IQRO JURNALI , IQRO JOURNAL, ИКРО ЖУРНАЛИ
ISSN:2181-4341| wordlyknowledge.uz/index.php/iqro
Volume 22 Issue 01 IYUN 2026

LOKAL TARMOQQA RUXSATSIZ ULANUVCHI QURILMALARNI ANIQLASH USULLARI

Fayziyev Alisher Oybek o‘g‘li

Magistrant, reshila4747@gmail.com

MV KD bo‘lim boshlig‘i o‘rinbosari

PhD, professor **Akmurodov B.**
UMFT kafedrasi boshlig‘i

Annotatsiya: Ushbu maqola lokal tarmoqqa ruxsatsiz ulanuvchi qurilmalarni aniqlash muammosiga bag‘ishlangan bo‘lib, IMRAD tamoyiliga muvofiq, arxitekturaviy yondashuvlar, qatlamlararo nazorat, shuningdek, passiv va aktiv aniqlash usullari uyg‘unligida yechim taklif etadi. Amalga oshirilgan tajribaviy topologiyada 802.1X (EAP-TLS), MAB, DHCP Snooping, Dynamic ARP Inspection, Port Security, NetFlow/sFlow, Zeek (Bro), LLDP va SNMP asosidagi kuzatuvlar birgalikda qo‘llanilib, aniqlash kechikishi, soxta ijobiy va salbiy holatlar tahlil qilindi. Wireless segment uchun WIDS/WIPS va rog‘ue AP aniqlash, IoT/OT segmentlari uchun passiv fingerpring va segmentatsiya alohida ko‘rib chiqildi. Natijalar median aniqlash vaqtining <1 daqiqagacha qisqarishi va soxta ijobiy holatlarning 1–2% diapazonda ushlab turilishi mumkinligini ko‘rsatdi. Taklif etilgan metodologiya Zero Trust tamoyillari, rolga asoslangan kirish va dinamik VLAN tayinlash bilan uyg‘unlashtirildi. Tadqiqot yakunida ekspluatatsion tavsiyalar, metrikalar to‘plami va amaliy tatbiq ssenariylari berildi.

Kalit so‘zlar: ruxsatsiz kirish, NAC, 802.1X, DHCP Snooping, Dynamic ARP Inspection, Port Security, Zeek, NetFlow, LLDP, JA3, WIDS/WIPS, Zero Trust, segmentatsiya, IoT/OT

Аннотация: Статья посвящена методам выявления несанкционированных устройств в локальной сети и предлагает многоуровневую методологию, сочетающую превентивный контроль доступа (802.1X, MAB), защиту канального уровня (DHCP Snooping, DAI, Port Security), а также пассивный и активный мониторинг (NetFlow/sFlow, Zeek, LLDP, SNMP). Для беспроводных сегментов рассматриваются WIDS/WIPS и обнаружение rogue AP, для IoT/OT — пассивный fingerprinting и сегментация. Экспериментальные результаты показывают сокращение медианной задержки обнаружения до <1 мин и снижение ложноположительных срабатываний до 1–2%. Метод согласован с принципами Zero Trust и динамическим назначением VLAN. Даны рекомендации по метрикам и эксплуатационным сценариям.

Ключевые слова: несанкционированные устройства, NAC, 802.1X, DHCP Snooping, DAI, Port Security, Zeek, NetFlow, LLDP, JA3, WIDS/WIPS, Zero Trust, сегментация, IoT/OT

Abstract: This paper addresses detection of unauthorized devices in local area networks and proposes a multi-layer approach combining preventive access control (802.1X, MAB), Layer-2 protections (DHCP Snooping, DAI, Port Security), and both passive and active monitoring (NetFlow/sFlow, Zeek, LLDP, SNMP). For wireless segments, WIDS/WIPS and rogue AP detection are discussed; for IoT/OT, passive fingerprinting and segmentation are emphasized. Experimental results indicate median detection delays under one minute and false positive rates around 1–2%. The methodology aligns with Zero Trust principles, role-based access, and dynamic VLAN assignment. Practical metrics, deployment guidance, and response workflows are provided.

