

# CoChaT

## Canaux cachés dans les systèmes temporisés

### RÉSUMÉ

Les canaux cachés représentent une fuite d'information involontaire à partir d'un système. Ils constituent une faille de sécurité importante présente dans de nombreux systèmes. En effet, il est actuellement très difficile de détecter de tels canaux, et encore plus de les contrôler. De plus, certaines attaques tiennent compte non seulement des actions du système mais aussi des délais. La dimension temporisée du canal rend sa détection d'autant plus difficile.

Différentes structures peuvent être utilisées afin de modéliser les canaux cachés, des automates temporisés aux transducteurs. Cependant la majorité de ces modèles ont des limites théoriques de décidabilité qu'il faudra affiner.

### 1 Que sont les canaux cachés ?

Les canaux cachés sont un moyen, pour un utilisateur malveillant, d'utiliser de manière détournée un système ou un protocole de communication afin de transmettre de l'information en dehors du cadre prévu par celui-ci.

Dans le cas classique, ils reposent sur l'observation par un utilisateur de **bas niveau** des conséquences d'actions d'un utilisateur de **haut niveau**. Ces observations permettent à ces deux utilisateurs de faire transiter un message par le système, en utilisant ce dernier en dehors de son application première. L'exemple le plus marquant d'un tel canal est l'utilisation des **entêtes** de paquets TCP/IP pour faire passer des informations.

Dans le cas **temporisé**, l'utilisateur de bas niveau observe non seulement les conséquences d'actions de haut niveau, mais aussi les **délais** entre les actions, le cas extrême étant l'observation uniquement de délais du système. Toujours dans le cadre du protocole TCP/IP, on peut utiliser les temps d'arrivée des paquets pour faire transiter un message.

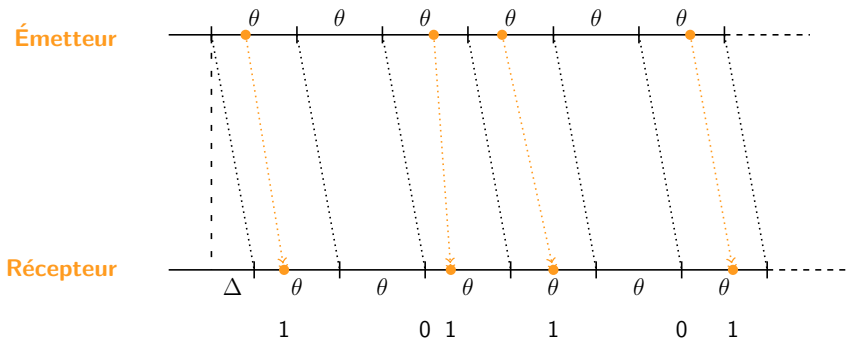
### 2 Canal caché temporisé dans TCP/IP

#### Principe général

- Nécessite un protocole préalable entre **Émetteur** et **Récepteur** afin de découper le temps en intervalles.
- Un paquet émis durant cet intervalle se décode en 1. Si rien n'est émis durant cet intervalle, un 0 est décodé.

#### Mise en œuvre

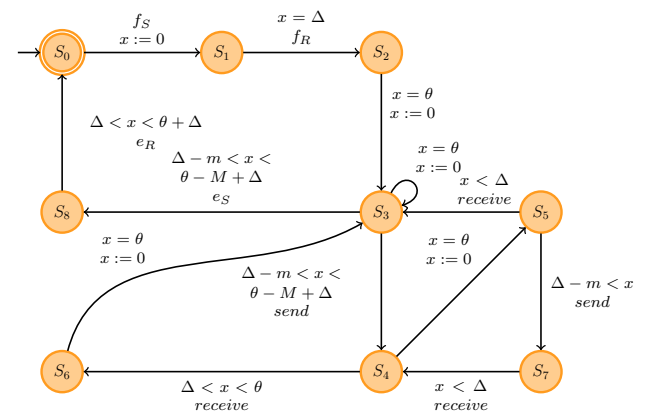
- Les intervalles de l'**Émetteur** et du **Récepteur** ont la même durée  $\theta$  et sont décalés de  $\Delta$ .
- Les intervalles doivent être assez grands pour compenser l'irrégularité du réseau.
- Expérimentalement: transmission à 16,6 octets/s.



### 3 Modélisation des canaux par automates temporisés

Sous certaines hypothèses sur le retard  $\Delta$ , la largeur d'intervalle  $\theta$ , et la vitesse de transmission des paquets (entre  $m$  et  $M$ ), le protocole réalisant un canal caché sur TCP/IP peut être mis sous la forme d'un automate temporisé.

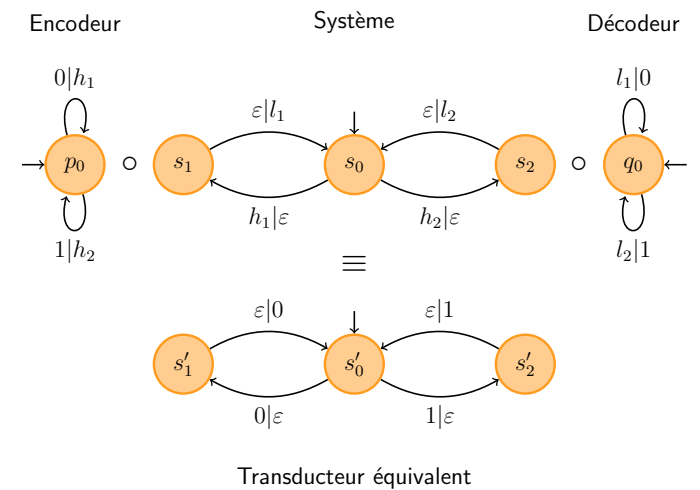
Automate temporisé modélisant le canal caché sur TCP/IP



### 4 Modélisation non temporisée par transducteurs

Un système, vu comme un transducteur, présente un canal caché si un encodeur et un décodeur permettent de faire passer n'importe quel mot binaire.

Cas d'école d'un canal caché



### 5 Travaux prévus

- Introduction du temps dans la modélisation par transducteurs
- Modélisation de canaux cachés via des logiques temporelles et temporisées (par exemple TCTL et TATL)
- Contrôle de canaux cachés
- Quantification de la fuite d'information
- Étude de cas réels