Un système multi-agents pour la détection d'intrusions

K. Boudaoud

Institut EURECOM
B.P. 193
06904 Sophia-Antipolis France
Phone: (33) 4 93 00 26 38
Fax: (33) 4 93 00 26 27

karima.boudaoud@eurecom.fr

RÉSUMÉ. Les réseaux varient continuellement, aussi bien en termes d'utilisateurs et de services offerts que de possibilités d'attaques. Des caractéristiques tel que l'adaptabilité, la distribution, et la coopération du paradigme système multi-agents permettent de gérer l'évolution des réseaux de manière contrôlée et efficace. Ainsi, les systèmes multi-agents peuvent être très adaptés pour gérer efficacement la sécurité des réseaux. Dans le cadre de cet article, nous nous focaliserons sur un aspect particulier de la gestion de sécurité, qui est la détection d'intrusions. Nous proposons une nouvelle approche pour la détection d'intrusions, basée sur les systèmes multi-agents.

MOTS-CLÉS : gestion de sécurité, détection d'intrusions, système multi-agents, modèle BDI

1. Introduction

Les réseaux et systèmes informatiques sont devenus aujourd'hui des outils indispensables pour le bon fonctionnement et l'évolution de la plupart des entreprises. Ainsi, les systèmes et réseaux informatiques sont déployés dans différents domaines comme la banque, les assurances, la médecine ou encore le domaine militaire. L'accroissement de l'interconnexion de ces divers systèmes et réseaux, les a rendus accessibles par une population diversifiée d'utilisateurs qui ne cesse d'augmenter. Ces utilisateurs, connus ou non, ne sont pas forcément pleins de bonnes intentions vis-à-vis de ces réseaux. En effet, ils peuvent essayer d'accéder à des informations sensibles pour les lire, les modifier ou les détruire ou encore tout simplement pour porter atteinte au bon fonctionnement du système. Dès lors que ces réseaux sont apparus comme des cibles d'attaques potentielles, les sécuriser est devenu un enjeu incontournable.

La sécurité des réseaux et systèmes peut se faire, soit de manière préventive, soit de manière réactive. Dans l'approche préventive, il s'agit de protéger les données et ressources du système ou réseau contre tout accès non autorisé ou abusif. Cependant, prévenir de toutes les violations de sécurité, apparaît quelque peu irréel. En effet, il est pratiquement impossible d'avoir un réseau complètement sûr et de le protéger contre toutes les attaques possibles. L'approche réactive permet de palier à cela, puisqu'elle consiste à essayer de détecter ces attaques au plutôt afin de réagir rapidement et d'éviter ainsi que de sérieux dommages soient causés. Cette seconde approche représente un mécanisme particulier de gestion de sécurité qui est la détection d'intrusions. Dans le cadre de cet article, nous nous intéressons à la seconde approche.

La majorité des systèmes de détection d'intrusions existants [1][2] sont basés sur des techniques d'intelligence artificielle. Cependant, ces systèmes sont généralement développés pour des environnements bien définis et n'offrent pas une solution à certaines caractéristiques des réseaux telles que la variation des comportements utilisateurs et des services offerts, la complexité et l'évolution croissante des types d'attaques auxquels ils peuvent être sujets, la rapidité des attaques qui peuvent survenir simultanément sur plusieurs machines, etc. Une solution multi-agents nous semble en effet très appropriée pour ce type de problèmes.

Nous allons donc commencer par introduire la détection d'intrusions, puis nous présenterons le modèle organisationnel du système multi-agents (SMA). Dans une troisième section nous décrirons le modèle fonctionnel d'un agent de sécurité. Puis nous expliciterons le modèle d'information de l'agent de sécurité. Enfin, nous présenterons de manière générale une implémentation de notre système. Finalement, nous terminerons par une conclusion et quelques remarques sur les travaux futurs.

