Analyse spectrale d'outils classiques de DDoS

Laurent GALLON et Julien AUSSIBAL

LIUPPA-CSYSEC
IUT des Pays de l'Adour - 371 rue du ruisseau – BP 201 – 40004 Mont de Marsan cedex
laurent.gallon@univ-pau.fr
aussibal.julien@etud.univ-pau.fr

Résumé. L'objectif de ce papier est d'analyser les variations de trafic générées par un outil de DDoS classique : TFN2k. La caractérisation du trafic est basée sur la mesure de divers paramètres réseaux (nombre de paquets par seconde, nombre d'octets par seconde, nombre de connexions TCP par seconde). L'analyse des ces mesures est effectuée par des outils issus du traitement du signal (densité spectrale de puissance, décomposition en ondelettes). Nous montrons que cet outil d'attaque peut être caractérisé par une « signature spectrale » spécifique, qui doit pouvoir être utilisée dans les outils de détections d'attaques.

1 Introduction

Les attaques en Dénis de Service ont pour objectif de consommer tout ou partie des ressources d'une cible, afin de l'empêcher de pouvoir rendre ses services de façon satisfaisante. Les premiers types d'attaques en Dénis de Service ne mettaient en cause qu'un seul attaquant (DoS), mais rapidement, des attaques évoluées sont apparues, impliquant une multitude de « soldats », aussi appelés « zombies » (DDoS).

Jusqu'à récemment, les attaques en DoS et DDoS étaient perpétrées par des « hackers » ne cherchant que l'exploit, et la renommée. Aujourd'hui, de véritables organisations criminelles se sont mises en place autour de ces outils. Une étude récente de McAfee [1] estime que 70% des attaques sur Internet sont effectuées par des groupes criminels organisés. Ainsi, certains hackers se sont spécialisé dans la « levée » d'armées de « zombies », qu'ils peuvent ensuite louer à d'autres hackers pour attaquer une cible particulière. Avec la forte augmentation du nombre d'échanges commerciaux sur Internet, le nombre de chantages au Déni de Service est lui aussi en très forte progression : un hacker lance une attaque en DoS ou DDoS contre une entreprise, et lui demande une rançon pour arrêter cette attaque ! Tous ces exemples montrent combien il est devenu essentiel de pouvoir détecter efficacement ces attaques (à l'aide de systèmes de détection d'intrusion (IDS) ou de prévention d'intrusion (IPS)), et de mettre en place des contre mesures.

Les systèmes de détection d'attaques en dénis de service sont basés sur deux approches. La première est une approche par signature, qui consiste à analyser le contenu des différents paquets reçus [2,3]. On considère que les paquets issus d'une attaque

ont un format spécifique, appelé « signature ». Cette approche, qui est la plus répandue aujourd'hui dans les IDS, possède certaines limitations : chaque attaque possède une multitude de variantes (la simple variation d'un bit dans les paquets issus de deux attaques similaires suffit pour générer deux signatures différentes), et de nombreux faux positifs peuvent apparaître (par exemple, dans le cas ou une application génère des paquets légitimes, mais correspondant à une signature d'attaque).

La deuxième approche se base sur la définition d'un profil d'attaque. Ce profil peut être défini, par exemple, grâce à l'analyse des caractéristiques spectrales du trafic au cours de l'attaque. Plusieurs travaux récents ont en effet montré que les anomalies de trafic (variations importantes du trafic) engendraient une variation conséquente des caractéristiques spectrales de ce trafic [4,5,6,15,16]. Ces anomalies peuvent aussi bien être des attaques en dénis de service, que d'autres phénomènes plus légitimes, comme par exemple des « flash crowd ».

L'objectif de ce papier est d'étudier les modifications du trafic engendrées par un outil classique d'attaque en dénis de service : TFN2K (Tribal Flood Network 2000). Dans un premier temps, nous donnons brièvement une définition des dénis de service. Nous décrivons ensuite les principaux outils d'attaque en DDoS existants. Enfin, nous décrivons les analyses effectuées sur les mesures de trafic, et les résultats obtenus.

Notons que cette étude est effectuée dans le cadre du de l'ACI Sécurité & Informatique, et plus particulièrement du projet METROSEC. Ce projet a pour objectif le développement d'outils de détection d'anomalies de trafic. Une plateforme s'appuyant sur le réseau RENATER a été mise en place, avec plusieurs points de mesure (Toulouse, Paris, Lyon, Pau). Les mesures du trafic sont effectuées à l'aide d'outils de métrologie (mesures passives et actives). Les analyses utilisent des outils issus du domaine du traitement du signal (analyse spectrale, ondelettes, filtres de Kalman, …).

