Détection d'attaques DDoS utilisant des méthodes statistiques

1st Clément Boin
OVHcloud
Roubaix, France
clement.boin@ovhcloud.com

3rd Tristan Groléat
OVHcloud
Brest, France
tristan.groleat@ovhcloud.com

3rd Xavier Guillaume
OVHcloud
Roubaix, France
xavier.guillaume@ovhcloud.com

5th Gilles Grimaud
Univ. Lille, CNRS, Centrale Lille, UMR 9189 CRIStAL
F-59000 Lille, France
gilles.grimaud@univ-lille.fr

6th Michaël Hauspie
Univ. Lille, CNRS, Centrale Lille, UMR 9189 CRIStAL
F-59000 Lille, France
michael.hauspie@univ-lille.fr

***Abstract*—Les attaques DDoS restent un problème majeur malgré les efforts de la communauté scientifique et industrielle pour fournir des solutions de détection efficaces. Les fournisseurs de solution cloud sont des cibles de choix pour les cyber-criminels en raison de leur clientèle et de leur infrastructure. La volumetrie du trafic qui transite via ces infrastructures rend difficile l'utilisation de la plupart des méthodes de l'état de l'art pour protéger les réseaux contre de telles attaques. Dans cet article, nous abordons la piste prometteuse des méthodes statistiques pour obtenir une méthode de détection plus efficace.**

***Index Terms*—DDoS, Cloud, Statistiques, Hyperscalers**

I. Introduction

Les attaques par déni de service (Denial of Service, DoS) et déni de service distribué (Distributed Denial of Service, DDoS) sont connues depuis plusieurs décennies par la communauté industrielle et scientifique. Ces attaques sont utilisées pour rendre un service ou une ressource inaccessible en surchargeant les serveurs ou les réseaux avec une grande quantité de trafic. Ces attaques sont de plus en plus courantes et sophistiquées, et représentent un défi récurent pour la communauté. Il existe plusieurs approches pour détecter les attaques DDoS, mais de nombreux défis subsistent pour améliorer et rendre plus résiliente la détection de celles ci. En effet, les cyber-criminels cherchent continuellement des nouveaux moyens de contourner les systèmes de détection. De plus, des nouveaux paradigmes tels que le cloud computing, bousculent continuellement la manière dont les attaques sont mises en œuvre.

Comme nous le verrons dans la suite de ce papier, les fournisseurs de services cloud (ou *cloud providers*) sont des cibles de choix pour les attaques DDoS. Ils offrent un large catalogue de ressources pour leurs clients et sont souvent utilisés pour héberger des sites web et des services importants comme les plate-formes de commerce électronique, les systèmes bancaires en ligne, les services de diffusion vidéo, etc. Ces services sont cruciaux pour les entreprises et les individus, de sorte que les perturbations causées par les attaques DDoS peuvent avoir des conséquences économiques importantes faisant de ces fournisseurs des cibles de choix.

Après avoir parcourus l'état de l'art, les récents développement sur la détection d'attaques s'articulent autour de plusieurs grandes thématiques. Parmi celles-ci, nous pouvons citer l'apprentissage automatique [1], la détection d'anomalie en utilisant des modèles statistiques [2], ou des méthodes de détection reposant sur des signatures d'attaques [3], etc. Nous avons choisi d'étudier les méthodes utilisant des statistiques, puisque, comme nous le verrons, elles nous paraissent les plus à même d'être utilisées dans des environnements soumis à un trafic important tels que ceux gérés par les cloud providers.

II. Les cloud providers et les attaques DDoS

Un fournisseur de service cloud est une entreprise qui offre des services, tels que l'hébergement de sites web, la gestion de bases de données, le stockage de données, la mise à disposition de serveurs virtuels (VPS), etc. Les clients peuvent accéder à ces services via Internet et payer uniquement pour les ressources qu'ils utilisent de manière mensuelle ou à l'heure. OVHcloud est un exemple de cloud provider.

Ces fournisseurs cloud sont des cibles de choix pour des attaques DDoS. Ils disposent de ressources informatiques importantes, mais cela signifie également qu'ils peuvent être la cible d'attaques de grande ampleur, comme nous l'avons vu par le passé. Les attaques DDoS utilisant des milliers, voire des millions d'appareils IoT pour envoyer un grand nombre de requêtes malveillantes vers une cible spécifique, sont fréquentes [4].

