Safim@ge : projets de recherche

Alain Maillet[1], Fred Rivard[2], Remi Lehn[3] ,Pierrick Bruneau[3] ,Florent Autrusseau[4]

[1] Alcatel-Lucent, Le Mail 44700 Orvault

[2] Industrial Software Technology, 1 rue de la Nöé, 44321 Nantes Cedex, France

[3] LINA (équipes COD et Atlas-GRIM), École polytechnique de l'Université de Nantes, rue C. Pauc 44300 Nantes

[4] IRCCyN, École polytechnique de l'Université de Nantes, rue C. Pauc 44300 Nantes

alain.maillet@alcatel-lucent.fr

fred.rivard@ist-eu.com

{remi.lehn,pierrick.bruneau,marc.gelgon,fabien.picarougne}@univ-nantes.fr

florent.autrusseau@univ-nantes.fr

1.Introduction

Le projet Safim@ge , démarré en Février 2007, consiste en la réalisation d'une plate-forme matérielle et logicielle d'inspection de paquets IP en temps réel (DPI) dans des flux à haut débit Il propose également l'étude et le développement d'applications prouvant le potentiel de la plate-forme. L'applications traitant de l'interception légale IP est développée en priorité ceci pour répondre le plus rapidement possible aux attentes prioritaires du projet ANR de sécurité globale

N.b. Les fonction DPI offertes par cette plateforme permettent d'analyser en temps réel le contenu des échanges sur l'internet : par exemple le contenu des mails, des conversations, d'échanges P2P, l'identité des intervenants, la recherche de marquages/tatouages sur tous types de données (images, vidéo, logiciel, …) etc.

Les articles développés ci-après par les différents partenaires du projet permettent de présenter succinctement l'avancement du projet pour les aspects plateforme et application interception légale IP et surtout de présenter les programmes de recherche en cours associés au projet Safim@ge.

2.Avancement du projet

En accord avec la construction initiale du projet nous disposons depuis Novembre 2007 dans les locaux d'Alcatel-Lucent d'Orvault d'un démonstrateur (au form factor PCIx) utilisant une version intermédiaire du processeur de service réseau cible (OCTEON 3860 avec 16 cores) et disposant dès maintenant les services suivants :

- Plateforme de « Deep packet inspection (DPI ») offrant des débits variant de 1 GB (Niveau 7) jusqu'à d' 10 Gb (Niveau 3)
- Application d'interception légale IP (gestion incluse) prenant en compte une bonne partie des protocoles les plus utilisés.
- Shop cost de la plateforme très bas par rapport aux performances atteintes

Ce premier aboutissement rapide a été en partie obtenu via le portage du classifieur de flux IP (AFC) de la société QOSMOS sur le processeur Octeon de Cavium. N.b : cette opération de portage a fait l'objet d'un contrat d'exclusivité entre Alcatel-Lucent et Qosmos .

En parallèle de ces développements les partenaires du projet (IST, IRCCyN et LINA) poursuivent également leurs travaux de recherche pour enrichir les services offerts par la plateforme :

- IST analyse l'introduction d'une machine JAVA virtuelle très performante sur la plateforme Safim@ge
- L'IRCCyN mène ses travaux de recherche sur le tatouage des données appliqués sur la plateforme Safim@ge
- LINA mène des travaux de recherche sur la reconstitution de sessions et la classification des données multimédia appliqués sur la plateforme Safim@ge

3.JVM optimisée pour Safim@ge (IST)

Une machine virtuelle Java [4] est un processeur capable d'exécuter des fichiers de codes binaires (bytecode) générés à partir de sources Java. Ce processeur est composé de plusieurs composantes inter-dépendantes :

- un moteur d'exécution d'instructions.
- un gestionnaire de mémoire qui alloue les objets et s'occupe de leur libération de manière automatique grâce au Garbage Collector (GC).
- un ordonnanceur de tâches (scheduler) qui permet l'exécution en parallèle et la synchronisation de threads Java.
- une interface entre le monde natif et le monde Java. L'appel de code natif, tel que le C, depuis Java s'effectue via cette interface.

Une machine virtuelle réalise une abstraction de la plate-forme d'exécution matérielle permettant ainsi la portabilité au niveau binaire d'applicatifs Java et leur exécution dans d'excellente condition de sécurité.

