

# PROJET COPS

Troisième réunion le 29 et 30 Mars 2007

A propos de la notion de confiance

Fahima Cheikh

Lilac

IRIT

# Plan

- Introduction
- Domaines de recherche
- Sécurité informatique
- Intelligence artificielle
- Notre approche

# Introduction

- Comment définir la confiance?
- Comment représenter la confiance?
- Comment mettre à jour la confiance?

# Domaines de recherche

Sécurité informatique

- Trust-negotiation
- Gestion d'obligations

Intelligence artificielle

- Logique
- Modèle probabiliste

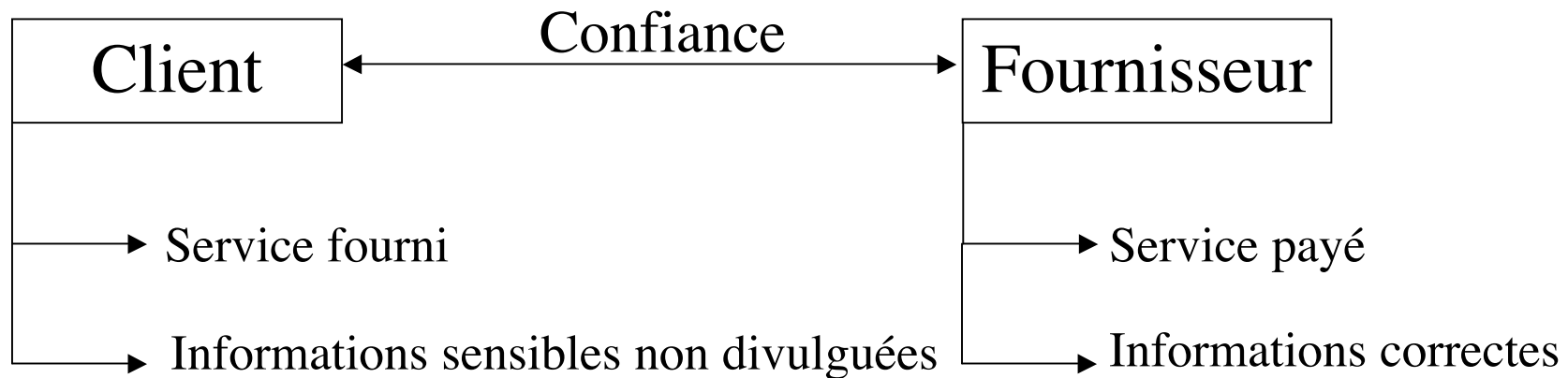
# Sécurité informatique

# Trust-negotiation

- Hypothèse: les agents ne sont pas étrangers les uns aux autres.
- Hypothèse  $\longrightarrow$  Approches basées sur l'identité
- Dans les systèmes ouverts cette hypothèse n'est pas vérifiée

# Trust-negotiation

- Dans une transaction commerciale:



- Echange des certificats  
( $C = \langle \text{Issuer}, \text{Owner}, \text{Type}, \text{Attr}, \rangle$ )

# Trust-negotiation[9]

- Exemple

## Client

Certificats

*C1*: identifiant PayPal

*C2*: carte de crédit permanente

Politiques de la négociation

*C1*: exige *S1*

*C2*: exige *S2*

## Fournisseur

Certificats

*S1*: PayPal fournisseur

*S2*: évaluation du fournisseur=bon

Politiques de la négociation

		Niveau de suspicion		
		Bas	Moyen	Haut
<i>S1</i>	libre	libre	libre	
<i>S2</i>	libre	libre	exige <i>C2</i>	

# Trust-negotiation

Certificats exigés		Montant de l'achat	
		<100	≥100
Niveau de Suspicion (NS)	Faible <0.33	C1   C2	C2
	Moyen ≥ 0.33 < 0.66	C1   C2	C2
	Haut ≥ 0.66 < 1.0	C2	C1&C2

$NS = \langle S_{ds}, S_l, S_o \rangle$  où  $S_{ds}, S_l$  et  $S_o$  ont des valeurs entre 0 et 1

# Trust-negotiation

- *CREDENTIAL\_LIMIT\_EXCEEDED*
  - Le client envoie un nombre anormal de certificats (augmente  $S_{ds}$ )
- *POLICY\_LIMIT\_EXCEEDED*
  - Le client demande un nombre anormal de certificats (augmenter  $S_l$ )
- *CERTIFICATE\_INTEGRITY\_ERROR*
  - Signature non valide du certificat, certificat endommagé, ...  
(augmentation du  $S_o$  de 0.1)

