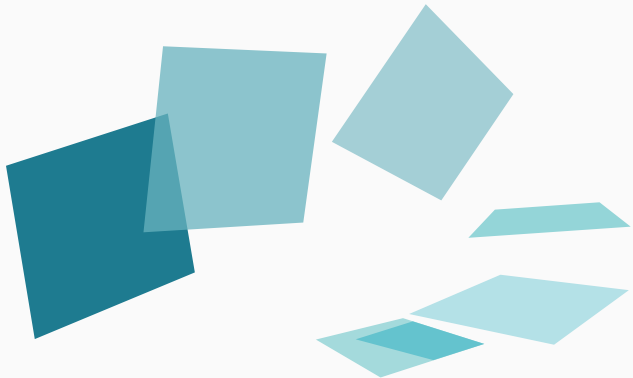
Analyse et inférence de propriétés dans les protocoles industriels

Stuxnet, Duqu, Flame vs Aramis

Emmanuel Perrier

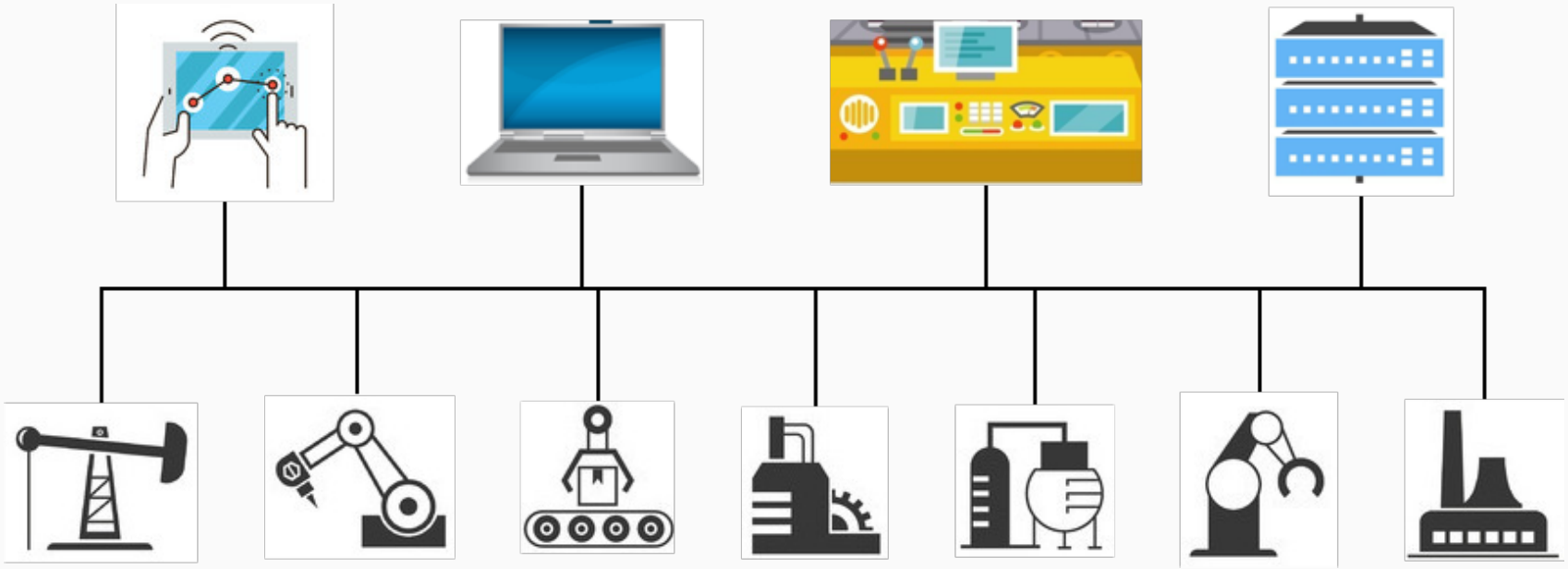
Laboratoire d'Informatique de Grenoble
Équipes Drakkar et Vasco



L I G

Afadl, 7 juin 2016

SCADA : Supervisory Control and Data Acquisition



Comment améliorer la sécurité ?

- Cartographier l'environnement, détecter une modification dans l'environnement
- Identification de paramétrage applicatif, mise en évidence de paramétrages erronés
- Détection d'attaques (DoS, malware, ...)
- Filtrage fin du trafic

Comment améliorer la sécurité ?

