Vérification automatique d'exigences pour les politiques d'échange d'information

Exigences de Diffusion et de Non-diffusion d'information

Rémi Delmas, Thomas Polacsek

ONERA, Département Traitement de l'Information et Modélisation
2, avenue Edouard Belin BP74025, 31055 TOULOUSE Cedex 4
{remi.delmas,thomas.polacsek}@onera.fr

RÉSUMÉ. *Que cela soit pour la surveillance de la Terre ou même la gestion des relations inter-entreprises, il existe de plus de plus d'organisations interconnectées formant des systèmes d'information décentralisés avec des échanges d'information. Dans de tels cas, nous avons l'exigence que si une information cruciale vient à être connue par l'un des agents, alors les agents concernés par cette information doivent absolument être avertis. Parallèlement, il peut être nécessaire de prévenir tout risque de diffusion d'information n'ayant pas vocation à être divulguée. Dans cet article, nous nous focaliserons plus précisément sur deux types d'exigences antagonistes qui sont, d'une part, la nécessité de partager de l'information et, d'autre part, l'obligation de ne pas diffuser certaines informations. Fort d'une expression formelle de ces deux exigences, nous verrons comment il est possible de les concilier dans une unique politique à l'aide d'une opération de filtrage d'information dont la spécification apparaît naturellement. De plus, nous expliquerons comment des solveurs SMT peuvent être utilisés pour analyser automatiquement des propriétés des politiques.*

ABSTRACT. *Whether be it for Earth observation, risk management or even companies relations, more and more interconnected organizations form decentralized systems in which the exchange, in terms of diffusion or non-diffusion of information between agents, can have critical dimension. In this paper, we present a formal framework to specify information exchange policies for such kinds of systems and two specific requirements, the need-to-share and the non-diffusion requirements, as well as properties strongly related to them. Wiser from these formal definitions, we see how to reconcile these sometimes two antagonist requirements in a same policy specification with information filtering operations. We also explain how we use state of the art theorem provers to perform automatic analysis of these policies.*

MOTS-CLÉS : *analyses de politique d'échange, exigences des SI, méthodes formelles, vérification, solveurs SMT.*

KEYWORDS: *exchange policy analysis, IS requirements, formal methods, verification, SMT solvers.*

1. Introduction

Aujourd'hui, de par l'omniprésence des relations numériques, nous avons une interconnexion sans précédent entre les personnes, les entreprises et les organisations. Ces ensembles d'acteurs interconnectés forment des systèmes décentralisés où de l'information est échangée. Prenons pour exemple les systèmes de surveillance des débris spatiaux, Space Situation Awareness (SSA). Dans de tels systèmes, les capacités d'observation spatiales, appartenant à différentes nations et opérateurs privés ou publics, sont mutualisées afin de construire une information complexe et, s'il y a un risque de collision pour un satellite, diffuser une alerte aux agents concernés. La mission d'un tel système est donc de prévenir les opérateurs de satellites lorsqu'une collision potentielle entre des objets en orbite est détectée. Plus précisément, le système doit, en cas de risque de collision, envoyer des informations aux bons agents afin de leur permettre d'éviter la collision, tout en garantissant qu'aucune information sensible sur les objets en orbite, comme leur nature exacte, leurs trajectoires, leurs capacités de manœuvre, *etc.* ne soit divulguée.

Un autre cas de systèmes décentralisés où des agents s'échangent de l'information est celui des systèmes de surveillance faisant partie du système d'observation globale de la Terre (GEOSS[1]). Concernant la prévention des catastrophes naturelles, nous avons un ensemble de partenaires qui partagent des informations dans le but de générer des alertes en cas de risque de catastrophe naturelle. L'exigence ici est que les autorités qualifiées *doivent absolument être averties* dès que des données annonçant une catastrophe sont connues afin que des mesures de protection et de gestion de crise soient prises. Mais cette exigence est contrebalancée, par exemple, par la nécessité de prévenir tout risque de diffusion d'informations confidentielles sur les moyens d'observation de la terre des membres participant à l'effort de surveillance.

Nous avons donc des systèmes dans lesquels l'exigence principale est que, dans certains cas, un agent *doit être absolument averti*. En fait la véritable exigence est un *besoin de connaître* des agents, qui doivent connaître certaines informations pour pouvoir accomplir leurs missions. Cependant, comme nous nous intéressons aux échanges d'information, nous pouvons reformuler cette exigence en exigence de *diffusion* qui signifie que puisqu'un agent a besoin d'une information, quand celle-ci est connue par un autre agent du système, elle doit absolument lui être communiquée. Parallèlement, parce que différentes organisations interviennent dans ces systèmes, il faut prévenir la diffusion d'informations privées ou sensibles entre organisations. Les exigences à concilier dans ces systèmes sont donc antagonistes : d'une part, veiller à ce que des acteurs reçoivent toujours toutes les informations dont ils ont besoin pour accomplir leurs missions respectives ; d'autre part, garantir qu'aucune information sensible ne sera diffusée de manière incontrôlée, ce que nous nommons exigence de *non-diffusion*.

Pour cela, il est nécessaire de spécifier clairement et sans ambiguïté les exigences de diffusion et de non-diffusion, c'est-à-dire les conditions sous lesquelles un

1. Global Earth Observation System of Systems

agent a l'obligation, l'autorisation ou l'interdiction de communiquer des informations aux autres agents du système. Nous appelons une telle spécification une *politique d'échange*. Un des avantages de disposer d'une politique d'échange exprimée formellement est de pouvoir réaliser des vérifications automatiques, via des outils d'aide à la spécification/vérification, utilisables dès les premières étapes du processus de conception.

