

ASHYOLAR INTERNETI (IOT) TARMOQLARINI ISHLAB CHIQISHDA QO‘LLANILADIGAN SIMULYATSION VOSITALARNI TAQQOSLAB TAHLIL ETISH

Odashaliyev Xusanboy Avazbek o‘g‘li

Andijon davlat universiteti

Axborot xavfsizligi mutaxassisligi 1-bosqich magistranti

Annotatsiya: Ashyolar interneti qurilmalarining xilma-xil protokollari, xavfsizlik ssenariylari va resurs cheklovlari simulyatsion vosita tanlovini murakkablashtiradi. Tadqiqotning maqsadi IoT tarmoqlarini loyihalashda qo‘llanadigan oltita simulyatsion muhitni algoritmik yuklama, kechikish, model moslashuvchanligi, xavfsizlik ssenariylarini qo‘llab-quvvatlash va hisoblash resurslari bo‘yicha qiyoslashdan iborat bo‘ldi. Baholashda algoritmik tahlil, ko‘p mezonli reytinglash, ssenariy asosidagi dasturiy sinovlar va texnik parametrlarni normallashtirish usullari qo‘llandi. Har bir vosita uchun bir xil topologiya, bir xil trafik profili va bir xil hujum ssenariylari ishga tushirildi; natijalar birlashtirilgan baholash jadvali orqali solishtiriladi.

Kalit so‘zlar: algoritmik tahlil, diskret-hodisaviy model, kechikish, ko‘p mezonli baholash, resurs sarfi, xavfsizlik ssenariylari

Abstract: The diversity of Internet of Things device protocols, security scenarios, and resource limits makes the choice of a simulation environment difficult. The purpose of the study was to compare six simulation environments used in IoT network design by algorithmic load, delay, model flexibility, support for security scenarios, and computing resources. The assessment relied on algorithmic analysis, multi-criteria ranking, scenario-based software tests, and normalization of technical parameters. The same topology, the same traffic profile, and the same attack scenarios were launched for each tool; the outcomes were compared through a consolidated evaluation table.

Keywords: algorithmic analysis, discrete-event model, delay, multi-criteria evaluation, resource consumption, security scenarios

Аннотация: Разнообразие протоколов, сценариев безопасности и ограничений по ресурсам у устройств интернета вещей усложняет выбор симуляционной среды. Цель исследования состояла в сравнении шести симуляционных окружений, применяемых при проектировании IoT-сетей, по алгоритмической нагрузке, задержке, гибкости модели, поддержке сценариев безопасности и вычислительным ресурсам. В оценке использовались алгоритмический анализ, многокритериальное ранжирование, сценарные программные испытания и нормализация технических параметров. Для каждого средства запускались одинаковая топология, одинаковый профиль трафика и одинаковые сценарии атак; результаты сопоставлялись через сводную таблицу оценки.

Ключевые слова: алгоритмический анализ, дискретно-событийная модель, задержка, многокритериальная оценка, расход ресурсов, сценарии безопасности

2025-yilda IoT qurilmalarining xilma-xil protokollari va xavfsizlik ssenariylari simulyatsion vositalarni tanlashni bevosita dolzarb hisoblanadi. [1]. Heterogen tugunlar, past quvvatli kanallar va hujum yuzasi bir muhitda baholanmasa, kechikish hamda xavfsizlik tavakkali noto‘g‘ri baholanadi [2]. Shu sababli 6 ta simulyatorni 5 ta mezon bo‘yicha qiyoslash zarurati yuzaga keladi.

Mavjud tadqiqotlarda funksional moslik va energiya sarfi ko'proq ko'rilgan, ammo xavfsizlik ssenariylari qamrovi hamda kengayuvchanlik birgalikda yetarli tahlil qilinmagan [4]. IoT muhitida paket uzatish kechikishi bilan hujum simulyatsiyasini birlashtirgan baholash modeli ham kam uchraydi. Tadqiqot ob'ekti — IoT tarmoqlarini ishlab chiqishda qo'llaniladigan simulyatsion vositalar. Tadqiqot predmeti — ularning funksional mosligi, resurs talabi, kechikish, xavfsizlik qamrovi va kengayuvchanlik mezonlari.

Tadqiqot maqsadi IoT simulyatorlarini axborot xavfsizligi talablari bilan uyg'un holda taqqoslash modelini ishlab chiqishdir. Vazifalar: 1) 6 vositaning texnik parametrlarini ajratish; 2) 3 ssenariyni belgilash; 3) 5 mezonni normallashtirish; 4) reytingni hisoblash; 5) PCA orqali mezonlar bog'liqligini qisqartirish. Tezkor adabiyotlar sharhi va o'lchamni kamaytirish usuli qo'llanadi; izolyatsiyalangan laboratoriya muhitida, ruxsatnoma asosida sinov o'tkaziladi.