# Gestion d'obligations[2]

R= access(customer,loan, approve) ←  
in(customer,buyer),  
reliable(customer,score,time),(score $\geq$ 7.2),  
computePay(customer,loan,monthlyPayement),  
monthlyIncome(customer,income), (income  
 $\geq$ 3 $\times$ monthlyPayement)

# Gestion d'obligations

## OBL Definition:

payByDate(customer, loan, time, payment,  
penalty, upscore, downScore)

**FUL:** [Action List: {send(acknowledgeReceipt,  
customer, time, loan, payement),  
send(adjustReliability, system, time, customer,  
upScore)}]

# Gestion d'obligation

**DEF:**[OBL: payByExtendedDate(customer, time',  
payment+penalty)]

[Action List:

{send(reminder,customer,time,loan,payment+penalt  
y)}

send(adjustReliability,system,time,customer,-  
downScore)]

# Intelligence artificielle

# Logique[3]

- Logique dynamique de confiance et d'engagement

- Formules

$$\varphi ::= p \mid \neg \varphi \mid \varphi \wedge \psi \mid \langle \alpha \rangle \varphi \mid C_{i,j}(\alpha \geq \beta) \mid T_{i,j}(\alpha \geq \beta)$$

$\langle \alpha \rangle \varphi$ : «  $\alpha$  est **exécutable** et après son exécution il est le cas que  $\varphi$  »

$C_{i,j}(\alpha \geq \beta)$ : « l'agent  $i$  est plus **engagé** envers l'agent  $j$  à faire  $\alpha$  qu'à faire  $\beta$  »

$T_{i,j}(\alpha \geq \beta)$ : « l'agent  $i$  a plus **confiance** en l'agent  $j$  à la suite de l'exécution de  $\alpha$  qu'à celle de  $\beta$  »

# Logique

- Actions

$$\alpha ::= a \mid \neg\alpha \mid \alpha \cup \beta \mid \alpha \cap \beta \mid \alpha; \beta \mid \alpha^*$$

$\neg\alpha$ : opérateur pour la négation d'action  
(obligation)

$\alpha \cap \beta$ : opérateur de synchronisation des agents  
(communication)

# Logique

- Exemple
  - Agents  $G = \{1, 2\}$
  - Actions atomiques  $A = \{a_i(1), a_i(2) \mid i \in G\}$
  - $a_i(n)$ : l'agent  $i$  prend  $n$  pièces de monnaie

$$[a_1(1)]C_{2,1}(a_2(1) > a_2(2))$$

$$C_{i,j}(\alpha > \beta) \rightarrow T_{j,i}(\alpha > \beta)$$

$$C_{i,j}(a_i(1) \geq a_i(2)) \rightarrow T_{j,i}(a_i(1) > a_i(2))$$

# Modèle probabiliste[1]

- Des agents interagissent entre eux et se donnent des notes entre 0 et 10.
- 0 signifie des actions mauvaises, mal faites, ...
- 10 signifie des actions bonnes, bien faites, ...
- Chaque agent  $x$  possède un degré d'optimisme noté  $O_x$  et d'un degré de confiance en soi noté  $C_x$  qui vont de 0 (pas de confiance) à 10 (confiance total).

# Modèle probabiliste

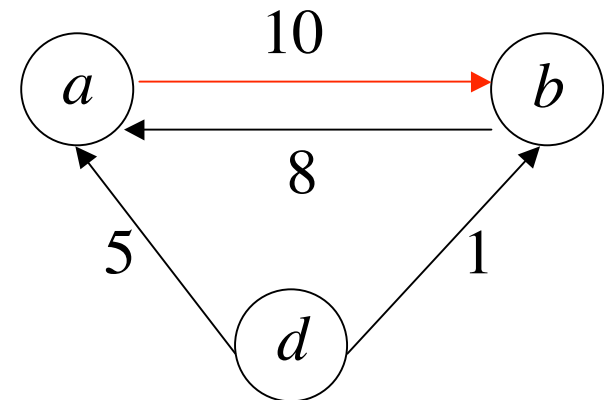
Calcul de  $c(d,a)$ , la confiance de  $d$  en  $a$ :

- Les agents qui notent  $a$  sont  $b$  et  $d$ .
- L'importance de  $d$  est  $C_d$ , la confiance en soi de  $d$ .
- L'importance de la note de  $b$  est la confiance de  $d$  en  $b$ , quant les notes de  $a$  sont retirées, notée  $c(d, b, \{a\})$ .

