

ELEKTRON TARMOQ RESURLARIDAGI ANOMAL HOLATLARNI ANIQLASH BOSQICHLARI

Fozilov Fayzullo Fatxulla o'g'li¹, Abdusadikov Murodjon Abdukarimovich²

¹ Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

¹ f.fozilov@tuit.uz, ² murodjon1991@icloud.com

Annotatsiya: Hozirgi vaqtda elektron tarmoq resurslari hayotimizning ajralmas qismi bo'lib, ularning ishonchliligi va xavfsizligi asosiy rol o'ynaydi. Tarmoq trafigidagi va elektron resurslarning xatti-harakatlaridagi anomaliyalarni doimiy monitoring qilish va aniqlash ma'lumotlar barqarorligi va yaxlitligini ta'minlash zaruriyatiga aylandi. Ushbu maqola statistik va xatti-harakatlar modellari asosida elektron tarmoq resurslarida anomaliyalarni aniqlash algoritmi va dasturiy ta'minotini taqdim etadi. Biz taklif etilayotgan yondashuvning samaradorligini real ma'lumotlar asosida tahlil qilamiz va statistik natijalarni jadval shaklida taqdim etamiz.

Kalit so'zlar: anomaliya, anomaliyani aniqlash, tarmoq anomaliyasini aniqlash, DDoS, tarmoq elektron resurslari, mashinali o'qitish, axborot xavfsizligi.

KIRISH

Veb-serverlar, ma'lumotlar bazalari va tarmoq qurilmalari kabi onlayn elektron resurslar tashkilotlar va foydalanuvchilar uchun juda muhimdir. Ushbu resurslarning g'ayritabiiy xatti-harakatlari potentsial xavfsizlik muammolari, kiber hujumlar yoki uzilishlarni ko'rsatishi mumkin. Imzoga asoslangan an'anaviy aniqlash usullari ko'pincha yangi va murakkab hujumlarga qarshi samarasiz. Shu munosabat bilan statistik va xatti-harakatlar modellariga asoslangan anomaliyalarni aniqlash algoritmlari tobora muhim rol o'ynamoqda.

Mavjud yondashuvlarni ko'rib chiqish

Anomaliyalarni aniqlashning mavjud yondashuvlarini quyidagi toifalarga bo'lish mumkin:

Imzo tahlili: Kuzatilgan ma'lumotlarni ma'lum hujum imzolari bilan taqqoslash asosida. Ma'lum tahdidlarga qarshi samarali, ammo yangilarini aniqlay olmaydi.

Statistik tahlil: Oddiy xatti-harakatlarni aniqlash va anormalliklarni ta'kidlash uchun statistik usullardan foydalanadi. Noma'lum hujumlarga qarshi samarali, ammo noto'g'ri ijobiy natijalar berishi mumkin.

Xulq-atvor tahlili: foydalanuvchi yoki tizim xatti-harakatlarini modellashtiradi va ushbu xatti-harakatlardan chetga chiqish asosida anomaliyalarni aniqlaydi. Keyinchalik

murakkab, ammo samaraliroq yondashuv.

Mashinani o'rganish:

Ma'lumotlarni normal va g'ayritabiiy qilib tasniflash uchun mashinani o'rganish algoritmlarini qo'llaydi. Moslashuvchanlik va moslashuvchanlikni ta'minlaydi.

Ushbu maqolada taklif qilingan yondashuv anomaliyalarni aniqlashning aniqligini oshirish uchun statistik va xatti-harakatlar tahlilini birlashtiradi.

Anomal holatlarni aniqlash bosqichlari

Taklif etilayotgan algoritm quyidagi bosqichlarni o'z ichiga oladi:

Ma'lumotlarni yig'ish:

HTTP so'rovlari, DNS so'rovlari, TCP ulanishlarini o'z ichiga olgan tarmoq trafigini monitoring qilish.

Elektron resurslardan (masalan, veb-server, ma'lumotlar bazasi) kirish jurnallari va voqealar to'plami.

Ma'lumotlarni oldindan qayta ishlash:

Dublikatlarni va ahamiyatsiz ma'lumotlarni olib tashlash.

To'g'ri statistik tahlilni ta'minlash uchun ma'lumotlarni normallashtirish.

Ma'lumotlarni tahlil qilish uchun mos formatga aylantirish (masalan, vaqt seriyasi).

tahlil:

Har xil

parametrlar bo'yicha o'rtacha, median, standart og'ish kabi asosiy statistik ko'rsatkichlarni hisoblash (masalan, vaqt birligidagi so'rovlar soni, uzatilgan ma'lumotlar hajmi, javob vaqti).

Oddiy taqsimotdan og'ishlarni aniqlash uchun statistik testlardan foydalanish (masalan, Z-test, t-test).

Xulq-atvorni tahlil qilish:

To'plangan ma'lumotlar asosida normal xatti-harakatlarni modellashtirish, foydalanuvchi profilini yaratish, oddiy xatti-harakatlar modellarini yaratish kabi usullardan foydalanish.

Hozirgi xatti-harakatni baholang va uni model bilan solishtiring.

Anomaliyalarni aniqlash:

Statistik va xatti-harakatlar parametrlari uchun chegaralarni aniqlang. Agar kuzatilgan qiymatlar belgilangan chegaralardan tashqariga tushsa, anomaliyalarni aniqlang.

Anomaliyalar aniqlanganda ogohlantirishlarni yarating.

Dasturiy ta'minot

Dasturiy ta'minot Python bilan ishlab chiqilgan quyidagi kutubxonalardan foydalanish:

pyshark

- tarmoq trafigini olish va tahlil qilish uchun . pandas va numpy - ma'lumotlarni qayta

ishlash va tahlil qilish uchun.

ma'lumotlarni vizualizatsiya qilish uchun.

arxitekturasi quyidagi modullardan iborat:

yig'ish moduli: Tarmoq trafigini va jurnallarni yig'ish uchun mas'ul.