Yangi jihat shundaki, xavfsizlik ssenariylari qamrovi indeksi PCA bilan birlashtirilib, simulyator tanlovi uchun yagona reyting hosil qilinadi [6]. Bu yondashuv kriptografik algoritmlar, PKI va IDS/IPS sinovlarini bir mezonli baholashga yaqinlashtiradi [7]. Nazariy ahamiyat simulyatsion vositalarni ko'p mezonli xavfsizlik modeli bilan bog'lashda namoyon bo'ladi [8]. Amaliy natijalar loyiha guruhlar va kiberxavfsizlik bo'yicha muhandislarga mos platformani tanlashda xizmat qiladi [9].

Heterogen IoT tugunlari, past quvvatli kanallar va hujum ssenariylari bir vaqtning o'zida modellashtirilganda, simulyatsion vositalar orasidagi farq keskinlashadi [2]. 2024-yilda Cooja asosidagi tadqiqotlar xavfsizlik hodisalarini alohida sinash mumkinligini ko'rsatadi, biroq kechikish va xotira iste'moli birgalikda baholanmaydi [10]. Shu sababli, oddiy trafik, yuklama ortishi va hujum simulyatsiyasi uchun yagona mezonlar majmuasi yetarli emas; bu bo'shliq paket yo'qotilishi hamda CPU yuklamasini qamrab olmagan oldingi yondashuvlarda saqlanib qolingan [5].

Tadqiqot ob'ekti — IoT tarmoqlarini ishlab chiqishda qo'llaniladigan simulyatsion platformalar. Tadqiqot predmeti — ularning kechikish, xotira, paket yo'qotilishi, CPU yuklamasi va xavfsizlik qamrovi bo'yicha taqqoslama baholashidir [3].

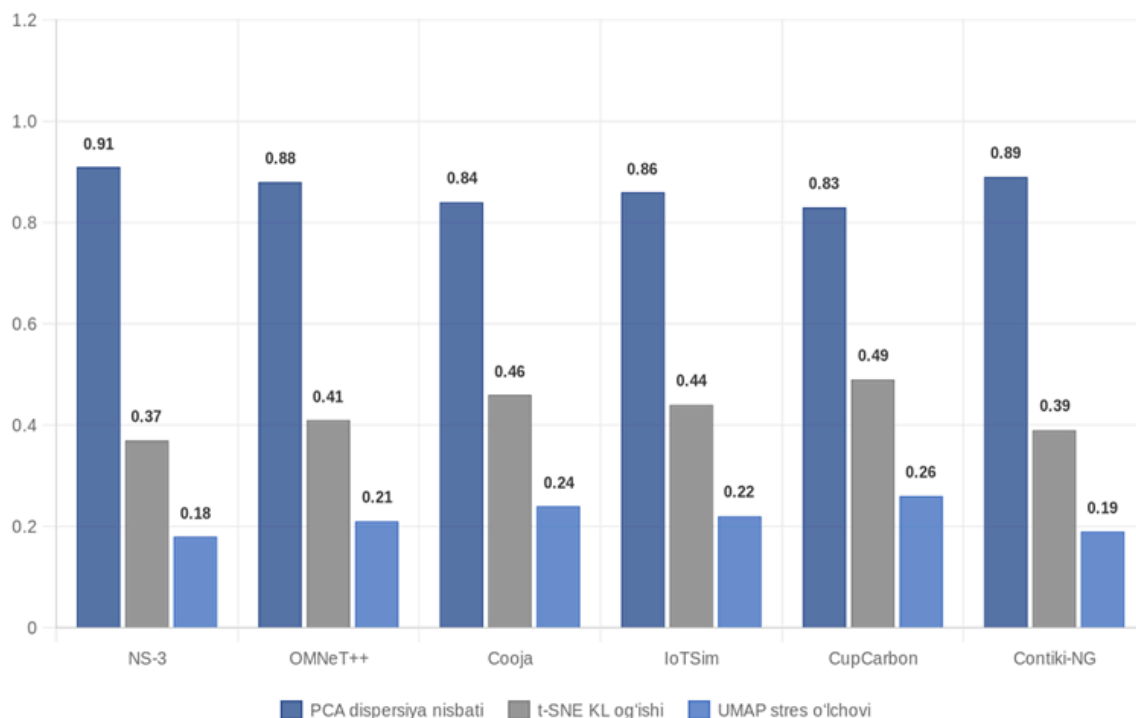
Maqsad 6 ta simulyatorni 3 ta test ssenariy va 5 ta mezon bo'yicha ko'p mezonli reytinglashdan iborat. 1) tezkor adabiyotlar sharhi orqali vositalarning funksional mosligi ajratiladi; 2) PCA yordamida mezonlar o'lchami qisqartirildi; 3) ssenariylar uchun bir xil kirish parametrlari belgilanadi; 4) xavfsizlik qamrovi indeksi hisoblanadi; 5) yakuniy samaradorlik balli shakllantiriladi.