2 Les attaques en Déni de Service (DoS) et Déni de Service Distribué (DDoS)

Un déni de service est une attaque réseau ayant pour objectif d'empêcher un serveur ou un réseau de rendre ses services de façon satisfaisante. Le déni de service est effectué en consommant une grande partie des ressources de la victime. Ces ressources peuvent être réseau (bande passante, buffers, …) ou logicielles (failles dans les applications ou systèmes d'exploitation). Dans tous les cas, l'objectif est de consommer tout ou partie des ressources dont la victime a besoin pour rendre ses services.

2.1 Définition des DoS et DDoS

Il existe deux grands types de dénis de service : les dénis de service « simples » (DoS) et les dénis de service distribués (DDoS).

Les dénis de service « simples » sont les premiers à être apparus. Dans ce type d'attaque, le hacker lance seul son attaque contre la victime. La plupart du temps, le

hacker cache son identité réseau (adresse IP et ports UDP/TCP) en se faisant passer pour une, voire plusieurs autres machines (spoofing). Ainsi, il ne peut pas être reconnu par la victime (fig. 1).

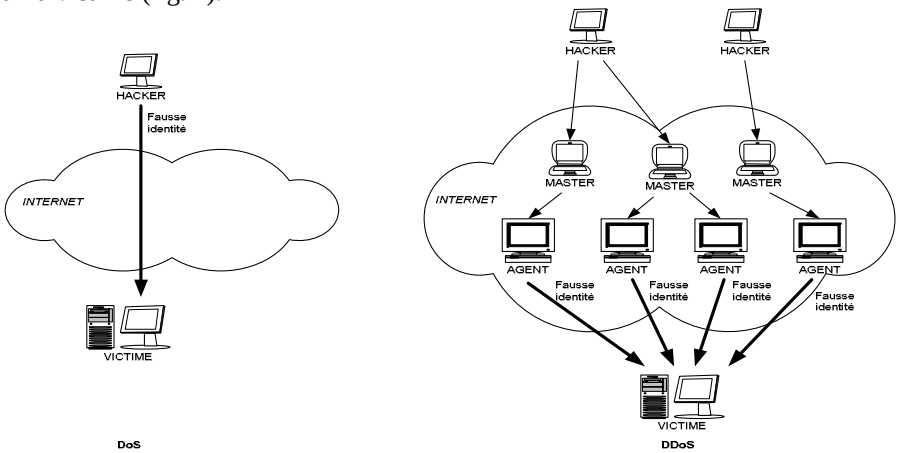

Fig. 1. DoS et DDoS

Les dénis de service distribués sont plus complexes. Ils mettent en œuvre une armée d'attaquants (appelés « agents », ou « zombies »), contrôlée par un ou plusieurs « généraux » (appelés « maîtres »). Chaque agent génère une attaque DoS simple vers la victime. Les « généraux » donnent les ordres d'attaques aux agents, et sont eux-mêmes pilotés par un ou plusieurs hackers (fig. 1). Une telle architecture permet de multiplier la puissance de l'attaque. Elle complexifie l'identification par la victime des hackers. Mais de telles attaques nécessitent au préalable une phase de corruption de machines sur Internet, afin d'y installer des agents, et de pouvoir plus tard « lever » (utiliser) cette armée d'attaquants. Notons que certains hackers se sont spécialisés dans la corruption et la levée d'armée d'attaquants, qu'ils louent ensuite à d'autres hackers souhaitant perpétrer des attaques. Ainsi, une même armée d'attaquants peut être utilisée pour plusieurs attaques différentes …

2.2 Quelques attaques classiques en DoS et DDoS

Il existe une multitude d'attaques différentes en déni de service. Parmi les plus connues, on trouve les attaques en UDP, ICMP ou TCP flooding. L'objectif de ces attaques est d'envoyer un maximum de paquets (UDP, ICMP ou TCP) à la victime afin de saturer sa bande passante. L'attaque en TCP SYN exploite quant à elle une faille dans la phase de mise en place de la connexion dans le protocole TCP. Cette attaque sature le buffer des connexions en cours d'établissement, empêchant ainsi la mise en place des connexions légitimes. Enfin, l'attaque Smurf utilise une amplification pour inonder la victime de paquets ICMP : les attaquants envoient des paquets ICMP à une adresse de diffusion, en se faisant passer pour la victime ; toutes les machines faisant partie de cette adresse de diffusion répondent alors à la victime, et saturent sa bande passante (flooding)

