# TARMOQ TRAFIKIDA SHIFRLANGAN PAKETLARDAN TAHDIDLARNI ANIQLASH (ENCRYPTED TRAFFIC ANALYSIS)

***Umarov B.A[1]., Aminjonova R.A[2].***

*[1]FarDU katta o'qituvchisi p.f.f.d(PhD).* ***umaumarov@mail.ru.***

*[2]FarDU talabasi.* ***aminjonovaruxshona63@gmail.com***

*Annotatsiya. Ushbu maqolada zamonaviy tarmoq infratuzilmasida shifrlangan paketlardan tahdidlarni aniqlash masalasi (Encrypted Traffic Analysis, ETA) batafsil o'rganiladi. HTTPS, TLS va VPN texnologiyalari foydalanuvchi maxfiyligini ta'minlayotgan bo'lsa-da, zararli faoliyatni aniqlashni murakkablashtiradi. Tadqiqotda paket mazmunini ochmasdan, faqat oqim statistikasi, paket xususiyatlari va metama'lumotlarga asoslangan sun'iy intellekt yondashuvi ishlab chiqildi. Olingan natijalar shifrlangan trafikda tahdidlarni aniqlashning samarali va maxfiylikni saqlaydigan usullarini ko'rsatadi.*

*Kalit so'zlar: shifrlangan trafik, tarmoq xavfsizligi, Encrypted Traffic Analysis, sun'iy intellekt, mashinaviy o'rganish, tahdidlarni aniqlash.*

Kirish. Internet trafikining asosiy qismi so'nggi yillarda shifrlangan protokollar orqali uzatilmoqda. Bu foydalanuvchi ma'lumotlarini himoya qiladi, lekin zararli faoliyatni aniqlashni qiyinlashtiradi. Botnetlar, ma'lumotlar sizib chiqishi va boshqa zararli dasturlar shifrlangan kanal orqali faoliyat yuritadi. An'anaviy tarmoq monitoringi, odatda, paket mazmunini tekshirishga tayanadi, ammo shifrlangan trafikda bu ishlamaydi. Shu sababli, paket mazmunini ochmasdan trafik xatti-harakatlarini tahlil qilishga asoslangan ETA yondashuvlari dolzarb ilmiy yo'nalishga aylandi.

Adabiyotlar tahlili va metodologiya. So'nggi tadqiqotlar shifrlangan trafikni aniqlashda turli yondashuvlar mavjudligini ko'rsatadi. Ba'zi ishlarda TLS sessiyalarining vaqt xususiyatlari, paket o'lchamlari va oqim davomiyligi asosida ilovalarni aniqlashga urinishlar mavjud. Boshqalarda esa statistik va xulq-atvor xususiyatlari yordamida zararli trafikni aniqlashga e'tibor qaratilgan. Shu bilan birga, chuqur o'rganish (Deep Learning) va neyron tarmoqlarni qo'llash orqali yangi tahdidlarni aniqlash samaradorligini oshirishga intilishlar mavjud.

Ushbu tadqiqotda metodologiya quyidagi tarzda tashkil etildi: shifrlangan tarmoq oqimlaridan to‘plangan ma’lumotlar tahlil qilindi. Ma’lumotlarga paketlar soni, o‘rtacha va maksimal paket hajmi, oqim davomiyligi, paketlar orasidagi vaqt intervali, TLS qo‘l siqish (handshake) parametrlari va sertifikat bilan bog‘liq belgilar kiritildi. Shu bilan birga, oqimdagi anomal xatti-harakatlarni aniqlash uchun statistika asosida xususiyatlar ajratildi.

Keyinchalik, to‘plangan ma’lumotlar tozalandi, shovqin va takroriy yozuvlar olib tashlandi, normallashtirish amalga oshirildi. Ushbu xususiyatlar asosida mashinaviy o‘rganish algoritmlari yordamida modellar o‘qitildi: qaror daraxtlari (Decision Trees), tasodifiy o‘rmon (Random Forest), qo‘llab-quvvatlovchi vektor mashinalari (SVM) va gradient kuchaytirish (Gradient Boosting) texnologiyalari. Modellar tarmoq oqimlaridagi normal va zararli xatti-harakatlarni farqlash uchun ishlatiladi.

