M2 Recherche – Proposition de stage

Détection d'anomalies sur du trafic Internet

Responsables de stage

Bruno Baynat Bruno.Baynat@lip6.fr
Thomas Begin Thomas.Begin@lip6.fr
Serge Fdida Serge.Fdida@lip6.fr

Contexte

Les attaques DDoS (Distributed Deny of Service) représentent une menace majeure pour la majorité des réseaux raccordés à Internet (par exemple en mettant hors service un site Web ou un réseau d'entreprise). Le trafic engendré par une attaque DDoS constitue un trafic qualifié « d'illégal » qui se mélange au trafic dit « légal », et qui vise à rendre indisponible les ressources du système attaqué. Les méthodes de détections d'anomalies doivent être rapides et dynamiques pour permettre à l'administrateur du système de réagir vite. Ces contraintes ont conduit un certain nombre de chercheurs à proposer des méthodes de détection d'anomalies qui reposent sur une approche purement statistique.

Des estimateurs statistiques du trafic (typiquement basés sur des caractéristiques établies du trafic Internet) sont estimés à partir d'une trace mesurée dans des conditions supposées « normales » (sans attaque). Ces calculs aboutissent à des valeurs de référence supposant caractériser le trafic normal. Ces mêmes estimateurs sont alors calculés en temps réel sur le trafic mesuré afin de détecter l'arrivée d'anomalies. Si, à un instant donné, l'écart entre les valeurs fournies par les estimateurs et les valeurs de référence dépasse un certain seuil de tolérance, la méthode signale une anomalie. Généralement, ces méthodes souffrent de plusieurs limites. D'une part, elles sont généralement sensibles à une montée « légale » de la charge conduisant à une « fausse » alarme (alarme qui n'a pas lieu d'être). Ce problème est dû à la comparaison avec une référence statique prédéfinie. D'autre part, la connaissance des mécanismes statistiques de détection rend aisé, pour celui qui souhaite procéder à une attaque, le contournement de la détection (comme par exemple les attaques DDoS de faible intensité).

Objectifs du stage

Ce stage a pour objectif la recherche d'une méthode de détection d'anomalies du trafic Internet qui réponde aux défauts majeurs des méthodes courantes. Pour cela, la méthode reposera sur un modèle constructif du trafic dont le calibrage se fera automatiquement et à la volée à partir des mesures. Un modèle correctement calibré devra être capable de générer un trafic synthétique « statistiquement proche » du trafic mesuré « légal ». Si une mesure est prise pendant une période d'attaque, la comparaison de celle-ci avec les prédictions du modèle devra résulter en une différence significative que la méthode sera donc capable de détecter.

L'intégration d'un modèle au cœur de la méthode devrait permettre d'affiner les capacités de détection de la méthode, notamment en rendant possible la distinction entre une montée de charge « légale » et une montée de charge résultant d'une attaque.

Différents points de recherche seront étudiés :

- La détermination d'un modèle de trafic adapté permettant de reproduire certaines caractéristiques du trafic circulant et observé sur les réseaux ;
- La définition d'une fonction permettant d'évaluer la ressemblance « statistique » entre deux trafic.

Mots-clefs : Détection d'anomalies, Modélisation, Calibrage, Mesures.

Période visée

Le stage, d'une durée de 5 mois, se déroulera à partir d'avril 2009, dans les locaux du LIP6.

Rémunération

Le stage est rémunéré conformément aux stages de M2 Recherche, suivant le même barème.

Moyens et environnement

L'étudiant disposera de tous les moyens matériels et logiciels nécessaire au bon déroulement du stage et sera intégré dans l'équipe de recherche du laboratoire.

Bibliographie

P. Barford, J. Kline, D. Plonka, and A. Ron. A signal analysis of network traffic anomalies. In IMW '02: Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurment, pages 71–82, New York, NY, USA, 2002. ACM Press.

P. Huang, A. Feldmann, and W. Willinger. A non-instrusive, wavelet-based approach to detecting network performance problems. In IMW '01: Proceedings of the 1st ACM SIGCOMM Workshop on Internet Measurement, pages 213–227, New York, NY, USA, 2001. ACM Press.

S. Jin and D. Yeung. A covariance analysis model for ddos attack detection. In ICC' 04: Proceedings of the IEEE International Conference on Communications, volume 4, pages 1882–1886, june 2004.

J. Jung, B. Krishnamurthy, and M. Rabinovich. Flash Crowds and Denial of Service Attacks: Characterization and Implications for CDNs and Web Sites. In WWW '02: Proceedings of the 11th international conference on World Wide Web, Honolulu, HI, May 2002.

L. Li and G. Lee. Ddos attack detection and wavelets. In ICCCN' 03: Proceedings of the International Conference on Computer Communications and Networks, 2003.

J. Mirkovic, J. Martin, and P. Reiher. A taxonomy of ddos attacks and ddos defense mechanisms. In ACM SIGCOMM Computer Communication Review, volume 34, April 2001.

P. Owezarski. On the impact of DoS attacks on Internet traffic characteristics and QoS. In ICCCN '05: Proceedings of the 2005 International Conference on Computer Communications and Networks, pages 269–274. IEEE, October 2005.

P. Borgnat, N. Larrieu, P. Owezarski, P. Abry, J. Aussibal, L. Gallon, G. Dewaele, K. Boudaoud, L. Bernaille, A. Scherrer, Y. Zhang, Y. Labit. Détection d'attaques de déni de service par un modèle non gaussien multirésolution. Colloque Francophone d'Ingénierie des Protocoles (CFIP'2006), Tozeur (Tunisie), p. 303-314, 30 octobre - 3 novembre 2006.