Zeitschrift: Bulletin Electrosuisse
Herausgeber: Electrosuisse, Verband für Elektro-, Energie- und Informationstechnik
Band: 95 (2004)
Heft: 19

Artikel: La qualité de service dans un réseau local sans fil
Autor: Robert, Stephan / Emery, Vincent / Hasanovic, Mesud
DOI: https://doi.org/10.5169/seals-857989

La qualité de service dans un réseau local sans fil

Expériences sur une plateforme réelle

La récente évolution et le déploiement réussi des réseaux locaux sans fil dans le monde ont ouvert la voie pour un accroissement des activités de recherche, développement et standardisation dans ce domaine. Les mécanismes mis en œuvre deviennent de plus en plus complexes, ceci pour assurer des fonctions exigées par certaines applications: qualité de service, sécurité, mobilité. Cet article va montrer, au travers d'expériences menée sur une plateforme réelle, quelles sont les limitations actuelles de la qualité de service avec le matériel disponible sur le marché et d'autre part comment elle est affectée par différents schémas de sécurité.

Stephan Robert, Vincent Emery, Mesud Hasanovic

Les cinq dernières années, nous avons assisté à l'émergence des réseaux locaux sans fil WLAN (Wireless Local Are Networks) dans les entreprises, chez les privés et dans les lieux publics. Il y a une très grande variété de produits WLAN disponibles sur le marché, ce qui les a rendu aussi populaires que les réseaux câblés Ethernet. Néanmoins, pour une large palette d'applications requérant une certaine qualité de service ou QoS (Quality of Service), le défi est de taille pour les réseaux sans fil. Dans les entreprises, les réseaux WLAN présentent une alternative flexible et complémentaire au réseau câblé. Il y a donc également une motivation importante pour continuer d'augmenter le débit des réseaux locaux sans fil. Dans les accès publics (Hotspots) on attend des réseaux WLAN qu'ils puissent fournir un accès Internet à haut débit. Dans les environnements privés, les défis sont également de taille car on veut pouvoir offrir simultanément la distribution de la vidéo à haute définition, un accès Internet à haut débit, la téléphonie à l'intérieur de la maison. De telles applications demandent de l'efficacité, de la robustesse, un certain niveau de sécurité, et de la QoS, aux réseaux WLAN.

Protocoles utilisés pour les applications multimédia

Les applications multimédia audio et vidéo ont besoin de protocoles au niveau application (selon le modèle OSI). Le protocole le plus utilisé est le protocole RTP (Real-Time Transport Protocol) à cause de ses fonctionnalités spécifiques au multimédia. De plus, il fonctionne au dessus de UDP (User Datagram Protocol) qui est standard dans le monde Internet. Les applications sont en général divisées en deux catégories: streaming et conferencing. La première catégorie a pour but de livrer des flots audio ou vidéo d'un serveur à un client. La seconde catégorie implique une interaction entre deux entités. Nous avons testé les deux catégories avec la vidéo pour la première et la voix sur IP/vidéoconférence pour la seconde.

Les exigences de base pour un protocole multimédia est que les applications similaires puissent interagir ensemble. Pour l'audio comme pour la vidéo, il existe plusieurs schémas de codage. RTP est un protocole qui donne le choix entre plusieurs schémas de codage. De plus, il est capable de déterminer une relation temporelle parmi les données reçues, ce qui lui permet de les redonner à l'application au temps approprié après les avoir stockées en mémoire. Il est également capable de synchroniser l'audio et la vidéo d'un même émetteur. Une autre fonction importante est celle de l'indication de la perte de paquets. Les applications en temps réel ne sont en général pas disposées pour utiliser TCP (Transport Control Protocol) car les données qui seraient retransmises à la suite de leur perte arriveraient trop tard et ne seraient plus utiles. Les applications doivent donc prendre des dispositions lorsque le réseau perd des paquets. MPEG par exemple va prendre des dispositions lorsque des paquets sont perdus. Une autre fonction importante de RTP est l'indication des limites des trames. Pour une application vidéo, il est utile de savoir quel ensemble de paquet correspond à une trame. En audio on arrive ainsi à discriminer les temps de silence des temps actifs. Une dernière fonction de RTP concerne l'identification des utilisateurs, qui est plus pratique que les adresses IP (comme par exemple utilisateur@domaine.ch). Le protocole doit rester peu gourmand en ressources réseau, ceci notamment à cause des paquets qui sont petits et ne doivent pas introduire de grands retards. Les grands paquets vont introduire des retards à cause de la «packetisation». C'est d'ailleurs pour ceci qu'ATM (Asynchrone Transfert Mode) a choisi un format de cellule petit (53 octets). Le protocole de contrôle en temps réel RTCP (Real-Time Transport Protocol) a comme