$$c(d,a) = \frac{2 \times O_d + 5 \times C_d + 8 \times c(d,b,\{a\})}{2 + C_d + c(d,b,\{a\})}$$

A.N: si  $C_d=5$  et  $O_d=5$

$$c(d,a) = 5,70$$



Graphe d'interactions

# Tableau récapitulatif

Confiance	Sécurité informatique	
	Trust-negotiation	Gestion d'obligation
Interprétation	- Compétence, qualification[10,11] - Niveau de suspicion [9]	- Satisfaction des engagement[2]
Calcul	- Qualitatif[10,11] - Taille d'un chemin[6] - Probabilité[9]	- Score
Mise à jour	- Type d'erreur[9]	- Obligation satisfaite + - Obligation non satisfaite -

# Tableau récapitulatif

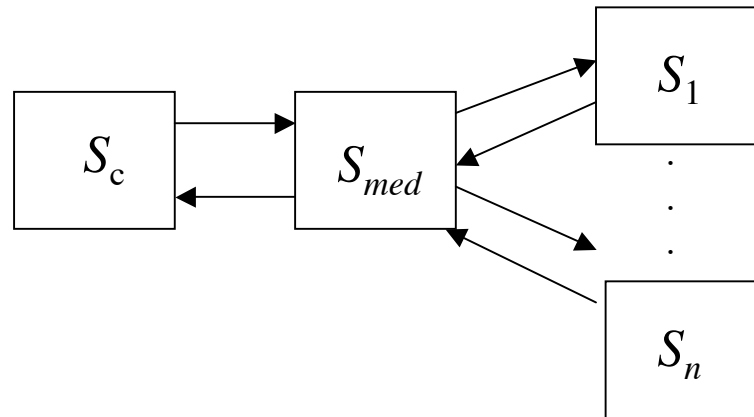
	Intelligence artificielle	
Confiance	Logique	Modèle probabiliste
Interprétation	<ul style="list-style-type: none"> <li>- Tenir ses engagements[3]</li> <li>- Performance[4]</li> <li>- Qualification (réponse correcte)[5]</li> </ul>	<ul style="list-style-type: none"> <li>- Assurance, réputation [1,7,8]</li> </ul>
Calcul	<ul style="list-style-type: none"> <li>-Qualitatif[3,5]</li> <li>- Quantitatif <math>\in [0,1]</math>, [4]</li> </ul>	<ul style="list-style-type: none"> <li>- Moyenne entre confiance directe (propre interaction) et confiance indirecte</li> </ul>
Mise à jour	<ul style="list-style-type: none"> <li>- Niveau d'engagement[3]</li> </ul>	<ul style="list-style-type: none"> <li>- Refaire le calcul</li> </ul>

# Notre approche

# Problème de la composition de service

- Entrée: un ensemble fini  $C = \{S_1, \dots, S_n\}$  de services, un service client  $S_c$  et un service but  $S_{but}$ .
- Sortie: existe-il un service médiateur  $S_{med}$  tel que le comportement de  $\{S_c, S_{but}\}$  est équivalent à celui de  $\{S_c, S_{med}\} \cup C$

