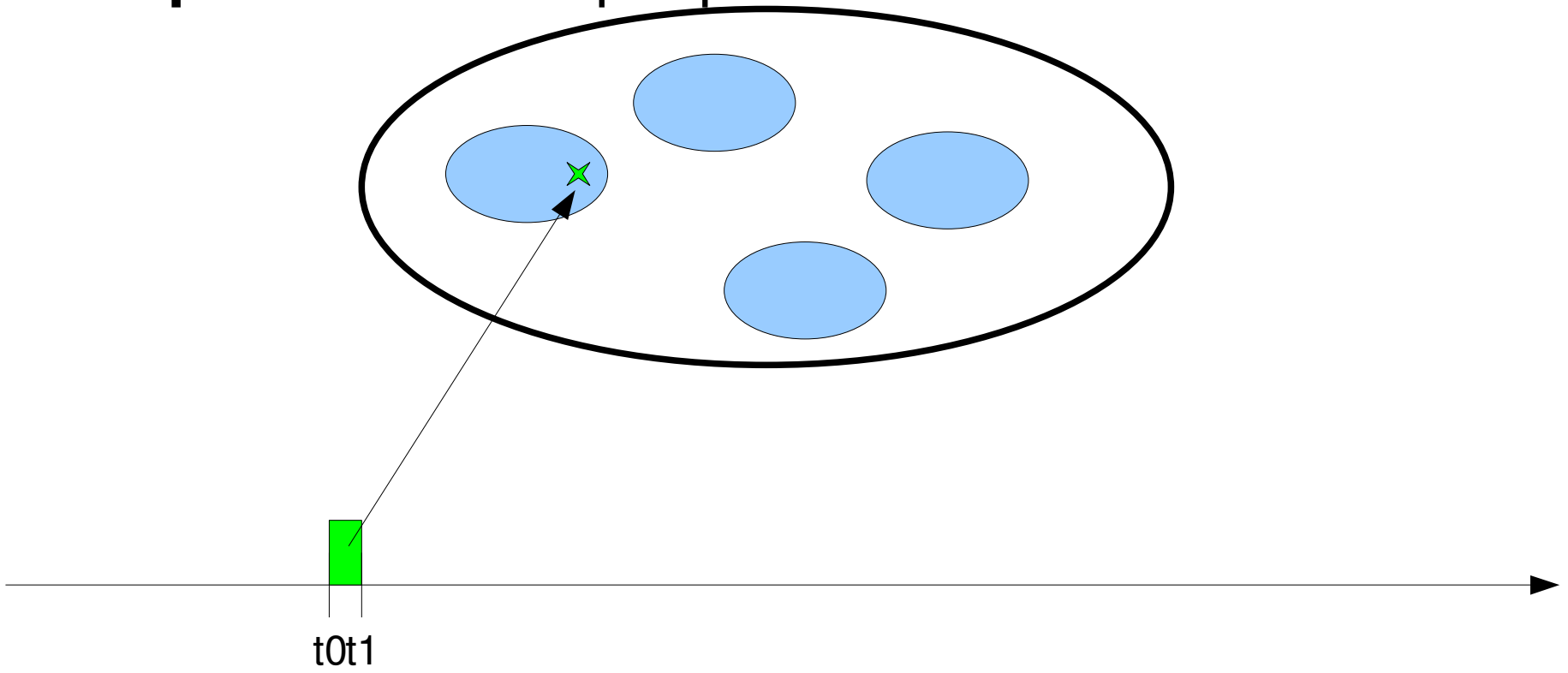
Détection adaptative d'anomalie

- Initialisation :
  - Construction d'un modèle de comportement normal
  - Modèle = ensemble de *clusters*