AES	Advanced Encryption Standard
ATM	Asynchronous Transfer Mode
IP	Internet Protocol
IPSec	IP Security
MPEG	Motion Picture Expert Group
RTCP	Real-Time Transport Control Protocol
RTP	Real-Time Transport Protocol
RTSP	Real-Time Streaming Protocol
SAP	Session Announcement Protocol
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SMS	Short Message Service
SQL	Structured Query Langage
TCP	Transport Control Protocol
TKIP	Temporal Key Integrity Protocol
UDP	User Datagram Protocol
WEP	Wired Equivalency Protocol
WiFi	Wireless Fidelity
WLAN	Wireless Local Area Networks
WEP	Wired Equivalent Privacy

objectif de transmettre des paquets de contrôle périodiquement à tous les participants d'une session. C'est un protocole de contrôle des flux RTP qui permet de véhiculer des informations sur les participants d'une session. Les protocoles RTP et RTCP se situent au niveau de l'application et doivent utiliser des protocoles de transport sous-jacents, TCP ou UDP. Généralement, c'est UDP qui est utilisé.

Maintenant, nous allons supposer que nous aimerions initier une conversation téléphonique ou par vidéoconférence avec un certain nombre de participants à un moment donné. Admettons que nous ayons décidé d'utiliser une adresse IP de multicast pour la transmission des données et de les envoyer avec RTP sur UDP. Comment allons-nous informer les participants? Par messagerie électronique? L'IETF (Internet Engineering Task Force) a créé un groupe de travail pour étudier cette problématique. Les protocoles définis dans ce contexte varient en fonction des applications. Pour MBone (vidéoconférence), on utilise SDP (Session Description Protocol) et SAP (Session Announcement Protocol). Pour la téléphonie sur Internet, on utilise SIP (Session Initiation Protocol). Sur notre plateforme, nous avons utilisé SIP.

SIP est un protocole de signalisation point-à-point utilisant le modèle client – serveur. Il permet d'établir rapidement des liaisons téléphoniques sur un réseau informatique équipé de téléphones adaptés (téléphones IP). Il est possible d'établir des liaisons entre des téléphones normaux et des téléphones IP à condition d'avoir une passerelle entre les deux types de réseaux. SIP offre plusieurs services en plus de l'établissement de liaisons, comme par exemple la mise en attente, le transfert et la déviation d'appels. Avec ce protocole est introduit une nouvelle notion de «mobilité personnelle». Il est ainsi possible d'appeler une même personne successivement sur son téléphone fixe de son travail, son téléphone portable et finalement sur son téléphone privé par exemple.

Le protocole SIP (www.sipcenter.com) est un protocole de signalisation uniquement, au niveau de l'application. Il ne va pas transporter la voix. D'autres protocoles le feront, comme RTP/RTCP, d'après ce qui a été vu plus haut. Pour résumer, l'agent SIP a deux fonctions de base:

- écouter les messages SIP qui lui sont destinés,
- envoyer des messages SIP en suivant les instructions de l'utilisateur.

Le serveur SIP va relayer les messages pour essayer d'atteindre l'utilisateur plutôt que de rediriger le trafic vers une adresse IP ou vers une machine.

