TARMOQ TRAFIGIDAGI ANOMAL HARAKATLARNI ANIQLASH

Yuldoshev Ozodxon Juraxonovich
Samarkand Davlat Universiteti
Mustaqil tadqiqotchi

Annotatsiya: Tarmoq trafigidagi anomal harakatlarni aniqlash zamonaviy axborot texnologiyalari va kiberxavfsizlik sohasida muhim ahamiyat kasb etadi. Internet va boshqa tarmoqlar orqali uzatiladigan ma'lumotlarning hajmi va murakkabligi kundan-kunga ortib borayotgani sababli, tarmoq trafigidagi noan'anaviy, ya'ni anomal harakatlarni aniqlash tarmoq xavfsizligini ta'minlashda asosiy vazifalardan biriga aylangan. Anomal harakatlar tarmoqdagi odatiy faoliyatdan farq qiluvchi, xavf tug‘dirishi mumkin bo‘lgan yoki tarmoqning ishlashiga salbiy ta'sir ko‘rsatadigan harakatlar sifatida qaraladi. Bu harakatlarni aniqlash orqali kiberhujumlarni oldini olish, tarmoqdagi nosozliklarni aniqlash va bartaraf etish imkoniyati paydo bo‘ladi.

Kalit so‘zlar: tarmoq, ma'lumotlar, anomal harakatlar, dasturlar, hodisalar, kiberxavfsizlik, internet.

Tarmoq trafigidagi anomal harakatlar turli ko‘rinishlarda namoyon bo‘lishi mumkin. Masalan, tarmoqda ma'lumotlarni noqonuniy o‘g‘irlash, xizmatni rad etish hujumlari, zararli dasturlar tarqalishi, tarmoq qurilmalarining noto‘g‘ri ishlashi yoki xakerlik harakatlari kabi hodisalar anomal harakatlar sifatida ko‘riladi. Ushbu hodisalar tarmoqning normal ishlashiga to‘sqinlik qilishi, ma'lumotlarning maxfiyligini buzishi va tizimlarning ishonchliligini pasaytirishi mumkin. Shu sababli, tarmoq trafigidagi anomal harakatlarni aniqlash tizimlari va metodlari ishlab chiqish va takomillashtirish dolzarb masala hisoblanadi. Anomal harakatlarni aniqlash jarayoni bir nechta bosqichlardan iborat bo‘lib, ulardan biri tarmoq ma'lumotlarini yig‘ishdir. Tarmoq qurilmalari va monitoring tizimlari yordamida trafigi haqidagi ma'lumotlar to‘planadi. Ushbu ma'lumotlarga paketlar

hajmi, manzil va port raqamlari, protokollar turi, uzatilish vaqti va boshqa atributlar kiradi. Keyingi bosqichda to‘plangan ma’lumotlar tahlil qilinadi va odatiy trafigi xususiyatlari aniqlanadi. Bu jarayon uchun statistik usullar, mashina o‘rganish algoritmlari va sun’iy intellekt texnologiyalari keng qo‘llaniladi. Statistik usullar yordamida tarmoq trafigining o‘rtacha qiymatlari va dispersiyalari hisoblanadi, shuningdek, normal taqsimotdan chetga chiqishlar aniqlanadi. Ushbu usullar oddiy va tez bajariladigan bo‘lsa-da, murakkab va o‘zgaruvchan trafigi holatlarini to‘liq qamrab olishi qiyin. Shu sababli, zamonaviy yondashuvlarda mashina o‘rganish algoritmlari keng qo‘llaniladi. Ushbu algoritmlar tarmoq trafigidagi naqshlarni o‘rganib, odatiy holatlardan farq qiluvchi anomal harakatlarni aniqlashga yordam beradi. Masalan, klasterlash, klassifikatsiya va neyron tarmoqlar kabi usullar trafigi ma’lumotlarini chuqur tahlil qilish imkonini beradi.[1]