La machine virtuelle sur la plateforme Safim@ge doit permettre le développement rapide de services à forte valeur ajoutée.

IST développe la MicroJvm-Safimage qui est une machine virtuelle Java dédiée à la plate-forme Safimage. Dans ce sens elle est optimisée pour fonctionner sur l'Octeon (processeur MIPS 16 coeurs) et utilise les capacités matérielles spécifiques de cette architecture destinée aux applications « réseaux ». Elle implémentera un ensemble de fonctionnalités génériques au Java embarqué (CLDC/MIDP) et offrira également des services spécifiques à la plate-forme.

3.1Une MicroJvm optimisée pour l'Octeon

L'un des enjeux du projet est l'exploitation, par la MicroJvm-Safimage, des ressources de l'Octeon et cela de manière transparente pour le développeur.

L'Octeon offre deux niveaux de mémoire cache (L1 et L2). Chaque coeur possède son propre cache L1 de quelques dizaines de kilo-octets. Afin d'optimiser l'exécution de la MicroJvm-Safimage sur un coeur, le maximum de code de la MicroJvm-Safimage devra pouvoir tenir dans ce cache.

Le cache L2 est une mémoire très rapide partagée entre tous les coeurs mais sa faible quantité (2 à 4 Mo) en fait une ressource critique. Au travers de différents mécanismes l'Octeon offre la possibilité de partitionner le cache entre les différents coeurs. Le scheduler quand à lui devra distribuer les threads sur ces différents coeurs. Les algorithmes de répartition de charges devront permettre une utilisation optimal du cache. Pour cela, les threads utilisant des ressources communes sont affectés au même coeur.

Les cas d'utilisation de la plate-forme Safimage entraînent une durée de vie longue pour certains objets, ce qui constitue une donnée très structurante pour la réalisation du garbage collector (GC). Par exemple, un GC générationnel permet une segmentation des objets en fonction de leur durée de vie. Les objets les plus récents sont analysés par le GC régulièrement alors que les objets les plus anciens le sont plus rarement. Les objets ayant une longue durée de vie ne pénalisent donc pas le système et les objets ayant une courte durée de vie sont rapidement libérés. Afin de satisfaire les contraintes temps réel du système, le GC est également incrémental pour permettre son exécution en parallèle de l'application.

3.2Génération d'un Java accéléré

Plusieurs techniques existent afin d'accélérer l'exécution de code Java : l'optimisation du bytecode, la compilation du bytecode en binaire natif ou la traduction du source Java en un langage natif tel que le C.

La MicroJvm-Safimage aura un double niveai d'optimisation : soit au niveau bytecode (SOAR), soit au niveau natif (FNI/IceTea). Le SOAR (Smart Optimizer And Romizer) est un outil qui retraite le code binaire Java, le compactant et l'optimisant pour la MicroJvm-Safimage. Par exemple, seules les classes et méthodes nécessaires à l'application sont embarquées.

Pour accélérer le code identifié comme critique par le développeur, il est possible de convertir en librairies natives du code Java source en IceTea source. IceTea est un langage objet ayant une syntaxe Java. Il peut être compilé en C ou en directement en code machine natif. Cette technique d'accélération permet d'avoir du code Java aussi rapide que du code asm/C.

La communication entre le monde Java et le monde natif est pris en charge par une passerelle appelée Fast Native Interface (FNI) [5]. Depuis le monde Java, des méthodes IceTea peuvent être appelées en vue d'accéder à des fonctions spécifiques du matériel ou bien afin d'accélérer l'exécution Java. Depuis les parties de code IceTea, les méthodes et objets Java sont également manipulables via FNI très simplement en utilisant les syntaxes habituelles, la gestion de la "frontière Java-natif(C/IceTea/asm)" étant totalement transparente pour l'ingénieur qui n'a pas à se soucier des problématique liées à la gestion automatique de la mémoire sous le contrôle du GC de la MicroJvm-Safimage

4.Tatouage des données (IRCCyN)

Nous avons été témoins au cours des dernières années d'une explosion très importante des données numériques. Le nombre d'ordinateurs "personnels" a augmenté de façon très significative et l'accès aux connections haut débit a rendu la distribution des données numériques très facile et rapide. En outre, les équipements analogiques sont à présent remplacés par leurs successeurs numériques. La protection de contenus numériques est d'ores et déjà cruciale. La protection des données numériques se fait par le biais du tatouage. Le tatouage doit être inséré de façon robuste, il ne doit pas pouvoir être supprimé sans provoquer une dégradation des données multimédia.