Problèmes de sécurité

Une difficulté concernant la sécurité des réseaux WLAN, ou WiFi (Wireless Fidelity) vient de ce que tout le monde dans le voisinage peut l'utiliser si ce dernier n'est pas correctement protégé. Il est conseillé de suivre les instructions du réseau WiFi pour se prémunir des attaques mais nous verrons qu'il n'est pas possible d'être complètement protégé avec la technologie actuelle au niveau de la liaison de données. Les réseaux IEEE 802.11b proposent un système de sécurité au niveau de la liaison de données, appelé WEP (Wired Equivalency Protocol) qui utilise un schéma de cryptage utilisant l'algorithme RC4. Or il a été démontré par Fluher, Mantin et Shamir en 2001 que cet algorithme comporte certaines failles. Tous les détails sont reportés dans [4,7]. Il faut noter que les réseaux de type IEEE 802.11g utilisent un autre schéma de cryptage, AES (Advanced Encryption Standard, csrc.nist.gov). Pour réaliser une attaque contre un réseau WiFi crypté, il suffit par exemple de charger un petit utilitaire gratuit appelé «Airsnort» (airsnort.shmoo.com) développé par le groupe «Shmoo» et de le faire fonctionner sur une plateforme appropriée (l'utilitaire a été développé sur une plateforme Linux). Quand le réseau à analyser est déterminé il suffit d'attendre que le logiciel capture un certain nombre de paquets intéressants qui vont permettre de briser la clé utilisée. Chaque fois que 10 paquets intéressants sont collectés, une clé de cryptage est calculée et une fois que le nombre de paquets intéressants est suffisant, la clé est déterminée et affichée. L'expérience menée nous a permis de constater qu'il était possible de trouver une clé de cryptage d'une longueur de 64 bits après une heure environ (dépend de la structure de la clé) lorsque le trafic échangé est intense (900 paquets/seconde). En réalité, le trafic échangé entre la station de base et le client WiFi est bien moindre. Les clés de 128 bits peuvent être trouvées en quelques heures (5 à 15 heures environ).

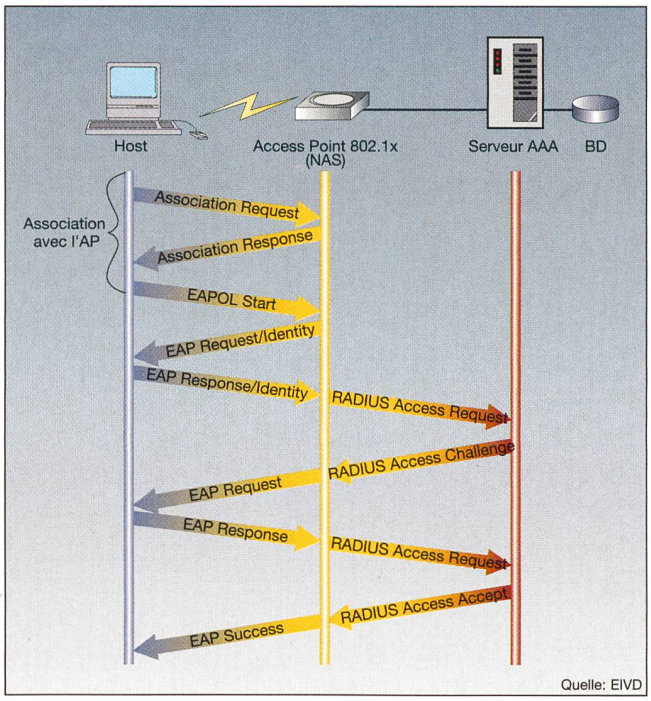

Figure 1 Schéma d'authentification global

La vérification de l'utilisateur est conseillée lorsque le propriétaire du réseau WiFi désire connaître l'identité des personnes qui utilisent son réseau. Outre l'identification au niveau de la liaison de donnée qui est effectuée à l'aide d'une clé mémorisée par le client WiFi, il est possible d'utiliser un serveur d'authentification qui exige par exemple un mot de passe (ou une clé, un certificat) à chaque utilisateur. Le serveur possède un acompte pour chaque utilisateur autorisé à utiliser les ressources du réseau. L'acompte enregistre les paramètres de connexion de chaque utilisateur (état et durée de la connexion). Une base de données enregistre toutes ces informations. On parle alors d'un schéma AAA pour «Authentification, Autorisation and Acounting». Un des protocoles qui a été mis sur pied dans la communauté Internet et qui est très utilisé s'appelle Radius (Remote Authentification Dial In User Service). Il est basé sur un mode opératoire client – serveur et est spécifié dans les RFC 2865 (Request For Comments) et RFC 2866 (www.ietf.org). La version que nous avons utilisée est basée sur Linux et se nomme FreeRadius (www.frontios.com). En général, une organisation va essayer de centraliser les informations relatives à ses clients à un endroit, ce qui est facilité par un serveur Radius associé à une base de données. Dans notre cas la base de données choisie est

