Verification in the Wild. IEEE WACV. 2016.
7. Wang X., Xie L., Dong C., Shan Y. Real-ESRGAN: Training Real-World Blind Super-Resolution with Pure Synthetic Data. ICCV Workshops. 2021. P. 1905–1914.
8. Chen Y., Tai Y., Liu X. et al. FSRNet: End-to-End Learning Face Super-Resolution with Facial Priors. CVPR. 2018. P. 2492–2501.

Моделювання мережевих атак на основі аналізу графу мережевих взаємодій

УДК 004.056.55

Дмитро Хіжняк[1], Геннадій Шаповалов[2]

Національний університет «Одеська політехніка»,
[1]9480560@stud.op.edu.ua, [2]shapovalov@op.edu.ua

Сучасні комп'ютерні мережі функціонують в умовах постійного зростання кількості кіберзагроз. Особливо поширеними є атаки типу port scan, DoS/DDoS та brute force, які спрямовані на порушення доступності сервісів або отримання несанкціонованого доступу до систем [1]. Традиційні методи виявлення атак, засновані на сигнатурах, мають обмежену ефективність, особливо щодо нових або модифікованих типів атак [2].

Одним із перспективних підходів є використання графового аналізу, який дозволяє представити мережевий трафік у вигляді орієнтованого графа, де вузли відповідають IP-адресам або хостам, а ребра — мережевим взаємодіям між ними [3]. Такий підхід дає можливість враховувати структуру взаємозв'язків у мережі та виявляти аномальні патерни поведінки.

Метою роботи є моделювання мережевих атак **з** використанням графового аналізу та розробка застосунку для виявляти у мережі аномальних патернів поведінки.

Для оцінки поведінки вузлів використовується інтегральний показник аномальності, що формується на основі нормалізованих графових метрик, зокрема ступеня вершини, інтенсивності трафіку та кількості унікальних з'єднань:

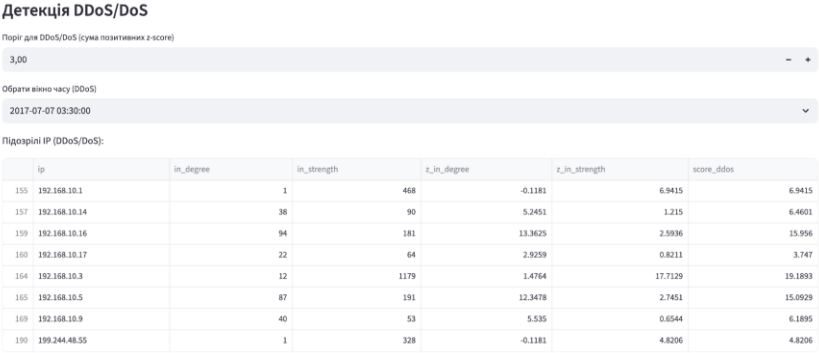
$$z(x_t) = \frac{x - \mu_t}{\sigma_t},$$

де x_t - значення метрики в момент часу t (або у вікні Δt), μ_t та σ_t - середнє і стандартне відхилення метрики у базовому періоді (наприклад, у попередніх k вікнах).

За підходом, що використано в роботі, аналіз структури графа дозволяє виділити характерні ознаки можливих атак. Для port scan типовим є сценарій «один до багатьох», для DDoS — «багато до одного», тоді як brute force характеризується інтенсивними повторюваними з'єднаннями між обмеженою кількістю досліджуваних мережевих вузлів.

Реалізація запропонованого підходу виконана у вигляді програмного застосунку, що здійснює обробку flow-даних, побудову графа мережевих

взаємодій та обчислення відповідних метрик. Для експериментальної перевірки використано набір даних CICIDS2017 [4].



Детекція DDoS/DoS

Поріг для DDoS/DoS (сума позитивних z-score)

3,00

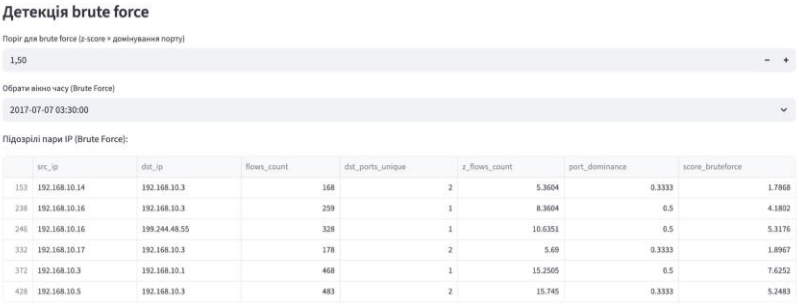
Обрати вікно часу (DDoS)

2017-07-07 03:30:00

Підозрілі IP (DDoS/DoS):

	ip	in_degree	in_strength	z_in_degree	z_in_strength	score_ddos
155	192.168.10.1	1	468	-0.1181	6.9415	6.9415
157	192.168.10.14	38	90	5.2451	1.215	6.4601
159	192.168.10.16	94	181	13.3625	2.5936	15.956
160	192.168.10.17	22	64	2.9259	0.8211	3.747
164	192.168.10.3	12	1179	1.4764	17.7129	19.1893
165	192.168.10.5	87	191	12.3478	2.7451	15.0929
169	192.168.10.9	40	53	5.535	0.6544	6.1895
190	199.244.48.55	1	328	-0.1181	4.8206	4.8206

Рис.1. Результати виявлення підозрілих вузлів для DoS/DDoS у вибраному часовому вікні



Детекція brute force

Поріг для brute force (z-score × домінування порту)

1,50

Обрати вікно часу (Brute Force)

2017-07-07 03:30:00

Підозрілі пари IP (Brute Force):

	src_ip	dst_ip	flows_count	dst_ports_unique	z_flows_count	port_dominance	score_bruteforce
153	192.168.10.14	192.168.10.3	168	2	5.3604	0.3333	1.7868
238	192.168.10.16	192.168.10.3	259	1	8.3604	0.5	4.1802
246	192.168.10.16	199.244.48.55	328	1	10.6351	0.5	5.3176
332	192.168.10.17	192.168.10.3	178	2	5.69	0.3333	1.8967
372	192.168.10.3	192.168.10.1	468	1	15.2505	0.5	7.6252
428	192.168.10.5	192.168.10.3	483	2	15.745	0.3333	5.2483

Рис.2. Результати виявлення brute force для підозрілої пари вузлів

Аналіз адекватності у порівнянні з експериментальними даними свідчить про те, що отримані результати підтверджують доцільність використання графових характеристик, що дозволяє ефективно виявляти типові мережеві атаки та їх поведінкові патерни.

1. Lippmann R. et al. The 1999 DARPA Off-Line Intrusion Detection Evaluation // Computer Networks. — 2000.
2. Sommer R., Paxson V. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection // IEEE Symposium on Security and Privacy. — 2010.
3. Newman M. Networks: An Introduction. — Oxford University Press, 2010.
4. Sharafaldin I., Lashkari A. H., Ghorbani A. A. Toward Generating a New Intrusion Detection Dataset // ICISSP. — 2018.