Les perturbations causées par ces attaques peuvent avoir des conséquences économiques importantes pour les entreprises et pour les utilisateurs qui dépendent du service attaqué. Les attaques DDoS peuvent également causer des perturbations pour les fournisseurs de services eux-mêmes, entraînant des pertes financières et une réputation endommagée. Notamment, ces dernières années, des travaux on été menés pour comprendre les motivations des cyber-criminels à lancer des attaques

This work is also supported by CNRS IRCICA UAR-3380

DDoS [5]. Parmi les motivations identifiées, on peut citer les suivantes :

- **extorsion** : en visant des entreprises publiques ou privées, ils proposent ensuite de stopper l'attaque si la victime paye une rançon ;
- **activisme** : pour faire passer un message ou encore protester contre les agissements d'une entreprise ;
- **sabotage** : un concurrent, un client mécontent, ou encore juste pour prouver qu'ils en sont capables, les cyber-criminels peuvent lancer des attaques pour saboter les activités commerciales ou les services d'une entreprise ou d'une organisation ;
- **diversion** : des attaques DDoS de grande ampleur peuvent également être lancées pour dissimuler d'autres activités malveillantes, comme le vol de données ou l'espionnage.

Les cloud providers sont alors soumis à une pression croissante pour garantir la disponibilité et la sécurité des services, cette garantie étant bien souvent définie dans un contrat. C'est pourquoi la mise en place de mesures de sécurité protégeant leur infrastructure et leurs clients contre ces attaques est nécessaire. De plus, les solutions mises en place doivent évoluer pour contrer les améliorations constantes mises en œuvre par les cyber-criminels pour échapper à la vigilance des fournisseurs.

III. Etat de l'art sur la détection d'attaques DDoS

La recherche académique et industrielle sur la détection des attaques DDoS a connu un développement important au cours des dernières années. Les chercheurs ont développé des méthodes pour détecter les attaques DDoS en utilisant des techniques d'apprentissage automatique, d'analyse de comportement, de filtrage de trafic et de défense distribuée. Dans cette section, nous allons détailler celles qui concentrent les efforts de recherches à l'heure actuelle, puis nous expliquerons pourquoi nous avons choisi d'étudier plus en profondeur les méthodes reposant sur des statistiques.

A. Systèmes basées sur les signatures

Les systèmes de détection d'attaques basés sur les signatures [3] utilisent des signatures prédéfinies pour identifier les flux suspects dans le trafic réseau. Ils comparent les flux entrants et sortant avec des signatures connues d'attaques DDoS, et si un flux correspond à une signature, il est considéré comme une attaque potentielle.

Les avantages de cette méthode sont principalement sa simplicité et sa rapidité. Les signatures peuvent être mises à jour rapidement pour prendre en compte de nouvelles attaques et les systèmes peuvent fonctionner en temps réel.

Cependant, les attaques peuvent facilement échapper à la détection en utilisant des techniques telles que l'obfuscation de paquets ou en modifiant les signatures. De plus, les systèmes de signature peuvent souffrir de faux positifs si les signatures sont mal définies ou si des paquets légitimes sont mal classés comme des attaques. Enfin, les systèmes basés sur les signatures sont souvent coûteux en termes de ressources humaines pour maintenir les signatures à jour et peuvent également entraîner une surcharge de travail pour les équipes en charge de celles ci.

Enfin, la détection basée sur les signatures nécessite généralement un accès aux données applicatives (requêtes et réponses HTTP par exemple) qui est souvent impossible à obtenir, soit pour des raisons techniques (chiffrement) ou des raisons éthiques (protection de la vie privée des usagers).

B. L'apprentissage automatique

Les techniques d'apprentissage automatique sont étudiées dans la littérature pour détecter des attaques DDoS appliquées aux cloud providers. Ces techniques peuvent être utilisées pour identifier des modèles de trafic normaux et détecter tout écart par rapport à ces modèles, ce qui peut indiquer une attaque.

Parmi les techniques d'apprentissage on distingue généralement l'apprentissage supervisé et l'apprentissage non supervisé.