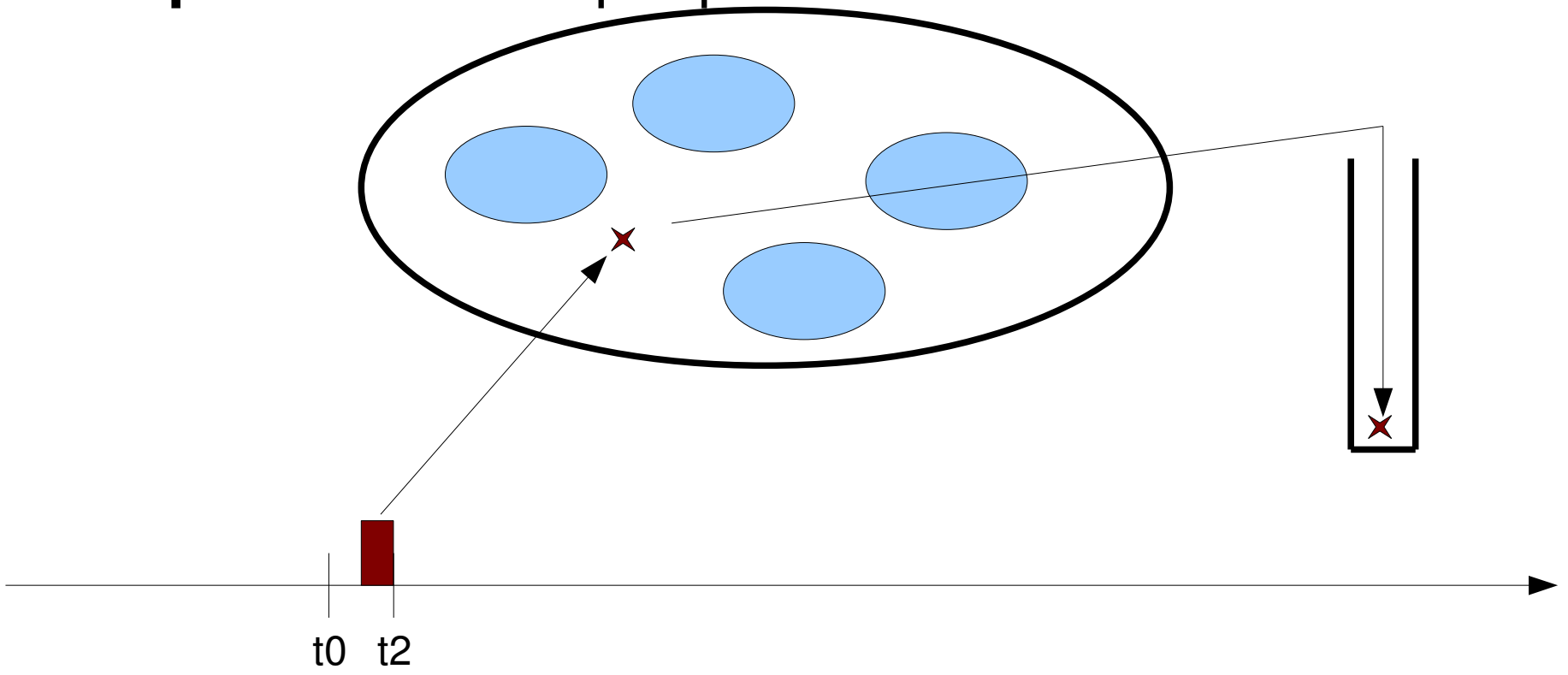
Détection adaptative d'anomalie

- Régime permanent : analyse d'un nouvel exemple
  - **Normal** : mise à jour du *cluster*
  - **Suspicieux** : exemple placé dans un réservoir