Plusieurs taxonomies des attaques en DoS/DDoS ont été proposées dans le passé. Dans [13], R. B. Lee propose une classification orientée ressource attaquée. Cette approche distingue essentiellement les attaques destinées à consommer tout ou partie de la bande passante de la victime, et les attaques visant une ressource particulière de la victime (connexions TCP, …). Les moyens mis en œuvre pour réaliser ces attaques diffèrent en fonction du type de ressource visée : l'inondation (« flooding ») par beaucoup de paquets pour la consommation de la bande passante, et l'exploitation de failles logicielles (« exploit ») pour une ressource particulière. Dans [14], Mirkovic et al. proposent une classification orientée mécanismes réseaux. Les attaques peuvent être classifiées suivant plusieurs critères, comme par exemple la manière dont l'attaque est préparée et lancée, ou encore les effets de l'attaque sur la victime, … Dans [15], Hussain et al. proposent une classification orientée analyse spectrale du trafic. A partir des certaines mesures de paramètres réseaux, des seuils de variation sont définis, permettant ensuite de classifier les différentes attaques. Enfin, dans [12], nous proposons une classification orientée réseau, basée sur les variations de certains paramètres réseaux (actifs et passifs). Cette dernière classification a été défini pour servir de support à la définition de « signatures spectrales » des attaques en DoS/DDoS.

2.3 Quelques outils classiques de DDoS

Plusieurs outils spécialisés dans la supervision d'attaque en DDoS ont été développés ces dernières années, et sont accessibles librement sur Internet. En règle générale, ils sont constitués de plusieurs programmes à installer sur les différentes machines participant à l'attaque : programme « maître », programme « agent ». Il ne reste aux hackers qu'à corrompre des machines sur Internet (c'est-à-dire réussir à accéder à ces machines pour y installer ces programmes) pour lever leur armée d'attaquants.

Parmi les outils les plus célèbres, nous pouvons citer :

Trinoo [7] : UDP flooding
Tribe Flood Network (TFN) et TFN2k [8] : UDP/TCP/TCP SYN flooding, Smurf
Stacheldraht [9] : UDP/TCP/TCP SYN flooding, Smurf
Schaft [10] : UDP/TCP/ICMP flooding
MStream [11] : TCP ACK flooding

Nous nous restreindrons à l'étude de TFN2k dans la cadre de ce papier.

3 Analyse spectrale des DoS et DDoS

Les dernières études traitant de la détection d'attaques en Dénis de Service se penchent non plus sur la structure des paquets issus des outils d'attaque (approche « signature »), mais sur les caractéristiques du trafic généré par ces attaques (« approche profil »). Ces caractéristiques sont tirées de mesures métrologiques du trafic Internet

(nombre de paquets par seconde, nombre d'octets par seconde, nombre de paquets TCP par seconde, interarrivée des paquets, …), analysées par des outils issus du traitement du signal.

Il a été montré dans [18] que les mesures statistiques d'ordre 1 (moyenne, variance) des mesures métrologiques ne permettent pas de caractériser le trafic Internet. En effet, la grande variabilité de ce trafic fait que la variance est plus importante que la moyenne. Il est alors impossible de se baser sur des seuils dans ces mesures, sans provoquer un grand nombre de « faux positifs ». La solution est donc d'évaluer les moments d'ordre 2. Intuitivement, ces moments permettent de voir l'évolution du trafic dans le temps. Le principal outil utilisé dans la littérature est l'autocorrélation de mesures métrologiques, qui permet de mettre en exergue les périodicités existant dans le trafic. Les résultats sont souvent présentés sous forme de densité spectrale de puissance, qui est obtenue en calculant la transformée en série de Fourier discrète de la fonction d'autocorrélation.

Dans [15], Hussain and al. utilisent la densité spectrale de puissance pour caractériser les attaques en DoS et DDoS. Chaque trace de trafic (nombre de paquets toutes les 30 secondes) est considérée comme une série temporelle. Les résultats montrent que les attaques DoS font plutôt apparaître des pics de puissance dans les fréquences hautes, alors que les attaques en DDoS font apparaître des pics de puissance dans les fréquences basses.