Modellar samaradorligi aniqlik (Accuracy), sezgirlik (Recall), aniqlik (Precision) va noto‘g‘ri ijobiy (False Positive) ko‘rsatkichlari orqali baholandi. Shu bilan birga, turli shifrlash protokollarida modellarni sinash orqali ularning moslashuvchanligi ham tekshirildi. Tadqiqot natijalari shuni ko‘rsatdiki, metama’lumotlar va oqim xususiyatlariga asoslangan ETA modellarining aniqligi 80–90% gacha yetishi mumkin, bu esa foydalanuvchi maxfiyligini buzmasdan tahdidlarni aniqlash imkonini beradi.

Natijalar. Tajriba natijalari shuni ko‘rsatdiki, paket mazmunini ochmasdan tahdidlarni aniqlash mumkin. Oqim davomiyligi va paket hajmining o‘zgaruvchanligi zararli trafikni bashorat qilishda asosiy belgi sifatida namoyon bo‘ldi.

| Ko‘rsatkich | An’anaviy monitoring | AI asosidagi ETA |
|---|---|---|
| Paket mazmuniga kirish | Talab etiladi | Talab etilmaydi |
| Aniqlik | Past–o‘rtacha | 80–90% |
| Maxfiylikka ta’siri | Salbiy | Saqlanadi |
| Yangi tahdidlarni aniqlash | Cheklangan | Moslashuvchan |

*1-jadval. Shifrlangan trafikda tahdidlarni aniqlash natijalari*

Muhokama. Olingan natijalar shuni ko‘rsatadiki, ETA va sun’iy intellekt texnologiyalari shifrlangan trafikni tahlil qilishda samarali. Bu foydalanuvchi maxfiyligini buzmasdan tarmoq xavfsizligini oshirish imkonini beradi. Ta’lim muassasalari, korporativ va keng tarmoqlarda ETA tizimlarini joriy etish axborot xavfsizligini kuchaytiradi.

Shuningdek, model samaradorligi tarmoq sharoitlari va ma’lumotlar to‘plamining sifatiga bog‘liq. Kelgusida chuqur o‘rganish va real vaqtli oqim tahlilini qo‘llash orqali murakkab tahdidlarni aniqlash imkoniyatlari yanada kengaytirilishi mumkin.

Xulosa. Shifrlangan tarmoq trafikida tahdidlarni aniqlash an’anaviy usullarga nisbatan murakkab bo‘lsa-da, ETA va sun’iy intellekt yondashuvlari samarali yechim beradi. Taklif etilgan metodlar axborot xavfsizligini oshiradi, foydalanuvchi maxfiyligini saqlaydi va zamonaviy tahdidlarga moslashuvchan javob beradi. Bu yondashuv ta’lim, korporativ va umumiy tarmoq infratuzilmalari uchun muhim ilmiy-amaliy ahamiyatga ega.

FOYDALANILGAN ADABIYOTLAR

1. Anderson, B., et al. (2017). *Encrypted Traffic Analysis: A Survey.* ACM Computing Surveys, 50(4).

2. Shbair, W., et al. (2016). *Efficient Classification of Encrypted Traffic Using Machine Learning.* IEEE Conference on Communications and Network Security.

3. Rezaei, S., & Liu, X. (2019). *Deep Learning for Encrypted Traffic Classification.* IEEE Transactions on Network and Service Management, 16(3).

4. Draper-Gil, G., et al. (2016). *Characterization of Encrypted and VPN Traffic.* Proceedings of IMC.

5. Kompyuter tarmoqlari va axborot xavfsizligi bo‘yicha zamonaviy ilmiy manbalar.