Dans cet article, la section 2 présente un rappel du language PEPS[2] précédemment défini dans (Cholvy *et al.*, 2012) (Delmas et Polacsek, 2013) (Delmas et Polacsek, 2014) et qui permet de spécifier formellement une politique d'échange d'information, ainsi que l'outil PEPS-analyzer associé au langage. Dans la section 3, nous donnons un exemple de politique d'échange qui nous permettra d'illustrer l'ensemble des concepts étudiés dans ce papier. Les sections 4 et 5 sont dédiées respectivement aux exigences de diffusion et de non-diffusion. Malgré l'antagonisme de ces deux types d'exigences, nous verrons dans la section 6 comment un opérateur de filtrage d'information permet de les concilier dans une même politique sans incohérence. Enfin, la section 7 conclut le papier et donne quelques perspectives à ces travaux.

2. Spécification de politiques d'échange

2.1. PEPS

PEPS est un cadre formel outillé pour la spécification et la vérification de politiques de diffusion d'information. Techniquement PEPS est bâti sur la logique du premier ordre multi-sortée[3] avec égalité (MSFOL) (Gallier, 1987). Il permet l'utilisation de sortes, de constantes, de fonctions, de prédicats, de variables sortées $x : \mathcal{S}$, de quantificateurs universels ($\forall$) et existentiels ($\exists$), et enfin de l'égalité ($=$) et des connecteurs logiques usuels ($\neg$, $\wedge$, $\vee$, $\Longrightarrow$).

Le langage PEPS est extensible, l'utilisateur peut déclarer ses propres sortes, fonctions et prédicats. Toutefois, il est nativement pourvu de sortes, fonctions et prédicats prédéfinis couvrant les concepts de base des politiques. Ainsi, les sortes $\mathcal{A}$, $\mathcal{I}$ et $\mathcal{T}$ représentent respectivement les agents, les informations et les sujets sur lesquels les informations portent ; le prédicat $K(a, i)$ signifie que l'agent a connaît l'information i et le prédicat $Topic(i, t)$ signifie que l'information i se rapporte au sujet t (appelés *D-prédicats* pour prédicats de domaine).

Contrairement à la logique déontique standard, notre langage ne dispose pas d'un opérateur d'obligation générique (Castanẽda, 1975). En effet, nous nous concentrons uniquement sur la notion d'*obligation d'envoyer une information d'un agent vers un autre* et pas sur la notion d'obligation en général. Par conséquent, nous avons trois prédicats dédiés, appelés *prédicats normatifs* (*N-prédicats*, par opposition aux D-prédicats) : $O_{Send}(a, b, i)$, $P_{Send}(a, b, i)$ et $F_{Send}(a, b, i)$, qui modélisent respec-

2. PEPS est l'acronyme récursivement défini par : PEPS *for exchange policy specification*
3. on peut voir une *sorte* comme un *type*

tivement l'obligation, l'autorisation et l'interdiction pour un agent a d'envoyer à un agent b une information i.

Notons que pour exprimer la notion d'obligation et les concepts associés inhérents à une politique, nous aurions pu choisir d'utiliser une logique déontique. Cependant, les outils de preuve pour les logiques modales sont beaucoup moins efficaces que les outils de preuve pour les logiques standard comme les solveurs SAT ou SMT (Sebastiani et Vescovi, 2009). Par conséquent, en n'utilisant pas un opérateur modal, nous perdons en expressivité, mais, dans le cadre d'analyses automatiques, nous gagnons en efficacité.

Dans la logique déontique standard, les modalités d'obligation et de permission sont reliées par l'axiome (D) qui exprime que si p est obligatoire alors p est également permis. Dans PEPS, nous traduisons cet axiome par une propriété de logique, que nous appelons également (D) et qui exprime le fait que s'il est obligatoire pour un agent d'envoyer une information à un autre agent alors il est également permis de l'envoyer.

Définition 1

$$(D) \quad \forall a, \forall b, \forall i, O_{Send}(a, b, i) \implies P_{Send}(a, b, i)$$

De plus, nous définissons les *règles d'échange* comme des formules qui spécifient sous quelles conditions un agent à l'obligation, l'interdiction ou la permission d'envoyer une information à un autre agent. Nous appelons une *politique d'échange* (EP) un ensemble de règles d'échange.

Définition 2 (Règle d'échange)
Une règle d'échange est une formule PEPS fermée *de l'une des formes suivantes :*

$$\forall x_1, \ldots, \forall x_n, \ (\phi \implies O_{Send}(t_1, t_2, t_3))$$
$$\forall x_1, \ldots, \forall x_n, \ (\phi \implies P_{Send}(t_1, t_2, t_3))$$
$$\forall x_1, \ldots, \forall x_n, \ (\phi \implies F_{Send}(t_1, t_2, t_3))$$

où :

– $x_1, \ldots, x_n$ *sont toutes les variables présentes dans* ϕ, t_1, t_2 *et* t_3 *;*
– ϕ *est une formule sans quantificateur et sans* N-prédicats *;*
– t_1, t_2 *sont des termes de sorte* $\mathcal{A}$ *;*
– t_3 *est un terme de sorte* $\mathcal{I}$*.*

À cela nous devons ajouter une description formelle du domaine, notée Σ. La déclaration des sortes et des prédicats nécessaires pour décrire le domaine associé à une application particulière est laissée à l'utilisateur. Techniquement, PEPS est extensible uniquement avec de nouveaux types, des fonctions et des D-prédicats, mais il n'est pas possible d'introduire de nouveaux N-prédicats.