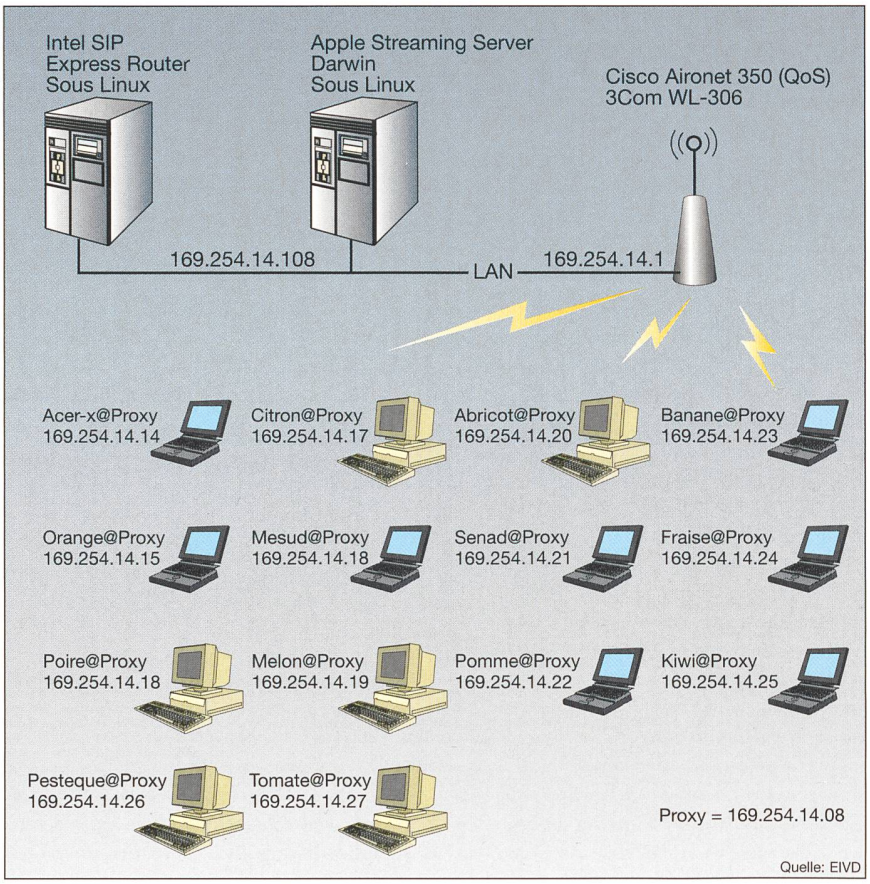

Figure 2 Plateforme de test
Plateforme de test pour les mesures de qualité de service effectuées avec du trafic voix et vidéo

de type MySQL (www.mysql.com) car déjà implémentée sous Linux. Il suffit d'installer, de configurer le serveur et de créer la base Radius. C'est ensuite avec des requêtes SQL (Structured Query Langage) qu'il sera possible de gérer les utilisateurs. Un interface graphique existe pour la base de donnée, ce qui en facilite son utilisation.

Les messages sont échangés entre le point d'accès et le serveur Radius et non entre l'utilisateur et le serveur. Lorsque un point d'accès est configuré pour utiliser Radius, chaque utilisateur qui désire se connecter doit lui transmettre ses données d'authentification. Ensuite, le point d'accès va envoyer ces données vers le serveur. Le paquet envoyé s'appelle Access Request et permet de faire une demande d'authentification. Les attributs présents dans ce paquet sont le nom d'utilisateur et le mot de passe (ou un autre identificateur). A la réception du message, le serveur vérifie le secret partagé avec l'utilisateur. Il s'agit d'une chaîne de caractères échangée préalablement de manière sûre (physiquement en général). Si le nom du client est valide, le serveur va vérifier son mot de passe, sinon la requête sera rejetée (d'autres critères peuvent être utilisés pour l'authentification comme l'adresse IP ou un numéro de port). Si le mot de passe est correct, le serveur va envoyer un défi à l'utilisateur à l'aide d'un paquet appelé Access Challenge. L'utilisateur reçoit un nombre pseudo aléatoire à crypter à l'aide d'un secret partagé avec le serveur, qui peut avoir plusieurs formes (Smartcard, clé publique gérée par des certificats). La réponse sera donnée au serveur à l'aide d'un paquet nommé Access Response. Ensuite le serveur va répondre avec un paquet qui sera soit Access Accept si la requête est acceptée ou Accept Reject si elle est rejetée. C'est alors que l'utilisateur peut accéder aux ressources que le réseau propose.