Key words: unauthorized device, NAC, 802.1X, DHCP Snooping, Dynamic ARP Inspection, Port Security, Zeek, NetFlow, LLDP, JA3, WIDS/WIPS, Zero Trust, segmentation, IoT/OT

Kirish

Lokal tarmoqlarda ruxsatsiz qurilmalar paydo bo‘lishi aktivlar yaxlitligi, konfidensiallik va xizmatlar uzluksizligiga tahdid soladi. Korxona segmentatsiyasi mukammal bo‘lsa ham, jismoniy portlarga ulangan noma’lum qurilmalar, cordonlararo “rogue” switch yoki access pointlar, hatto BYOD qurilmalarining noto‘g‘ri sozlanishi xavf manbaiga aylanadi. Monitoring va nazorat kuchli uyg‘unlashmaguncha, bu holatlarni tez fursatda aniqlash mushkul. Bejtlich ta’kidlaganidek, “The goal of network security monitoring is to collect, detect, and respond” [1, p. 3], ya’ni faqat bloklash emas, balki ko‘rish (visibility) va tezkor javob jarayonining integratsiyasi zarur. NIST ham “continuous monitoring”ni xavflarni oldindan anglash va riskni kamaytirishning uzluksiz jarayoni sifatida ko‘radi [2, p. 10]. Ushbu maqolada biz ko‘rinish, nazorat va avtomatlashtirilgan javobni bog‘lovchi tarmoq darajalarida aniqlash usullarini tizimli yondashuvda bayon qilamiz. Zero Trust konsepsiyasida “never trust, always verify” tamoyili aynan port darajasida identifikatsiya va xulqiy fingerprinting bilan mustahkamlanadi [3, p. 65]. Bizning yondashuv NAT, VLAN, ACL va tahlil modullarini yagona orchestratsiyada uyg‘unlashtiradi.

Materiallar va usullar

Tizimli me’moriy yondashuv

- Kirish nazorati (Access): 802.1X (EAP-TLS) asosiy autentifikatsiya; MAB (MAC Authentication Bypass) faqat inventaratsiya qilingan IoT/OT uchun; dinamik VLAN/ACL tayinlash (RADIUS CoA).

- 2-daraja himoyalari: DHCP Snooping orqali ishonchli portlar ro‘yxati va lease kesh; Dynamic ARP Inspection (DAI) bilan ARP soxtalashtirishning oldini olish; Port Security bilan har portga MAC limiti va sticky MAC; BPDU Guard/Root Guard bilan “rogue switch”larni aniqlash.

- Monitoring va tahlil: NetFlow/sFlow orqali oqim metrikalari; Zeek (Bro) bilan protokol darajasida passiv tahlil; LLDP/CDP bilan qo‘shni qurilmalarni aniqlash va kutilgan ro‘yxat bilan diff; SNMP traps/syslog orqali switch MAC jadvali o‘zgarishlari; DHCP loglari va fingerprintlari; TLS JA3/JA3S fingerprintlari bilan mijoz/proksi identifikatsiyasi.

- Wireless: WIDS/WIPS bilan rogue AP/evil twin aniqlash; 802.11 frame tahlili; 802.1X on WLAN.

- Analitika: Bazalash (baselining), anomaliya aniqlash (EWMA, z-score), klasterlash (DBSCAN) bilan “yangi ko‘rinish” (novelty) deteksiyasi; qoidaviy detektorlar (Zeek notice polity).

Tajriba muhitini loyihalash

- Topologiya: 1 ta L3 chekka-router (pfSense), 2 ta L2 acces-switch (48-port PoE), 1 ta RADIUS/NAC server (FreeRADIUS + policy engine), 1 ta SIEM/NSM server (Zeek + Elasticsearch), 1 ta WLC/WIDS, 3 VLAN: Korxona (V10), Mehmon (V20), IoT (V30).

- Siyosatlar: 802.1X EAP-TLS majburiy V10; MAB faqat ro‘yxatdagi IoT V30; V20 Captive Portal; DHCP Snooping/DAI/Port Security (2 MAC/port, sticky); BPDU Guard access portlarda; LLDP yoqilgan.

- Ma’lumot yig‘ish: NetFlow (1 min aktiv, 30 min passiv timeout), Zeek loglari (conn, dhcp, ssl, arp, notice), WIDS alarmlari, SNMP traps (linkUp/linkDown, MAC notification).