2. Caractéristiques des systèmes de détection d'intrusion

Le rôle d'un système de détection d'intrusions est de détecter aussi bien un intrus essayant de causer des dommages au système qu'un utilisateur légitime abusant des ressources. Le système de détection d'intrusions doit s'exécuter constamment sur le système, en travaillant en arrière - plan, et ne notifiant l'administrateur de sécurité que lorsqu'il détecte quelque chose qu'il considère comme suspicieux ou illégal [3]. Les systèmes de détection d'intrusions offrent une défense lorsque les vulnérabilités systèmes sont exploitées et cela sans qu'il y ait nécessité de remplacer des équipements très coûteux. Parmi les systèmes existants, nous pouvons citer DIDS (Distributed Intrusion Detection System) [1] et CSM (Cooperating Security Manger) [2]. DIDS a été conçu pour surveiller un réseau local LAN. Sa nature centralisée représente un désavantage majeur dans le cas de réseaux WAN où les communications avec l'entité gestionnaire peuvent congestionner le réseau. CSM a été développé pour un environnement distribué. Cependant, il ne peut pas être facilement portable vers un autre environnement. En règle générale, les systèmes de détection d'intrusions existants sont mal adaptés à la complexité croissante des réseaux et des attaques auxquels ils sont sujets. Traditionnellement, ils utilisent des méthodes basées sur des modèles de système expert, des modèles statistiques, réseaux de neurones, etc. Ces systèmes sont généralement développés pour des réseaux et systèmes bien définis et ne sont pas adaptés à des environnements dynamiques. En effet, les paramètres des modèles utilisés sont prédéfinis. Ainsi, si une nouvelle attaque doit être détectée, il est très difficile de modifier le système de détection d'intrusions. Globalement, l'architecture des systèmes existants est monolithique.

Dans cette architecture, l'analyse des données collectées par une ou plusieurs entités distribuées n'est effectuée que par un seul module (DIDS). Cette approche présente deux inconvénients majeurs. D'une part, elle présente un point de rupture, dans le cas où l'entité centrale serait attaquée et d'autres part le déploiement de ce type de systèmes à grande échelle est limité. Dans d'autres systèmes, tel que CSM, l'analyse des données est effectuée sans l'utilisation d'une entité centralisée ce qui résout les problèmes engendrés par l'approche monolithique. Cependant, il existe encore certains inconvénients tel que : 1) la difficulté de s'adapter aux changements qui peuvent se produire dans le réseau et aux comportements des utilisateurs qui varient considérablement ; 2) la difficulté de mise à jour de ces systèmes, lorsque l'on veut améliorer ou rajouter de nouvelles méthodes de détection.

Pour une détection d'intrusions efficace, il est très important de considérer certaines caractéristiques :

- La *distribution* : un grand nombre d'attaques réseaux se caractérisent par des comportements anormaux à différents éléments du réseau (serveur, routeur,…). Il est donc très important de distribuer les fonctions de détection à plusieurs entités qui surveillent différents points du réseau.
- *L'autonomie:* des échanges excessifs d'informations entre les entités distribuées peuvent congestionner le réseau. Il serait donc plus judicieux de laisser l'entité, surveillant un élément réseau, effectuer une analyse locale et détecter les comportements intrusifs locaux. Ainsi, les entités distribuées doivent être autonomes.
- *La délégation :* La dynamicité des réseaux nécessite de pouvoir modifier, à n'importe quel moment, les fonctions de détection d'intrusions pour les adapter aux changements se produisant dans le réseau surveillé. Cela est possible grâce au modèle de délégation. Les tâches déléguées sont envoyées aux entités autonomes. Chaque entité aura à exécuter sa propre tâche. Lorsque de nouvelles tâches doivent être ajoutées, ceci est fait dynamiquement.
- La *communication* et *coopération* : la complexité des attaques coordonnées ne facilite pas leur détection par une seule entité. En effet, chaque entité n'ayant qu'une vue locale restreinte du réseau, il lui est très difficile de détecter ce type d'attaques. La détection de ce genre d'attaques, nécessite une corrélation des différentes analyses effectuées à différents points du réseau. Les différentes entités doivent alors se communiquer leurs analyses et coopérer afin de détecter efficacement les attaques coordonnées.
- La *réactivité* : l'objectif majeur de la détection d'intrusions est de réagir rapidement lorsqu'une attaque se produit afin de limiter les dommages qui peuvent être causés.
- L'*adaptabilité* : les politiques de sécurité d'une entreprise peuvent changer. Dans ce cas l'administrateur doit changer et/ou rajouter de nouvelles politiques afin de modifier et réadapter les tâches de détection d'intrusions. Le système de détection d'intrusions doit alors s'adapter à ces changements.