Anomal harakatlarni aniqlash uchun ishlatiladigan yana bir yondashuv bu qoidalar asosida aniqlashdir. Bu usulda oldindan belgilangan qoidalar va shartlar asosida trafigi tahlil qilinadi va qoidalar buzilganda ogohlantirishlar beriladi. Ushbu usul oddiy va tushunarli bo‘lsa-da, yangi va ilg‘or hujumlarni aniqlashda yetarli darajada samarali bo‘lmasligi mumkin. Shu sababli, ko‘p hollarda qoidalar asosidagi yondashuv mashina o‘rganish bilan birgalikda qo‘llaniladi. Tarmoq trafigidagi anomal harakatlarni aniqlash tizimlari real vaqt rejimida ishlashi muhimdir. Chunki ko‘plab kiberhujumlar qisqa vaqt ichida amalga oshiriladi va ularga tezkor javob berish zarur. Real vaqt rejimida ishlaydigan tizimlar tarmoqdagi har qanday noan’anaviy faollikni darhol aniqlab, xavfsizlik bo‘yicha choralar ko‘rish imkonini beradi. Shu bilan birga, tizimlarning samaradorligi va aniqligi hamda noto‘g‘ri ogohlantirishlar soni muhim mezonlardir. Noto‘g‘ri ogohlantirishlar ko‘p bo‘lsa, xavfsizlik xodimlari ish samaradorligi pasayadi va haqiqiy tahdidlarni payqash qiyinlashadi.[2]

Anomal harakatlarni aniqlashda yuzaga keladigan asosiy muammolardan biri bu katta hajmdagi ma’lumotlarni qayta ishlash zarurati. Tarmoq trafigi doimiy ravishda katta hajmda ma’lumot uzatadi, bu esa tahlil jarayonini murakkablashtiradi. Shuning uchun, samarali ma’lumotlarni oldindan filtrlash, qisqartirish va muhim atributlarni tanlash muhim ahamiyatga ega. Shuningdek, bulutli hisoblash va katta ma’lumotlar texnologiyalari ushbu jarayonlarni tezlashtirish va samaradorligini oshirish uchun keng qo‘llanilmoqda. Tarmoq trafigidagi anomal harakatlarni aniqlash sohasida zamonaviy tadqiqotlar va amaliyotlar yangi yondashuvlarni ishlab chiqishga qaratilgan. Sun’iy intellekt va chuqur o‘rganish metodlari yordamida murakkab naqshlar va ilg‘or hujumlarni aniqlash imkoniyati oshmoqda. Shu bilan birga, avtomatlashtirilgan tizimlar yordamida xavfsizlik bo‘yicha qarorlar qabul qilish jarayoni tezlashmoqda. Bunday yondashuvlar tarmoq xavfsizligini yangi bosqichga olib chiqmoqda.[3]

Xulosa:

Xulosa qilib aytganda, tarmoq trafigidagi anomal harakatlarni aniqlash zamonaviy kiberxavfsizlik tizimlarining ajralmas qismi hisoblanadi. Bu jarayon tarmoqning normal ishlashini ta’minlash, kiberhujumlarga qarshi kurashish va ma’lumotlarning xavfsizligini saqlash uchun muhimdir. Zamonaviy texnologiyalar va algoritmlar yordamida tahlil qilish, real vaqt rejimida aniqlash va avtomatlashtirish imkoniyatlari tarmoq xavfsizligini yangi darajaga olib chiqmoqda. Shu bilan birga, bu sohada doimiy ravishda yangi metodlar va yondashuvlar ishlab chiqilishi zarur, chunki tarmoq tahdidlari ham doimiy ravishda rivojlanib boradi. Anomal harakatlarni aniqlash tizimlarini takomillashtirish va ularni amaliyotga joriy etish orqali tarmoq infratuzilmasining barqarorligi va xavfsizligini ta’minlash mumkin.

Foydalanilgan adabiyotlar:

1. Axmedov, S. (2023). Tarmoqdagi zararli trafik turlari va ularni aniqlash usullari. «Innovatsion Tadqiqotlar», 5-son, 45-53-betlar.

2. Qodirov, N. (2022). Tarmoq trafigidagi anomal harakatlarni aniqlashda sun’iy intellekt texnologiyalarining roli. «Axborot Texnologiyalari», 12-son, 112-120-betlar.

3. Tursunov, B. (2024). Kiberxavfsizlikda tarmoq trafigini monitoring qilish metodlari. Toshkent: O‘zbekiston Milliy Universiteti Nashriyoti.

4. Karimova, L. (2023). Tarmoq trafigidagi g‘ayritabiiy harakatlarni aniqlashning statistik usullari. «Ilmiy Izlanishlar», 8-son, 75-84-betlar.

5. Rustamov, J. (2021). Tarmoq xavfsizligi: Anomal harakatlarni aniqlash va oldini olish. Toshkent: Texnika Nashriyoti.

6. Islomov, D. (2023). Mashina o‘rganish asosida tarmoq trafigida anomaliyalarni aniqlash. «Kompyuter Ilmlari», 10-son, 98-107-betlar.