Le tatouage (appelé watermark) peut par exemple être utilisé à des fins de protection de droits d'auteurs, en insérant des informations sur le créateur des données, il peut être utilisé pour prouver des droits de propriété dans un tribunal. Une autre application intéressante du tatouage et le suivi de copies illicites (appelé fingerprinting).

Ici, le créateur des données insère de façon secrète, des informations relatives aux destinataires (aux clients) des contenus. Si des copies illégales sont trouvées sur des réseaux, il devient alors aisé de déterminer la source des copies illégales. Parmi les autres applications, nous pouvons citer les systèmes de contrôle automatisé pour la diffusion radio/TV, authentification des données, ou encore la transmission de données secrètes (stéganographie). Chaque application du tatouage dispose de ses propres contraintes. Néanmoins, les exigences la plus répandue demeurent l'invisibilité des données insérées, la capacité du tatouage, ainsi que la robustesse de la marque qui doit rendre les données fortement dégradées après une tentative de suppression du tatouage.

4.1Tatouage de documents multimédia

Notre objectif est de proposer un algorithme de tatouage opérant dans le standard de compression vidéo H.264/AVC [1]. Ce dernier est le standard de compression vidéo le plus récent. Il a été proposé par Video Coding Experts Group (VCEG), de l'ITU-T et le Moving Picture Experts Group (MPEG) de l'ISO/IEC. Il utilise des outils de compression de la littérature et propose des améliorations significatives pour une large gamme d'applications, tels que la visio-phonie, la visio-conférence, la télévision, le stockage, le streaming vidéo, le cinéma numérique et bien d'autres encore. En comparaison avec les standards précédents, tel que MPEG2, MPEG4 apporte de nouvelles caractéristiques. Par exemple, contrairement aux standards précédents, MPEG4/AVC ne propose pas uniquement une prédiction temporelle (modes de prédiction inter, I,P,B), mais apporte aussi une prédiction spatiale (modes de prédiction intra, I,P,B). Afin d'augmenter le taux de compression, de nombreuses composantes de MPEG4/AVC sont prédites, comme les macroblocs, les modes de prédictions, les vecteurs de mouvement, etc. De ce fait, la complexité de MPEG4 est nettement plus élevée que celle des standards précédents. Le tatouage de vidéos H.264 est un défi, car très peu de redondance est présente dans un tel standard [2].

Nous avons opté pour les outils officiels (JM software) pour implémenter la technique de tatouage [3]. Afin d'ajouter l'algorithme de tatouage dans le codeur JM, et la technique de détection dans le décodeur JM, nous proposons une analyse tant du codeur que du décodeur, et expliquons en détail la façon d'intégrer nos fonctions dans ces programmes. Ensuite, deux nouvelles techniques de tatouage nommées "Pair/Impair" et "système linéaire" seront présentées.

4.1.1Tatouage « Pair/Impair »

Le but est ici de modifier les coefficient résiduels pour les rendre soit pairs, soit impairs. L'avantage d'un tel algorithme est bien sur sa faible complexité, la capacité importante qu'il fournit, et son importante flexibilité. Cependant, l'inconvénient est la faible robustesse. Une telle technique pourrait résister à des attaques du type traitement d'image/vidéo, mais pas à un ré-encodage de la vidéo. Cet algorithme serait par conséquent adapté à une problématique de fingerprinting ou de stéganographie, mais ne permettrait pas une application à la protection des droits d'auteurs.