Dans la suite, nous appellerons *spécification d'une politique d'échange*, dénotée par EPS, le couple formé par la politique d'échange proprement dite EP et par les contraintes du domaine Σ, auxquelles nous ajoutons la propriété (D).

Définition 3 (Spécification d'une politique d'échange)

$$\mathcal{EPS} \equiv \Sigma \wedge (\bigwedge_{r \in EP} r) \wedge D$$

Enfin, nous utiliserons la notation $P \models Q$ pour dire que Q est une conséquence logique de P, *i.e.* que tout modèle de P est aussi un modèle de Q.

2.2. *Vérification automatique de politiques d'échange*

Dans cette section nous allons brièvement présenter les mécanismes sous-jacents à notre outil PEPS-analyzer, puis nous présenterons l'ensemble des propriétés génériques, propres aux politiques d'échange, pouvant être automatiquement vérifiées à l'aide de cet outil.

2.2.1. PEPS-*analyzer*

PEPS-analyzer est un outil d'aide à la spécification de politiques d'échange. Il permet de vérifier des propriétés sur les politiques et, si ces propriétés ne sont pas vérifiées, renvoie des contre-exemples. Ainsi, par interaction avec l'outil, il est possible, à l'aide des contre-exemples renvoyés, de mettre au point incrémentalement une politique qui répond réellement aux exigences souhaitées. Cette tâche devient très difficile voire impossible pour un humain à mesure que la spécification grandit : sur des exemples simples d'une dizaine de règles seulement, la combinatoire des interactions les différentes règles fait qu'il est impossible d'identifier humainement toutes les incohérences entre règles, de garantir la complétude de la politique ou de garantir l'absence de redondance entre règles.

Concrètement, PEPS-analyzer ramène le problème de vérification d'une propriété à un problème de satisfiabilité. Ainsi, vérifier que $P \models Q$ (Q est conséquence logique de P), avec P et Q des formules de la MSFOL, revient à vérifier à l'aide d'un solveur SMT (Satisfiability Modulo Theories) que la formule $P \wedge \neg Q$ est insatisfiable.

Si la première version de PEPS-analyzer implémentait un encodage purement booléen de la MSFOL dans un univers borné et utilisait un solveur SAT (Delmas et Polacsek, 2013), la nouvelle version de l'outil délègue le raisonnement dans la MSFOL à un solveur externe de type SMT, qui gère les quantificateurs nativement.

PEPS-analyzer est développé en Scala et il s'appuie sur le solveur SMT Z3 (de Moura et Bjørner, 2008).

2.2.2. *Des propriétés génériques*

L'outil PEPS-analyser permet de vérifier automatiquement quatre propriétés génériques sur les politiques : la *consistance*, l'*applicabilité*, la *minimalité* et la *complétude*.

Une politique est *consistante* s'il n'existe pas de cas où il est à la fois interdit et obligatoire (ou permis) pour un agent d'envoyer une information à un autre agent. L'*applicabilité* correspond au fait que la politique ne régisse pas des situations qui n'existent pas ou n'arrivent jamais, et une politique est *minimale* s'il n'existe pas de règle qui puisse se déduire des autres (et est donc inutile).

Nous pouvons définir la propriété de complétude comme suit : *"dans toutes situations et pour toutes informations, la politique indique si un agent qui connaît cette information à l'obligation, la permission ou l'interdiction de l'envoyer aux autres agents."* Cette définition est assez standard et correspond à celle donnée par (Akl et Denning, 1987) (Denning *et al.*, 1987) dans le contexte des politiques de contrôle d'accès. Cependant, dans les phases préliminaires de conception, il n'est pas strictement nécessaire qu'une politique soit complète. Il peut être utile de n'avoir une politique complète que pour certains sous domaines de son domaine d'application. En effet, une politique peut être conçue dans le cadre d'une collaboration entre des parties bien distinctes, chacune portant seulement attention au sous-ensemble des sujets qui la concernent. Par exemple, dans le cadre de l'observation de la Terre, les opérateurs militaires peuvent vouloir s'assurer que la politique est complète pour tout ce qui concerne le sujet militaire sans s'intéresser aux autres sujets.

Nous proposons donc une définition paramétrée de la complétude, que nous appelons T-complétude. Une politique d'échange est dite T-complète si et seulement si pour tout agent qui connaît une information pertinente sur un sujet T, la politique spécifie si l'agent a l'obligation, la permission ou interdiction de l'envoyer à un autre agent.