En considérant ces six caractéristiques, il apparaît très clairement qu'un SMA est très approprié au problème de détection d'intrusions. L'approche adoptée pour la conception de ce SMA est basée sur deux niveaux : 1) un niveau ***macro*** qui décrit la structure organisationnelle et fonctionnelle du SMA et 2) un niveau ***micro*** qui décrit l'architecture de l'agent de sécurité. Les deux paragraphes suivants décrivent ces deux niveaux

3 Modèle organisationnel du système multi-agents

Le niveau ***macro*** de conception d'un SMA conduit à la description de son organisation. Celle-ci est définie par l'ensemble des classes d'agents caractérisés par des rôles qui leur sont affectés et par l'ensemble des relations entre ces rôles [4]. Un rôle peut être défini comme un ensemble d'activités ou de tâches qu'un agent doit exercer afin que l'organisation atteignent ses objectifs. Pour pouvoir décrire les différents rôles, il est donc nécessaire d'identifier les tâches que doivent être remplies par le SMA. Pour exécuter ces tâches, un ensemble de compétences est nécessaire.

3.1 Identification des compétences

Nous distinguons deux types de compétences : ***gestion*** et ***surveillance***. Les compétences de *surveillance* peuvent être définies en fonction des types d'activités à surveiller. Ainsi, nous identifions cinq types de surveillance :

- ***surveillance externe*** pour la surveillance des activités externes ;
- ***surveillance extranet*** pour la surveillance des activités extranets ;
- ***surveillance intranet*** pour la surveillance des activités intranets ;
- ***surveillance interne*** pour la surveillance des activités internes ;
- et ***surveillance locale*** pour la surveillance d'activités locales.

Pour ce qui est des compétences de *gestion*, nous distinguons deux types :

- ***gestion des politiques de sécurité*** du réseau,
- et ***gestion de sécurité d'un réseau*** distribué ou local.

3.2 Identification des rôles

En fonction des compétences précédentes, nous identifions les rôles suivants :

- le rôle de ***gestionnaire de politiques de sécurité*** qui gère les politiques de sécurité et dialogue avec l'officier de sécurité ;
- le rôle de ***gestionnaire extranet*** qui décrit les fonctions de gestion de sécurité d'un réseau distribué. Elles concernent la détection d'attaques complexes se produisant à différents points du réseau distribué. En d'autres termes, un agent ayant ce rôle aura une vue globale du réseau et sera chargé de détecter les attaques coordonnées. Il aura également à spécifier les fonctions de surveillance et de détection aux agents de plus bas niveau. Ce rôle gère la sécurité du réseau distribué par rapport aux réseaux externes et entre les réseaux locaux constituants le réseau distribué ;
- le rôle de ***gestionnaire intranet*** qui gère la sécurité du réseau local constitué d'un ou plusieurs domaines. Il concerne la surveillance des activités et la détection des attaques complexes et coordonnées au sein du réseau local et entre ses différents domaines ;
- le rôle de ***surveillant local extranet*** qui englobe les fonctions de *surveillance externe et extranet* au sein du réseau local. Autrement dit, ce rôle est associé à la fonction de détection des attaques provenant ou en direction d'un réseau externe ou extranet ;
- le rôle de ***surveillant local intranet*** qui représente les fonctions de *surveillance interne et intranet* du réseau local. Il concerne aussi la détection des attaques provenant ou en direction d'autres réseaux locaux du même réseau distribué ;
- et enfin le rôle de ***surveillant local interne*** qui définit la fonction de *surveillance locale*, i.e. : la surveillance des activités *locales* à un domaine. Il concerne la détection des attaques locales à un domaine.

3.3 Structure organisationnelle

L'architecture de gestion de sécurité proposée est hiérarchique. Elle est constituée de plusieurs agents ayant différents rôles et distribués à différents points du réseau. L'organisation hiérarchique des agents permet d'assurer une analyse et détection aussi bien locale que globale. L'intérêt est d'essayer de détecter les attaques au plutôt. En effet, chaque agent, à son niveau, aura sa propre vision du réseau qui sera limité par le domaine qu'il doit surveiller et qu'il est chargé de sécuriser. Dans cette architecture, nous distinguons deux couches de fonctionnalités d'agents, relatives aux rôles d'agents identifiés dans la section précédente : une ***couche gestionnaire*** et une ***couche locale***.