Les dernières études du trafic Internet ont permis de mettre en évidence certaines propriétés intéressantes, et notamment des caractéristiques d'auto similarité et de dépendance à long terme (LRD). Dans [17], P. Abry et D. Veitch mesurent cette LRD (facteur de Hurst) grâce à une décomposition en ondelettes du trafic observé. La décomposition en ondelettes est un outil permettant de décomposer le trafic initial en une somme de sous trafics, ayant chacun une périodicité différente.

Dans [4], Larrieu et Owezarski montrent que le trafic Internet fait apparaître des invariants d'échelles dans la dépendance à long terme. De plus, ces invariants sont modifiées lors d'apparition de d'anomalies dans le trafic (comme par exemple une attaque).

Dans [16], Barford and al. utilisent la décomposition en ondelettes pour caractériser les ruptures de trafic (attaques, flash crowds, …) Ainsi, Barford and al. définissent trois bandes de fréquence principales : la bande des hautes fréquences, la bande des fréquences moyennes, et la bande des basses fréquences. Ils montrent que les attaques apparaissent dans la bande des fréquences hautes. Néanmoins, leur technique de mesure, basé sur la récolte de valeurs SNMP toutes les 5 minutes, ne leur permet pas d'être très précis sur la nature des attaques détectées.

Nous proposons, dans la suite de cet article, d'analyser le comportement spectral de certains outils classique de DDoS, en utilisant les méthodes décrites dans [15] et [16]. Nous montrons que des différences apparaissent entre les différents outils, permettant ainsi de les caractériser.

4 Analyse de trafic d'attaques

Ce paragraphe est consacré à l'étude du comportement de l'outil classique d'attaques en DDoS TFN2k. Pour cela, nous avons utilisé cet outil sur une plateforme fermée constituée de plusieurs PC Linux, et d'une sonde de mesure DAG qui nous a permis de mesurer certains paramètres réseaux (nombre de paquets par seconde, nombre d'octets par seconde, nombre de connexions TCP par seconde). Le trafic de notre réseau local a été renvoyé vers la plateforme (mirroring) afin de pouvoir mélanger trafic d'attaque et trafic légitime. Plusieurs simulations ont été effectuées, afin d'évaluer les caractéristiques spectrales des attaques en fonction du nombre de zombies attaquants. Nous avons commencé avec une attaque DoS (un seul zombie), puis nous avons effectué une attaque avec trois zombies, et enfin nous avons terminé avec une attaque impliquant six zombies.

Les outils d'analyse des paramètres réseaux mesurés sont la densité spectrale de puissance et la décomposition en ondelettes. Nous présentons ci-dessous les résultats observés pour chaque simulation.

4.1 Analyse de TFN2k

La figure 2 montre la mesure du nombre d'octets par seconde pour l'attaque en DoS (un seul zombie). L'attaque est très visible (nombre d'octets très important au cours de l'attaque). Mais on voit aussi apparaître un comportement variable du zombie au cours de l'attaque. Cette variation est relativement importante, et caractéristique du zombie TFN2k (comme nous allons le montrer par la suite).

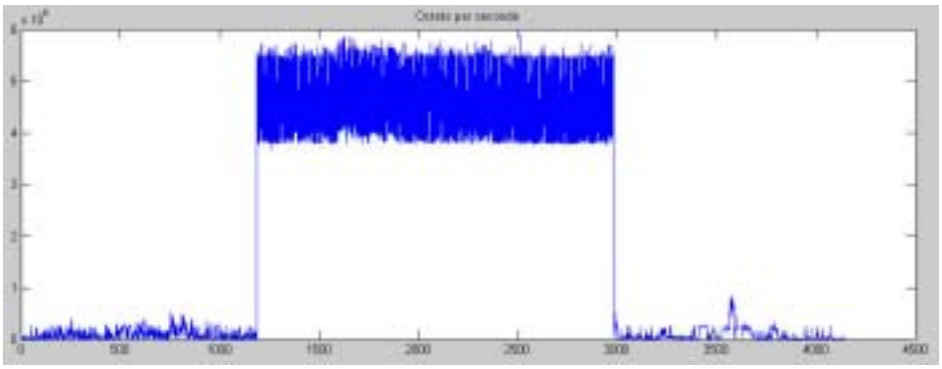

Fig. 2. Nombre d'octets par seconde

La figure 3 donne la densité spectrale de puissance correspondante. On peut noter l'apparition de fréquences caractéristiques (0,46 Hz et 0,33 Hz) qui correspondent aux périodicités introduites par le comportement variable du zombie. Nous définissons cet ensemble de fréquences comme la « signature spectrale » d'un zombie TFN2k.

