Αντιμετώπιση Επιθέσεων DDoS στο Επίπεδο Δεδομένων με Μεθόδους Μηχανικής Μάθησης

Οι επιθέσεις άρνησης παροχής υπηρεσιών (Distributed Denial of Service, DDoS) αποτελούν ένα από τα επικρατέστερα προβλήματα για τους διαχειριστές δικτυακών υποδομών. Οι επιθέσεις αυτές στοχεύουν σε δίκτυα, εφαρμογές ή/και υπηρεσίες, προσπαθώντας να παρεμποδίσουν την ομαλή λειτουργία τους.

Για την αποδοτική αντιμετώπιση (mitigation) επιθέσεων DDoS έχουν μελετηθεί πολυάριθμες μέθοδοι. Ανάμεσα σε αυτές τις μεθόδους, εκείνες που βασίζονται σε μοντέλα μηχανικής μάθησης (machine learning) έχουν αποδειχθεί ιδιαίτερα υποσχόμενες. Η υλοποίηση των μοντέλων αυτών πραγματοποιείται, συνήθως, στο επίπεδο χρήστη (user space) λόγω της ευκολίας ανάπτυξής τους με δημοφιλή frameworks, π.χ. scikit-learn, TensorFlow ή PyTorch [1].

Ωστόσο, η επεξεργασία δικτυακής κίνησης ανά πακέτο στο user space εισάγει σημαντικές καθυστερήσεις στην αντιμετώπιση επιθέσεων. Ως αποτέλεσμα, οι user space μηχανισμοί ασφαλείας αδυνατούν να ανταποκριθούν στο διαρκώς αυξανόμενο μέγεθος των σύγχρονων επιθέσεων DDoS. Για το σκοπό αυτό αναζητούνται λύσεις σε σύγχρονες τεχνολογίες προγραμματισμού στο επίπεδο δεδομένων (data plane) δικτυακών συσκευών (switches) ή καρτών δικτύου που επεξεργάζονται τη δικτυακή κίνηση χωρίς να την προωθήσουν στο user space.

Η διπλωματική θα διερευνήσει την αποδοτική αντιμετώπιση επιθέσεων DDoS με μοντέλα machine learning υλοποιημένα στο data plane. Συγκεκριμένα, θα χρησιμοποιηθούν μία ή περισσότερες τεχνολογίες προγραμματισμού σε data planes, όπως είναι το XDP framework [2], η γλώσσα P4 [3] και το DPDK [4]. Η διπλωματική θα επικεντρωθεί (i) στην αποδοτική εξαγωγή των features από τη δικτυακή κίνηση και (ii) την ακριβή απεικόνιση των μοντέλων μηχανικής μάθησης στο data plane [5, 6]. Τα data plane μοντέλα θα συγκριθούν με τα αντίστοιχα στο user space.

Για την πειραματική αξιολόγηση των παραπάνω μοντέλων θα χρησιμοποιηθούν δημόσια διαθέσιμα σύνολα δεδομένων καλόβουλης και κακόβουλης δικτυακής κίνησης, τα οποία χρησιμοποιούνται ευρέως στη βιβλιογραφία, π.χ. [7].

[1] Top Machine Learning Frameworks to Use, https://www.bmc.com/blogs/machine-learning-ai-frameworks/
[2] T. Høiland-Jørgensen et al., “The Express Data Path: Fast Programmable Packet Processing in the Operating System Kernel”, in the 14th international conference on emerging networking experiments and technologies, December 2018
[3] P. Bosshart et al., “P4: Programming Protocol-independent Packet Processors”, in the ACM SIGCOMM Computer Communication Review, July 2014
[4] DPDK, https://www.dpdk.org/
[5] C. Zheng et al., “Automating In-Network Machine Learning”, in arXiv preprint arXiv:2205.08824, May 2022
[6] B. M. Xavier et al, “Programmable switches for in-networking classification”, in IEEE Conference on Computer Communications (INFOCOM), May 2021
[7] DDoS Evaluation Dataset (CIC-DDoS2019), https://www.unb.ca/cic/datasets/ddos-2019.html
[8] N. Kostopoulos, S. Korentis, D. Kalogeras & V. Maglaris, “Mitigation of DNS Water Torture Attacks within the Data Plane via XDP-Based Naive Bayes Classifiers”, in Proc. of the 10th IEEE International Conference on Cloud Networking – IEEE CloudNet 2021, Virtual Event, November 2021.