- La ***couche gestionnaire*** gère la sécurité globale d'un réseau. Dans cette couche, nous distinguons trois niveaux d'agents gestionnaires : un agent gestionnaire des politiques de sécurité, un agent gestionnaire extranet et plusieurs agents gestionnaires intranet. L'agent gestionnaire extranet contrôle les agents gestionnaires intranet, qui lui reporte les analyses pertinentes. Il effectue ensuite d'autres analyses afin de confirmer ou non la détection d'une attaque. Il peut aussi demander d'autres traitements et déléguer de nouvelles tâches de surveillance aux agents gestionnaires intranet. L'agent gestionnaire extranet a également la responsabilité de distribuer les agents locaux aux différents agents gestionnaires intranet. L'agent gestionnaire intranet contrôle les agents locaux et analyse les rapports envoyés par ces agents.
- La ***couche locale*** gère la sécurité d'un domaine. Elle est constituée d'un groupe d'agents locaux, qui ont des rôles de surveillance spécifiques. Nous distinguons trois types d'agents locaux : agent local extranet, agent local intranet et agent local interne.

Les domaines sont définis par des agents de la couche gestionnaire. Dans la *couche locale*, un domaine représente un groupe de ressources réseaux, qui sont regroupés soit suivant l'organigramme de l'entreprise en termes de départements, soit suivant des niveaux de sécurité qui sont spécifiés par les politiques de sécurité de l'entreprise. Dans la *couche gestionnaire*, un domaine représente soit le réseau distribué de l'entreprise soit un réseau local de ce même réseau distribué.

La couche gestionnaire interagit avec la couche locale en :

- envoyant des messages sous formes de buts à atteindre, dérivés des politiques de sécurité spécifiées dans la couche gestionnaire ;
- déléguant des fonctions de surveillance/détection spécifiques ;
- demandant des informations particulières : le niveau de suspicion d'un utilisateur, la suite d'événements générés par un utilisateur, etc. ;
- spécifiant les différents domaines à surveiller ;
- recevant les rapports pertinents ou résultats d'analyses et alarmes.

L'interaction entre ces deux couches permet la détection des attaques globales en corrélant les différentes analyses de la couche locale.

Dans ce modèle multi-agents hiérarchique, chaque agent gestionnaire a la capacité de contrôler des agents spécifiques et d'analyser des données, alors que les agents locaux surveillent des activités spécifiques en vue de réaliser une analyse temps réel localisée.

Les agents d'un même niveau communiquent et s'échangent leurs connaissances et analyses afin de détecter les activités intrusives de manière coopérative. Cette communication entre les agents permet de tracer les utilisateurs dans le réseau.

