SUN'IY NEYRON TARMOQLAR YORDAMIDA TARMOQ HUJUMLARI IZLARINI ANIQLASH VA BOTNET TRAFIKINI KLASSIFIKATSIYALASH USULI

Ramazonova Madina Shavkatovna
Muxammad al – Xorazmiy nomidagi TATU "Kiberxavfsizlik va kriminalistika" kafedrasi assistenti.
Email: abdujabbor.madina1989@gmail.com
Rahmanqulova Mashhura Ruziboyevna
"Kiberxavfsizlik markazi" davlat unitar korxonasi, hodimi.
Email:m.raxmanqulova@csec.uz

Annotatsiya. Hozirgi kundan kiber makon o'sib borishi bilan kiberxavfsizlik sohasida faoliyat olib boruvchilar qiyinchiliklarga duch keladi. Butun dunyo bo'ylab kiberxavfsizlik bo'yicha tadqiqotchilarni qiynayotgan jiddiy xavfsizlik muammolari bir bu – Botnet hujumlaridir. Botnet hujum boshlash yoki zararli faoliyatni amalga oshirish uchun xaker tomonidan qo'llaniladigan tizimlar tarmog'i. Botnet kiberhujumni amalga oshirishda vositasi sifatida boshqa har qanday vositalardan ko'ra kengroq ta'sirga ega. Bu Botnet asosan (DDoS), SPARM (pochta yoki soxta sharh) va boshqa kiber jinoyatlar qatorida firibgarlikni amalga oshirishda asosiy omil hisoblanadi. Bu kiberhujum deb ataladigan ko'pgina faoliyatlarda bir xil darajada qo'llaniladi. Maqolada botnet hujum trafiklari va uning oqibatlari ko'rib chiqiladi hamda sun'iy neyron tarmog'iga asoslangan Botnetni aniqlash va tafiklarini klassifikatsiyalash taklif qiladi.

Kalit so'zlar: Botnet,IDS,HIDS,NIDS, Sun'iy intellect,Supervised Machine Learning, Unsupervised Machine Learning, Naive Bayes algoritmi.

Аннотация. С ростом киберпространства сегодня специалисты по кибербезопасности сталкиваются с проблемами. Одной из серьезных проблем безопасности, которая преследует исследователей кибербезопасности по всему миру, являются атаки ботнетов. Ботнет — это сеть систем, используемых хакерами для запуска атак или осуществления вредоносных действий. Ботнет оказывает более широкое влияние, чем любой другой инструмент для осуществления кибератак. Этот ботнет в основном является ключевым фактором в совершении мошенничества, включая (DDoS), SPARM (рассылка спама или спама) и другие киберпреступления. Он в равной степени используется во многих видах деятельности, которые называются кибератаками. В статье рассматривается трафик атак ботнетов и его последствия, а также предлагается метод обнаружения и классификации трафика ботнетов на основе искусственных нейронных сетей.

ISSN 3030-3907

Ключевые слова: ботнет, IDS, HIDS, NIDS, искусственный интеллект, контролируемое машинное обучение, неконтролируемое машинное обучение, наивный байесовский алгоритм.

Abstract. With the growth of cyberspace today, cybersecurity professionals are facing challenges. One of the serious security challenges that is plaguing cybersecurity researchers around the world is Botnet attacks. A botnet is a network of systems used by hackers to launch attacks or carry out malicious activities. A botnet has a wider impact than any other tool in carrying out cyberattacks. This botnet is mainly a key factor in committing fraud, including (DDoS), SPARM (spamming or spamming) and other cybercrimes. It is equally used in many activities that are called cyberattacks. The article reviews botnet attack traffic and its consequences and proposes a method for detecting and classifying botnet traffic based on artificial neural networks.

Keywords: Botnet, IDS, HIDS, NIDS, Artificial intelligence, Supervised Machine Learning, Unsupervised Machine Learning, Naive Bayes algorithm.

Kirish.

Botnet(inglizcha botnetdan, bot "robot" va net - "tarmoq") noqonuniy va zararli harakatlarni amalga oshirish uchun ishlatiladigan zararli dasturlar bilan zararlangan qurilmalar guruhi: spam yuborish, ma’lumotlarni o‘g‘irlash, to‘lov dasturini tarqatish, soxta reklamalarni yuborish va DDoS hujumlaridir.