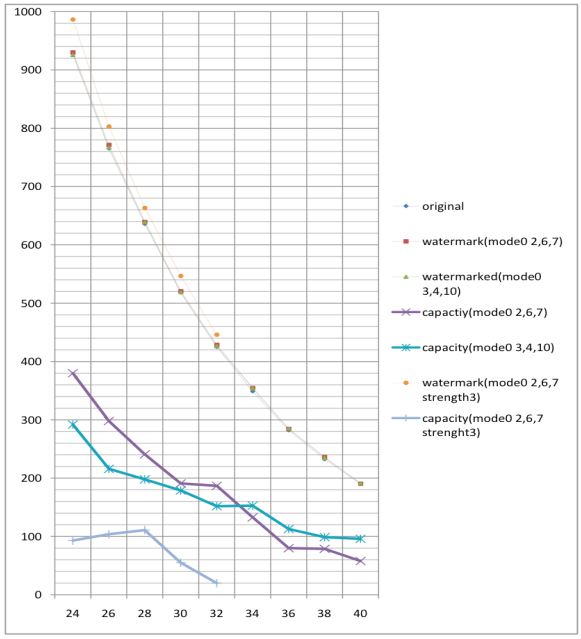


FIG. 1 : Capacité et bit-rate pour différents modes de prédiction.

4.1.2La résolution du système linéaire

Notre but ici est de conserver le mode de prédiction, afin de maintenir le bit-rate inchangé. Un système linéaire est établi basé sur le principe de la prédiction spatiale et la transformée entière.

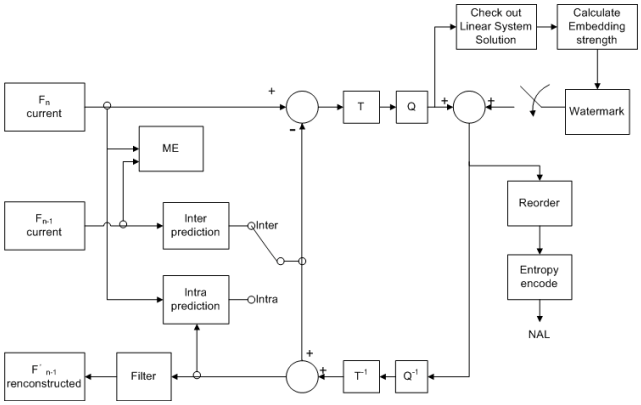
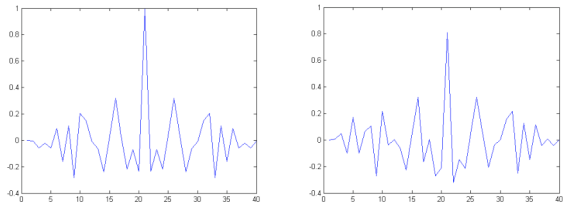


FIG. 2 : La technique de tatouage proposée

Ce système linéaire est utilisé pour déterminer les coefficients à modifier, ainsi que la force pouvant être appliquée sur ces coefficients. Le tatouage est inséré selon une technique basée sur la corrélation. Une telle insertion devrait conserver le bit-rate, ainsi que les modes de prédiction. De plus, la robustesse face au ré-encodage devrait être sensiblement améliorée. Cette méthode de tatouage serait particulièrement adaptée dans une problématique de protection des droits d'auteurs, ou une robustesse aux distorsions est fortement souhaitable.



(a) *(b)*

FIG. 3 : Résultats de corrélation après ré-encodage. *(a)* Qp=24, *(b)* Qp=28.

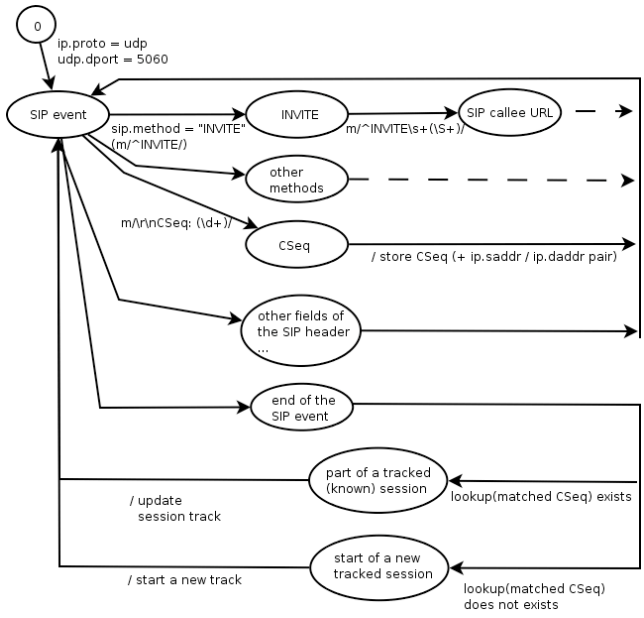
5.Reconstitution de session (LINA)