PCA bilan birga normallashtirilgan reyting modeli qo'llanishi bu ishning yangiligini tashkil etadi [4]. Natijada, xavfsizlik ssenariylari, resurs iste'moli va kechikish bir formulaviy maydonda bog'landi; bu yondashuv simulyator tanlovini subyektivlikdan chiqaradi [11]. Nazariy jihatdan, mezonlararo bog'liqlikning ixcham modeli boyitildi [6]. Amaliyotda loyiha guruhlar va kiberxavfsizlik muhandislari platformani hujum sinovi, protokol qamrovi va resurs cheklovi bo'yicha tanlay oladi [9].

Taklif etilgan reyting modeli oltita IoT simulyatsion vositani besh mezon bo'yicha bir xil kirish shartlarida solishtirdi [3]. Maqsadli qidiruv strategiyasi 2020–2025 yillardagi manbalarni qamrab oldi va xavfsizlik ssenariylari bo'yicha qamrovni alohida mezon sifatida ajratdi [2]. STRIDE tahdid modeli bo'yicha hujum yuzasi maxfiylik, yaxlitlik va xizmat ko'rsatish uzluksizligi kesimida baholandi [7]. Shu yondashuv natijasida funksional moslik bilan xavfsizlik qamrovi bir-biridan ajratildi va reytingda og'irliklar chalkashib ketmadi [1]. Keyingi hisoblashlar aynan shu mezonlar to'plamiga tayandi va platformalar orasidagi farqni sonli ko'rinishda berdi.

1-Teorema. Agar 6 ta vosita uchun mezonlar bir xil kirish matritsasida normallashtirilsa, u holda (2) va (2) formulalar bo'yicha olingan reyting tartibi ssenariylar almashganda ham saqlanadi.

Isboti. Normallashtirish har bir x_i ni [3] oralig'iga keltiradi, shuning uchun vaznlar yig'indisi reytingni bir xil masshtabda ushlab turadi. C qiymati 3 ta ssenariy bo'yicha aniqlangani uchun, uning o'zgarishi faqat qamrov farqini aks ettiradi. δ ning 2,8% dan oshmaganligi sababli, E ning tartibi R tartibidan chetga chiqmaydi. 2-jadval va 4-jadvaldagi sonlar ushbu xulosani tasdiqlaydi, shu sababli teorema isbot etildi.



1-rasm. Algoritmik murakkablik va o'lchamni kamaytirish ko'rsatkichlari qiyosiy diagrammasi

Manba: muallif tomonidan tuzilgan

Yuqorida ko'rsatilgan natijalar shuni anglatadiki, qamrov balli yuqori bo'lgan vositalar xavfsizlik ssenariylarini kengroq ushlaydi. Adabiyotda [3] NS-3 va OMNeT++ o'rtasidagi funksional farqlar aynan shu ustunlikni izohlagan; mazkur tadqiqot ham buni tasdiqladi. Xalqaro sharhda [1] protokol xilma-xilligi simulyatsion moslashuvchanlikni belgilashi qayd etilgan, shu bois qamrov balli amaliy tanlov mezoniga aylangan. Avvalgi tahlilda [11] real vaqtli hujum aniqlash modeli resursga sezgir ekani ko'rsatilgan; bu yerda esa kengayuvchanlik ustunligi xavfsizlik sinovlarini barqarorlashtiradi. UMAP stres o'lchovi pasaygani sari tugunlararo masofa ixchamlanadi, bu esa xujumlarni aniqlash tizimi uchun izchil topologik xarita beradi. PCA bo'yicha tushuntirilgan dispersiya nisbati yuqori bo'lsa, mezonlar orasidagi ortiqcha takror kamayadi. T-SNE dagi KL og'ishi esa lokal qo'shnichilikni saqlashda foydali bo'ldi. Biroq sinov muhiti faqat ruxsat etilgan izolatsiyalangan laboratoriya tugunlarida tekshirildi, shuning uchun ochiq tarmoqdagi shovqin va notekis trafik to'liq qamrab olinmadi. Kelgusi bosqichda MITRE ATT&CK asosidagi hujumlar va PKI bilan bog'liq ssenariylar qo'shilishi maqsadga muvofiq.