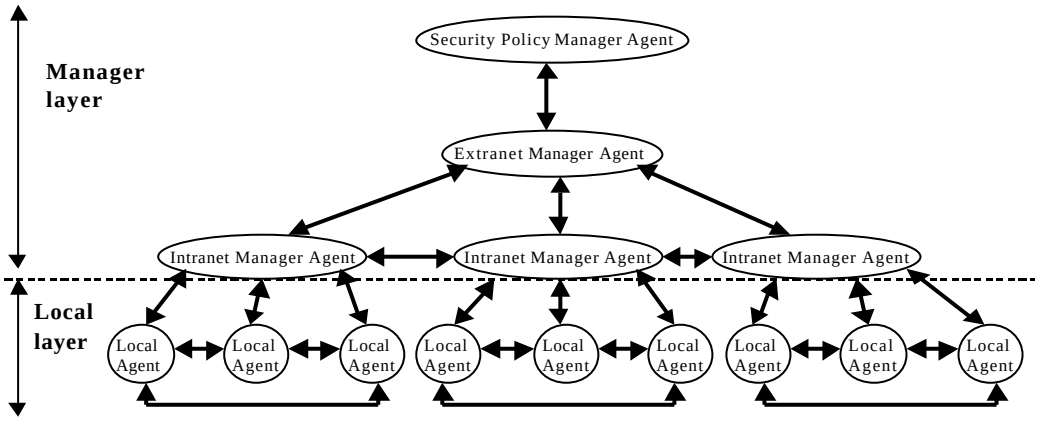

Figure 1 : Structure organisationnelle du système multi-agents

4. Modèle fonctionnel d'un agent de sécurité

Le système de détection d'intrusions doit pouvoir s'adapter à un environnement complexe, de part son évolution et sa variation continuelles, en termes de comportements utilisateurs (surtout dans le cas par exemple de la mobilité) et de problèmes de sécurité (nouvelles politiques de sécurité, nouvelles failles de sécurité, nouvelles attaques de sécurité,…). La connaissance manipulée par le système de détection d'intrusions varie donc constamment et cette dynamicité complexifie la gestion de la sécurité des réseaux. D'autres part, le système de gestion de sécurité doit respecter des contraintes temporelles et par conséquent réagir au plutôt lorsque des événements indiquent un état anormal du réseau (exemple une congestion du réseau due à une attaque de déni de service). Les agents doivent ainsi allier des capacités cognitives à des capacités réactives. Chaque agent réalise deux types de fonctions : des fonctions qui lui permettent de gérer ses interactions avec son environnement et les autres agents et des fonctions qui lui permettent de délibérer. Ces fonctions sont décrites dans les paragraphes suivants.

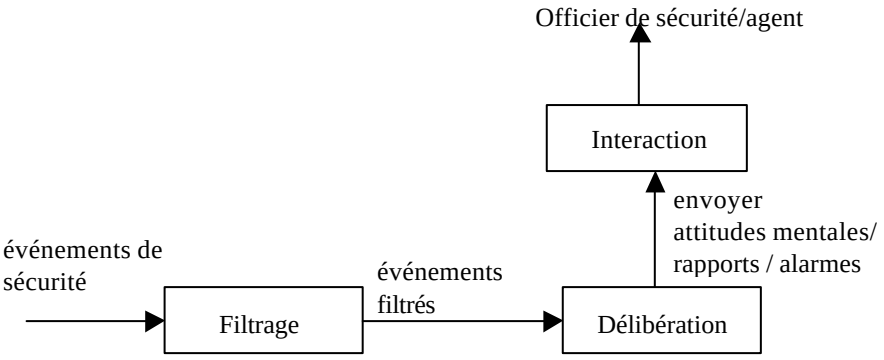

Figure 2 : Interactions entre les fonctions d'un agent de sécurité

4.1 Fonction d'interaction

Cette fonction gère les communications entre :

- l'agent et ses voisins,
- l'agent et son manager (agent gestionnaire ou l'officier de sécurité)
- et l'agent et ses subordonnés.

Elle permet ainsi aux agents de se communiquer leurs analyses, décisions et connaissances. L'agent peut alors faire part de ses croyances et de ses suspicions aux autres agents gestionnaires et/ou locaux. Il peut aussi leur communiquer les buts à atteindre.

La fonction d'*interaction* avec l'officier de sécurité n'existe qu'au niveau de l'*agent gestionnaire des politiques de sécurité* et de l'*agent gestionnaire extranet*. Elle assure la réception des spécifications et requêtes de l'officier de sécurité ; en l'occurrence la spécification des politiques de sécurité qui sont reçues et traitées par l'agent gestionnaire des politiques de sécurité. Elle gère la délivrance des rapports de sécurité et l'envoie des alarmes lorsqu'une attaque est détectée. L'officier de sécurité peut également demander des informations supplémentaires ou des confirmations. Il peut, par exemple, demander l'état courant de sécurité du réseau, la liste des récentes attaques détectées ou la liste des utilisateurs suspicieux.

4.2 Fonction de collecte d'événements

Un ***événement*** de sécurité est caractérisé par son *type*, son *point d'observation*, un *attribut temporel* et un ensemble d'*attributs non temporels*. L'attribut temporel représente l'instant où s'est produit l'événement.

Suivant le type de l'événement et son point d'observation, nous identifions différentes classes d'événements. Chaque classe est caractérisée par des attributs non temporels qui lui sont propres, en plus de ceux qui sont communs à toutes les classes (voir figure 3).

La fonction de *collecte d'événements* permet de récupérer les événements de sécurité que l'agent est chargé d'observer. En effet, les événements se produisant dans l'environnement de l'agent (réseau), ne sont pas tous collectés :

- ils sont filtrés suivant les classes d'événements à observer. Ces classes sont spécifiées à l'agent lorsqu'il reçoit un but de détection.
- Ainsi, au moment où un événement se produit dans le réseau, l'agent teste son appartenance à l'ensemble de ces classes. S'il appartient à cet ensemble, il est collecté.
- Les événements filtrés sont ensuite rangés dans une file en attente d'être traités par la fonction de délibération.