Définition 4 (T-complétude)
Soit $EPS = \langle \Sigma, EP \rangle$ la spécification d'une polique d'échange et T une constante de sorte $\mathcal{T}$. EPS est T-complète si et seulement si :

$$\mathcal{EPS} \models \forall a, \forall b, \forall i,$$
$$(K(a,i) \wedge Topic(i,T) \implies (P_{Send}(a,b,i) \vee O_{Send}(a,b,i) \vee F_{Send}(a,b,i)))$$

3. Exemple

Nous allons ici introduire un exemple qui nous permettra d'illustrer l'utilisation de PEPS ainsi que les différents points développés dans les sections suivantes. Considérons des agents qui disposent de moyens d'observation de la Terre et qui décident de

participer à une coalition pour la gestion des risques sismiques. Dans le cadre de cette coalition, il existe un groupe d'agents particulier : le *Groupe de Gestion des Risques Sismiques*, noté GRS, dont la mission est de prévenir les fausses alertes, d'organiser les évacuations et de gérer la communication avec le public. La politique de ce système se compose pour le moment de quatre règles :

$r1$ *"Tout agent non membre du GRS doit communiquer toute information relative aux risques sismiques à au moins un membre du GRS."*

$r1b$ *"Tout agent non membre du GRS a la permission de communiquer des informations relatives aux risques sismiques à n'importe quel membre du GRS."*

$r2$ *"Il est interdit, pour tout agent non membre du GRS, de communiquer des informations relatives aux risques sismiques à toute personne non membre du GRS."*

$r3$ *"Les membres du GRS ont la permission de communiquer les informations relatives aux risques sismiques à quiconque."*

La règle $r1$ découle clairement de l'exigence de diffusion : il y a une nécessité à ce que les agents communiquent toute information relative à une catastrophe sismique à un membre du GRS pour permettre au GRS d'accomplir sa mission. La règle $r1b$ complète la règle $r1$: tout agent externe au GRS sait ainsi s'il a le droit de communiquer une information relative aux risques sismiques aux autres agents du GRS en plus de celui avec lequel il a l'obligation de communiquer. La règle $r2$ a pour but de prévenir tout risque de panique par la diffusion brutale d'informations au grand public.

Notons que la règle $r3$ relève d'un processus d'appréciation qui n'est pas modélisé, et qui n'a pas forcément vocation à l'être au sein de la politique d'échange : le choix réalisé par un membre du GRS d'émettre ou pas un avertissement au public. Ici, c'est bien le prédicat de permission d'envoyer une information qui permet de modéliser la politique à ce niveau d'abstraction.

Pour pouvoir modéliser cette politique en PEPS nous devons d'abord déclarer une nouvelle constante geo, de sorte $\mathcal{T}$, qui représente le sujet *risque sismique*. Nous déclarons aussi un nouveau prédicat de domaine GRS, qui s'applique sur la sorte $\mathcal{A}$, et qui modélise l'appartenance au groupe GRS. Ainsi, $GRS(a)$ est vrai lorsque l'agent a est élément du groupe GRS, et faux lorsqu'il ne l'est pas[4]. La politique de notre exemple se modélise donc en PEPS comme suit :

---

4. Nous avons choisi de modéliser l'appartenance à un groupe de la façon la plus simple possibe. Ici, chaque groupe est caractérisé par un prédicat portant sur des agents et indiquant l'appartenance ou pas de l'agent au groupe. Nous aurions tout aussi bien pu introduire une sorte pour les groupes et un prédicat d'appartenance à un groupe de la forme $member(g, a)$.

$$
\begin{array}{rlll}
r1: & \forall a, \forall i, \exists b, K(a,i) \wedge Topic(i, geo) \wedge \neg GRS(a) \wedge \ GRS(b) & \Longrightarrow & O_{Send}(a,b,i) \\
r1b: & \forall a, \forall i, \forall b, K(a,i) \wedge Topic(i, geo) \wedge \neg GRS(a) \wedge \ GRS(b) & \Longrightarrow & P_{Send}(a,b,i) \\
r2: & \forall a, \forall i, \forall b, K(a,i) \wedge Topic(i, geo) \wedge \neg GRS(a) \wedge \neg GRS(b) & \Longrightarrow & F_{Send}(a,b,i) \\
r3: & \forall a, \forall i, \forall b, K(a,i) \wedge Topic(i, geo) \wedge \ GRS(a) & \Longrightarrow & P_{Send}(a,b,i)
\end{array}
$$

Nous rajoutons à cela la contrainte de domaine *"Toute information concerne au moins un sujet"* : $d: \ \forall i, \exists t, \ Topic(i,t)$.

A l'aide de notre outil PEPS-analyzer, nous pouvons automatiquement vérifier que la spécification $\langle \{d\}, \{r1, r1b, r2, r3\} \rangle$ est geo-complète, consistante, applicable et minimale.

4. Exigence diffusion : la propriété de vigilance

Dans les systèmes tels ques GEOSS ou le SSA, certains acteurs ont un rôle particulier : pour accomplir leur mission ils doivent absolument connaître toute information relative à un sujet donné. Dans notre exemple, les agents du groupe GRS doivent être prévenus de tout ce qui se rapporte au risque sismique. Par conséquent, nous définissons la propriété dite de T*-vigilance* pour un groupe comme le fait qu'un groupe d'agents est toujours correctement informé relativement à un sujet précis T.

Définition 5 (T-vigilance pour un groupe G)
Soit $EPS = \langle \Sigma, EP \rangle$ la spécification d'une politique d'échange, T une constante de sorte $\mathcal{T}$ et G un prédicat sur la sorte $\mathcal{A}$ caractérisant un groupe d'agents. Alors G est T-vigilant dans EPS si et seulement si :

$$\mathcal{EPS} \models (\forall a, \forall i, \exists b, K(a,i) \wedge Topic(i,T) \wedge \neg G(a) \wedge G(b) \implies O_{Send}(a,b,i))$$

Remarquons que dans le cas où le groupe se résume à un unique agent et où cet agent est T-vigilant sur tous les sujets possibles, alors la propriété se résume au fait que tout autre agent du système doit envoyer tout ce qu'il connaît à cet agent, en d'autres termes, nous sommes face à un agent que nous pouvons qualifier d'*omniscient*.