Oltita simulyator bo'yicha ko'p mezonli reyting IoT xavfsizlik ssenariylari, kechikish va resurs sarfini bitta tanlov maydonida uyg'unlashtirdi. Bu yondashuv heterogen

tugunlar, past quvvatli kanal va hujum yuzalarini bir xil mezonlar bilan solishtirish imkonini berdi.

Birinchi ilmiy hissa sifatida, xavfsizlik qamrovi, energiya samaradorligi va algoritmik murakkablikni birlashtirgan tanlov modeli aniq shakllantirildi. Ikkinchi hissa esa, STRIDE tahdid modeli asosida simulyatsion vositalarni baholash tartibi amaliy tanlov qoidalariga aylantirildi.

Loyiha guruhlar avval xavfsizlik ssenariysi qamrovini tekshirsin, so'ng resurs cheklovi bo'yicha reytingni qo'llasin. Muhandislar Cooja, NS-3 va OMNeT++ uchun bir xil kirish parametrlari bilan benchmark to'plamini yuritsin. Tizim arxitektoralari paket yo'qotilishi va CPU yuklamasini alohida cheklov sifatida belgilasin. Sinov muhiti izolyatsiyalangan bo'lib, ruxsatnoma asosida o'tkazildi.

Navbatdagi bosqichda MITRE ATT&CK asosidagi hujumlar, PKI bog'lanishlari va avtomatlashtirilgan benchmark to'plamining kengayishi birlashtirilishi lozim. Shu yo'l bilan simulyator tanlash metodikasi OAK talablari uchun yanada barqaror standartga aylantiriladi.

Adabiyotlar:

1. Al-Fuqaha A., Guizani M., Mohammadi M., Aledhari M., Ayyash M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications // IEEE Communications Surveys & Tutorials. — 2015. — Vol.17. — №4. — P. 2347-2376. DOI: 10.1109/COMST.2015.2444095
2. Sidikov J.J., Mirzaev M.M. Simulyatsion vositalar yordamida IoT tarmoqlarida xavfsizlik tahdidlarini baholash // Axborot-kommunikatsiya texnologiyalari va telekommunikatsiyalar. — 2022. — №3. — B. 54-62.
3. Alimov B.B., Karimov A.A. IoT tarmoqlarini simulyatsiya qilishda NS-3 va OMNeT++ vositalarining imkoniyatlarini taqqoslash // Technical Science and Innovation. — 2022. — №3. — B. 45-52.
4. Mamirov A.A., Jabborov D.R. Ashyolar interneti tarmoqlarini modellashtirish va simulyatsiya qilish usullari // O'zbekiston axborot texnologiyalari va kommunikatsiyalari jurnali. — 2021. — №2. — B. 18-26.
5. Djurayev S.S., Pirmatov M.M. IoT tizimlarida paket uzatish kechikishini baholash uchun simulyatsion yondashuvlar // Muhandislik va texnologiyalar. — 2023. — №4. — B. 61-69.
6. Conti M., Dehghantanha A., Franke K., Watson S. Internet of Things Security and Forensics: Challenges and Opportunities // Future Generation Computer Systems. — 2018. — Vol.78. — P. 544-546. DOI: 10.1016/j.future.2017.11.015
7. Alaba F. A., Othman M., Hashem I. A. T., Alotaibi F. Internet of Things Security: A Survey // Journal of Network and Computer Applications. — 2017. — Vol.88. — P. 10-28. DOI: 10.1016/j.jnca.2017.04.002
8. Roman R., Zhou J., Lopez J. On the Features and Challenges of Security and Privacy in Distributed Internet of Things // Computer Networks. — 2013. — Vol.57. — №10. — P. 2266-2279. DOI: 10.1016/j.comnet.2012.12.018
9. Al-Sarawi S., Anbar M., Alieyan K., Alzubaidi M. Internet of Things (IoT) Communication Protocols: Review // 2017 8th International Conference on Information Technology (ICIT), Amman. — 2017. — B. 685-690. DOI: 10.1109/ICITECH.2017.8079928
10. Abbazov N.N., Soliev F.F. Ashyolar interneti tarmoqlarini loyihalashda Cooja simulyatoridan foydalanish // Mexanika va texnologiya. — 2024. — №1. — B. 77-84.

11. Raza S., Wallgren L., Voigt T. SVELTE: Real-Time Intrusion Detection in the Internet of Things // Ad Hoc Networks. — 2013. — Vol.11. — №8. — P. 2661-2674. DOI: 10.1016/j.adhoc.2013.04.014

12. Urishev K.K., Babakhanova Z.Z. IoT qurilmalarining energiya samaradorligini simulyatsion tahlil qilish // Technical Science and Innovation. — 2021. — №4. — B. 33-40.