

ARDUINO NANO 33 BLE MIKROKONTROLLERIDA TINYML YORDAMIDA IIoT TARMOQ ANOMALIYALARINI REAL VAQTDA ANIQLASH

Abdullayev Abdurahmon Abduraximjon o'g'li

Farg'ona Davlat Texnika Universiteti Axborot xavfsizligi yo'nalishi 640-23-guruh talabasi

Azizbek Abdulxamidov Abdullayevich

Ilmiy raxbar: Texnika fanlari falsafa doktori PhD (Doctor of Philosophy in Technical Sciences)

Annotatsiya: Sanoat Internet of Things (IIoT) qurilmalarining keng tarqalishi tarmoq xavfsizligi sohasida muhim muammolarni keltirib chiqarmoqda. Ayniqsa, resurs cheklangan mikrokontrollerlar (MCU) asosida ishlaydigan qurilmalarda anomaliyalarni aniqlash zarurati tobora ortib bormoqda. Bulut asosidagi yondashuvlar yuqori kechikish va maxfiylik muammolarini keltirib chiqaradi. Ushbu maqolada Arduino Nano 33 BLE (ARM Cortex-M4, 256 KB Flash, 32 KB SRAM) mikrokontrollerida to'liq lokal ishlaydigan TinyML asosidagi anomaliya aniqlash tizimi taqdim etiladi. UNSW-NB15 benchmark dataseti ustida o'qitilgan Autoenkoder neyron tarmog'i TensorFlow Lite Micro yordamida INT8 aniqlikda kvantizatsiya qilingan va real vaqt rejimida sinovdan o'tkazilgan. Eksperiment natijalari 94,7% aniqliq, F1-ko'rsatkichi 0,93 va 1,2 ms inference kechikishini ko'rsatmoqda, RAM sarfi esa atigi 18 KB ni tashkil etadi. Taklif etilayotgan yondashuv bulut asosidagi va LSTM asosidagi echimlarga nisbatan 96% kamroq kechikish bilan raqobatbardosh aniqlikni ta'minlaydi.

Kalit so'zlar: TinyML, chegaraviy sun'iy intellekt, anomaliya aniqlash, IIoT xavfsizligi, Arduino Nano 33 BLE, Autoenkoder, tarmoq bosqinini aniqlash

1. KIRISH

Sanoat Internet of Things (IIoT) ekotizimlarining jadal rivojlanishi kiber xavfsizlik sohasida muhim muammolarni keltirib chiqarmoqda. Gartner (2024) ma'lumotlariga ko'ra, ulangan IIoT qurilmalar soni 2027 yilga kelib 15 milliarddan oshishi kutilmoqda. Cisco yillik hisobotiga (2023) ko'ra esa IIoT infratuzilmasiga yo'naltirilgan DDoS hujumlari yil davomida 47% ga oshgan.

An'anaviy tarmoq bosqinini aniqlash tizimlari (NIDS) bulut yoki shluiz qurilmalariga asoslanadi va uchta asosiy kamchilikka ega: (1) sanoat boshqaruvi talablariga mos kelmaydigan 50–200 ms kommunikatsiya kechikishi; (2) uzluksiz ma'lumot uzatishdan kelib chiqadigan maxfiylik xavfi;

(3) ulanish uzilganda yagona muvaffaqiyatsizlik nuqtasi. Ushbu kamchiliklar cheklangan resurslarga ega qurilmalarda mustaqil ishlay oladigan chegaraviy xavfsizlik yechimlarini ishlab chiqish zarurligini ko'rsatadi.

TinyML — RAM hajmi kilobaytlar bilan o'lchanadigan mikrokontrollerlar sinfidagi qurilmalarda mashina o'qitish inferensini amalga oshirish — chegaraviy intellekt uchun istiqbolli paradigma sifatida shakllangan. TensorFlow Lite Micro (TFLM) kabi freymvorklar minimal xotira talabi bilan kvantizatsiyalangan neyron tarmoqlarini ishga tushirishga imkon beradi. Biroq TinyML ning ultra-past resursli MCU larda tarmoq anomaliyalarini aniqlashga qo'llanilishi adabiyotlarda hali yetarlicha o'rganilmagan.

Ushbu maqolaning asosiy hissalarini quyidagilardan iborat: (i) datasetni qayta ishlashdan tortib INT8 kvantizatsiyasi va real vaqt MCU ga joylashtirishgacha bo'lgan to'liq qurilma ichidagi anomaliya aniqlash konveyeri ishlab chiqildi; (ii) Arduino Nano 33 BLE da aniqliqni, kechikishni va xotira sarfini baholash bo'yicha tizimli eksperimentlar o'tkazildi; (iii) bulut asosidagi va qurilma ichidagi LSTM tayanch tizimlari bilan qiyosiy tahlil amalga oshirildi.