À l'aide de PEPS-analyzer nous pouvons vérifier que la politique d'exemple $\langle \{d\}, \{r1, R1b, r2, \ idr3\} \rangle$ vérifie la propriété de geo-vigilance pour le groupe GRS. Notons qu'ici la règle $r1$ est l'instanciation directe de la propriété de vigilance pour le thème geo.

5. Exigence de non-diffusion : les propriétés de restriction

Si la propriété T-vigilance permet de vérifier qu'un groupe d'agents donné reçoit toujours toute information relevant du sujet T, il peut être intéressant, de façon duale,

de vérifier que toute information traitant d'un sujet particulier (comme, par exemple, le sujet *confidentiel*) ne doit pas être envoyée à un groupe d'agents, à un agent unique ou bien tout simplement ne doit pas être envoyée du tout.

Nous définissons la propriété de *restriction de la diffusion d'information concernant un sujet à un groupe donné* selon trois cas : soit il est interdit aux agents hors du groupe de s'échanger une information de ce sujet ; soit il est interdit pour un agent hors du groupe de communiquer une information de ce sujet à un membre du groupe ; soit il est interdit aux membres du groupe de communiquer une information de ce sujet hors du groupe.

Définition 6 (T-restriction à un groupe G)

Soit $EPS = \langle \Sigma, EP \rangle$ la spécification d'une politique d'échange, T une constante de sorte $\mathcal{T}$ et G un prédicat sur la sorte $\mathcal{A}$ caractérisant un groupe d'agents, nous avons alors :

(a) T-out-out-restriction pour G dans EPS si et seulement si :

$$\mathcal{EPS} \models (\forall a, \forall b, \forall i, K(a,i) \wedge Topic(i,T) \wedge \neg G(a) \wedge \neg G(b) \implies F_{Send}(a,b,i))$$

(b) T-out-in-restriction pour G dans EPS si et seulement si :

$$\mathcal{EPS} \models (\forall a, \forall b, \forall i, K(a,i) \wedge Topic(i,T) \wedge \neg G(a) \wedge G(b) \implies F_{Send}(a,b,i))$$

(c) T-in-out-restriction pour G dans EPS si et seulement si :

$$\mathcal{EPS} \models (\forall a, \forall b, \forall i, K(a,i) \wedge Topic(i,T) \wedge G(a) \wedge \neg G(b) \implies F_{Send}(a,b,i))$$

Pour finir, nous ajoutons aux propriétés de restriction ci-dessus la propriété de T-restriction stricte qui signifie que tout échange d'information relative à T est interdit entre agents, quels qu'ils soient. Notons que cette propriété n'est qu'un cas particulier de la définition 6 avec G le groupe vide (modélisé par $\forall a, G(a) \equiv \bot$).

Définition 7 (T-restriction stricte)

Soit $EPS = \langle \Sigma, EP \rangle$ la spécification d'une politique d'échange et T une constante de sorte $\mathcal{T}$, nous avons la T-restriction stricte dans EPS si et seulement si :

$$\mathcal{EPS} \models (\forall a, \forall b, \forall i, K(a,i) \wedge Topic(i,T) \implies F_{Send}(a,b,i))$$

Sur notre exemple de surveillance de risques sismiques, nous pouvons vérifier, à l'aide de PEPS-analyzer, que la politique $\langle \{d\}, \{r1, r1b, r2, r3\} \rangle$ satisfait la geo-out-out-restriction pour le groupe GRS. En effet, aucune information relative à geo ne

peut être envoyée entre agents hors du groupe GRS, par contre, les agents du GRS peuvent recevoir ces informations des agents extérieurs aux groupes et ils ont aussi la permission de communiquer ces informations avec les agents hors du groupe.

6. Diffusion et non-diffusion

6.1. *Incompatibilité entre la vigilance et la restriction*

Enrichissons notre exemple en supposant maintenant qu'il existe dans le système des informations que nous qualifierons de *sensibles*. Pour prévenir la diffusion de telles informations nous rajoutons dans la politique de notre exemple la règle $r4$ suivante : *"il est interdit de s'échanger toute information relative au sujet sensible"*. Afin de pouvoir modéliser cette nouvelle règle dans PEPS, nous introduisons une nouvelle constante de sorte $\mathcal{T} : sens$, qui représente le sujet *sensible*.

$$r4 : \quad \forall a, \forall b, \forall i, K(a, i) \wedge Topic(i, sens) \implies F_{Send}(a, b, i)$$

À l'aide de PEPS-analyzer nous découvrons que, malheureusement, l'ajout de $r4$ rend la politique $\langle \{d\}, \{r1, r1b, r2, r3, r4\} \rangle$ inconsistante.

En effet, considérons le cas où un agent connaît une information relative à la fois à geo et $sens$, comme une image prise par un satellite montrant un risque de catastrophe naturelle sur un site civil jouxtant un site militaire sensible. Dans ce cas là, la règle $r1$ oblige l'agent à envoyer cette information à au moins un agent du GRS, alors que $r4$ interdit à ce même agent d'envoyer l'information à quiconque et donc, à fortiori, à un agent du GRS, ce qui viole la propriété de consistance. Remarquons que les règles $r3$ et $r4$ entraînent également une inconsistance en permettant et en interdisant simultanément la diffusion d'information portant sur geo et $sens$.