La reconstitution de sessions est une des fonctions importantes pour l'inspection passive de trafic. Elle a pour objectif de reconstituer les messages générés par l'utilisation de chaque application par chaque utilisateur à partir du trafic capturé sous forme de trames ou de paquets individuels. Les débits envisagés, qui sont, dans notre cas, ceux d'équipements de réseaux d'opérateurs (de l'ordre de la dizaine de Gbits/s.) et la nécessité d'une réponse en temps réel impose de placer le problème dans le cadre de l'analyse de flux de données (*data streaming*) pour lesquels un certain nombre de problèmes et méthodes ont été définies [6]. Un des principes fondamentaux de ces approches est de traiter des flux de données séquentiels en temps réel et sans stockage a priori de l'ensemble des données. Il existe des méthodes génériques efficaces pour ce type de problèmes, telles que l'utilisation d'automates à états finis résultats de la compilation d'expressions rationnelles [7,8].

5.1Principe de la solution

Un des enjeux du suivi de sessions pour le projet est de prendre en charge des protocoles à plusieurs niveaux, au dessus du niveau transport, à des fins multiples : servir de support aux autres modules -de tatouage ou d'analyse de contenus multimédia par exemple- du projet, dans ce cas, il s'agit d'un suivi principalement de niveau session, mais également de servir de support à la prise de décisions de haut niveau, dans ce cas, il est nécessaire de reconstituer le plus fidèlement possible des messages applicatifs afin d'en extraire les informations les plus pertinentes pour les décideurs. Un certain nombre d'approches existent pour l'identification de protocoles [9] ou la classification de trafic [10]. Contrairement aux approches classiques, nous partons cependant de l'hypothèse que nous devons traiter des flux de données ou des messages au niveau applicatifs et non des paquets indépendants. Par ailleurs, nous prenons en compte que nous avons un ensemble de protocoles applicatifs en constante évolution nécessitant un dispositif facile à faire évoluer, basé sur un certain nombre de comportement applicatifs génériques (applications synchrones, échange de fichiers pair-à-pair, client-serveur, par exemple). L'intégration de dispositifs d'analyse de nouveaux protocoles se fait alors par rétroconception assistée de méthodes de fouilles de flux de données et par implémentation de spécifications publiques. La figure 4 correspond à un extrait d'un automate permettant un suivi de session SIP. L'objectif est donc de fournir un ensemble d'outils permettant de construire facilement de tels nouveaux automates, adaptés à chaque nouveau protocole.

FIG. 4 : Extrait d'automate pour le suivi de sessions SIP.



6. Classification de données multimédia (LINA)

La surveillance des messages transitant sur le réseau, au delà des attributs liés à l'expéditeur ou le(s) destinataire(s), implique l'examen du contenu même du message. Une part importante des contenus qu'il est important de surveiller est de nature multimédia audiovisuelle, soit parce que le contenu visuel ou acoustique est initialement l'objet d'intérêt, soir parce qu'ils un vecteur de dissimulation d'information dont la surveillance est plus aisée. Le premier cas peut consister en des images au contenus illicites, tandis que l'exemple type du second cas est typiquement illustré par les pourriels contenant du texte dans des images, avec des altérations visuelles visant à rendre la discrimination délicate, illustrent typiquement le second cas. La classification de telles données procède généralement par un mécanisme inductif, c.a.d. requérant une aptitude à la généralisation à partir d'un ensemble fini d'exemples d'apprentissage, mécanisme généralement construit sur des critères statistiques.

Le projet Safimage est centré sur une plateforme ultra-rapide de traitement des flux. L'objectif du projet, relatif à la classification des données multimédia, est l'élaboration de techniques d'apprentissage/classification rapides, typiques de ce qui pourrait être mis en oeuvre sur la plateforme visée. Parce qu'on travaille sur des flux, on s'intéressera à des solutions d'apprentissage incrémentale, et parce qu"un opérateur de surveillance est susceptible d'interagir avec le système, on privilégiera une approche semi-supervisée.