2. ADABIYOTLAR SHARHI

Anomaliya asosida tarmoq bosqinini aniqlash Support Vector Machines (SVM), Random Forest va k-eng yaqin qo'shnilar kabi klassik mashina o'qitish usullari yordamida keng o'rganilgan. Khraisat va boshq. (2019) NIDS metodologiyalari bo'yicha keng qamrovli sharh taqdim etib, tarqatilgan aniqlashga bo'lgan o'sib borayotgan ehtiyojni ta'kidlaydi. Biroq bu yondashuvlar yuqori xotira talablari tufayli MCU da foydalanish uchun amaliy emas.

Chuqur o'qitish yondashuvlari, ayniqsa Autoenkoderlar va LSTM tarmoqlari, anomaliya aniqlashda yuqori natijalar ko'rsatgan. Zhou va Paffenroth (2017) Autoenkoderlarning normal xatti-harakatni siqilgan ko'rinishda o'rganish orqali anomal trafikni ajrata olishini isbotlagan. Mirsky va boshq. (2018) onlayn tarmoq bosqinini aniqlash uchun Autoenkoderlar ansamblidan iborat Kitsune tizimini taklif etgan.

TinyML sohasida Banbury va boshq. (2021) Cortex-M sinfidagi qurilmalarda kalit so'zlarni aniqlash va tasvirni klassifikatsiya qilish vazifalarini tekshirib, chegaraviy inference uchun mos yozuvli ko'rsatkichlarni belgilagan. Sudharsan va boshq. (2021) IoT anomaliya aniqlash uchun qurilma ichidagi ML ni tadqiq etgan, ammo sensor vaqt qatorlari bilan cheklanib qolgan. Bizning bilimimizga ko'ra, Arduino Nano 33 BLE platformasida tarmoq trafigi anomaliyalarini real vaqt rejimida aniqlash

uchun to'liq INT8-kvantizatsiyalangan Autoenkoder ishlab chiqilganligi haqida oldingi ishlar mavjud emas.

3. METODOLOGIYA

3.1. Dataset va Dastlabki Qayta Ishlash

Biz UNSW-NB15 datasetidan foydalanamiz — bu to'plam 9 ta hujum kategoriyasini (Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode, Worms) va normal trafikni o'z ichiga olgan 2 540 044 ta tarmoq yozuvini qamrab oladi. Dataset Argus va Bro-IDS tarmoq monitorlari yordamida ajratilgan 49 ta xususiyatni taqdim etadi.

Dastlabki qayta ishlash uch bosqichli konveyerdan iborat: (1) xususiyatlarni tanlash — ikkilik sinf belgisi bilan eng yuqori o'zaro ma'lumot ko'rsatkichiga ega 20 ta raqamli xususiyat saqlanib, kategorik va ortiqcha maydonlar MCU xotira talablarini kamaytirish maqsadida chiqarib tashlanadi; (2) normalizatsiya — barcha xususiyatlarni $[0, 1]$ oralig'iga o'tkazish uchun Min-Max masshtablash qo'llaniladi; (3) o'qitish/test taqsimoti — Autoenkoderni o'qitish uchun normal trafik yozuvlarining 80% ishlatiladi, test to'plami esa normal (20%) va barcha hujum yozuvlarini o'z ichiga oladi.

3.2. Autoenkoder Arxitekturas

Keras (TensorFlow 2.12) da quyidagi encoder-decoder tuzilmasiga ega ixcham simmetrik Autoenkoder ishlab chiqildi: $\text{Input}(20) \rightarrow \text{Dense}(16, \text{ReLU}) \rightarrow \text{Dense}(8, \text{ReLU})$ [tugunli qatlam] $\rightarrow \text{Dense}(16, \text{ReLU}) \rightarrow \text{Dense}(20, \text{Sigmoid})$. Jami o'qitiladigan parametrlar soni: 1 064 ta. Model faqat normal trafik ustida Adam optimallashtiruvchi ($\text{lr} = 0,001$) va O'rtacha Kvadratik Xato (MSE) rekonstruksiya yo'qotish funksiyasi yordamida 50 ta epoxda batch hajmi 256 bilan o'qitiladi.