Le problème d'inconsistance soulevé ici n'est pas spécifiquement lié à l'exemple. Plus généralement, si l'on considère une politique munie d'une propriété de T_1-vigilance pour un groupe G_1 et d'une propriété de T_2-restriction pour un groupe G_2 alors, suivant les règles du domaine, il peut être possible de construire des modèles satisfaisant les deux propriétés et où il est à la fois obligatoire et interdit d'envoyer une information. Ces modèles ont tous la même structure : au moins une information concerne les deux sujets, T_1 et T_2, et les prédicats de groupe G_1 et G_2 sont tels qu'il existe des agents à l'intérieur et à l'extérieur de G_1 et de G_2 qui satisfont les prémisses des propriétés de T_1-vigilance et T_2-restriction.

6.2. *Une solution ad-hoc*

Afin de prévenir les possibles conflits entre les exigences de diffusion et de non-diffusion, nous proposons d'introduire un nouvel opérateur, pour le moment sans si-

gnification particulière, de signature $p(i : \mathcal{I}) : \mathcal{I}$, qui prend en entrée une information et retourne une information.

Dans notre exemple, nous voulons que cet opérateur permette d'*oublier* la partie sensible d'une information. Par conséquent nous posons les deux contraintes de domaine suivantes pour représenter le comportement de notre opérateur abstrait : ($p1$) une information produite par p n'est plus pertinente pour le sujet $sens$ et ($p2$) une information relative au sujet geo le reste après application de p.

$$\begin{array}{ll} p1: & \forall i, \neg Topic(p(i), sens) \\ p2: & \forall i,\ Topic(i, geo) \implies Topic(p(i), geo) \end{array}$$

Nous devons maintenant adapter la politique d'échange de notre exemple pour préciser dans quels cas l'opérateur abstrait p doit être utilisé.

Premièrement, nous séparons la règle $r1$ en deux nouvelles règles, $r11$ et $r12$, pour exprimer le fait que ($r11$) si une information est liée à des risques sismiques et qu'elle n'a pas de caractère sensible, alors il est obligatoire de l'envoyer à un membre du GRS au moins, mais ($r12$) si cette information est également sensible alors il faut envoyer non pas i elle même, mais l'information résultant de l'application de p.

$$\begin{array}{l} r11 : \forall a, \forall i, \exists b, K(a, i) \wedge Topic(i, geo) \wedge \neg Topic(i, sens) \wedge \neg GRS(a) \wedge GRS(b) \\ \qquad\qquad \implies O_{Send}(a, b, i) \\ r12 : \forall a, \forall i, \exists b, K(a, i) \wedge Topic(i, geo) \wedge Topic(i, sens) \wedge \neg GRS(a) \wedge GRS(b) \\ \qquad\qquad \implies O_{Send}(a, b, p(i)) \end{array}$$

Deuxièmement, sur le même modèle que $r1$ et pour les mêmes raisons, nous décomposons la règle $r1b$ en deux nouvelles règles $r1b1$ et $r1b2$:

$$\begin{array}{l} r1b1 : \forall a, \forall i, \forall b, K(a, i) \wedge Topic(i, geo) \wedge Topic(i, sens) \wedge \neg GRS(a) \wedge GRS(b) \\ \qquad\qquad \implies P_{Send}(a, b, p(i)) \\ r1b2 : \forall a, \forall i, \forall b, K(a, i) \wedge Topic(i, geo) \wedge \neg Topic(i, sens) \wedge \neg GRS(a) \wedge GRS(b) \\ \qquad\qquad \implies P_{Send}(a, b, i) \end{array}$$

Troisièmement, nous modifions la règle $r3$ en $r3'$ pour exprimer le fait que tout membre du GRS est autorisé à communiquer une information liée à des risques sismiques à tout autre agent, à la condition que cette information ne soit pas sensible.

$$\begin{array}{l} r3' : \forall a, \forall b, \forall i, K(a, i) \wedge Topic(i, geo) \wedge \neg Topic(i, sens) \wedge GRS(a) \\ \qquad\qquad \implies P_{Send}(a, b, i) \end{array}$$

Nous pouvons à présent vérifier à l'aide de PEPS-analyzer que cette nouvelle politique, $\langle \{d, p1, p2\}, \{r11, r12, r1b1, r1b2, r2, r3', r4\} \rangle$, est geo-complète, $sens$-

complète, consistante, applicable, minimale et satisfait la restriction stricte pour le sujet $sens$.