Réalisation de la plateforme

Une plateforme a été mise sur pied à l'Ecole d'Ingénieurs du Canton de Vaud (EIVD) sur laquelle il s'est agit de sélectionner du matériel qui soit capable de supporter la qualité de service pour des applications voix et vidéo. La norme 802.11e qui implémente cette fonctionnalité est en phase terminale de spécification mais aucun produit l'intégrant n'est encore officiellement disponible sur le marché. Par contre, il existe un certain nombre d'alternatives pour remédier à ce manque, venant de constructeurs connus: Spectralink, Vocera, Cisco, Symbol Technologies. La solution qui a été retenue est celle de Cisco, notamment à cause de la possibilité de mise à jour de l'implémentation (propriétaire) vers une solution normalisée (IEEE 802.11e), de la disponibilité du matériel, de la compatibilité avec du matériel Linux. La série choisie a été Aironet 350 [2] (cartes PCMCIA, cartes PCI, point d'accès).

Au niveau des téléphones, un certain nombre de logiciels basés sur SIP (Softphones) ont été installés sur des ordinateurs portables. De plus, des agendas personnels (PDA) pouvant établir des communications sans fil ont été utilisés. Ils offrent les fonctionnalités nécessaires pour la transmission de la voix et de la vidéo tout en étant de taille réduite. Pour la voix (protocole de signalisation SIP), le serveur Iptel-SER a été installé (www.iptel.org). Ce produit est gratuit, robuste et s'installe dans un environnement Linux. Il peut agir en tant que proxy ou serveur de redirection. Il dispose entre autres d'extensions pour l'administration (par le Web), une passerelle SMS (Short Message Service) et la possibilité de faire de l'authentification avec un serveur Ra-

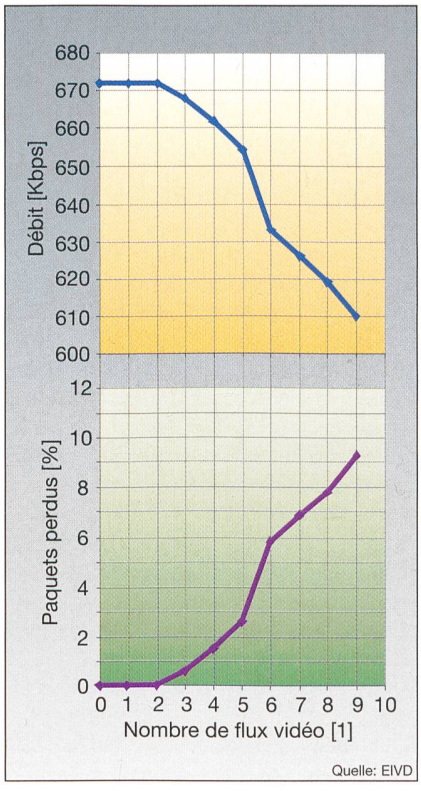

Figure 3 Performance de la vidéo sur WLAN
Largeur de bande vidéo et taux de perte des paquets (trafic unidirectionnel), sans QoS, en fonction du nombre de flux vidéo.

dius. La plateforme a ainsi pu être testée pour des mesures de performances avec inclusion de schémas de sécurité. Les clients SIP gratuits sont très nombreux à fonctionner sous Windows. Quelques-uns sont également disponibles sous Linux. Les clients utilisés pour les expériences ont été Windows Messenger (installé sur la dernière version du système d'exploitation de Microsoft), X-Lite (www.xten.com): solution retenue et Eyepmedia (www.eyepmedia.com).

Les serveurs les plus connus pour diffuser de la vidéo sont Realnetworks et Microsoft mais ils ont le désavantage d'être payants. Le serveur choisi est gratuit et s'exécute sous Linux: Darwin d'Apple [1] qui est compatible avec le standard MPEG-4, largement utilisé pour diffuser des vidéos de haute qualité. Le transport des contenus est assuré par les protocoles standards RTP et RTSP. Le client de lecture vidéo choisi est Quicktime qui est capable de lire des flux MPEG-4.

Un certain nombre d'outils sont disponibles pour l'analyse du trafic, dont IPerf qui est gratuit. Ce programme s'exécute sous Linux et sous Windows, ne nécessite aucune installation, est paramétrable (spécification du champ ToS, Type of Service, des paquets IP) et relativement simple à utiliser (lignes de commande). D'autre part, il est toujours en développement. Cependant, un inconvénient concerne la présentation des fichiers de mesure, qui n'est pas exploitable directement. Il faut faire une mise en forme de la collection des données pour en extraire les mesures intéressantes.

