ANALYSIS OF DYNAMIC FLOW SECURITY MANAGEMENT ALGORITHMS IN SOFTWARE-DEFINED NETWORKING (SDN) ENVIRONMENTS

Raxmonaliyev Samandar Muzaffar o'g'li

Tashkent University of Information Technologies named after Muhammad al-Khwarizmi

Phone: +998 77 023 77 07 E-mail: samandarraxmonaliyevgg@gmail.com

Abstract. While Software-Defined Networking (SDN) offers flexibility by decoupling control and data planes, architectural centralization increases vulnerability to Distributed Denial of Service (DDoS) attacks targeting the core controller. This study evaluates a Shannon entropy-based dynamic filtering model for real-time anomaly isolation within OpenFlow-based SDNs. Simulations utilizing Mininet and the Ryu controller demonstrated that the system identifies anomalous flows in under 12 milliseconds. The algorithmic intervention reduced controller CPU utilization from 98% to 42%, preserving legitimate throughput at 91.5%. Transitioning to dynamic reactionary algorithms represents a fundamental strategic solution for ensuring centralized network continuity.

Keywords: SDN, OpenFlow, dynamic routing, cybersecurity, flow table, Shannon entropy, DDoS.

Annotatsiya. Dasturiy ta'minot bilan boshqariladigan tarmoqlar (SDN) boshqaruv va ma'lumotlar tekisligini ajratish orqali moslashuvchanlikni ta'minlasa-da, markaziy kontrollerga qaratilgan DDoS xurujlarga nisbatan zaiflikni oshiradi. Mazkur tadqiqot OpenFlow protokoli asosida oqimlar xavfsizligini dinamik boshqarish uchun Shennon entropiyasiga tayanuvchi modelni baholaydi. Mininet va Ryu kontrolleri yordamida o‘tkazilgan simulyatsiyalar tizim anomal oqimlarni 12 millisekunddan kam vaqtda aniqlashini isbotladi. Algoritmik aralashuv kontrollerning CPU yuklamasini 98% dan 42% gacha tushirdi va tranzaksiyalar o'tkazuvchanligini 91.5% darajasida saqlab qoldi.

Oqimlarni dinamik boshqarishga o'tish markazlashgan infratuzilmalarning operatsion uzluksizligini kafolatlovchi strategik yechimdir.

Kalit so'zlar: SDN, OpenFlow, dinamik marshrutlash, kiberxavfsizlik, oqimlar jadvali, Shennon entropiyasi, DDoS.

Kirish. Dasturiy ta'minot bilan boshqariladigan tarmoqlar (SDN) boshqaruv (control plane) va ma'lumotlarni yo'naltirish (data plane) qatlamlarini ajratish orqali tarmoq resurslarini optimallashtirish imkonini beradi. Arxitekturaviy markazlashuv tizimning asosiy zaif nuqtasini ham yuzaga keltirib, kontroller kiberjinoyatchilarning nishoniga aylanadi. Xakerlar IP manzillarni soxtalashtirish (spoofing) orqali tarmoqqa minglab noma'lum paketlarni yuborishadi, natijada kommutator har bir yangi paket uchun kontrollerga "Packet-In" so'rovini jo'natishga majbur bo'ladi. Bu holat kontrollerning resurslarini yeb bitiradi va TCAM xotirasini soxta qoidalar bilan to'ldirib tashlaydi. Tadqiqot maqsadi SDN muhitida kontroller resurslarini zoriqtirmaydigan, matematik yengil va real vaqtda o'z-o'zini moslashtiruvchi dinamik algoritmik arxitekturani ishlab chiqish va sinovdan o'tkazishdir.

Materiallar va metodlar. Kvazi-eksperimental simulyatsiya izolyatsiya qilingan Mininet (v 2.3.0) virtual tarmoq laboratoriyasida, Python tilidagi ochiq kodli Ryu kontrolleri hamda OpenFlow 1.3 protokoli yordamida amalga oshirildi. Oqimlarni tahlil qilish uchun kontroller yadrosiga Shennon entropiyasi algoritmi integratsiya qilindi. Algoritm tarmoqdagi Destinatsiya IP manzillari (DIP) va Portlari (DP) bo'yicha ehtimollik taqsimotini hisoblaydi. DDoS hujum yuz berganda, oqimlar taqsimotidagi xilma-xillik keskin kamayib, entropiya qiymati tushib ketadi.

Kuzatish oynasi (1 soniya) davomida H qiymati dinamik ostonaviy me'yordan (Threshold) pastga tushsa, anomaliya rejimi faollashadi. Kontroller zudlik bilan hujumchi IP manzillar uchun eng yuqori ustuvorlikdagi "Drop" qoidasini yaratib, to'g'ridan-to'g'ri chetki kommutatorga (TCAM xotirasini tejovchi timeout parametrlari

bilan) o'rnatadi.