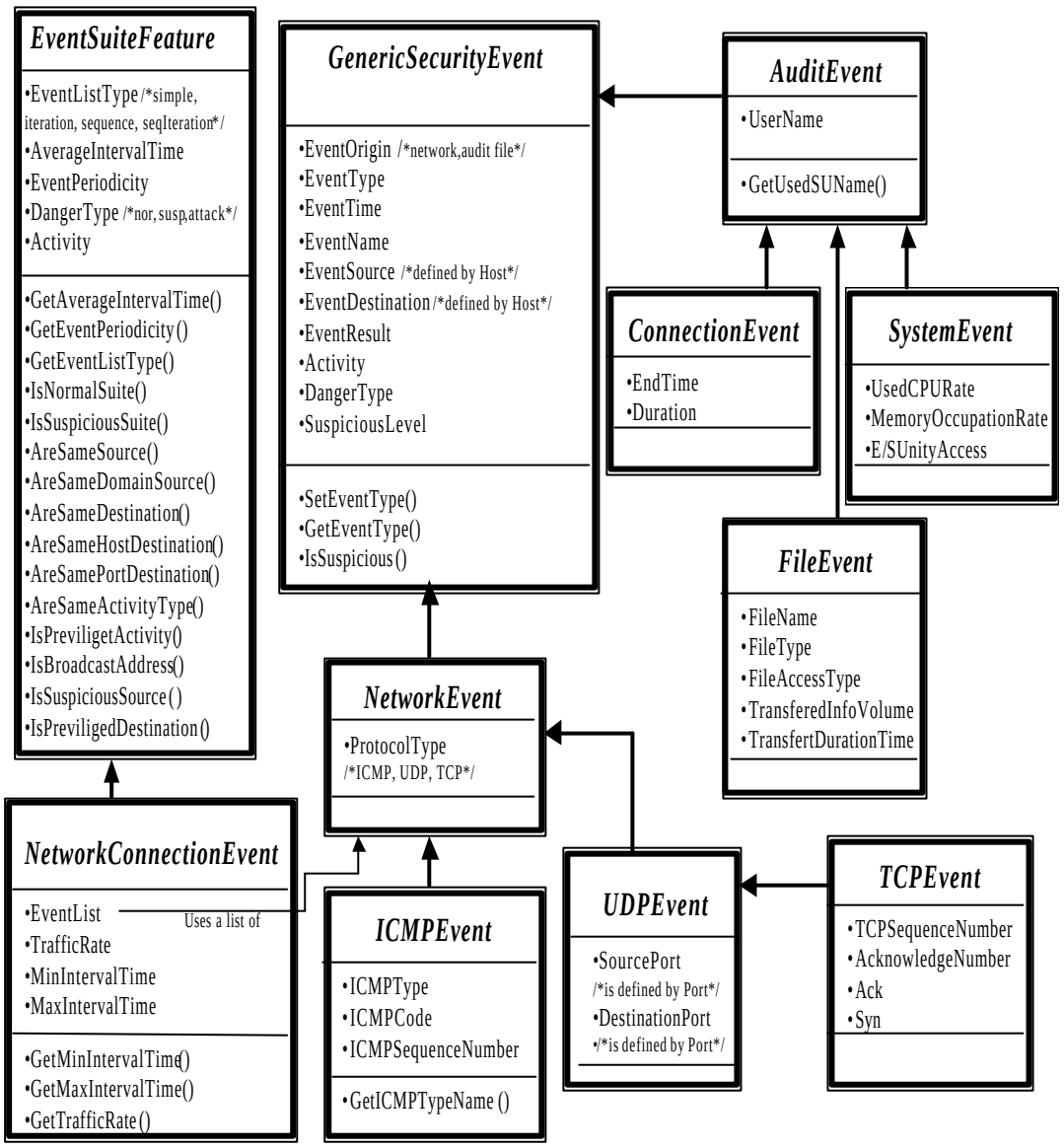

Figure 3 : Classes UML des événements de sécurité

4.3 Fonction de délibération

La résolution du problème de détection d'intrusions doit prendre en compte des caractéristiques importantes du réseau tels que : 1) sa variation continue, notamment en termes d'utilisateurs et de services offerts ; 2) et la variation de ses problèmes de sécurité tels que de nouvelles vulnérabilités et types d'attaques de plus en plus complexes. Etant donné, le caractère non prédictible du comportement de l'environnement de l'agent (réseau), nous avons donc adopté une solution BDI, [5][6] pour la modélisation du système de détection d'intrusions.