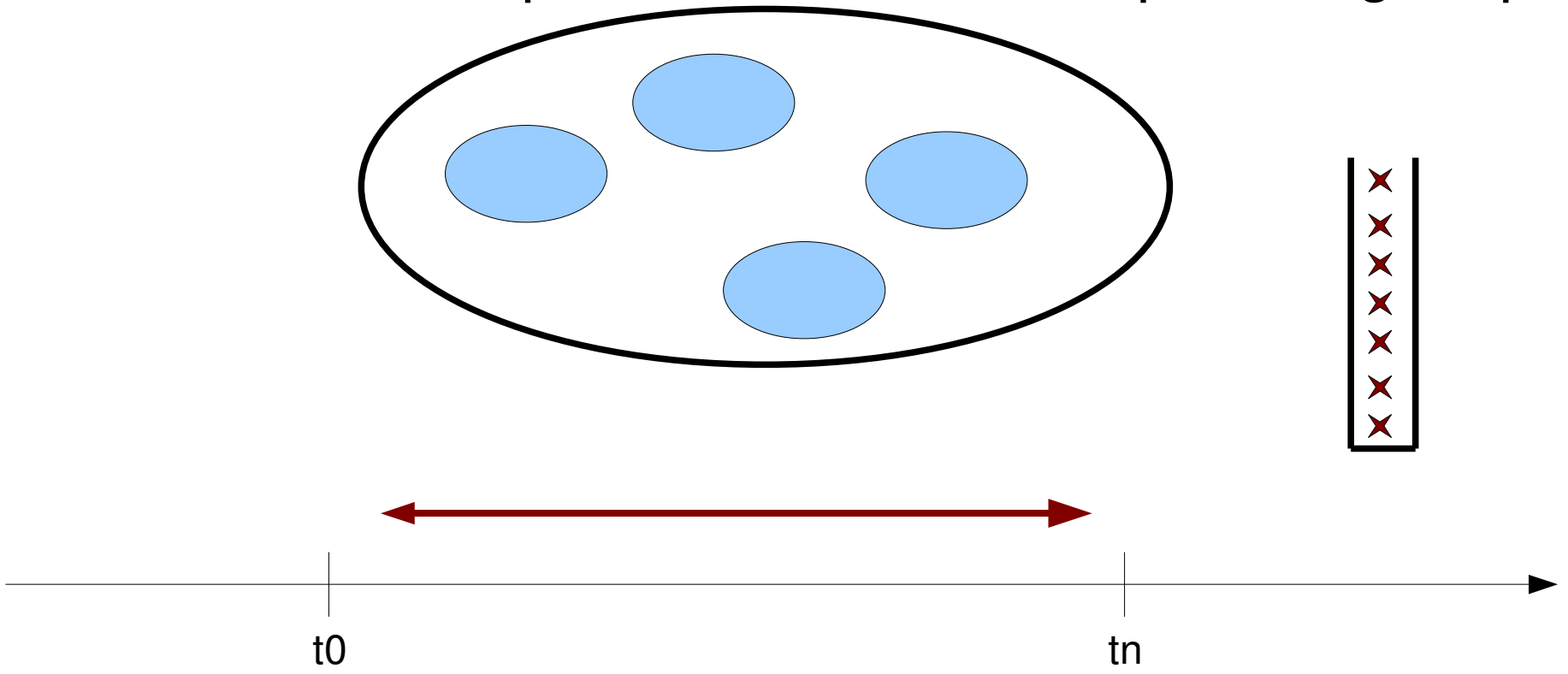
Détection adaptative d'anomalie

- Régime permanent : analyse d'un nouvel exemple
  - **Normal** : mise à jour du *cluster*
  - **Suspicieux** : exemple placé dans un réservoir