L'apprentissage supervisé consiste à utiliser des jeux de données étiquetés pour apprendre à détecter les attaques DDoS. Une fois le modèle entraîné, il est utilisé pour détecter les attaques sur des données réelles. Les avantages de l'apprentissage supervisé pour détecter des attaques DDoS sont une précision élevée et une capacité à détecter des modèles dans les données d'attaque. Cependant, les inconvénients incluent la nécessité de grandes quantités de données d'entraînement étiquetées et la vulnérabilité aux biais dans les données d'entraînement [6].

Dans l'apprentissage non supervisé, il est question d'entraîner un modèle sur un jeu de données non étiquetées. On peut citer les techniques de regroupement (*clustering*) ou les réseaux de neurones auto-encodeurs [7].

Ces techniques permettent de détecter les anomalies dans les données de trafic réseau. En particulier, à l'inverse des techniques de détection par signature, ces techniques peuvent détecter des anomalies provenant d'attaques non connues à l'avance. Elles peuvent également s'adapter aux changements dans les modèles de trafic et s'améliorer au fil du temps.

Cependant, ces techniques d'apprentissage présentent certaines limitations. Tout d'abord, elles nécessitent des données d'entraînement de qualité, ce qui peut être difficile à obtenir pour certaines attaques. De plus, elles peuvent également être sensibles aux biais dans les données d'entraînement et peuvent ne pas être efficaces pour détecter certaines formes d'attaques. Enfin, il est important de noter que l'utilisation de ces techniques nécessite des ressources importantes en termes de calcul et de stockage pour fonctionner correctement.

C. Analyse et modélisation statistiques

L'usage de techniques d'analyse et de modélisation statistique est répandu dans la littérature mais leur application aux cas d'usage des cloud providers est peu étudiée. Ces techniques permettent de détecter des anomalies dans les données de trafic réseau en extrayant un modèle statistique

du trafic réel et en étudiant l'écart entre le trafic observé et ce modèle.

Les avantages de ces techniques sont qu'elles peuvent être facilement implémentées et utilisées — puisqu'elles se basent sur des méthodes éprouvées — et qu'elles ne nécessitent pas beaucoup de ressources, ce qui les rend adaptées pour une utilisation dans les environnements à fort trafic. Ces techniques permettent traiter de grandes quantités de données, ce qui les rend utiles pour les systèmes de détection d'attaques DDoS à grande échelle.

Ces techniques présentent cependant certaines limitations. Le système doit être correctement calibré, sous peine de générer un nombre important de faux positifs ou de faux négatifs. À l'instar des techniques par apprentissage, la qualité des jeux de données utilisés pour élaborer le système est importante. De plus, les techniques d'attaques plus complexe (obfuscation, poly-morphisme, etc.) peuvent rendre la détection plus difficile.

IV. Méthodes statistiques

Nous avons choisi d'étudier les systèmes qui reposent sur de l'analyse et de la modélisation statistique. Ces systèmes présentent l'avantage d'être plus robustes face aux nouvelles attaques [8]. Il est plus simple de faire évoluer ces systèmes pour prendre en compte aussi bien un nouveau type d'attaques qu'une évolution d'une attaque existante, ce qui présente un certain avantage par rapport aux méthodes reposant sur des signatures d'attaques.

Pour détecter des comportements malveillants au sein d'un trafic, nous allons chercher à mesurer des grandeurs numériques associées au trafic. Ces grandeurs peuvent être par exemple: le ratio de paquets TCP SYN sur TCP SYN+ACK, la taille des paquets, le nombre d'IP sources en communication avec une IP destination, etc.

Pour chacune de ces grandeurs, il est possible de définir une valeur moyenne et un écart type. On peut alors envisager de construire un modèle du trafic comme une corrélation valide des ces différentes valeurs. La procédure de détection d'attaque consiste alors en l'observation d'une déviation de ces mesures sur le trafic en cours par rapport à ce modèle.