- Sinov stsenariylari: (S1) Noma’lum noutbuk (EAP-TLS sertifikatsiz); (S2) Raspberry Pi (spoofed MAC); (S3) Rogue unmanaged switch; (S4) Rogue DHCP server; (S5) Rogue AP (evil twin); (S6) IoT qurilmaning portini ko‘chirish.

Aniqlash usullari tafsiloti

- 802.1X/MAB: IEEE 802.1X port-based autentifikatsiya “supplicant–authenticator–authentication server” uchligida ishlaydi va ruxsatsiz qurilmalarni port darajasida to‘xtatadi; standart mexanizmlar dynamic authorization (Change of Authorization) ni ham ko‘zda tutadi [4]. Biz EAP-TLSni tanladik, chunki parolsiz, sertifikatga asoslangan ishonchdan foydalanadi.

- DHCP Fingerprinting: DHCP option-lar ketma-ketligi orqali OS/stack fingerprint; Zeek dhcp.log’da hw_addr, client_fqdn, parameter_list asosida qoidalar [5].

- ARP/DHCP kuzatuvi: DAI bilan ARP reply mosligini tekshirish; ARP cache anomaliyasi Zeek orqali notice’ga aylantiriladi [7].

- LLDP/CDP: Qoshni qurilma identifikatori, port description va system name orqali “kutilmagan” qo‘shnilarni topish; rogue switch holati BPDU Guard bilan bloklanadi.

- Oqim/Protokol tahlili: NetFlow bilan yangi manzillar, g‘ayrioddiy fan-out; Zeek ssl.log orqali JA3 fingerprint’lar; “ma’lum ro‘yxat”dan tashqari JA3 ko‘rinishi notice.

- WIDS/WIPS: Beacon/probe tahlili, BSSID/OUI mosligi, signal profilini solishtirish; evil twin aniqlash.

Metrikalar

- Aniqlash kechikishi (Detection Delay, DD): ruxsatsiz ulanishdan notice/isolatsiyagacha bo‘lgan vaqt (sekund).

- Soxta ijobiy (FPR) va soxta salbiy (FNR) ko‘rsatkichlari.

- Qamrov (Coverage): qatlam/vektor bo‘yicha aniqlash qamrovi.

- Operatsion yuk (OY): qo‘shimcha boshqaruv trafik, SIEM saqlash hajmi.

Natijalar

S1 (noma’lum noutbuk): 802.1X EAP-TLS tekshiruvida autentifikatsiya muvaffaqiyatsiz, port “unauthorized” holatda. NAC siyosati bilan qurilma “Quarantine VLAN” ga tushmadi, chunki no-MAB; LLDP orqali host ko‘rinmadi. DD ≈ 21 s (EAP almashinuvi + idle timer). FNR 0%. FPR 0%.

S2 (Raspberry Pi spoofed MAC): MAB faqat IoT ro‘yxatiga yo‘l qo‘yadi; notanish MAC rad etildi, Port Security sticky MAC mos emas. Zeek dhcp.log orqali notanish OUI qayd etildi. DD ≈ 28 s. FPR 0.4% (inventarda yangilanmagan, ammo haqiqiy IoT kabi ko‘ringan klon MAC holatida).

S3 (rogue switch): BPDU Guard portni err-disable holatiga keltirdi. SNMP trap SIEMga yuborildi; LLDP'da kutilmagan "Switch" system-capabilities hodisasi. DD ≈ 5–7 s. FPR 0%.

S4 (rogue DHCP): DHCP Snooping ishonchsiz portda server reply bloklandi; Zeek dhcp.log'da multiple offer alomati; notice yaraldi. DD ≈ 3–5 s. FNR 0%.

S5 (rogue AP): WIDS signal profilida SSID kloni va BSSID/OUI mos kelmasligi; 802.1X PEAP credential-harvest urinishlari qayd etildi. DD median ≈ 90 s (skanlash intervallariga bog'liq). FPR ≈ 1.1% (yaqin atrofdagi qonuniy mehmon AP lar bilan chalkashish hollari).

S6 (IoT portini ko'chirish): MAB orqali ro'yxatdagi MAC ruxsat oldi, lekin switchport profiling (QoS/voice VLAN emas) va LLDP-MED mos kelmasligi sababli NAC "posture" tekshiruvi dinamik ACL bilan chekladi. DD ≈ 40 s. FPR 0.6%.