Mesures

Cette partie expose les résultats des mesures effectuées sur la plateforme avec et sans qualité de service (QoS). Le détail de toutes les mesures est reporté en [5]. Dans un premier temps, les mesures (débits) ont été effectuées pour le flux descendant. Les flux vidéo sont composés de lectures vidéo par des clients. Le trafic (considéré comme étant faible) est donc unidirectionnel bien que la signalisation soit bidirectionnelle. La vidéo est compressée avec un format MPEG-4 et nécessite une largeur de bande d'environ 670 kb/s (mesuré individuellement) avec de paquets UDP de 1450 octets. Cette application n'est pas interactive, c'est pourquoi les paquets peuvent être de taille relativement importante. Les mesures se sont effectuées de la manière suivante (figure 2): La vidéo est acheminée depuis le serveur de vidéo Darwin en direction des stations munies de clients Quicktime, par Ethernet et ensuite par voie aérienne. Deux stations sont choisies pour effectuer les mesures dont une va générer du trafic de fond et l'autre faire l'analyse des performances. Le serveur Darwin diffuse la vidéo avec le protocole RTSP (Real Time Streaming Protocol).

La figure 3 montre les performances obtenues avec des flux vidéo traversant un point d'accès 802.11b. Jusqu'à quatre flux simultanés, on peut considérer que la qualité de la vidéo est bonne mais se dégrade à partir du cinquième flux (l'image se déforme ou se fige par moment). Par contre, elle ne devient plus acceptable à partir du sixième flux. La perte de paquets devient importante à partir du sixième flux: 6%. Nous avons observé qu'une perte relativement faible de paquets nuit grandement à la qualité de la vidéo. Alors qu'une perte de 25% sur les paquets voix est encore acceptable [5], une perte de 7% sur les paquets vidéo ne permet pas à l'application de fonctionner correctement. Pour comprendre ce qu'il se passe il faut se rappeler que les paquets vidéo sont relativement importants et que la perte d'un paquet engendre une perte de données relativement importante. D'autre part, notre oreille est certainement plus tolérante que notre œil. Des mesures ont été effectuées avec du trafic de fond et il a été également trouvé qu'à partir de cinq flux, la qualité de la vidéo n'est plus acceptable.

Les mesures des performances se sont faites avec le matériel Cisco qui est relativement performant par rapport au matériel 3Com utilisé pour les mesures effectuées sans qualité de service. Le schéma de qualité de service appliqué par Cisco est propriétaire mais se veut compatible avec la norme 802.11e dès que cette dernière sera officialisée. Lors des tests il a néanmoins été trouvé que la différenciation des flux est bien effectuée pour le trafic unidirectionnel descendant (du serveur vidéo aux stations). Par contre, pour le trafic bidirectionnel, la qualité de service n'est plus assurée. Pour le trafic unidirectionnel, 12 stations ont été connectées au serveur vidéo, dont 6 étaient prioritaires. La qualité de la vidéo pour les stations prioritaires est tout à fait acceptable alors que pour les stations non prioritaires l'image reste figée. Dans le cas du trafic bidirectionnel, la vidéo se dégrade rapidement, ceci pour les flux prioritaires et non prioritaires, sans distinction nette entre les deux types de flux, ce qui n'est pas conforme à la norme 802.11e (figure 4). Pour le trafic descendant, nous avons clairement une différenciation des flux, basée sur leurs priorités, et ceci est géré par le point d'accès. Par

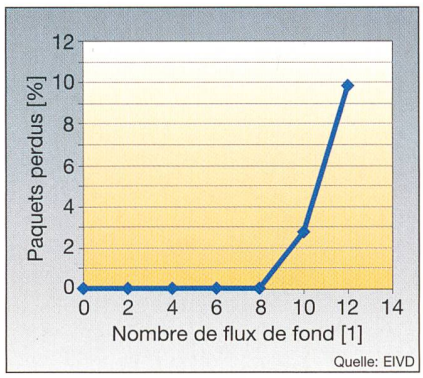

Figure 4 Performance de la vidéo sur WLAN
Taux de perte des paquets vidéo avec QoS (trafic bidirectionnel) en fonction du nombre de flux de fond.

contre, pour le trafic montant, il est nécessaire de régler les paramètres de la fenêtre de contention pour obtenir une différenciation de trafic, ce qui n'a manifestement pas encore été implémenté avec le matériel que nous avons testé. En résumé, la qualité de service offerte par le point d'accès permet de différencier les flux pour des applications descendantes, de type streaming par exemple, mais est totalement inefficace pour des applications fonctionnant dans les deux sens en temps réel, tel que la voix sur IP.