Dans le contexte d'un fournisseur de service cloud, étant donné les volumes de trafic rencontrés, il n'est pas envisageable de mesurer ces grandeurs sur l'intégralité des paquets qui transitent dans l'infrastructure. À titre d'exemple, le volume de trafic que l'on devrait observer pour traiter le cœur de réseau d'OVHcloud et de l'ordre de plusieurs tera octets par seconde, ce qui représente plusieurs ordres de grandeur supplémentaires par rapport aux jeux de données communément utilisés dans la communauté comme CIC-IDS [9]. En pratique, sur de tels volumes, il n'est possible d'observer qu'un résumé des paquets sous forme de flux Netflow ou sFlow [10] qui sont eux mêmes échantillonnés.

Notre travail actuel consiste alors à établir notre modèle sur l'échantillonnage du trafic réel. Puisque la mesure est le fait d'un échantillonage, nous devons considérer trois paramètres : le nombre d'échantillons observés n, la valeur estimée donnée sous la forme d'un intervalle de confiance I_c, et la probabilité p que la valeur réelle soit dans cet intervalle. Ces trois paramètres sont inter-dépendants. Il existe différentes formules de la théorie de l'échantillonnage[1] pour les calculer. Ces formules nous permettent de faire une estimation de la valeur réelle, non calculable à la volée.

En d'autres termes, nous pouvons déterminer l'intervalle entre la valeur estimée et la valeur attendue et utiliser ces formules pour calculer la probabilité de que nous observions cette valeur si le trafic est légitime. Un faisceau de seuils sur les probabilités des différentes mesures nous permet de lever une alarme.

V. Conclusion

Dans cet article, nous avons identifié les problématiques propres au traitement des flux de données réseau à des fins de cyber-sécurité dans le contexte d'un fournisseur de services cloud. Nous avons établi que ces flux ne pouvaient être traités que de façon échantillonnaire. Cet état de fait distingue notre problématique de celle généralement traitée dans l'état de l'art.

Dans la suite de nos travaux, nous nous proposons de caractériser un trafic à l'échelle d'un cloud provider dans le but 1) d'offrir à la communauté scientifique un jeux de données pertinent pour ce type d'infrastructure et 2) d'évaluer des approches statistiques dans un environnement de production.

References

[1] M. Suresh and R. Anitha, "Evaluating machine learning algorithms for detecting ddos attacks," in *Advances in Network Security and Applications: 4th International Conference, CNSA 2011, Chennai, India, July 15-17, 2011 4*. Springer, 2011, pp. 441–452.

[2] M. Nooribakhsh and M. Mollamotalebi, "A review on statistical approaches for anomaly detection in ddos attacks," *Information Security Journal: A Global Perspective*, vol. 29, no. 3, pp. 118–133, 2020.

[3] M. Alenezi and M. J. Reed, "Methodologies for detecting dos/ddos attacks against network servers," in *The Seventh International Conference on Systems and Networks Communications ICSNC*, 2012, pp. 92–98.

[4] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "Ddos in the iot: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.

[5] S. Traer and P. Bednar, "Motives behind ddos attacks," in *Digital Transformation and Human Behavior: Innovation for People and Organisations*. Springer, 2021, pp. 135–147.

[6] N. Mehrabi, F. Morstatter, N. Saxena, K. Lerman, and A. Galstyan, "A survey on bias and fairness in machine learning," *ACM Computing Surveys (CSUR)*, vol. 54, no. 6, pp. 1–35, 2021.

[7] X. Zhang, J. Gai, Z. Ma, J. Zhao, H. Ma, F. He, and T. Ju, "Exploring unsupervised learning with clustering and deep autoencoder to detect ddos attack," *Journal of Computers*, vol. 33, no. 4, pp. 29–44, 2022.

[8] H. Majed, H. N. Noura, O. Salman, M. Malli, and A. Chehab, "Efficient and secure statistical ddos detection scheme." in *ICETE (1)*, 2020, pp. 153–161.

[9] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, "Developing realistic distributed denial of service (ddos) attack dataset and taxonomy," in *2019 International Carnahan Conference on Security Technology (ICCST)*. IEEE, 2019, pp. 1–8.

[10] P. Phaal, S. Panchen, and N. McKee, "Rfc 3176 : Inmon corporation's sflow: A method for monitoring traffic in switched and routed networks," 2001.

[1] Nous considérons notamment la méthode de Wilson de score avec correction de continuité