KOMPYUTER TARMOQLARIDA TRAFIKNI FILTRLASHNING INTELEKTUAL USULLARI VA ALGORITMLARI TAHLILI

Samarov X. K.
(Muhammad Al-xorazimiy nomidagi TATU t.f.n. dotsent)
Teshaboyeva G.Q.
(Toshkent davlat agrar universiteti) "Raqamli ta'lim texnologiyalarini joriy etish va axborot xavfsizligini ta'minlash" bo'limi boshlig'i
Tursunov Bekzod Axrorovich
(TDAU PhD mustaql tadqiqotchi)
Toshkent davlat agrar universiteti "Raqamli ta'lim texnologiyalarini joriy etish va axborot xavfsizligini ta'minlash" bo'limi kontent menedjeri
Pochta manzil:b-tursunov87@mail.ru
https://doi. org/10.5281/zenodo.10910907

Annotatsiya: Ushbu ishda Kompyuter tarmoqlarida trafikni filtrlashning va Kompyuter tarmog'ining xavfsizligini yaxshilash uchun trafigini tahlil qilish orqali zararli yoki kiruvchi kontentni bloklash shunigdek cheklash uchun ishlatiladigan usullari va algoritmlar samaradorligini oshirish.

Kalit so'zlar: Kompyuter tarmoq trafikni filtrlashning xavfsizligini tahlil qilish usullari va algoritmlari.

1.Trafik Filtrlash:

- Trafik filtrlash, kompyuter tarmoqlaridagi ma'lumotlar to'plamini o'z ichiga oladi va ularga qarab tahlil qiladi.
- Ushbu tahlil natijasida, yaxshi va yomon trafik o'rtasidagi farq aniqlanadi.
- Filtrlashning asosiy maqsadi, zararli ma'lumotlarni ajratib olish va tarmoq xavfsizligini ta'minlashdir.

2.Intellektual Usullar:

- Intellektual usullar, trafik filtrlash uchun yozilgan texnikalar va algoritmlardir.
- Bu usullar, ma'lumot analizi va ma'lumotlar ustida iqtisodiy qarorlarni qabul qilishga yordam beradigan intellektual komponentlardan foydalanadi.
- Odatda, bu usullar masofavi o'rganish, ma'lumotlarni tahlil qilish, tahlil natijalarini tushunish kabi vazifalarni bajarishda ishlatiladi.

3. Algoritmlar:

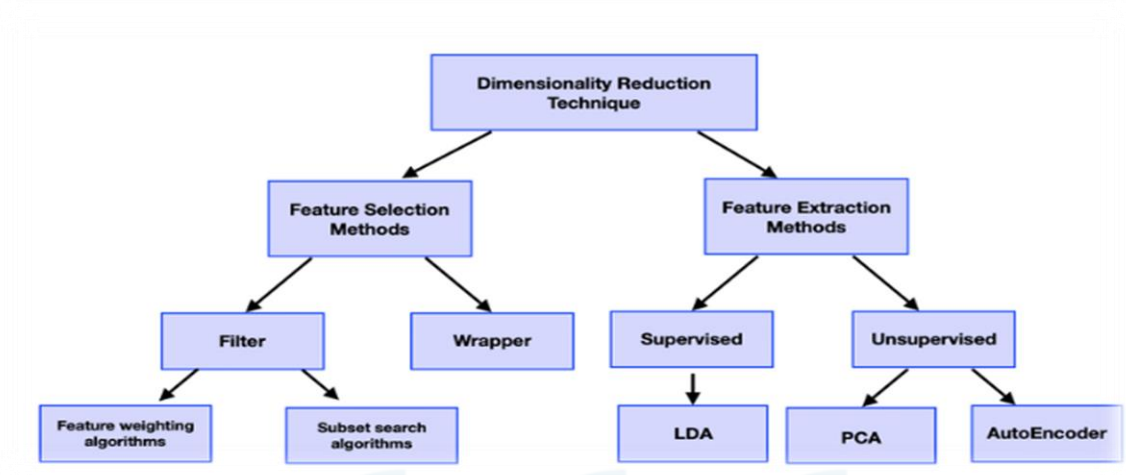
- Trafikni filtrlash uchun bir qancha algoritmlar mavjud.
- Shuningdek, ma'lumotlar ustida tahlil qilish, aniq maqsadlar uchun masofaviy o'rganish, ma'lumotlarni sinash va boshqa vazifalarni bajarish uchun vektoriga asoslangan algoritmlar, sinash uchun k-means, bayes qarorlash algoritmi, jadvallar ko'rinishida va boshqa vazifasiga mos ravishda algoritmlarni qo'llash mumkin.

Bu yalpi ma'lumotlar kompyuter tarmoqlarida trafikni filtrlashning intellektual usullari va algoritmlari haqida. Bir tahlil va amaliyot uchun tafsilotli jadval yoki dasturlarni ko'rib chiqishingiz tavsiya etiladi.