Botnetni muvofiqlashtirilgan hujumlarni amalga oshirish yoki firibgarlik harakatlarini amalga oshirish uchun masofadan boshqarilishi mumkin bo‘lgan buzilgan kompyuterlar guruhi sifatida tasavvur qilish mumkin. Botnetlarning uzluksiz rivojlanishi shuni anglatadiki, an’anaviy aniqlash yondashuvlari har doim bir qadam orqada qoladi. So‘nggi paytlarda tarmoq trafigining xatti-harakatlarini tahlil qilish Botnetni aniqlash muammosini hal qilish usuli sifatida paydo bo‘ldi. Xulq-atvorni tahlil qilish yondashuvi Botnetlarning ko‘rinmas trafigini aniqlash qobiliyatiga ega bo‘lish uchun umumlashtirishga harakat qilib, ularning hayot aylanishi davomida amal qiladigan umumiy naqshlarni ko‘rib chiqishga qaratilgan. Ushbu ish vaqt o‘tishi bilan o‘zgarib turadigan holatlar ketma-ketligi sifatida modellashtirish orqali tarmoq trafigining xatti-harakatlarini aniqlash uchun Recurrent Neural Networks (RNN) hayotiyligini tahlil qiladi. RNNni ketma-ket ma'lumotlar muammolariga qo‘llashning so‘nggi muvaffaqiyati ularni ketma-ket xatti-harakatlarni tahlil qilish vazifasiga munosib nomzod qiladi. RNN ning ishlashi ikkita asosiy masala, tarmoq trafigining nomutanosibligi va ketma-ketliklarning optimal uzunligini hisobga olgan holda baholanadi. Ikkala masala ham potentsial real hayotda amalga oshirishga katta ta'sir ko'rsatadi. Baholash stratifikatsiyalangan k-qatlamli o‘zaro tekshirish yordamida amalga oshiriladi va

ISSN 3030-3907

boshqa Botnetga tegishli ilgari ko‘rilmagan trafik bo‘yicha mustaqil test o‘tkaziladi. Dastlabki natijalar shuni ko'rsatadiki, RNN yuqori hujumni aniqlash tezligi va juda kichik noto'g'ri signal tezligi bilan trafikni tasniflashga qodir, bu esa uni real stsenariylarda amalga oshirish va joylashtirish uchun potentsial nomzodga aylantiradi. Biroq, tajribalar shuni ko'rsatdiki, RNN aniqlash modellarida osonlik bilan farqlanmaydigan trafik xatti-harakatlari bilan bog'liq muammolar, shuningdek, nomutanosib tarmoq trafigining ayrim holatlari mavjud.

Bosqinlarni aniqlash tizimlari (IDS)

IDS - bu tarmoqdagi zararli faoliyatni aniqlaganda signal beruvchi apparat yoki dasturiy ta‘minot vositasi. IDS - bu tarmoqning "ko‘zi". Bu zamonaviy tarmoqlarning xavfsizlik arxitekturasining muhim tarkibiy qismidir. Bu hujumlarning dastlabki bosqichlarini aniqlashga imkon beradi va shu bilan ularga qarshi kurashish imkoniyatini beradi. Bundan tashqari, ular turli xil hujumlarni aniqlashga imkon beradi, masalan: Xizmat ko‘rsatishni rad etish (DoS), Man in the Middle (MitM) va boshqalar. IDSlar belgilangan har qanday va barcha turdagi tarmoq trafigini kuzatishi va qayd etishi imkoniyatiga ega. IDSlar hujumlar sodir bo‘lganda ular haqida batafsil ma’lumot berishi mumkinligi sababli, u xavfsizlik hodimlariga nima bo‘lganini tushunishga yordam beradi. Shu sababli, kelajakda shunga o‘xshash hujumlar sodir bo‘lganda, tizimning xavfsizligi ushbu turdagi hujumlarni aniqlash va oldini olish uchun sozlanishi mumkin. IDS ning ikki turi mavjud: Tarmoq hujumlarni aniqlash tizimi (NIDS) va Xostga kirishni aniqlash tizimi (HIDS).

Tarmoq hujumlarni aniqlash tizimlari - bu tarmoqqa strategik nuqtalarda joylashtirilgan IDS. NIDS tarmoqda zararli harakatlar mavjudligini aniqlash uchun tarmoqning umumiy trafigini tahlil qiladi. NIDS sizning xostlaringizdan hujumlarni aniqlashga yordam beradi va ko‘pgina tashkilot tarmoqlari xavfsizligining asosiy komponenti hisoblanadi.

Xostga kirishni aniqlash tizimlari - bu tarmoqning barcha mijoz kompyuterlarida (xostlarida) joylashgan IDS. NIDSdan farqli o‘laroq, HIDS bitta xostning trafigini hamda uning faoliyatini tahlil qiladi, agar u g‘ayritabiiy xatti-harakatlarni aniqlasa, u signal beradi.