Natijalar. Oddiy yuklama rejimida Ryu kontrollerining CPU sarfi 12-15% ni tashkil qilib, oqimlarni yo'naltirish tezligi 980 Mbps gacha yetdi. Himoya algoritmlari o'chirilgan holatda tarmoqqa 50k pps SYN Flood hujumi yuborilganda, kontrollerning CPU sarfi 98% gacha keskin ko'tarildi, qonuniy foydalanuvchilarning paketlarini yo'naltirish 64% ga qisqardi, kechikish esa 2 ms dan 415 ms gacha sakradi.

Shennon entropiyasi algoritmi faollashtirilgach, tizim entropiya indeksining keskin qulashini 12 millisekund o'tib qayd etdi va himoya mexanizmini ishga tushirdi. Algoritmik aralashuv natijasida:

- Kontrollerga kelayotgan zararli so'rovlar 87% ga bloklandi.
- Kontroller CPU yuklamasi xavfsiz 42% gacha pasayib, barqarorlashdi.
- Qonuniy tranzaksiyalarning o'tkazish qobiliyati 91.5% saqlab qolindi.
- TCAM xotirasi dinamik tozalash evaziga faqatgina 35% to'ldi.

Algoritmik tahlilning o'zi tarmoq kechikishiga o'rtacha 1.6 ms qo'shimcha vaqt qo'shgan bo'lsa-da, bu kontroller falajlanishining oldini olish evaziga keladigan ulkan operatsion foyda bilan to'liq qoplanadi.

Muhokama. Eksperimental natijalar SDN arxitekturasida statik tarmoq ekranlari yirik DDoS hujumlari va flesh-kraud holatlarini farqlay olmasligini tasdiqlaydi. Entropiyaga asoslangan dinamik yondashuv paketlar soniga emas, xulq-atvori va taqsimot naqshlariga tayanadi. Bu algoritmni nol-kun (zero-day) hujumlariga nisbatan o'ta samarali qiladi. Biroq, kam intensivlikdagi yashirin xurujlarni (Slowloris) aniqlash uchun tizimni Tasodifiy O'rmon (Random Forest) kabi Mashinali O'qitish tasniflagichlari bilan integratsiya qilish zarur.

Ilmiy yangilik va amaliy ahamiyati. Tadqiqotning ilmiy yangiligi anomal oqimlarni izolyatsiya qilish uchun ostonaviy qiymati o'z-o'zini moslashtiruvchi modifikatsiyalangan entropiya algoritmik ramkasini taklif etishidadir. Bu mexanizm

dasturiy kontroller yadrosiga og'ir analitik yuklama bermasdan ishlaydi. Amaliy jihatdan, ushbu arxitektura yirik telekommunikatsiya tarmoqlari va ma'lumotlarni qayta ishlash markazlarida qimmatbaho apparat tizimlarisiz kuchli kiber-mudofaani ta'minlash uchun aniq texnologik yo'riqnoma bo'lib xizmat qiladi.

Xulosa. Arxitekturaviy markazlashuv tizimli kiberxavfsizlik choralarini qayta ko'rib chiqishni talab qiladi. Shennon entropiyasiga asoslangan oqimlarni dinamik boshqarish algoritmi zararli trafikni real vaqtda izolyatsiya qilishni avtomatlashtiradi, TCAM xotirasi to'lib qolishining oldini oladi va CPU resurslarini iqtisod qiladi. Zamonaviy korporativ tarmoqlarni modernizatsiya qilishda dinamik filtrlash algoritmlarini SDN kontrollerlariga majburiy integratsiya qilish barqarorlikni ta'minlovchi strategik imperativdir.

Foydalanilgan adabiyotlar

1. McKeown N, et al. OpenFlow: Enabling innovation in campus networks. *ACM SIGCOMM*. 2008;38(2):69-74.

2. Kreutz D, et al. Software-Defined Networking: A comprehensive survey. *Proceedings of the IEEE*. 2015;103(1):14-76.

3. Ahmad I, et al. Security in Software Defined Networks: A survey. *IEEE Communications Surveys & Tutorials*. 2015;17(4):2317-2346.

4. Bawany NZ, et al. DDoS attack detection and mitigation using SDN. *Arabian Journal for Science and Engineering*. 2017;42(2):425-441.

5. Wang R, et al. An entropy-based distributed DDoS detection mechanism in SDN. *IEEE Trustcom*. 2015;1:310-317.

6. Yan Q, et al. SDN and DDoS attacks in cloud computing environments. *IEEE Communications Surveys & Tutorials*. 2016;18(1):602-622.

7. Mousavi SM, St-Hilaire M. Early detection of DDoS attacks against SDN controllers. *ICNC*. 2015;1:77-81.

8. Cui N, et al. Intrusion detection system based on dynamic flow feature extraction in SDN. *Journal of Network and Computer Applications*. 2020;151:102500.