Faire coopérer deux approches :

- “Classification de flux applicatif et détection d’intrusion”, Maciej Korczyński, 2012

  $\hookrightarrow$ Classification du trafic
- “Détection de vulnérabilité au sein d’application web”, Karim Hossen, 2014

  $\hookrightarrow$ Inférence de modèle

Objectifs et buts de la classification du trafic

Buts :

- Filtrage du trafic
- Détection d'attaques
- Qualité de service

Moyens :

- Caractérisation du trafic (Web, VoIP, p2p, games, attack, ...)
- Caractérisation de l'application (Google, Skype, Dropbox, ...)
- Classification du protocole (HTTP, HTTPS, FTP, Skype, ...)

Difficultés :

- Trafic varié, inconnu
- Trafic chiffré
- Trafic complexe (port aléatoire, inhabituel, ...)

Approches pour la classification du trafic

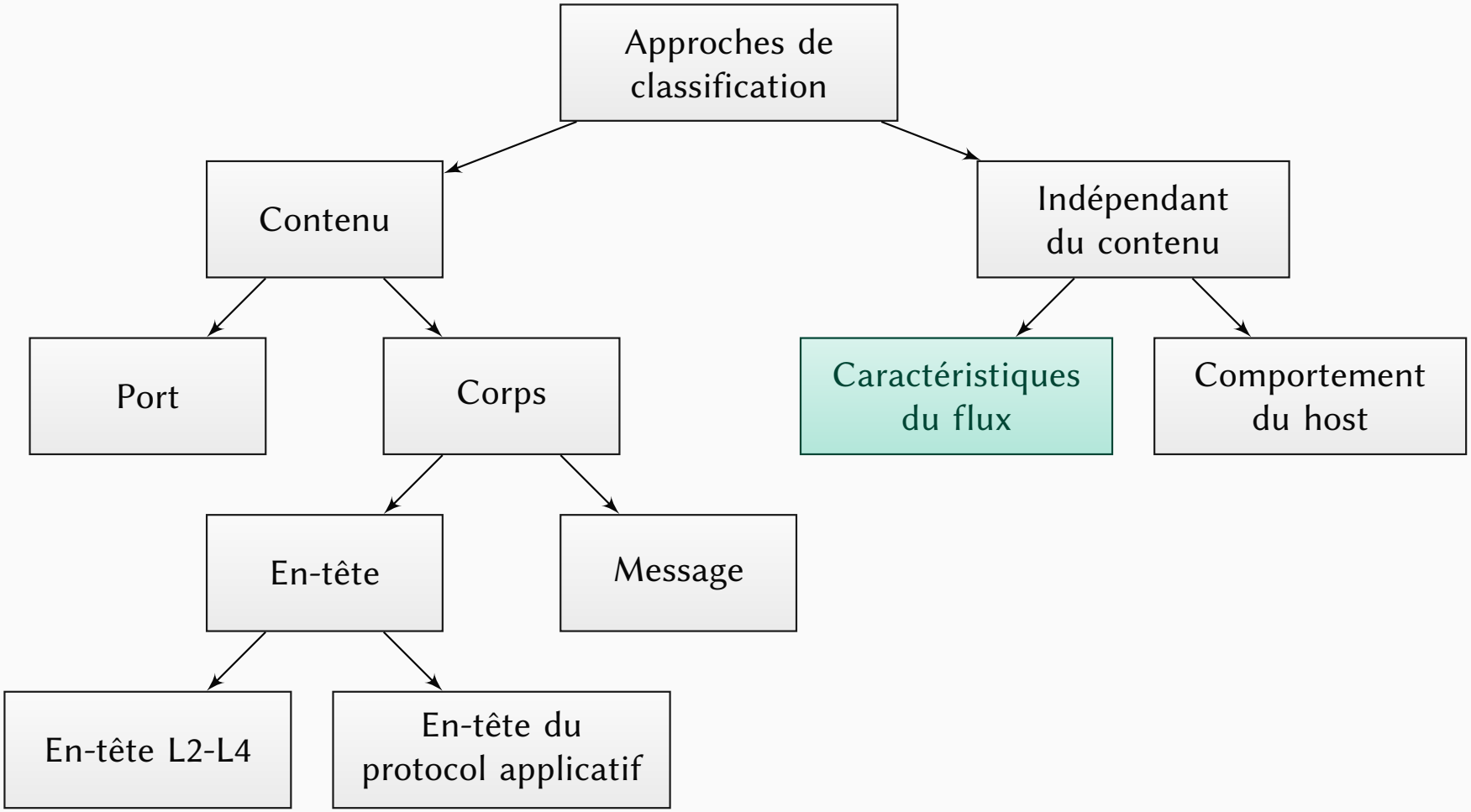


FIG. 1 : Approches pour la classification du trafic

Méthodes de classification de trafic

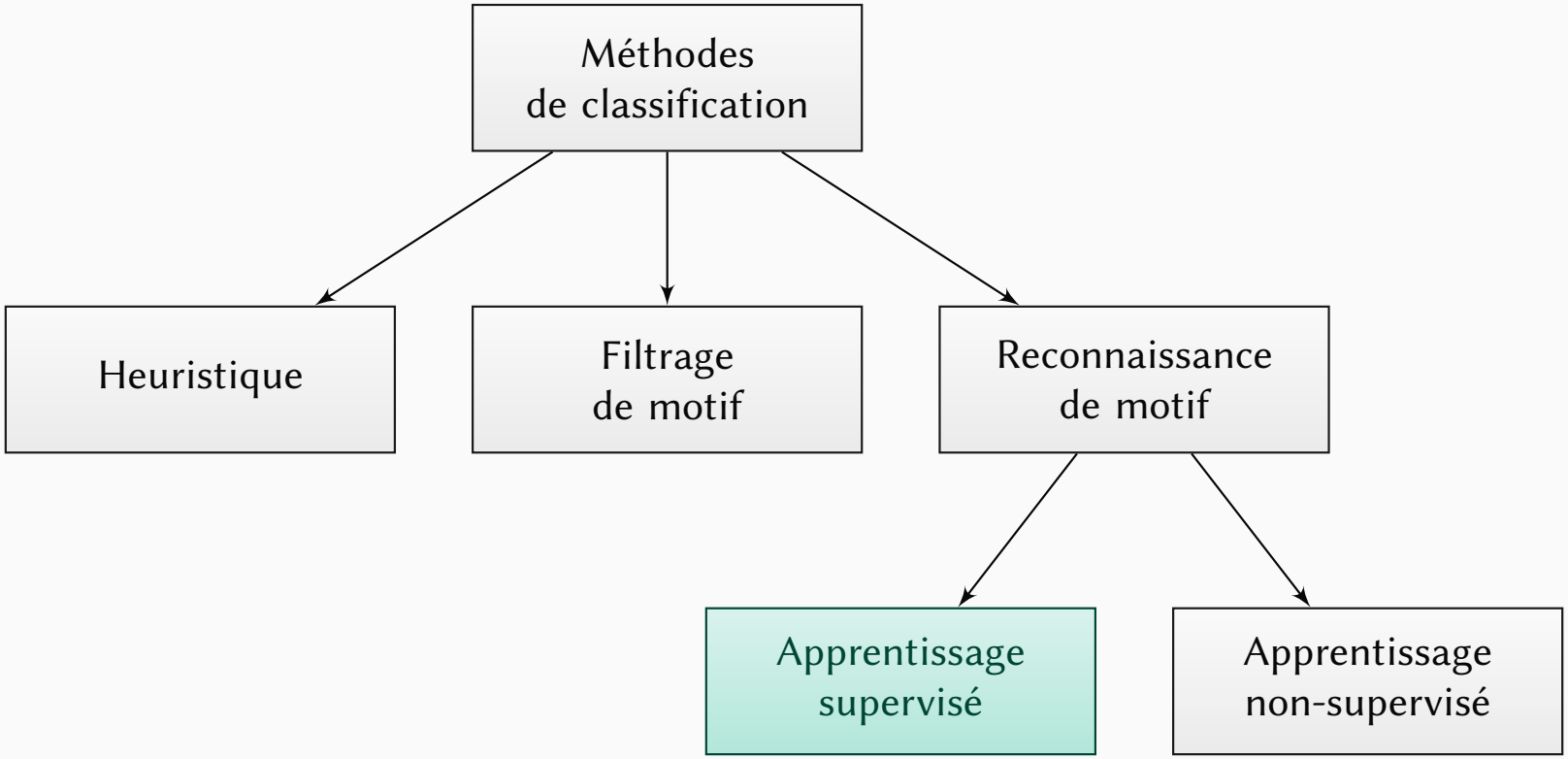


FIG. 2 : Méthodes de classification de trafic

Classification de trafic avec SPID

- Méthode d'apprentissage supervisé dans l'outil SPID (*Statistical Protocol IDentification*)