Cependant, cette nouvelle politique ne satisfait pas la propriété de geo-vigilance pour le GRS. En effet, quand une information concernant un risque sismique est aussi de nature sensible, c'est le résultat de l'application de la fonction p à cette information qui est envoyée au GRS alors que la propriété de vigilance définie initialement impose que cela soit l'information elle-même qui soit envoyée. Nous avions introduit la notion de vigilance afin de garantir que le GRS puisse réaliser sa mission, ce qui correspondait au fait que toute information relative à geo devait être envoyée au GRS. Finalement, l'important est qu'un membre du GRS soit prévenu et peu importe qu'il reçoive l'information initiale ou l'information après l'application de p, du moment que la partie concernant le sujet geo est préservée. Par conséquent, plutôt que de chercher à établir la geo-vigilance pour le groupe GRS, nous devons vérifier que la politique garantisse que si une information porte sur geo, alors doit être envoyée à un membre du GRS : soit cette information, soit le résultat de l'application de p, ce qui est résumé par la formule suivante :

$$\forall a, \forall i, K(a,i) \wedge \mathit{Topic}(i, geo) \wedge \neg GRS(a) \implies$$
$$(\exists b, GRS(b) \wedge (O_{Send}(a,b,i) \vee (\mathit{Topic}(p(i), geo) \wedge O_{Send}(a,b,p(i)))))$$

L'opérateur abstrait p agit comme un filtrage sur les sujets sur lesquels porte une information. Il correspond à une catégorie d'opérations effectuées régulièrement par les organismes qui gèrent des données sensibles, les opérations dites de *déclassification*, de *masquage*, d'*anonymisation*, *etc.*

6.3. *Un opérateur générique de filtrage d'information*

Afin de modéliser des opérations telles que la déclassification et ses variantes dans PEPS, nous introduisons un opérateur générique dit de *filtrage*, paramétré par des *modes de filtrage*. Chaque mode spécifie les sujets qui sont *conservés* ou *retirés* par l'opérateur.

Pour cela, nous introduisons : une nouvelle sorte $\mathcal{M}$, dont les éléments représentent les différents modes de filtrage ; un opérateur de filtrage $\mathit{filter}(m : \mathcal{M}, i : \mathcal{I}) : \mathcal{I}$ ainsi que deux prédicats $\mathit{preserves}(m : \mathcal{M}, t : \mathcal{T})$ et $\mathit{removes}(m : \mathcal{M}, t : \mathcal{T})$. Les axiomes suivants expriment le comportement de l'opérateur de filtrage en fonction du mode :

Définition 8 (F axiomes)

$$\begin{array}{rrcl}
\forall t, \forall m, & \mathit{preserves}(m,t) & \implies & \neg \mathit{removes}(m,t) \\
\forall i, \forall t, \forall m, & \mathit{Topic}(i,t) \wedge \mathit{preserves}(m,t) & \implies & \mathit{Topic}(\mathit{filter}(m,i),t) \\
\forall i, \forall t, \forall m, & \mathit{Topic}(i,t) \wedge \mathit{removes}(m,t) & \implies & \neg \mathit{Topic}(\mathit{filter}(m,i),t)
\end{array}$$

Le premier axiome garantit la cohérence entre les prédicats de préservation et de suppression : si un mode conserve un sujet, alors il ne le supprime pas. Le deuxième axiome stipule que si une information concerne un sujet qui est préservé par un mode, alors elle concerne toujours ce sujet après filtrage sous ce mode. Le troisième axiome est simplement le dual du deuxième concernant le prédicat de suppression.

L'opérateur ad-hoc p, défini dans la section précédente, est subsumé par l'opérateur filtrage générique. Dans notre exemple, nous introduisons une constante de sorte $\mathcal{M}$ $\mathit{filterSens}$, qui représente le mode de filtrage pour les informations à contenus sensibles et qui préserve les contenus relatifs aux risques sismiques. Concrètement, nous ajoutons la contrainte de domaine suivante qui spécifie les propriétés du filtrage pour ce mode :

$$f : \ \mathit{preserves}(\mathit{filterSens}, \mathit{geo}) \wedge \mathit{removes}(\mathit{filerSens}, \mathit{sens})$$

Il est important de noter que cette caractérisation des modes de filtrage à l'aide des prédicats $\mathit{preserves}$ et $\mathit{removes}$ n'est qu'une modélisation partielle des politiques de filtrage du monde réel. En effet, dans la pratique, d'autres conditions doivent être prises en compte pour l'utilisation de l'opérateur, telles que la capacité de l'agent à exécuter effectivement l'opération de filtrage, les caractéristiques du destinataire, *etc.* Toutes les conditions supplémentaires qui caractérisent les modes de filtrage pourraient être regroupées pour former une *politique de filtrage*, comparable à ce qui existe déjà pour les *politiques de déclassification*. Cependant, même si l'extensibilité de PEPS et la puissance expressive de la logique sous-jacente permettent de modéliser ces concepts, nous ne les développerons pas davantage dans cet article.

6.4. *Propriétés génériques de vigilance et de restriction*

Forts de la définition de l'opérateur de filtrage, nous pouvons redéfinir la propriété de vigilance en une version. Un groupe d'agents est dit T-vigilant si et seulement si tout agent, extérieur au groupe, connaissant une information relative au sujet T, a l'obligation d'envoyer à au moins un agent appartenant au groupe soit l'information soit l'information filtrée avec un mode de filtrage qui préserve les informations concernant le sujet T.