<https://scopusacademia.org/>

scipy - statistik tahlil uchun.

matplotlib va seaborn -

Dasturiy ta'minot

- Ma'lumotlarni

- Ma'lumotlarni

oldindan qayta ishlash moduli: Ma'lumotlarni normallashtirish va filtrlashni amalga oshiradi.

hisob-kitoblar va testlarni amalga oshiradi.

Oddiy xatti-harakatlarni modellashtiradi va hozirgi xatti-harakatlar bilan taqqoslaydi.

chegara qiymatlaridan og'ishlarni baholaydi va ogohlantirishlarni yaratadi.

grafik va jadvallar ko'rinishida taqdim etadi.

Tahlil va statistika

Taklif etilayotgan algoritim samaradorligini tahlil qilish uchun haqiqiy ma'lumotlar, shu jumladan oddiy trafik va simulyatsiya qilingan hujumlar bo'yicha test o'tkazildi. Quyidagi parametrlar o'lchandi:

Aniqlik: (**Accuracy**) To'g'ri tasniflangan ma'lumotlarning nisbati.

To'liqlik: (**Recall**) to'g'ri aniqlangan anomaliyalarning nisbati.

Aniqlik: (**Precision**) barcha aniqlangan anomaliyalar orasida haqiqiy anomaliyalar nisbati.

F1-ball: (**F1-score**) Aniqlik va eslab qolishning garmonik o'rtacha.

Noto'g'ri ijobiy ko'rsatkich (**False Positive Rate**): Noto'g'ri tasniflangan oddiy ma'lumotlarning foizi .

Tab. 1. Jadval ma'lumotlari:

Parametr	Ko'rsadgich
Ma'lumotlar miqdori	10000
Anomaliyalar soni	1500
Aniqlik	0,965
To'liqlik (eslab qolish)	0,920
Aniqlik	0,942

Parametr	Ko'rsadgich
F1 ball	0,931
Noto'g'ri ijobiy ko'rsatkich (FPR)	0,025

5.2. Statistik xulosalar:

Taklif etilgan algoritm anomaliyalarni aniqlashning yuqori aniqligini ko'rsatdi, bu aniqlik, eslab qolish va aniqlik qiymatlari bilan tasdiqlangan. F1-o'lchov qiymati anomaliyalarni aniqlashning to'liqligi va aniqligini ta'minlovchi natijalar muvozanatini ko'rsatadi. Noto'g'ri ijobiy ko'rsatkich algoritm bir nechta noto'g'ri musbatlarni hosil qilishini ko'rsatadi.

5.3. Grafik tahlil:

Trafik taqsimoti grafigi qanday anomal hodisalarni aniq ko'rsatdi, masalan. DDoS hujumlari yoki so'rovlar sonining keskin o'sishi odatdagi taqsimotdan chetga chiqdi. Quyidagi parametrlar asosida ma'lumotlarda g'ayritabiiy hodisalar aniqlandi: soniyada so'rovlar soni, uzatilgan ma'lumotlar hajmi, serverning javob vaqti, turli portlardan foydalanish

XULOSA

Ushbu maqola statistik va xatti-harakatlarning kombinatsiyasiga asoslangan elektron tarmoq resurslaridagi anomaliyalarni aniqlash uchun algoritm va dasturiy ta'minotni taqdim etdi. Haqiqiy ma'lumotlar bo'yicha test natijalari tavsiya etilgan yondashuvning yuqori samaradorligini ko'rsatdi. Statistik va xulq-atvor modellaridan foydalanish hujumlarning ma'lum va yangi turlarini, shuningdek, elektron resurslarning ishlashidagi nosozliklarni aniqlash imkonini beradi.

FOYDALANILGAN ADABIYOT

1. Dong S. et al., "Network abnormal traffic detection model based on semi-supervised deep reinforcement learning", IEEE Transactions on Network and Service Management, vol. 18, no. 4, pp. 4197-4212, 2021.
2. Yao H., Liu Y. and Fang C. "An abnormal network traffic detection algorithm based on big data analysis", International Journal of Computers Communications & Control, vol. 11, no. 4, pp. 567-579, 2016.

3. Khan, L. U., & Hayat, M. (2019). Anomaly detection in network traffic using machine learning: A survey. *Journal of King Saud University - Computer and Information Sciences*. DOI: 10.1016/j.jksuci.2019.07.008.
4. Tian C. Application of Homomorphic Encryption in Block Chain Data Security of the Internet of Things Network Security Technology and Application, 2018, 3, pp. 34–36.
5. Ahmed M., Naser Mahmood A., and Hu J., A survey of network anomaly detection techniques, *Journal of Network and Computer Applications*. 2016, 60, 19–31, <https://doi.org/10.1016/j.jnca.2015.11.016>, 2-s2.0-84950256593.
6. Zhang, Y., & Wang, L. (2018). A hybrid model for anomaly detection in network traffic. *Future Generation Computer Systems*, 79, pp.327-338. DOI: 10.1016/j.future.2017.09.010.
7. Raxmatov F.A., Xolmuminov O.T. Tarmoq elektron resurslariga DDOS hujumlari tahlili. *Raqamli Transformatsiya va Sun'iy Intellekt ilmiy jurnali*, 2024., № 2(2), Toshkent, -B. 133–137.
8. Tavoli R. Providing a method to reduce the false alarm rate in network intrusion detection systems using the multilayer perceptron technique and backpropagation algorithm, *Proceedings of the 5th Conference on Knowledge Based Engineering and Innovation (KBEI)*, March 2019, Tehran, Iran, IEEE.