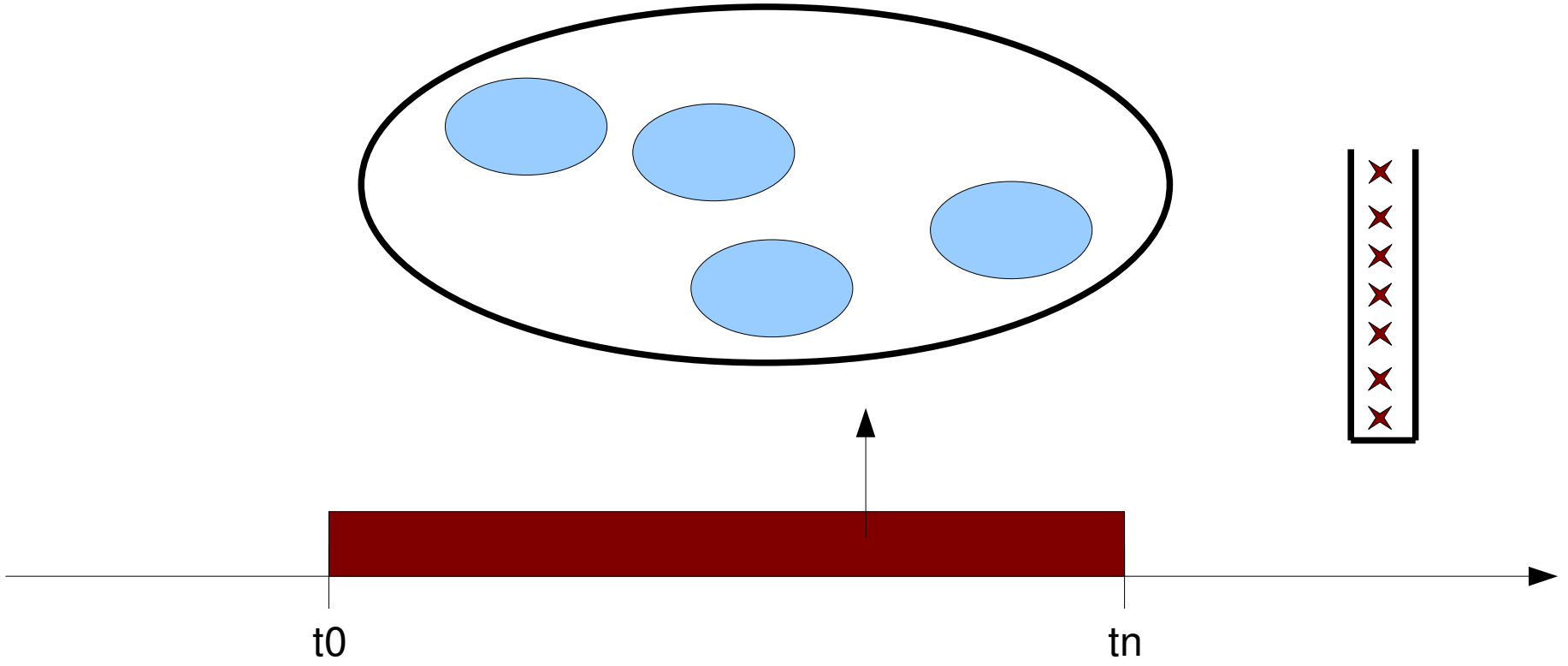
Détection adaptative d'anomalie

- Besoin de reconstruire tout le modèle
  - Si le réservoir est plein
  - Si le modèle n'a pas été reconstruit depuis longtemps



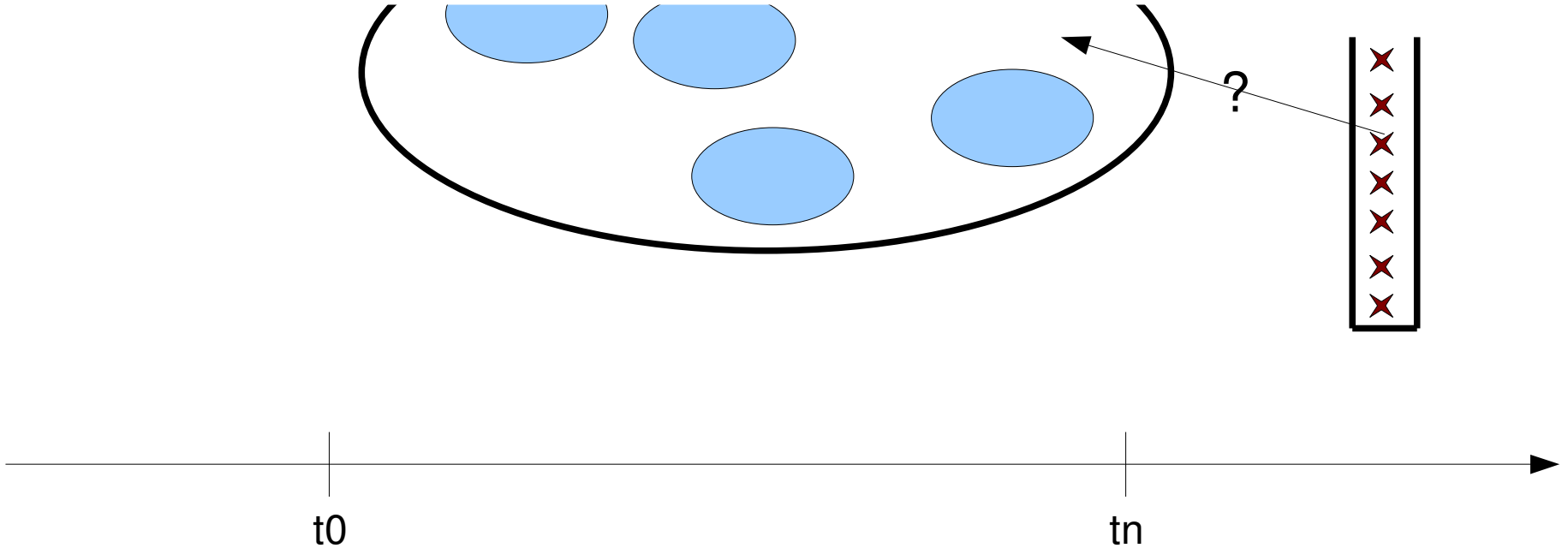
Détection adaptative d'anomalie

- Besoin de reconstruire tout le modèle
  - Si le réservoir est plein
  - Si le modèle n'a pas été reconstruit depuis longtemps