La figure 4 fait apparaître une partie de la décomposition en ondelettes du nombre de paquets par seconde. L'ondelette référence choisie est l'ondelette de Haar (le changement de cette ondelette n'apporte pas de variation significative dans les résultats).

Le détail de niveau 1 correspond à la partie du signal dont la périodicité est comprise entre 1 et 2 secondes (fréquences « hautes »). La partie approximation de niveau 5 correspond à la partie du signal dont la périodicité est supérieure à 32 secondes (fréquences basses). La partie détail de niveau 1 (D1) fait donc apparaître la variation de comportement du zombie au cours de l'attaque, alors que la partie approximation de niveau 5 (A5) fait apparaître la partie « continue » de l'attaque.

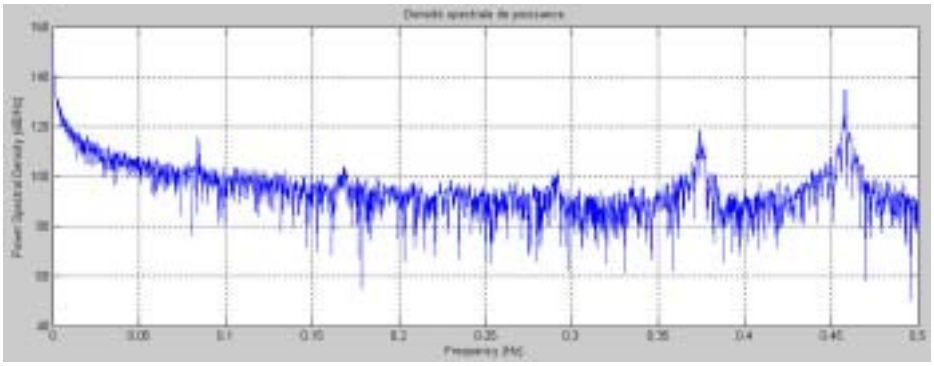

Fig. 3. Densité spectrale de puissance

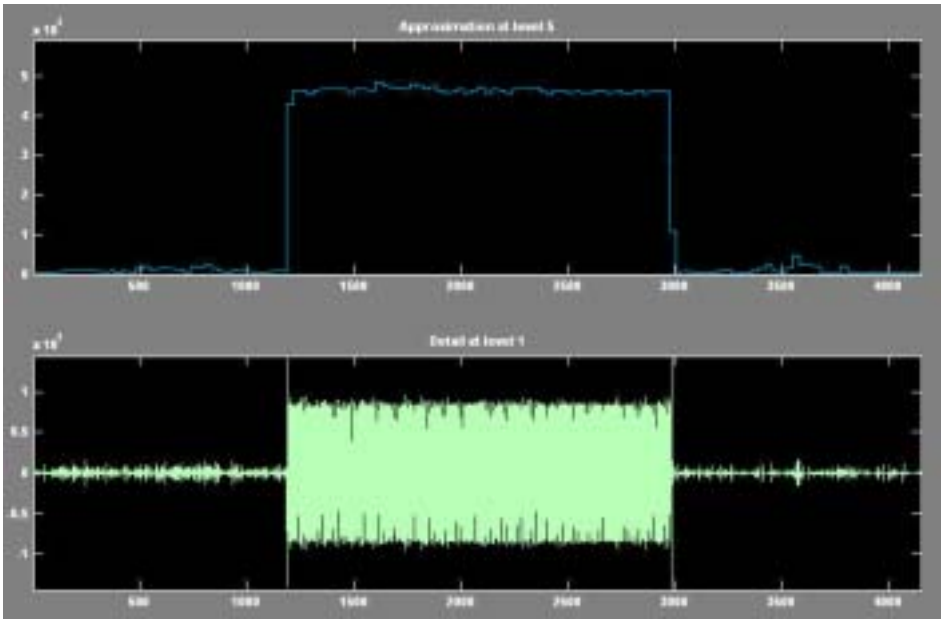

Fig. 4. Décomposition en ondelettes

La figure 5 montre la densité spectrale obtenue à partir du nombre d'octets par seconde lors d'une attaque à 3 zombies. Les fréquences caractéristiques (signature) apparaissent comme précédemment, mais légèrement décalées vers la zone des basses fréquences (0,44 Hz et 0,31 Hz).