IDS uchun uch xil aniqlash turi mavjud:Noqonuniy foydalanishni aniqlash, anomaliyalarni aniqlash va gibridni aniqlash.

Imzoni aniqlash deb ham ataladigan,noqonuniy foydalanishni aniqlash, tarmoq yoki xostda ma’lum bo‘lgan kirish shakllarini qidiradi. Har bir hujum o‘ziga xos imzoga ega, masalan, paketning foydali yuki, manba IP manzili yoki ma’lum bir sarlavha bo‘lishi mumkin. IDS ma’lum imzolar ro‘yxatida sanab o‘tilgan imzolardan biriga ega bo‘lgan hujumni aniqlasa, IDS signal berishi

ISSN 3030-3907

mumkin. Ushbu yondashuvning afzalligi ma’lum hujumlarni aniqlashning yuqori aniqligidir. Biroq, uning zaif tomoni shundaki, u noma’lum yoki oldindin uchramagan hujumlarga nisbatan (hujumdan oldin hech qachon ko‘rilmagan) samarasizdir.

Anomaliyani aniqlash tarmoq yoki xostning asosiy holati deb ataladigan normal holatini belgilaydi va bu asosiy chiziqdan har qanday og‘ish potentsial hujum sifatida xabar qilinadi. Masalan, anomaliyaga asoslangan IDS har bir xost tomonidan taqdim etiladigan xizmatlar, har bir xost tomonidan foydalaniladigan xizmatlar va kun davomidagi faoliyat hajmi kabi umumiy tarmoq trafigiga asoslangan bazani yaratishi mumkin. Shunday qilib, agar hujumchi yarim tunda ichki manbaga kirsa va agar bazada yarim tunda deyarli hech qanday faollik bo‘lmasa, IDS signal beradi. Anomaliyalarni aniqlashning afzalligi uning noma’lum bosqinchilik hujumlarini topish uchun moslashuvchanligidir.

Gibrid aniqlash yuqorida qayd etilgan ikkala aniqlashni usulini birlashtiradi. Odatda, ular anomaliya usullariga qaraganda xatoliklarni aniqlash tezligiga ega va yangi hujumlarni aniqlashi mumkin.

Hozirgi vaqtda o‘zlarini hujumlardan himoya qilishni xohlaydigan kompaniyalar uchun IDSning o‘zi etarli emas. IDS tobora ko‘proq Intrusion Prevention Systems (IPS) bilan almashtirilmoqda. IPS IDS ga o‘xshaydi, lekin ular muvaffaqiyatli bo‘lishidan oldin hujumlarni to‘xtatish uchun faol komponentlarga ega. Odatda, IPS IDS qoidalariga ega xavfsizlik devoridan iborat. IDS-dan farqli o‘laroq, IPS-lar inline joylashtiriladi, bu IPS trafikni u orqali o'tayotganda doimiy ravishda skanerlashini anglatadi. Shunday qilib, IPS foydalanuvchilari uchun tarmoq ishlashiga ta’sir qilishi mumkin bo'lgan tarmoqdagi trafik paketlarda muammolarini keltirib chiqarmaslik uchun tezkor bo‘lishi va yuqori hisoblash imkoniyatlariga ega bo‘lishi kerak.Ko‘pgina IPS ning asosiy kamchiliklaridan biri testlashni hujum deb aniqlashidir.Bunga qo‘shimcha ravishda, IPSlar va ayniqsa, tarmoqqa kirishni oldini olish tizimlari (NIPSs) tarmoqdagi yagona nosozlik nuqtasini tashkil qilganligi sababli, ular yuqori darajada barqaror va hujumlarga qarshi mustahkam bo‘lishi lozim.

Sun’iy intellekt

Internet va aloqaning jadal rivojlanishi uzatiladigan ma’lumotlarning hajmini o‘sishiga olib keldi. Ushbu ma’lumotlar hujumchilar qo‘lga kiritishga va doimiy ravishda ushbu ma’umotlarni o‘g‘irlash yoki buzish uchun yangi hujumlarni yaratadilar. Ushbu hujumlarning o‘sishi tizimlar xavfsizligi uchun muammo bo‘lib, hujumni aniqlashning eng katta muammolaridan biridir. Buzilishlarni aniqlash tizimi (IDS) tarmoq trafigini tekshirish orqali hujumlarni aniqlashga yordam beradigan vositadir. Garchi ko‘plab tadqiqotchilar yangi IDS

ISSN 3030-3907

yechimlarini o‘rgangan va yaratgan bo‘lsalar ham, yuqori aniqlikka ega bo‘lish uchun IDS hali ham takomillashtirilishi lozim.Hozirgi kunda ko‘plab xavfsizlik dasturlari Sun’iy intellekt (AI) texnologiyasi bilan chambarchas bog‘liq. Sun’iy intellekt ma’lumotlar to‘plamida muntazam ravishda o‘zgarishlarni topish uchun inson omilisiz algoritmni o‘qitadi. Shuning natijasida hujumlarni bashorat qilish yoki hujumlarni avtomatik ravishda oldini olish uchun foydalanish mumkin bo‘lgan model paydo bo‘ladi . IDS uchun, agar model yetarli darajada o‘qitilgan bo‘lsa, yani hujumlarni bashorat qilish ma’lum hujumlarni yoki noma’lum hujumlarni aniqlash uchun ishlatilishi mumkin.