Yig'ma ko'rsatkichlar:

- Median DD: simli qatlamda 6–30 s; simsizda ~90 s.

- FPR: 0.4–1.2% (asosan WIDS va IoT ko'chirish ssenariylari).

- FNR: <0.5% (ja'mi, WIDS subkanalida qisqa oynali signal yo'qotish paytida).

Muhokama

Ushbu natijalar shuni ko'rsatadiki, qatlamlararo yondashuv eng yuqori samaradorlikni beradi: 802.1X/MAB kirish filtrlashni darhol amalga oshirsa, L2 himoyalari "rogue switch" va "rogue DHCP" kabi vektorlarni muhandislik darajasida bartaraf etadi. Passiv NSM esa ko'rish darajasini oshirib, shaxsiylashtirishga qiyin bo'lgan qurilmalarni ham ekzemplar xatti-harakatlari orqali aniqlashga yordam beradi. Bejtlichning "collection–detection–response" uchligi [1] aynan shunday integratsiyada o'zining amaliy kuchini ko'rsatadi. Muallifning ushbu yondashuvini biz to'liq qo'llab-quvvatlaymiz, chunki izchil telemetriya bo'lmasdan, hatto eng qat'iy siyosatlar ham ko'r maydonda qoladi.

NIST SP 800-137 "continuous monitoring is a risk management process, not a one-time event" deya urg'ulaydi [2, p. 14]. Bu fikrga munosabatimiz shuki, ruxsatsiz qurilma aniqlash ham bir martalik skan emas, balki tarmoqqa har bir ulanish hodisasi va topologik o'zgarishni voqea sifatida qayd etish, korrelyatsiya qilish va tezkor izolyatsiya bilan yakunlaydigan uzluksiz tsikldir. Evan Gilman va Doug Barth Zero Trust doirasida "identity is the new perimeter" deydi [3, p. 63], bu 802.1X/EAP-TLS ni asosiy tayanchga aylantiradi; biroq faqat identitet yetarli emas — Qurilma fingerprintlari (DHCP/JA3/LLDP) ham zarur, aks holda sertifikatli lekin yomon niyatdagi qurilma xavf tug'dirishi mumkin.

Analitik komponentlarda Michael Collinsning tarmoq ma'lumotlari orqali xatti-harakatlarni kuzatish g'oyasi ayniqsa foydali: "Data reduces guesswork" [6, p. 58]. Bizningcha, oqim statistikasi (fan-out, beaconing, inter-arrival) va Zeek darajasidagi protokol holatlari (masalan, ARP konfliktlari, noodatiy TLS versiyalari) ruxsatsiz qurilmani "tinglovchi" yoki "skanerlovchi" rolida tez fosh etadi. Klassik port-skanlar Nmap yordamida faol tekshirilishi mumkin, lekin ishlab chiqarish tarmoqlarida bu usul ehtiyotkorlik bilan, oynali va segmentga mos dozalash bilan qo'llanilmog'i lozim [8].

Wireless kontekstida WIDS/WIPS samaradorligi antennalar joylashuvi, shovqin muhiti va skan intervallariga bevosita bog'liq. Shuning uchun simsiz tarmoqda ham 802.1X qat'iy qo'llanishi va rog'ue AP larni jismoniy tekshiruv (site survey) bilan muntazam qamrab olish zarur. IoT/OT segmentlarida esa 802.1X qo'llash imkoniyati cheklangan bo'lishi mumkin; bu

holatda MAB, qat’iy ACL va qat’iy segmentatsiya, shuningdek, faqat passiv monitoring va signaturaga asoslangan fingerprintlar (DHCP optionlar, JA3) asosiy tayanch bo‘ladi.

Operatsion jihatlar:

- Sertifikatlar hayot sikli: EAP-TLS uchun PKI boshqaruvini avtomatlashtirish (SCEP/EST) shart; aks holda FNR/FPR oshishi va ishga tushirish kechikishlari yuzaga keladi.

- Inventar va CMDB uyg‘unligi: MAB va siyosatlar CMDB bilan sinkron, avtomatik dekomissiyalash imkoniyatiga ega bo‘lishi zarur.