Dans cette partie [3], nous sommes intéressés par les performances d'une plateforme sécurisée. La première phase, d'authentification, qui consiste en l'échange de paquets EAP et Radius, ne va pas affecter les performances. Seulement quelques paquets sont échangés durant cette phase. La deuxième phase consiste à chiffrer les données. Cette opération contribue à des baisses de performance significatives. Le temps pour chiffrer les données, calculer et générer des clés de session est non négligeable. Pour effectuer les mesures de performance, il a fallu utiliser un point d'accès qui supportait le chiffrement AES et TKIP. Nous avons utilisé un point d'accès et une carte de type Buffalo (www.buffalotech.com) IEEE 802.11g (54 Mb/s) et avons mis à jour les pilotes des cartes. WEP est implémenté d'origine et IPSec [6] fonctionne au dessus du protocole MAC 802.11 et peut donc s'installer facilement (www.freeswan.org et www.ipsec-howto.org). Deux types de trafic ont été émulés: UDP (pour la voix et la vidéo) et TCP. La figure 5 illustre le débit obtenu pour TCP avec différents schémas de chiffrement. Les baisses de performance sont comparables à celles observées avec UDP. Lorsque les données ne sont pas chiffrées, le débit varie entre 17,3 et 21,3 Mb/s environ, avec une moyenne de 19,4 Mb/s, et est relativement fluctuant, à

cause des propriétés du media de transmission. Pour effectuer ces mesures, un logiciel nommé Chariot de NetIQ (www.netiq.com) a été utilisé. La figure 5 montre la comparaison des débits mesurés pour les schémas de chiffrement (encryption) suivants: WEP 128, AES, TKIP et IPSec. La baisse de performances est nette pour TKIP et IPSec mais pas pour AES et WEP 128. Les valeurs moyenne du débit mesuré sont respectivement 18,8 Mb/s pour WEP 128, 18,3 Mb/s pour AES, 14,9 Mb/s pour TKIP et 11,6 Mb/s pour IPSec. TKIP utilise WEP 128, donc on peut être surpris par les différences de débit observées. La baisse de performance de TKIP provient de la génération et de la gestion des clés qui se fait au niveau du firmware et qui prend donc passablement de temps. AES, par contre, est implémenté en hardware. Par rapport au débit mesuré sans chiffrement, la baisse obtenue est de 3% avec WEP 128 et de 5,6% avec AES, ce qui est acceptable. Elle est de 23% avec TKIP et de 40% avec IPSec. Les fonctionnalités d'IPSec et d'AES ne sont pas identiques. IPSec est un protocole qui permet d'effectuer du chiffrement de bout en bout (pour un VPN par exemple) alors que AES va uniquement chiffrer les données entre la carte réseau et le point d'accès.

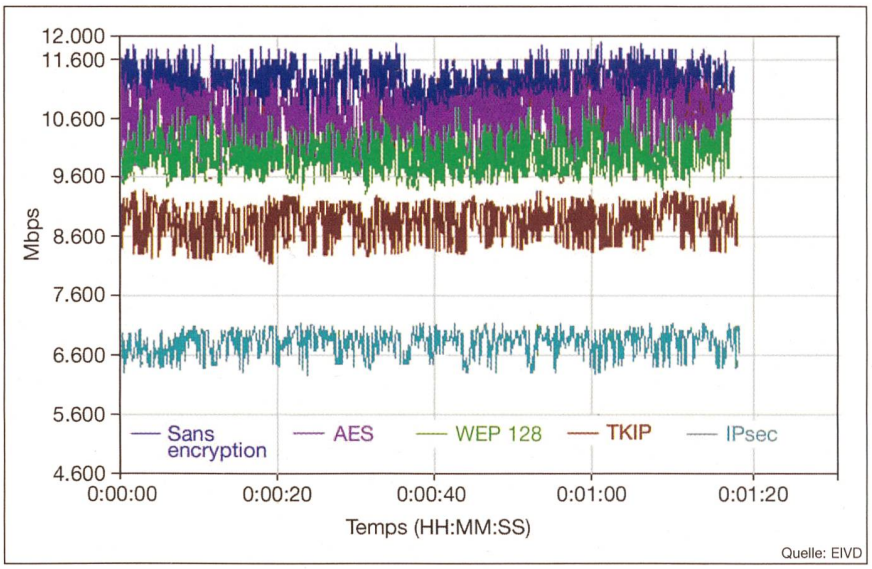

Figure 5 Débit des données cryptées pour le protocole TCP

La qualité de service est affectée

Les réseaux de données sans fil sont très faciles à déployer et leurs largeurs de bande sont acceptables pour la majorité des applications. Néanmoins, lorsque une certaine qualité de service et qu'une certaine sécurité sont requises, deux conclusions peuvent être tirées suite aux expériences menées:

- Lors des tests il a été trouvé que la différenciation des flux est bien effectuée pour du trafic unidirectionnel descendant (du serveur vidéo aux stations). Par contre, pour le trafic bidirectionnel, la qualité de service n'est plus assurée. Le matériel actuel et courant disponible sur le marché ne nous permet pas d'obtenir une qualité de service qui se rapproche de la norme IEEE 802.11e (attendue pour la fin de cette année), ceci malgré son état relativement stable.
- Les schémas de sécurité utilisés affectent la qualité de service de manière non négligeable. Une comparaison est faite pour AES, WEP 128, TKIP et IPSec. Il a été trouvé qu'une baisse significative des performances est observée pour TKIP (23%) et IPSec (40%).

Une plateforme de test relativement complète a été montée pour mettre en évidence certains problèmes. Dans un environnement réel, d'autres contraintes spécifiques aux opérateurs sont à prendre en compte, notamment en ce qui concerne l'authentification des utilisateurs qui peut s'effectuer avec la carte SIM si l'opérateur dispose en parallèle d'un réseau de type GSM.

Références

[1] *Apple, Darwin:* Streaming Server Administrator's Guide, 20 Novembre 2002.

[2] *Cisco Systems:* Release notes for Cisco Aironet 340 and 350 Series Access Points and 350 Series Bridges Running Firmware, Version 12.04, Novembre 2003.

[3] *V. Emery:* Comparaison de schémas de sécurité des réseaux 802.11, Travail de diplôme EIVD, Décembre 2003.

[4] *S. Fluhrer, I. Mantin and A. Shamir:* Weaknesses in the Key Scheduling Algorithm of RC4, Eight Annual Workshop on Selected Areas in Cryptography, 2001.

[5] *M. Hasanovic:* Qualité de la voix et des applications multimédia dans un réseau WLAN IEEE 802.11, Travail de diplôme EIVD, Décembre 2003.

[6] *Documentation Microsoft:* How to configure IPsec tunnelling in windows 2000, Microsoft Knowledge Base Article 252735, Novembre 2003.

[7] *A. Stubblefield, J. Ioannidis and A.D. Rubin:* Using the Fluher, Mantin and Shamir Attack to break Wep, AT&T Labs-Research, Florham Park, NJ, 2001.

Informations sur les auteurs

Dr. Ing. Dipl. EPFL **Stephan Robert** est professeur à l'Ecole d'Ingénieurs du Canton de Vaud (EIVD). **Vincent Emery** et **Mesud Hasanovic** sont Ing. Dipl. HES à l'EIVD.

Haute Ecole Spécialisée de la Suisse Occidentale (HES-SO)/Ecole d'Ingénieurs du Canton de Vaud (EIVD), 1401 Yverdon-les-Bains.

stephan.robert@eivd.ch

Quality of Service im drahtlosen Netzwerk

Nutzbare Bandbreiten in einem reellen WLAN-Netzwerk

Drahtlose Netzwerke (WLAN) können einfach aufgebaut werden. Wie steht es aber mit der Sicherheit und der Qualität der Dienste? Viele kommerzielle Produkte bieten einfache Verschlüsselungen wie WEP (Wired Equivalency Protocol) an. Diese können durch Tools, die im Internet heruntergeladen werden können, geknackt werden. Besser ist die IPSec-Verschlüsselung, die aber die Bandbreite im Netzwerk um 40% verschlechtert. Die Bandbreite im WLAN ist allgemein kleiner als in einem Netzwerk mit Kabeln. Theoretisch ist im WLAN eine Bandbreite von 54 MBit/s möglich. Wird es aber mit Videodaten belastet, die pro Kanal 670 KBit/s nutzen, verschlechtert sich die Qualität der Videobilder bereits ab dem fünften Kanal.