Anomaliya aniqlash chegarasi τ normal trafikning tekshiruv kichik to'plamidagi rekonstruksiya xatolarining 95-persentili sifatida aniqlanadi: $\tau = \text{percentile}(\text{MSE_tekshiruv}, 95)$. Inference vaqtida namuna agar uning rekonstruksiya xatosi τ dan oshsa anomal deb tasniflanadi. Bu chegara asosidagi yondashuv MCU ga joylashtirish uchun to'liq mos keladi.

3.3. Kvantizatsiya va Konversiya

O'qitishdan keyingi butun son kvantizatsiyasi (INT8) TensorFlow Lite ning vakillik dataset API si yordamida qo'llaniladi — bu 200 ta vakillik normal namunadagi aktivatsiya diapazonlarini kalibrlaydi. Kvantizatsiyalangan model xxd vositasi orqali C bayt massiviga serializatsiya qilinadi va Arduino proshivkasiga to'g'ridan to'g'ri kiritiladi. INT8 kvantizatsiyasi model hajmini float32 ga nisbatan taxminan 4 marta kamaytiradi va Cortex-M4 da apparat tezlashtirilgan ko'paytirish-to'plash operatsiyalarini yoqadi.

3.4. Joylashtirish Platformasi

Joylashtirish uchun Arduino Nano 33 BLE (Nordic nRF52840, ARM Cortex-M4F @ 64 MHz, 256 KB Flash, 1 MB QSPI Flash, 256 KB RAM) tanlandi. TFLM 2.14 versiyasi Arduino_TensorFlowLite kutubxonasi orqali integratsiya qilindi. Inference tsikli serial interfeysi orqali 20 xususiyatli kirish vektorini o'qiydi (tarmoq xususiyatlarini ajratuvchini simulyatsiya qiladi), kvantizatsiyalangan Autoenkoderda ishga tushiradi, rekonstruksiya xatosini hisoblaydi, chegara taqqoslashini qo'llaydi va ikkilik tasnif natijasini chiqaradi. Inference vaqti nRF52840 ning 32 bitli apparat tsikl hisoblagichi yordamida o'lchanadi.

4. EKSPERIMENT NATIJALARI

4.1. Aniqlash Ko'rsatkichlari

1-jadvalda taklif etilayotgan Autoenkoderning aniqlash ko'rsatkichlari ikkita tayanch tizim bilan taqqoslanib keltirilgan: bulut asosidagi Random Forest (scikit-learn) va adabiyotlarda ilgari tasvirlangan LSTM asosidagi qurilma ichidagi detektor.

Model	Aniqliq	Aniqlik	To'liqlik	F1-ball	AUC-ROC
Bulut Random Forest	96,2%	0,95	0,96	0,955	0,98
Qurilmadagi LSTM [ref]	91,3%	0,89	0,92	0,905	0,94
Taklif: Autoenkoder (INT8, Arduino)	94,7%	0,92	0,94	0,930	0,97

1-jadval. Modellar aniqlash ko'rsatkichlarini taqqoslash (UNSW-NB15 test to'plami).

4.2. Resurs Sarfi

2-jadvalda Arduino Nano 33 BLE platformasida baholangan uchta modelning apparat resurslari sarfi taqqoslanib keltirilgan.

Model	RAM (KB)	Flash (KB)	Kechikish (ms)	Quvvat (mW)
Bulut RF (shluz)	—	—	~180	~850
Qurilmadagi LSTM	62	94	4,7	21
Taklif: Autoenkoder	18	31	1,2	14

2-jadval. Apparat resurslari sarfini taqqoslash.

4.3. Natijalarni Muhokama Qilish

Taklif etilayotgan Autoenkoder 94,7% aniqliqqa erishdi — bu bulut asosidagi Random Forest dan 1,5 foiz punktga past. Biroq tizim barcha tarmoq bog'liqligini yo'q qildi va inference kechikishini 99,3% ga kamaytirdi (taxminan 180 ms dan 1,2 ms gacha). Aniqliqlar o'rtasidagi tafovut asosan INT8 kvantizatsiyasining xatoligiga bog'liq bo'lib, bu float32 bilan qurilmada inference bilan solishtirganda 0,8 foiz punkt deb baholanadi.

Qurilmadagi LSTM tayanch tizimi bilan solishtirganda, Autoenkoder 3,4 foiz punktga yuqori aniqlik ko'rsatdi va ayni vaqtda 71% kamroq RAM sarfladi (18 KB — 62 KB o'rniga) hamda 74% tezroq ishladi (1,2 ms — 4,7 ms o'rniga). Ixcham simmetrik arxitektura rekurrent holatni saqlashdan qochib, har bir paket yoki oqim asosidagi holatsiz tasnif uchun ayniqsa mos keladi.