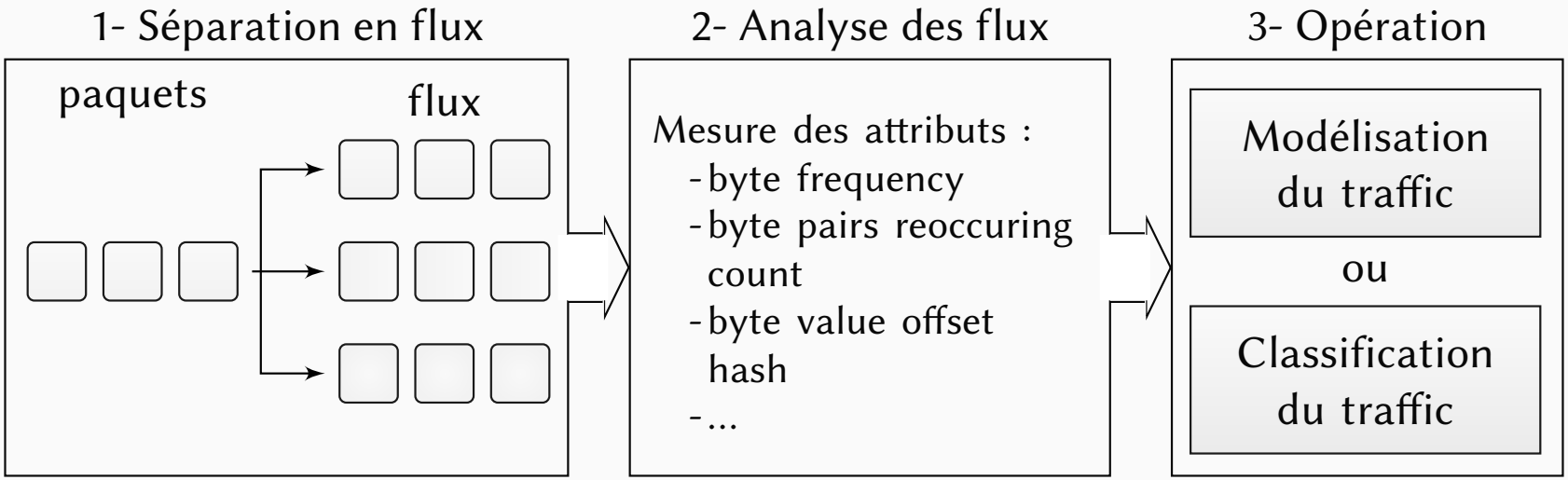


FIG. 3 : Principe de fonctionnement de SPID

- La classification du trafic résulte de la comparaison des deux distributions de probabilités obtenues lors de l'apprentissage et de la mesure en cours.

Définition et sélection des attributs

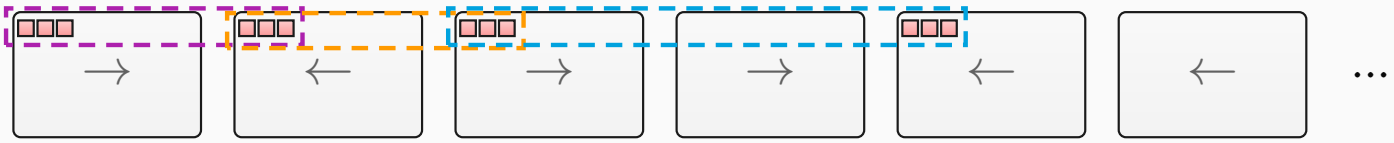
Il existe un ensemble d'attributs prédéfini qui sont efficaces pour les protocoles réseaux les plus répandus.

Exemples :

direction bytes meter : débit ascendant/descendant

action-reaction of first bytes : valeur des 3 premiers octets dans les deux premiers paquets de sens différent

byte value+offset : valeur combiné à la position des octets



- Sélection des attributs par une méthode d'introduction progressive.