6.1Principe de la solution

L'objectif de cette tâche est de montrer l'aptitude de la plateforme à traiter diverses applications potentielles surveillant des données multimédia. Aussi, nous considérons un cas assez général, commun à de très nombreuses applications, où il s'agit de réaliser une classification dans un espace multivarié d'attributs.

Dans les premiers travaux menés, nous privilégions une approche probabiliste. Entre autres avantages, elle permet de préserver l'incertitude sur les conclusions et d'en tirer parti, de manière bien formalisée, dans la phase de décision. La ou les classes d'intérêt sont modélisées par un mélange de loi gaussiennes, dont les paramètres sont estimés sur la base d'exemples, par des algorithmes de type EM. Les travaux en cours présentent les particularités suivantes :

- une estimation semi-supervisée a été introduite, permettant à tout instant à l'opérateur d'affecter des données à des classes, par exemple pour rectifier une classification automatique erronée ; l'apprentissage bénéficiera de cette réaction

- au delà du critère du maximum de vraisemblance, nous privilégions une estimation bayesienne du mélange, en particulier par l'approximation variationnelle, qui permet théoriquement de gérer efficacement (précisement et à faible coût) la détermination du nombre de composantes dans le mélange gaussien, et par conséquent l'aptitude du mélange à bien généraliser, si on considère le cas supervisé.

- une estimation incrémentale du modèle est réalisée, c.a.d. que le modèle peut être mis à jour de manière efficace, quand de nouvelles donnnées de la classe modélisée sont disponibles. L'approche que nous avons retenue s'y prête, car elle fonctionne par optimisation locale avec un mécanisme de prédiction/ajustement.

- Nous examinons la parallélisation de cette technique, à fin d'accélération : en particulier, la manière dont on va pouvoir fusionner, à faible coût, plusieurs modèle de la (ou les) classe(s) qu'on souhaite modéliser, pour que cette agrégation améliore l'estimation du modèle.

Références

[1] ankaj Topiwala, Gary J. Sullivan and Luthra Ajay. The h.264/avc advanced video coding standard:overiew and introduction to the fidelity range extensions. In SPIE Conference on Applications of Digital Image Processing XXVII.

[2] A.T.Ho, D.He, G.Qiu, P.Marziliano and Q.Sun. A hybird watermarking scheme for h.264/avc video. In Proc.17th Int.Conf.Pattern Recognition.

[3] H.264 Reference Software Group. http://iphome.hhi.de/suehring/html/. Online, 2004.

[4] *The Java™ Virtual Machine Specification*, Second Edition by Tim Lindholm and Frank Yellin. Addison-Wesley, 1999, ISBN 0-201-43294-3

[5] Fast Native Interface, Industrial Software Technology, http://www.ist-eu.com/ej/070275-FNI-IST-SPE-ESR003.pdf

[6] S. Muthukrishnan, *Data Streams: Algorithms and Applications*, 2003, http://athos.rutgers.edu/~muthu/stream-1-1.ps

[7] S. Kumar, B. Chandrasekaran, J. Turner, G. Varghese, *Curing Regular Expressions Matching Algorithms from Insomnia, Amnesia, and Acalulia*, tech. rep. Washington University in St. Louis, dept. of Comp. Sc. and Engineering, 2007, http://cse.seas.wustl.edu/Research/FileDownload.asp?744

[8] K. van Reeuwijk, H. Bos, *Ruler: high-speed traffic classification and rewriting using regular expressions*, tech. report, Vrije Universiteit Amsterdam, 2006, http://www.cs.vu.nl/~herbertb/papers/ruler_IR-CS-027.pdf

[9] G. Shu, D. Lee, *Network Protocol System Fingerprinting - A Formal Approach*, 25th IEEE Int. Conference on Computer Communications, 2006

[10] M. Crotti, M. Dusi, F. Gringoli, L. Salgarelli, *Traffic Classification through Simple Statistical Fingerprinting*, ACM SIGCOMM Computer Communication Review, vol. 37, no. 1, Jan. 2007, http://www.sigcomm.org/ccr/drupal/files/p7-v37n1b-crotti.pdf