Détection adaptative d'anomalie

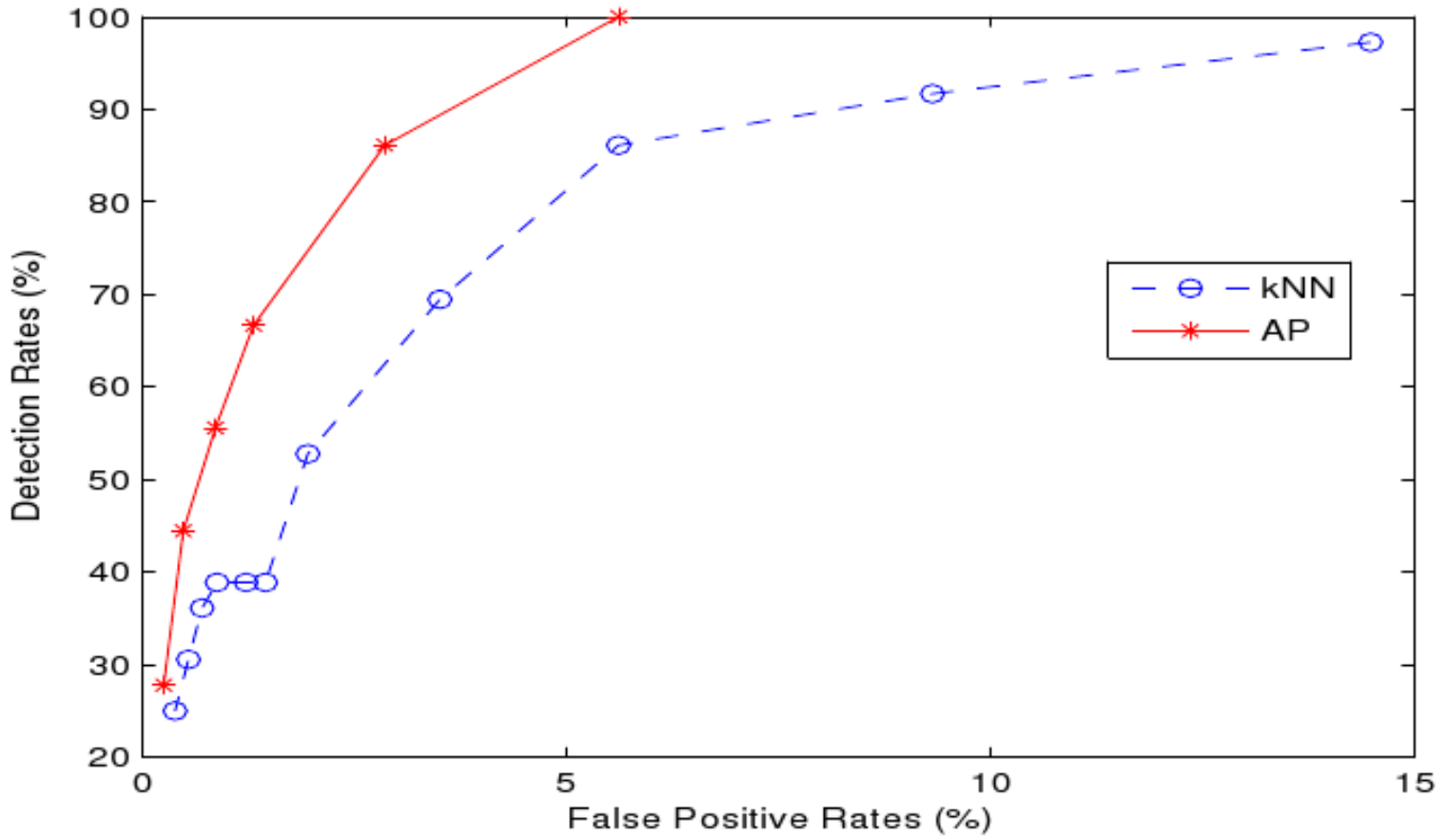
- Un exemple suspicieux est de nouveau analysé après la reconstruction
  - Si il est de nouveau outlier => c'est une **anomalie**
  - Si il n'est plus outlier => c'est une **requête normale**



Application à la détection d'intrusion

- Application à la détection d'intrusion à partir de log HTTP (Apache)
- Une requête HTTP est représentée comme un vecteur : distribution des caractères imprimables (dimension 95)
- Utilisation de deux algorithmes de clustering
  - k-NN
  - Affinity propagation

Résultats


100
90
80
70
60
50
40
30
20
0
5
10
15
Detection Rates (%)
False Positive Rates (%)
kNN
AP