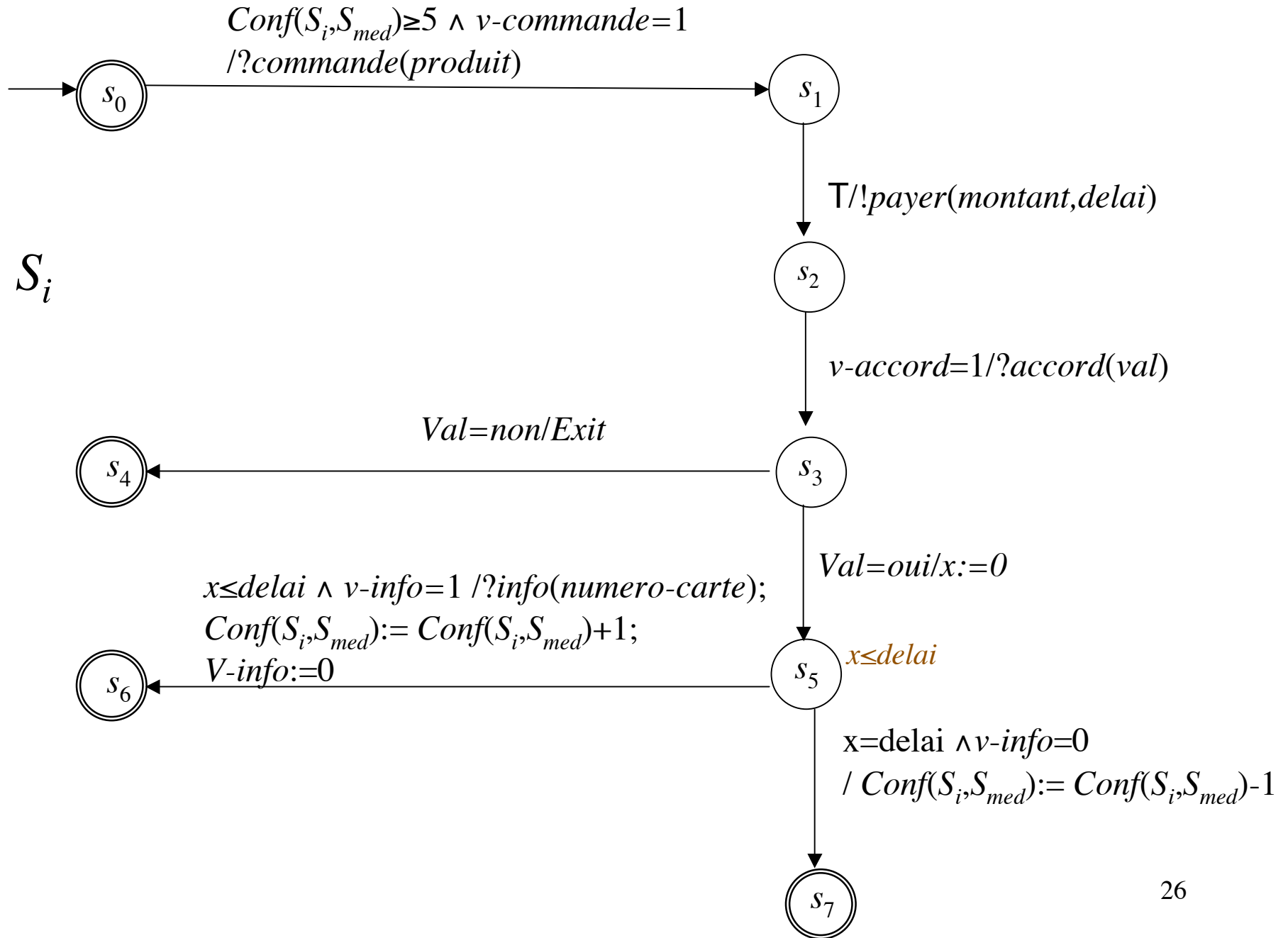
# Représentation de la confiance



<i>Conf</i>	$S_c$	$S_{med}$	$S_1$	$\dots$	$S_n$
$S_c$	indef	5	indef	indef	indef
$S_{med}$	6	8	2	$\dots$	9
$S_1$	indef	7	indef	indef	indef
$\dots$	indef	$\dots$	Indef	Indef	indef
$S_n$	indef	9	Indef	Indef	indef

# Mise à jour de la confiance

- Initialement la confiance entre les services a la valeur 5.
- Un service souhaite recevoir un message dans un certain **délai**.
- Si le message est reçu dans le délai alors la confiance augmente sinon elle diminue.



# Références

- [1] J. Ben-Naim. Autour de la fiabilité d'une information dans un réseaux scientifiques.
- [2] C. Bettini, S. Jajodia, X.Wang et D.Wijesekera. Obligation monitoring in policy management.
- [3] J. Broersen, M. Dastani, Z. Huang et L. Torre. Trust and commitment in dynamic logic.
- [4] C. Castelfranchi et R. Falcone. Principles of Trust for MAS: Cognitive anatomy, Social importance, and quantification.
- [5] M. Dastani, A. Herzig, Joris Hulstijn, et L. Torre. Inferring Trust.
- [6] M.Mecella, M. Ouzzani, F. Paci et E.Bertino. Access control enforcement for conversation-based Web servoces.
  
- [7] S. Ramchurn, N. Jennings, C. Sierra et L. Godo. A Computational trust model for multi-agent interactions based on confidence and reputation.
- [8] M. Rehak, L. Foltyn, M. Pechoucek et P. Benda. Trust model for open ubiquitous agent systems.
- [9] T. Rytov, L. Zhou, C. Neuman, T. Leithead et K. Seamons. Adaptative trust negotiation and access control.
- [10] H. Skogsrud, B. Benatallah et F. Casati. Trust-Serv: Model-Driven lifecycle management of trust negotiation policies for Web services.
- [11] W. Winsborough, K. Seamons et V. Jones. Automated trust-negotiation.