Résultats pour la classification des flux Skype

Tab. 1 : Performance de la reconnaissance du trafic Skype

Trafic	Précision %	Rappel %
Skype	100	100
Autre	100	100

Tab. 2 : Performance de la classification détaillée du trafic Skype

Service Skype	Précision %	Rappel %
voix	72.9	57.4
vidéo	60.3	73.2
skypeOut	100	96.6
chat	90.2	97.4
upload	100	96.9
download	100	97.5

Objectif et buts de l'inférence de modèle

Buts :

- Identifier le système ou sa configuration
- Détecter des défauts, des déviations ou des vulnérabilités
- Produire des oracles et des filtres de comportements complexes

Moyen :

- Modélisation formelle du comportement observable d'un système concret

Difficultés :

- Identifier les variables et leurs paramètres possibles
- Domaine de valeur complexe/important
- Valeur aléatoire ou dépendante de l'environnement
- Inférence des relations entre les entrées et les sorties

Principe de l'inférence

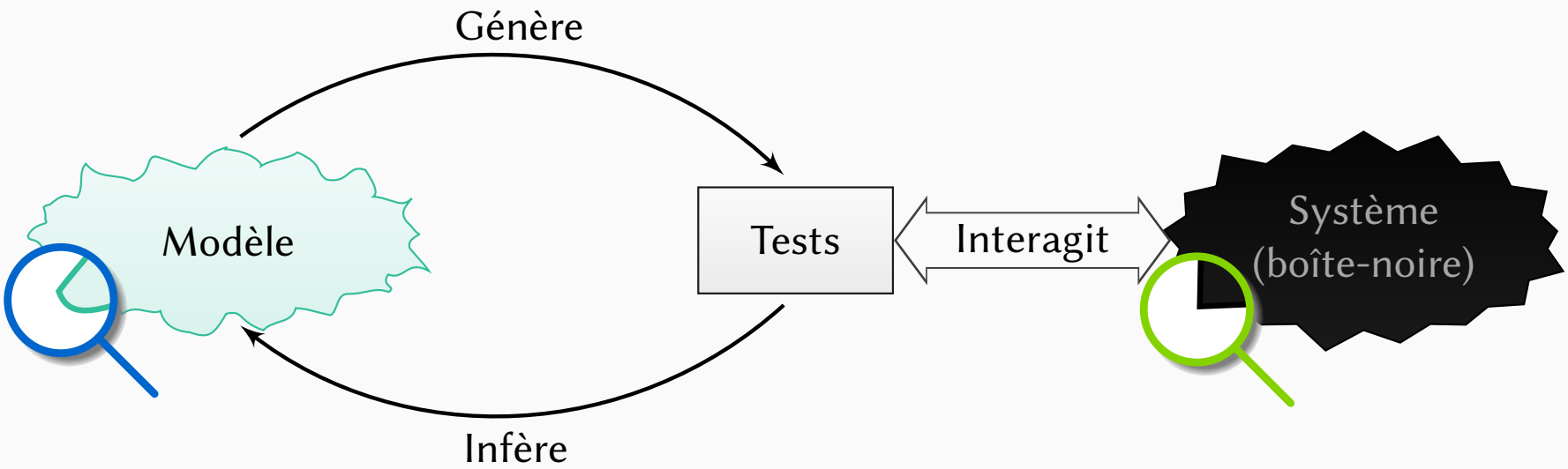


FIG. 4 : Principe de l'inférence

Démarche d'inférence

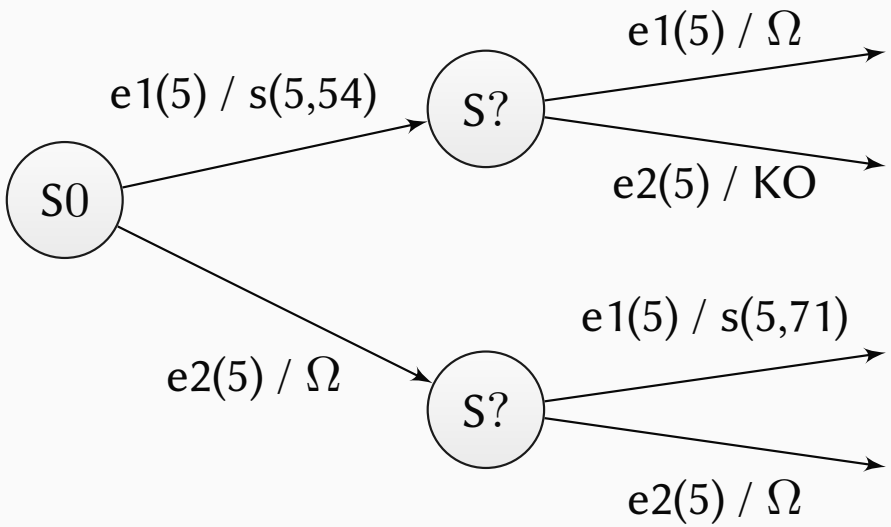


FIG. 5 : Exploration

Démarche d'inférence

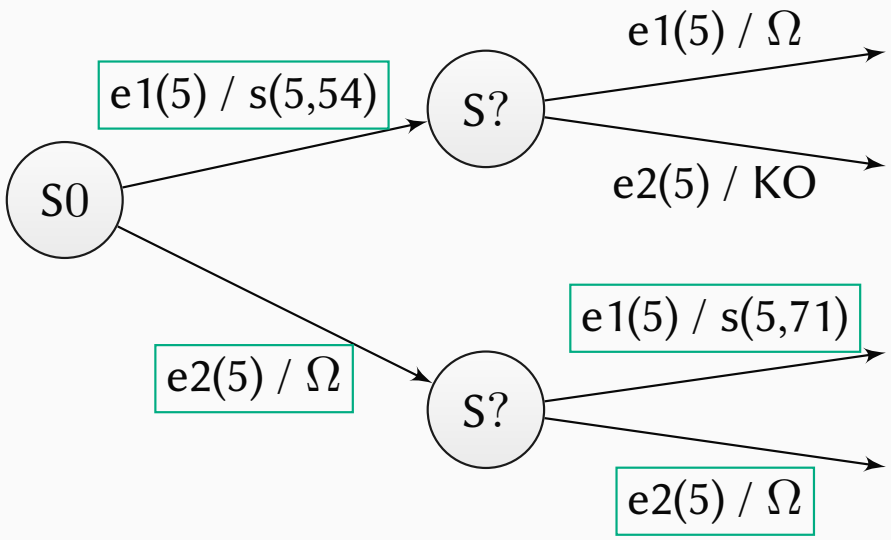


FIG. 5 : Exploration puis détection des états similaires

Démarche d'inférence

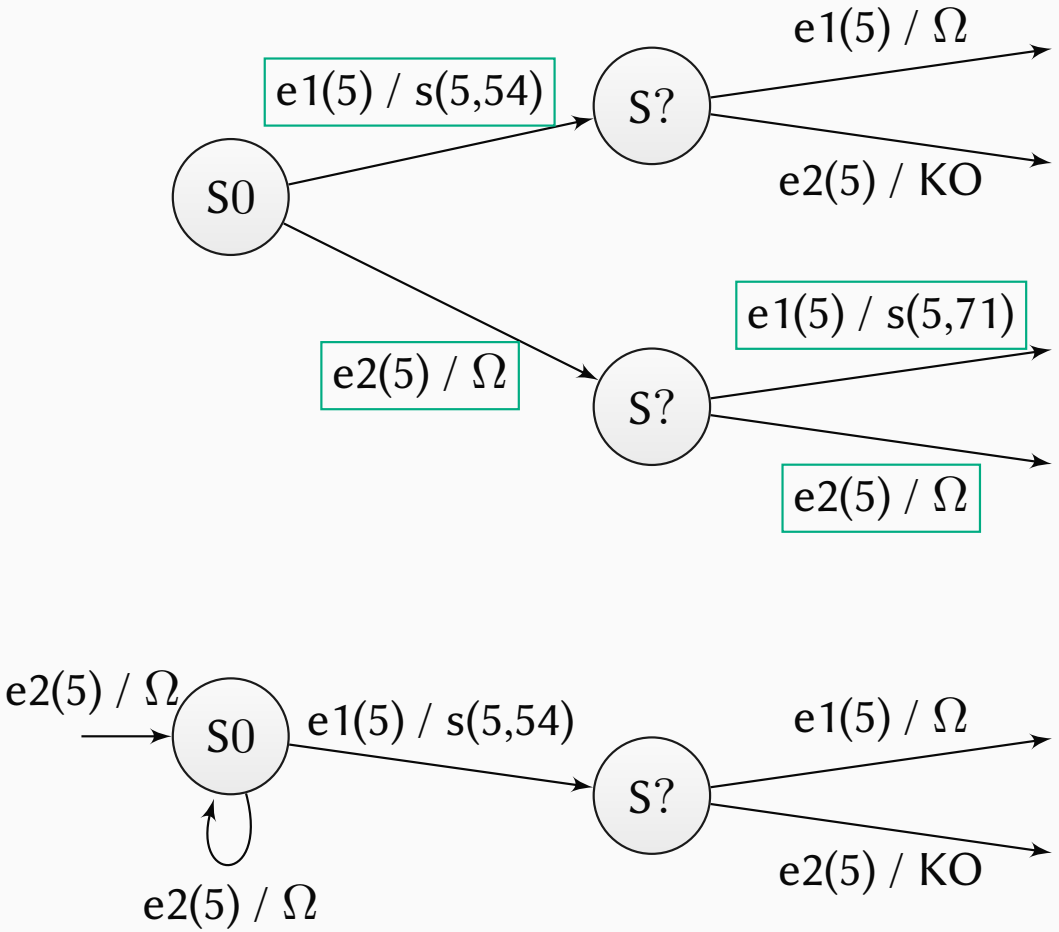


FIG. 5 : Exploration puis détection des états similaires

Résultats de la modélisation de serveur SIP

- Outil : *Simpa Infers Models Pretty Automatically* (SIMPA)
- En 26 requêtes ($\simeq$ 10 secondes)

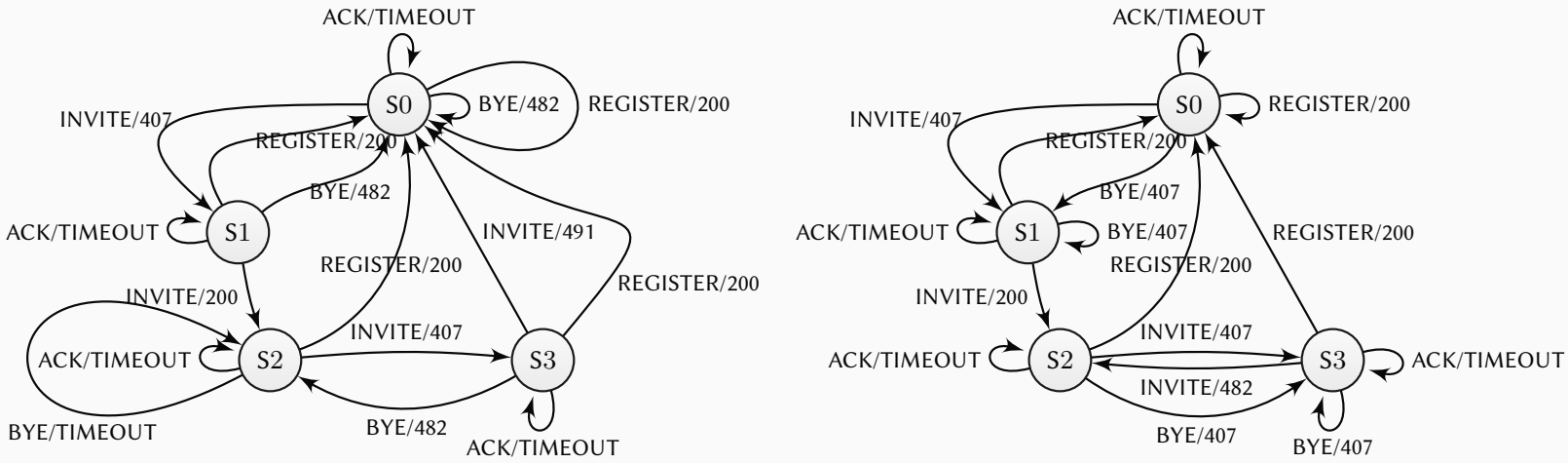


FIG. 6 : Modèles inférés sur sip2sip.net et iptel.org

Conclusion

Méthode de classification du trafic :

- permet une identification de trafic même chiffré
  - l'utilisation de plusieurs proxy ssl réduit l'intérêt
- la détection de l'activité d'un malware
- la différentiation des systèmes présents

Méthode d'inférence de modèle :

- fournit un modèle complet
- permet une analyse poussée du système et de son état
- nécessite une connaissance préalable : interface avec le système
- nécessite des interactions

$\Rightarrow$ Deux approches complémentaires.

Applications possibles

- assister la définition des règles de filtrage
- filtrage plus fin du trafic réseau
- mise en évidence de comportement déviant
- identification et vérification des systèmes OPC-UA
- la vérification des règles d'autorisation

Questions ?