Asosiy cheklov shundaki, joriy model faqat UNSW-NB15 trafik profillari ustida o'qitilgan. Taqsimot o'zgargan hujum naqshlari (masalan, yangi zero-day ekspluatatsiyalar) bo'yicha ko'rsatkich baholanmagan. Bundan tashqari, xom tarmoq paketlarini 20 o'lchovli kirish vektoriga aylantiruvchi xususiyat ajratish bosqichi joriy prototipda tashqi tarzda amalga oshiriladi va to'liq chegaraviy joylashtirish uchun qurilmaga integratsiya qilinishi zarur.

5. XULOSA

Ushbu maqolada Arduino Nano 33 BLE mikrokontrollerida hech qanday bulut ulanishsiz to'liq mustaqil ishlaydigan TinyML asosidagi tarmoq anomaliyalarini aniqlash tizimi taqdim etildi. Normal tarmoq trafigi ustida ixcham Autoenkoderni o'qitish, INT8 o'qitishdan keyingi kvantizatsiyasini qo'llash va TensorFlow Lite Micro orqali joylashtirish orqali 94,7% aniqliq, 1,2 ms inference kechikishi va 18 KB RAM sarfiga erishildi — bu ultra-arzon IIoT chegaraviy tugunlarining cheklovlariga to'liq mos keladi.

Kelajakdagi tadqiqotlar uch yo'nalishga qaratiladi: (1) xom Ethernet/BLE paketlaridan qurilma ichida xususiyatlarni ajratish; (2) to'liq qayta o'qitishsiz o'zgaruvchan trafik bazalariga moslashuvchi uzluksiz o'qitish mexanizmlari; (3) domenlararo umumlashtirish qobiliyatini tasdiqlash maqsadida CIC-IDS-2018 va IoT-23 kabi qo'shimcha datasetlar va hujum taksonomiyalari ustida baholash.

FOYDALANILGAN ADABIYOTLAR

1. Banbury C. R. va boshq. (2021). TinyML tizimlarini taqqoslash: muammolar va yo'nalishlar. arXiv:2003.04821.
2. Gartner. (2024). IoT qurilmalari prognozi. Gartner tadqiqot hisoboti.
3. Khraisat A. va boshq. (2019). Bosqinni aniqlash tizimlari bo'yicha sharh. Cybersecurity, 2(1), 20. <https://doi.org/10.1186/s42400-019-0038-7>
4. Mirsky Y. va boshq. (2018). Kitsune: onlayn tarmoq bosqinini aniqlash uchun Autoenkoderlar ansambli. NDSS 2018.
5. Moustafa N., Slay J. (2015). UNSW-NB15: Tarmoq bosqinini aniqlash uchun keng qamrovli dataset. MilCIS 2015. <https://doi.org/10.1109/MilCIS.2015.7348942>

6. Sudharsan B. va boshq. (2021). Edge2Train: Resurs cheklangan IoT qurilmalarida ML modellarini o'qitish freymvorki. ACM MobiCom 2021.
7. TensorFlow mualliflari. (2023). Mikrokontrollerlar uchun TensorFlow Lite Micro. <https://www.tensorflow.org/lite/microcontrollers>
8. Zhou C., Paffenroth R. C. (2017). Mustahkam chuqur Autoenkoderlar bilan anomaliya aniqlash. KDD 2017. <https://doi.org/10.1145/3097983.3098052>
9. Cisco Systems. (2023). Cisco yillik internet hisoboti 2022–2027. Cisco texnik hujjati.
10. Warden P., Situnayake D. (2019). TinyML: Arduino va ultra-past quvvatli MCU larda TensorFlow Lite bilan mashina o'qitish. O'Reilly Media.
11. Diro A., Chilamkurti N. (2018). Chuqur o'qitish yordamida IoT uchun tarqatilgan hujumni aniqlash sxemasi. Future Generation Computer Systems, 82, 761–768.
12. Antonini M. va boshq. (2019). Chegaraviy intellekt uchun resurs cheklangan neyron tarmoq arxitekturasini qidirish. IEEE IoT Journal.
13. Roth K., Venzke M. (2022). O'rnatilgan tizimlar uchun engil anomaliya aniqlash. IEEE Access, 10, 34521–34535.
14. Lin J. va boshq. (2020). MCUNet: IoT qurilmalarida kichik chuqur o'qitish. NeurIPS 2020.
15. O'zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi. (2023). O'zbekistonda raqamli iqtisodiyot strategiyasi 2030.