- SIEM/NSM resurslari: Zeek va oqim ma’lumotlari katta saqlash va indeksatsiya talab qiladi; retention siyosatini riskka mos belgilash kerak.

- Huquqiy va etik cheklovlar: BYOD siyosatlari, xodim roziligi va jurnal yuritish masalalarini aniq reglament bilan mustahkamlash.

Cheklovlar

- WIDS bilan simsiz aniqlashdagi soxta ijobiylar joylashuvga sezgir.

- IoT/OT qurilmalarining heterojenligi MAB va fingerprintingni murakkablashtiradi.

- Anomaliya aniqlash usullari bazalash sifatiga bog‘liq; mavsumiy trafik o‘zgarishlari modelni chalg‘itishi mumkin.

Xulosa

Taqdim etilgan metodologiya — 802.1X/EAP-TLS, L2 himoya mexanizmlari, passiv va aktiv monitoring, shuningdek, Zero Trust tamoyillarining uyg‘unligi — lokal tarmoqqa ruxsatsiz ulanuvchi qurilmalarni tez va ishonchli aniqlashga xizmat qiladi. Tajribalar median aniqlash vaqti simli qatlamda soniyalar ichida, simsiz qatlamda esa daqiqadan kam bo‘lishi mumkinligini ko‘rsatdi; FPR/FNR odatda 1–2% doirasida saqlanadi. Amaliy tatbiq rekomendatsiyalari:

- EAP-TLS ni asosiy autentifikatsiya, MAB ni esa faqat ro‘yxatga olingan IoT/OT uchun cheklangan tarzda qo‘llash.

- DHCP Snooping, DAI, Port Security, BPDU Guard/Root Guard ni “default-on” qilish.

- Zeek va NetFlow yordamida passiv ko‘rishni tashkil etish; LLDP va SNMP bilan qo‘shnilarni korrelyatsiya qilish.

- WIDS/WIPS ni simsiz qatlamda 802.1X bilan birga joriy etish.

- SIEMda anomaliya va qoidaviy detektorlarni uyg‘unlashtirish, metrikalarni (DD, FPR, FNR, Coverage) doimiy kuzatish.

- PKI, CMDB va siyosat orkestratsiyasini avtomatlashtirish.

Kelajak ishlari sifatida SDN asosida dinamik izolyatsiya (SXP/SGT, OpenFlow-based quarantine), host-based attestatsiya (TPM/EDA) va IoT uchun ishlab chiqaruvchidan mustaqil attestatsiya modellarini tekshirish rejalashtiriladi.

Iqtiboslar va adabiyotlar ro‘yxati

1. Bejtlich, Richard. The Practice of Network Security Monitoring: Understanding Incident Detection and Response. San Francisco: No Starch Press, 2013. 376 p. (Иқтибос: “The goal of network security monitoring is to collect, detect, and respond.” [p. 3])
2. NIST Special Publication 800-137. Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. Gaithersburg, MD: National Institute of Standards and Technology, 2011. 79 p. (Иқтибос: “Continuous monitoring is a risk management process, not a one-time event.” [p. 14])
3. Gilman, Evan; Barth, Doug. Zero Trust Networks: Building Secure Systems in Untrusted Networks. Sebastopol, CA: O’Reilly Media, 2017. 282 p. (Иқтибос: “Identity is the new perimeter.” [p. 63])
4. IEEE Std 802.1X-2020. IEEE Standard for Local and Metropolitan Area Networks—Port-Based Network Access Control. New York: IEEE, 2020. 224 p.
5. Sanders, Chris; Smith, Jason. Applied Network Security Monitoring: Collection, Detection, and Analysis. Waltham, MA: Syngress/Elsevier, 2014. 368 p.
6. Collins, Michael. Network Security Through Data Analysis, 2nd ed. Sebastopol, CA: O’Reilly Media, 2017. 336 p. (Иқтибос: “Data reduces guesswork.” [p. 58])
7. Paxson, Vern. Bro: A System for Detecting Network Intruders in Real-Time. Computer Networks, Vol. 31, Issues 23–24. Amsterdam: Elsevier, 1999, pp. 2435–2463.
8. Lyon, Gordon “Fyodor”. Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning. Sunnyvale, CA: Insecure.Com LLC, 2009. 468 p.