Définition 9 (T-vigilance pour un groupe G)
Soit $EPS = \langle \Sigma, EP \rangle$ la spécification d'une polique d'échange, T une constante de sorte $\mathcal{T}$ et G un prédicat sur la sorte $\mathcal{A}$ caractérisant un groupe d'agents, G est T-vigilant dans EPS si et seulement si :

$$\mathcal{EPS}, F \models (\forall a, \forall i, K(a,i) \wedge \mathit{Topic}(i,T) \wedge \ G(a) \implies$$
$$(\exists b, G(b) \wedge (O_{Send}(a,b,i) \vee \exists m, \mathit{preserves}(m,T) \wedge O_{Send}(a,b,\mathit{filter}(m,i)))))$$

Si nous revenons à notre exemple de prévention des risques sismiques, avec cette nouvelle définition de la vigilance, nous pouvons vérifier à l'aide de PEPS-analyser

que la politique $\langle\{d, f\}, \{r11, r12, r1b1, r1b2, r2, r3', r4\}\rangle$, réécrite avec l'opérateur *filter*[5], satisfait à la fois la nouvelle geo-vigilance et la geo-out-out-restriction pour le groupe GRS, la $sens$-restriction stricte, mais aussi la geo-complétude, la $sens$-complétude, la consistance, l'applicabilité et la minimalité.

7. Conclusion

Dans cet article, après avoir donné un bref rappel sur le langage PEPS et sur l'outil PEPS-analyzer, nous avons présenté et formalisé deux nouvelles classes de propriétés : les propriétés liées à l'exigence de diffusion et celles liées à l'exigence de non-diffusion d'information. Ainsi, nous avons montré que dans certains cas il est impossible de satisfaire ces deux exigences simultanément sans introduire un nouvel opérateur qui s'avère correspondre à une opération de filtrage d'information. Pour finir nous avons défini l'opérateur de filtrage de façon générique ainsi que redéfini la propriété de vigilance en fonction de cet opérateur générique.

Jusqu'à présent, nous nous sommes concentrés sur les concepts clés des politiques d'échange d'information. Dans des travaux futurs nous inclurons à ce cadre de spécification la modélisation des organisations qui composent le système. Nous devrons déterminer si certains concepts, comme celui des *rôles*, issus des modèles tels que OrBAC (Kalam *et al.*, 2003), peuvent être transposés dans notre cadre, tout en adaptant si besoin les propriétés de base que nous avons définies. Techniquement parlant, la nature extensive de PEPS permet de modéliser aisément de tels nouveaux concepts.

Par ailleurs, il pourrait être intéressant de faire le lien entre la spécification et l'implémentation de ces politiques. Dans le domaine des Architectures Orientées Services, (Barhamgi *et al.*, 2013) montrent qu'il est possible, dans le contexte du contrôle d'accès à l'information, de définir des modèles d'exécution paramétrés par des politiques de confidentialité et d'appliquer ces politiques à l'exécution. Ici, le lien entre la spécification de la politique et sa mise en œuvre par composition des services, est explicite. Nous pourrions étudier si cette approche peut être adaptée dans le cadre du contrôle de la diffusion d'information.

Bibliographie

Akl S. G., Denning D. E., « Checking Classification Constraints for Consistency and Completeness », *IEEE Symposium on Security and Privacy*, IEEE Computer Society, 1987, p. 196-201.

Barhamgi M., Benslimane D., Oulmakhzoune S., Cuppens-Boulahia N., Cuppens F., Mrissa M., Taktak H., « Secure and Privacy-Preserving Execution Model for Data Services », Salinesi C., Norrie M. C., Pastor O., Eds., *CAiSE*, vol. 7908 de *Lecture Notes in Computer Science*, Springer, 2013, p. 35-50.

5. toutes les occurrences de $p(i)$ dans les règles de la politique d'échange ont été remplacées par $filter(filterSens, i)$.

Castanẽda H. N., *Thinking and doing*, D. Reidel, Dordrecht, 1975.

Cholvy L., Delmas R., Polacsek T., « Vers une aide à la spécification d'une politique d'échange d'information dans un SI », *Actes du XXXème Congrès INFORSID, Montpellier, France, 29 - 31 mai 2012*, 2012, p. 352–370.

de Moura L., Bjørner N., « Z3 : An Efficient SMT Solver », *Tools and Algorithms for the Construction and Analysis of Systems, 14th International Conference, TACAS 2008, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2008, Budapest, Hungary, March 29-April 6, 2008. Proceedings*, vol. 4963 de *Lecture Notes in Computer Science*, Springer, 2008, p. 337-340.

Delmas R., Polacsek T., « Formal Methods for Exchange Policy Specification », Salinesi C., Norrie M. C., Pastor O., Eds., *CAiSE*, vol. 7908 de *Lecture Notes in Computer Science*, Springer, 2013, p. 288-303.

Delmas R., Polacsek T., « Exigences de confidentialité et de diffusion concernant les politiques d'échanges d'information », *Génie Logiciel*, vol. 111, 2014, p. 49–53, GL & IS.

Denning D. E., Akl S. G., Heckman M., Lunt T. F., Morgenstern M., Neumann P. G., Schell R. R., « Views for Multilevel Database Security », *IEEE Trans. Software Eng.*, vol. 13, n° 2, 1987, p. 129-140.

Gallier J. H., « *Logic for Computer Science : Foundations of Automatic Theorem Proving* », chapitre 10, p. 448-476, Wiley, 1987.

Kalam A. A. E., Benferhat S., Miège A., Baida R. E., Cuppens F., Saurel C., Balbiani P., Deswarte Y., Trouessin G., « Organization based access contro », *POLICY*, IEEE Computer Society, 2003, p. 120-131.

Sebastiani R., Vescovi M., « Automated Reasoning in Modal and Description Logics via SAT Encoding : the Case Study of K(m)/ALC-Satisfiability », *J. Artif. Intell. Res. (JAIR)*, vol. 35, 2009, p. 343-389.