La fonction de délibération est une fonction fondamentale de l'agent, sur laquelle repose son intelligence et son autonomie. Elle manipule les attitudes mentales de l'agent (croyances, suspicions, buts et intentions), qui sont développés dans la section 5. Grâce à cette fonction, l'agent est capable de raisonner et d'extrapoler en se basant sur ses attitudes mentales, ses connaissances et son expérience de manière rationnelle. Par conséquent, les décisions de l'agent dépendent de l'état de sécurité du réseau, de ses attitudes mentales, des croyances des autres agents et de l'évolution du système voisin (les autres agents).

5. Modèle d'information

Dans cette section, nous allons décrire le modèle d'information, qui repose sur l'architecture BDI [5][6]. Ce modèle représente les attitudes mentales de l'agent de sécurité.

5.1 Base de connaissances

La base de connaissances de l'agent contient deux types de connaissances :

1. les ***connaissance à caractère immédiat*** qui représentent les observations faites par l'agent sur son environnement. Leur validité a une durée de vie limitée dans le temps. Ces connaissances sont les événements de sécurité produits dans le réseau et observés par l'agent
2. les ***connaissances à caractère permanent*** qui représentent les connaissances nécessaires pour gérer la sécurité du réseau telles que la liste des utilisateurs connus/ groupes d'utilisateurs, la liste des machines connues, la liste des adresses connues (internes/externes, local/intranet/extranet), les adresses interdites, réservées et impossibles, la liste des utilisateurs ayant la fonction d'administrateur, la liste des administrateurs par machine, etc.

5.2 Les attitudes mentales

5.2.1 Croyances

Les croyances représentent la perception d'un agent sur le comportement du réseau et de son état de sécurité. Elles désignent aussi les connaissances qu'il a sur les autres agents et sur lui-même. Nous distinguons ainsi trois types de croyances:

- les ***croyances personnelles*** qui expriment les connaissances de l'agent sur son propre état (les informations le concernant, notamment le domaine qu'il doit surveiller) ;
- les ***croyances relationnelles*** qui représentent ce que sait l'agent des autres agents avec qui il communique. Ce sont donc toutes les informations (rôle, compétences,...) dont il a besoin pour communiquer avec eux;
- et les ***croyances environnementales*** qui regroupent les *croyances environnementales locales* et les *croyances environnementales des autres*. Les *croyances locales* désignent ce que l'agent croit sur le comportement et l'état de sécurité du réseau alors que les *croyances des autres* représentent les perceptions qu'ont les autres agents du réseau. Dans le cadre de ce travail, nous distinguons deux types de croyances environnementales:
    - les ***croyances schémas*** qui sont une description des schémas d'attaques à détecter, qui ne sont instanciées que lors de l'envoi d'un but ;
    - et les ***croyances scénarios*** qui représentent les suites d'événements de sécurité qui se sont produites dans le réseau. Une *croyance scénario* est associée à une ou plusieurs *croyances schémas.* Les *croyances scénarios* ont une validité temporelle qui dépend de la validité temporelle des événements constituant la suite d'événements de sécurité. Cette validité temporelle permet de traiter ces croyances et d'archiver celles qui ne sont plus valides temporellement.

5.2.2 Buts

Les buts représentent l'état que doit atteindre l'agent ; en l'occurrence ses objectifs. Nous distinguons trois types de buts :

- les ***buts de surveillance*** qui permettent de surveiller des activités spécifiques, par exemple les activités d'un certain utilisateur, ou les activités entrantes,…;
- les ***buts informationnels*** qui permettent de récupérer des informations spécifiques sur l'état de sécurité du réseau, par exemple les attaques détectées durant une période de temps, les utilisateurs suspects, les connexions courantes externes,… ;

- et les ***buts de détection*** qui permettent de spécifier les attaques à détecter et les mesures à prendre si une attaque est détectée. Ce sont les buts les plus importants dans le cadre de la détection d'intrusions. Un *but de détection* permet d'instancier une *croyance schéma*.