Kompyuter tizimlarida trafikni filtrlash - bu internet trafigini tahlil qilish orqali zararli yoki kiruvchi kontentni bloklash yoki cheklash uchun ishlatiladigan usul. Trafik filtrlash foydalanuvchilarning xavfsizligini ta'minlash, tarmoq samaradorligini oshirish va kirishni

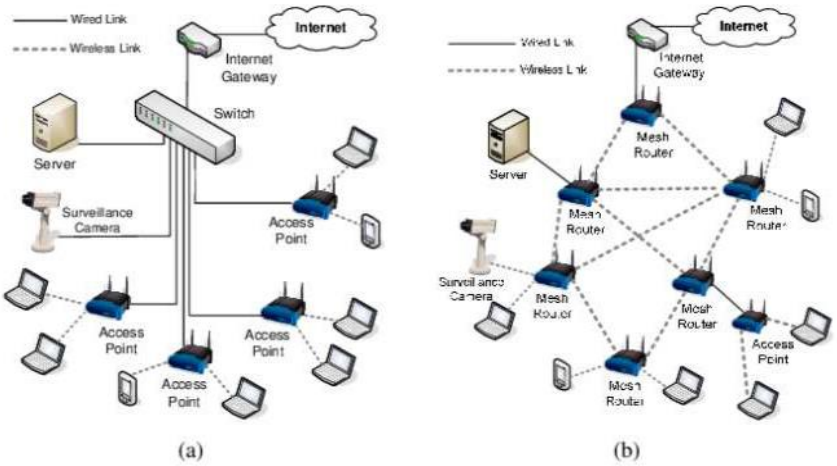
boshqarishni ta'minlash uchun ishlatiladi. Internet-trafikni filtrlash uchun ishlatiladigan ba'zi aqlli usullar va algoritmlar:

URL filtrlash: Ushbu usulda veb-saytlarning URL manzillari ma'lum mezonlarga muvofiq tekshiriladi va filtrlanadi. Masalan, zararli kontentni o'z ichiga olgan yoki taqiqlangan toifalarga kiruvchi veb-saytlar bloklanishi mumkin.



Kontent tahlili: Internet-trafik kontentni tahlil qilish texnikasi bilan skanerlanadi va zararli yoki keraksiz tarkibga ega sahifalar ma'lum kalit so'zlar, iboralar yoki iboralar yordamida aniqlanadi. Ushbu texnikada filtrlash uchun sun'iy intellekt va mashinani o'rganish algoritmlari bo'lishi mumkin.

IP-manzilni filtrlash: Internet-trafik manbai bo'lgan IP-manzillar tekshiriladi va ma'lum IP-manzillarga ega resurslar bloklanishi mumkin. Masalan, ma'lum bo'lgan zararli yoki spam IP manzillari bloklanishi mumkin.



Protokolni filtrlash: Filtrlash muayyan tarmoq protokollari yoki xizmatlari amalga oshirilishi mumkin. Masalan, P2P (Point-to-Point) fayl almashish protokollari yoki ma'lum aloqa protokollari bloklanishi mumkin.

Trafik statistikasi va xulq-atvor tahlili: Trafik filtrlash tizimlari tarmoqdagi foydalanuvchilarning trafik harakatlarini tahlil qilish orqali anomaliyalarni aniqlay oladi. Misol uchun, tarmoqda zararli hujum yoki botnet faoliyati mavjud bo'lganda, bu xatti-harakatlarni aniqlash va oldini olish mumkin.

Oq ro'yxat va qora ro'yxat: Filtrlash tizimlari ishonchli va ishonchsiz manbalarni aniqlash uchun oq ro'yxat yoki qora ro'yxat usullaridan foydalanishi mumkin. Oq ro'yxat ishonchli va xavfsiz manbalarga kirish imkonini beradi, qora ro'yxat esa zararli yoki kiruvchi manbalarni bloklaydi.

Joriy tahdidlar ma'lumotlari: Trafikni filtrlash tizimlari doimiy ravishda dolzarb tahdidlar ma'lumotlarini kuzatib boradi va ma'lum zararli manbalarni bloklaydi. Bu ma'lum zararli dasturlar, to'lov dasturlari yoki boshqa zararli kontentni o'z ichiga olgan veb-saytlarga kirishni bloklash uchun ishlatiladi.

Ushbu aqlli usullar va algoritmlar trafikni filtrlash tizimlariga zararli yoki kiruvchi kontentni samarali aniqlash va blokirovka qilish imkonini beradi. Xavfsizlik va kirishni boshqarish ehtiyojlariga muvofiq tuzilgan trafikni filtrlash tizimlari tarmoqlarning xavfsizligi va unumdorligini oshiradi. Biroq, filtrlashda foydalanuvchilarning shaxsiy huquqlarini himoya qilish va noto'g'ri blokirovka qilishning oldini olish kabi masalalarga e'tibor qaratish lozim.

References:

1. "Computer Networks: A Systems Approach" - Larry L. Peterson, Bruce S. Davie
2. "Network Security: Private Communication in a Public World" - Charlie Kaufman, Radia Perlman, Mike Speciner
3. "Deep Learning for Network Traffic Analysis and Cybersecurity: A Practical Guide to Using Machine Learning and Artificial Intelligence Techniques" - Seyed Ali Osmanoglu
4. "Traffic Anomaly Detection" - Pedro Casas, Marco Netto, Nuno Laranjeiro
5. "Machine Learning for Computer and Cyber Security: Principle, Algorithms, and Practices" - Sumeet Dua, Xian Du
6. https://www.sciencedirect.com/science/article/pii/S1110016823006014#kg005
7. https://www.jocm.us/uploadfile/2022/0121/20220121031227792.pdf
8. https://www.researchgate.net/publication/358202239_Intelligent_Traffic_Management_in_Next-Generation_Networks