La figure 6 donne la décomposition en ondelettes du nombre d'octets par seconde dans cette deuxième attaque. Le mélange des trois zombies donne une variation de comportement encore plus marquée que pour l'attaque en DoS, avec des intervalles de temps où la variation est forte, et des intervalles de temps où la variation est moindre. Ce sont les parties faisant apparaître peu de variation qui sont nouvelles : la cumulation des trafics des zombies commence à « lisser » le trafic d'attaque, et à diminuer sa variance.

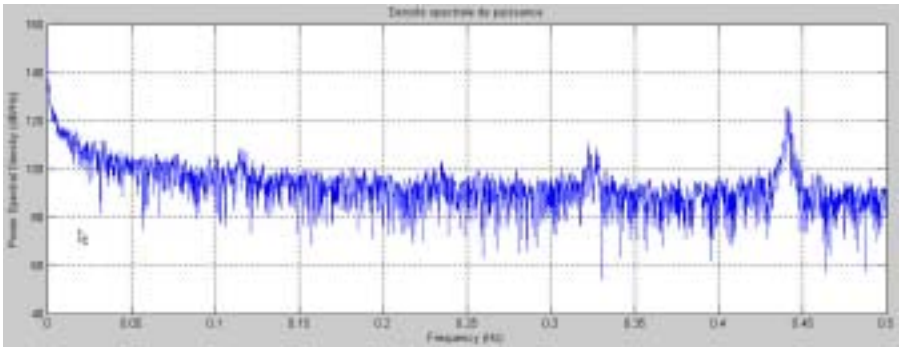

Fig. 5. Densité spectrale de puissance

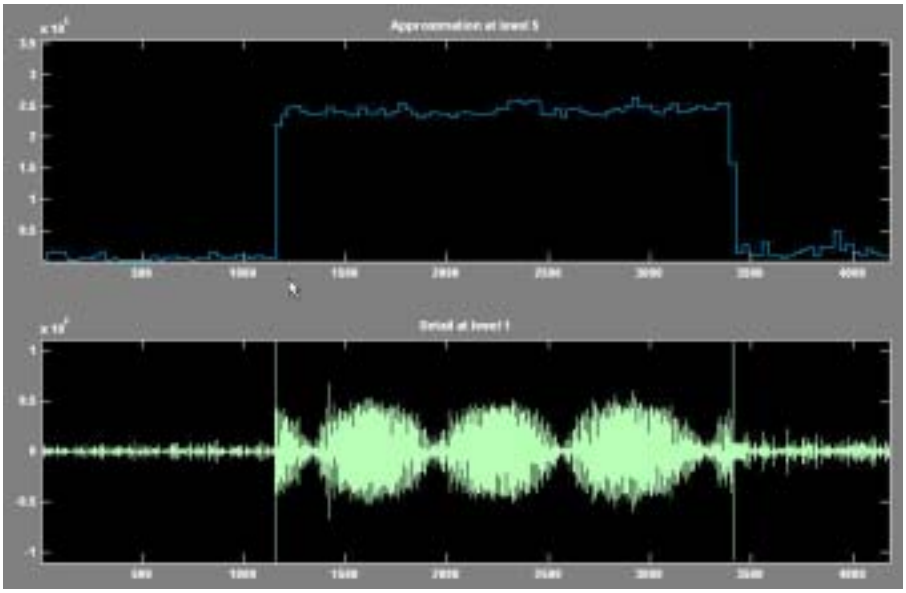

Fig. 6. Décomposition en ondelettes

Enfin, les figures 7 et 8 nous donnent la densité spectrale de puissance et la décomposition en ondelettes du nombre d'octets par seconde lors d'une attaque à 6 zombies. Les fréquences caractéristiques n'apparaissent plus. Elles ont en fait été décalées et noyées dans les basses fréquences. La décomposition en ondelettes nous montre que la

variation du trafic généré par les zombies est quasiment nulle devant la puissance des trafics cumulés.