5.2.3 Intentions

Les intentions représentent le plan d'actions que devra exécuter l'agent lorsqu'il aura détecté une attaque. Cela désigne par exemple, l'envoie de messages/d'alarmes à l'officier de sécurité ou à l'agent gestionnaire, la fermeture de la connexion établit par un attaquant, la reconfiguration du firewall,etc.

5.2.4 Suspicions

Cette attitude mentale, que nous avons introduit dans le cadre de la détection d'intrusions, exprime la suspicion qu'a un agent sur une *croyance scénario*. Lorsqu'un agent observe une séquence d'événements qui ne correspond ni à une séquence normale, ni à une séquence d'attaque alors il l'identifiera comme une séquence suspicieuse. Pour confirmer que cette suspicion est une attaque, il faudra à l'agent un complément d'informations ou de confirmations de la part d'autres agents. L'agent pourra dans ce cas dire aux autres agents: "je *suspecte* que cette séquence d'événements soit une attaque". Une *suspicion* est associée à une *croyance schéma* et est le résultat de l'analyse d'une *croyance scénario* par rapport à la *croyance schéma*.

6 Implémentation

Le modèle d'agent présenté a été implémenté en utilisant la plate-forme DIMA [7]. Cette plate-forme, caractérisée par une architecture d'agent modulaire, propose une extension du comportement unique d'un objet actif en un ensemble de comportements.
Dans le système implémenté, le comportement de l'agent peut se résumer en :

- lorsqu'il reçoit un *but de détection*, il met à jour l'ensemble de classes d'événements à filtrer.
- Dès lors qu'un événement se produit, il est filtré par le module de filtrage et envoyé au module de délibération.
- Le module de délibération mets ensuite à jour les *croyances scénarios* de l'agent et teste si elles correspondent à une *croyance schéma*. Si une *croyance schéma* est identifiée, un plan d'actions (*intentions*) est envoyé au module d'interaction afin qu'il soit exécuté.

Le prototype implémenté détecte des attaques connues tels que "doorknob rattling", "ping sweep" et "ICMP flooding".

7 Conclusion

Dans ce papier, nous avons présenté un système multi-agents pour la détection d'intrusions. Cette application, nous a permis de montrer l'utilité des méthodologies proposées par la communauté multi-agents [8]. D'autre part, nous avons utilisé le modèle théorique BDI et l'appliquer à un cas pratique. Cette application n'était pas aussi simple que la première étape "définition des structures organisationnelles". Elle a nécessité beaucoup de travail de conception et nous a notamment montré que le modèle BDI est trop théorique, seuls ses concepts de base sont réutilisables dans une application réelle.

Le système implémenté permet de détecter des attaques connues par les agents. Nous travaillons actuellement sur l'adaptation du comportement de ces agents pour l'apprentissage de nouvelles attaques pour réagir aux attaques non connues.

Bibliographie

[1] L.T. Heberlein, B.Mukherjee, et K.N.Levitt, "Network Intrusion Detection", IEEE Network Journal, pp. 26-41, May/June 1994.
[2] Maj.Gregory B. White, Eric A. Fisch, et Udo W. Pooch, "Cooperating Security Managers: A Peer-Based Intrusion Detection System", IEEE Network journal, pp. 20-23, January/February 1996.
[3] K. Price, "Intrusion Detection Pages", Université de Purdue, 1998.

http://www.cs.purdue.edu/coast/intrusion-detection/ids.html.
[4] J. Ferber, "Les Systèmes multi-agents, Vers une intelligence collective", Inter Editions 1995.
[5] A. S. Rao et M. P. Georgeff, "Modeling Rational Agents within a BDI-Architecture", Technical Note 14, 1991.
[6] A. S. Rao et M. P. Georgeff, "BDI Agents: From Theory to Practice", Technical Note 56, 1995.
[7] Z. Guessoum, "Un environnement opérationnel de conception et réalisation de systèmes multi-agents", Thèse de Doctorat, Université de Paris VI, France, 1996.
[8] J. Ferber et O. Gutknecht , " A meta -model for the analysis and design of organizations in multi-agent systems", ICMAS'1998.