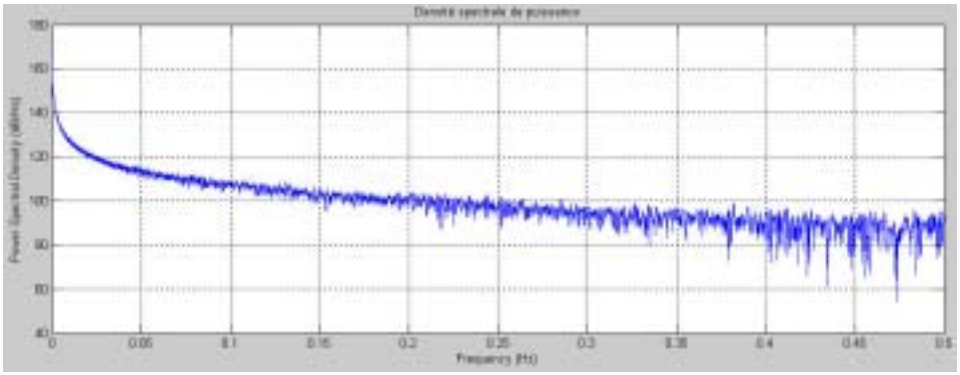

Fig. 7. Densité spectrale de puissance

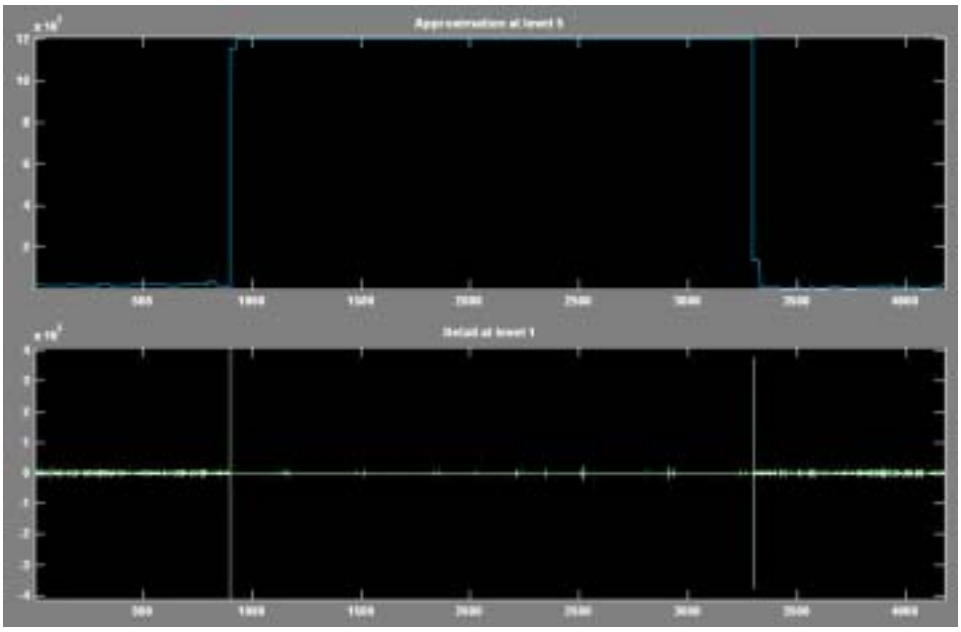

Fig. 8. Décomposition en ondelettes

4.2. Conclusion sur les résultats obtenus

La première simulation montre qu'un zombie TFN2k peut être caractérisé par une signature spectrale caractéristique, constituée de deux fréquences autour des 0,46Hz et 0,33 Hz. Les simulations suivantes ont montré que ces fréquences se décalent vers les

fréquences basses quand on augmente le nombre de zombies attaquants. A partie de 6 zombies, la signature disparaît, noyée dans la puissance de l'attaque globale.

Cette étude corrobore les résultats de Hussain et al. [15], qui ont montré que les attaques en DoS faisaient plutôt apparaître des fréquences hautes, alors que les attaques en DDoS faisaient plutôt apparaître des fréquences basses. En augmentant le nombre de zombie, et donc en passant d'une attaque en DoS à une attaque en DDoS, nous avons décalées les fréquences caractéristiques vers les basses fréquences

Ce résultat peut être utilisé dans les réseaux à la source des attaques par TFN2k. On peut en effet détecter dans ces réseaux les machines qui sont en train de participer à l'attaque en DDoS. Si ce nombre de machines ne dépasse pas trois ou quatre, la signature spectrale sera visible, et indiquera la présence de zombies TFN2k en activité.

5 Conclusion

Dans ce papier, nous avons étudié le comportement de l'outil d'attaque en DDoS TFN2k avec une approche profil. Les mesures métrologiques effectuées lors des attaques sont analysées par des outils issus du domaine du traitement du signal. Nous montrons qu'un zombie peut être caractérisé par une signature spectrale, mais que cette dernière disparaît quand le nombre de zombies attaquants devient important. Ce résultat peut être utilisé pour détecter une participation de quelques machines d'un réseau à une attaque DDoS par TFN2k.

Ce premier résultat doit être confirmé par l'étude des autres outils classiques d'attaque en DDoS : Stacheldraht, Trinoo, shaft, … Nous pensons que les zombies de chaque outil ont des comportements différents, qui doivent pouvoir être différentiés par analyse spectrale. Cette confirmation permettrait de pouvoir détecter les zombies des différents outils dans les réseaux sources, et donc de protéger ses machines et son réseau contre une participation à ces attaques.

References

1. David Neal, *Online firms face growing crime menace*, http://www.vnunet.com/news/1161404
2. David Moore, *Inferring Internet Denial-Of-Service Activity*, 10th Usenix Symposium, Washington, DC, August 2001
3. Jelena Mirkovic and Peter Reiher, *A taxonomy of DDoS attack and DDoS defense mechanisms*, ACM SIGCOMM Computer Communication Review, Volume 34, April 2004
4. P. Owezarski and N. Larrieu, *Internet traffic characterization – An analysis of traffic oscillations*, 7th IEEE INt. Conf. on High Speed Networks and Multimedia Communications (HSNMC 2004), juillet 2004, Toulouse, France
5. Chen-Mou Cheng, H.T. Kung and Koan-Sin Tan, *Use of spectral analysis in defense against DoS attacks*, IEEE Globecom 2002, Tapei, Tawain, November 2002

6. A. Hussain, J. Heidemann and C. Papadopoulos, *A framework for classifying Denial of Service attacks*, ACM Sigcomm 2003, Karlsruhe, Germany, August 2003
7. D. Dittrich, *The DoS Project's "trinoo" distributed denial of service attack tool*, http://staff.washington.edu/dittrich/misc/trinoo.analysis
8. D. Dittrich, *The "Tribe Flood Network" distributed denial of service attack tool*, http://staff.washington.edu/dittrich/misc/tfn.analysis
9. D. Dittrich, *The "stacheldraht" distributed denial of service attack tool*, http://staff.washington.edu/dittrich/misc/stacheldraht.analysis
10. S. Dietrich, *An analysis of the ``Shaft'' distributed denial of service tool*, http://security.royans.net/info/posts/bugtraq_ddos3.shtml
11. D. Dittrich, *The "mstream" distributed denial of service attack tool*, http://staff.washington.edu/dittrich/misc/mstream.analysis.txt
12. S. Farraposo, K. Boudaoud, L. Gallon and P. Owezarski, *Some issues raised by DoS attacks in the TCP/IP suite*, SAR 2005, Batz sur mer, juin 2005
13. Ruby B. Lee, *Taxonomies of Distributed Denial of Service Networks, Attacks, Tools and Countermeasures*, Princeton University. http://www.princeton.edu/~rblee/DDoS Survey Paper_v7final.doc
14. J. Mirkovic and P. Reiher. A Taxonomy of DDoS Attack and DDoS Defense Mechanisms, ACM SIGCOMM Computer Communication Review, Volume 34, Avril 2004
15. A. Hussain, J. Heideman, C. Papadopoulos, *A Framework for Classifying Denial of Service Attacks*, SIGCOMM'03, 25-29 Août 2003, Karlsruhe, Germany.
16. P. Barford, J. Kline, D. Plonka and A. Ron, *A signal analysis of network traffic anomalies*, ACM SIGCOMM Internet Measurement Workshop, November 2002, Marseille, France.
17. D. Veitch and P. Abry, http://www.cubinlab.ee.mu.oz.au/~darryl/secondorder_code.html
18. P. Owezarski and N. Larrieu, *Internet traffic characterization – an analysis of traffic oscillations*, 7th IEEE International Conference on High Speed Networks and Multimedia Communications (HSNMC'04), July 2004