Supervised Machine Learning (Nazorat ostidagi o‘qitish)

Nazorat ostidagi o‘qitish kirishni chiqish bilan taqqoslaydigan funktsiyani yaratish uchun belgilangan ma’lumotlardan foydalanadi. Funktsiya belgilangan o‘quv ma’lumotlaridan tuzilgan.Nazorat ostidagi o‘qitish ikki turdagi modellarga, tasniflash va regressiyaga bo‘lish mumkin.

Tasniflash modellari ma’lumotlarni muayyan toifalarga ajratish uchun ishlatiladi. Ma’lumotlar to‘plamidan u o‘zining xususiyatlaridan kelib chiqqan holda tegishli toifani taniydi. Model, kirish ma’lumotlarining xususiyatlarini to‘g‘ri tasniflash uchun qanday ekanligini tushunish uchun etiketli kirish va chiqish ma’lumotlariga o‘rgatiladi. Tasniflash modellari hujumlarni aniqlash uchun juda foydali. Masalan, tarmoqqa kiruvchi trafik uchun yaxshi o‘rgatilgan tasniflash modeli trafikni oddiy trafik yoki nomalum trafik deb ajratishi mumkin. Agar model yaxshi ishlasa, noma’lum trafik keyinchalik DoS, fishing, troyan, portlarni skanerlash va boshqalar kabi taniqli hujumlarning toifalariga ajratishi mumkin.
Regressiya modellari doimiy natijalarni bashorat qilish uchun ishlatiladi. Model mustaqil o‘zgaruvchilar va qaram o‘zgaruvchi o‘rtasidagi munosabatni tushunishga o‘rgatilgan. Regressiya modellari asosan bozor narxlari evolyutsiyasini bashorat qilish yoki tendentsiyalarni bashorat qilish uchun ishlatiladi. Umumiy regressiya algoritmlari - chiziqli regressiya, logistik regressiya, qarorlar daraxti kabi algoritmlar kiradi. Nazorat ostidagi o‘qitish asosiy afzalliklaridan biri natijalarni ishlab chiqarish uchun oldingi tajribalardan foydalanishdir. Bundan tashqari, oldingi natijalar aniq modelga erishish uchun ishlash mezonlarini optimallashtirish orqali algoritmni yaxshilash uchun ishlatilishi mumkin.

Nazorat ostidagi o‘qitish ko‘plab hisoblash muammolarini hal qilish uchun ishlatiladi. Biroq, model yaxshi natijalarga erishish uchun o‘quv bosqichida aniq va yaxshi kiritishga muhtoj.Katta ma’lumotlarni o‘qitish qiyin bo‘lishi mumkin, shuning uchun agar ma’lumotlar to‘plami juda katta bo‘lsa, nazorat qilinmaydigan o‘qitish ko‘pincha yaxshi tanlovdir.

ISSN 3030-3907

Unsupervised Machine Learning(Nazoratsiz o‘qitish)

Nazoratsiz o‘qitish belgilanmagan ma’lumotlar bilan ishlatiladi. Nomidan ko‘rinib turibdiki, nazoratsiz o‘qitish foydalanuvchi tomonidan modelni yaxshilash uchun nazorat qilinmaydi. Model o‘z-o‘zidan yaxshilanadi, chunki u berilgan ma’lumotlar to‘plamidan ma’lumotlarni topadi. Odatda, algoritm turli xil ma’lumotlarni bir xil o‘xshashlik yoki farqlarga ega bo‘lgan toifalarga guruhlaydi.Nazorat qilinmaydigan o‘qitish katta ma’lumotlarni tahlil qilish uchun foydalidir.Nazoratsiz o‘qitishni klasterlash, assotsiatsiya va o‘lchovlarni kamaytirishning uchta turiga bo‘linish mumkin(1-rasm).



1-rasm nazoratsiz o‘qitish toifalari

Unsupervised Machine Learning Categories (Nazoratsiz o‘qitish toifalari).

Klasterlash (Clustering) - belgisiz ma’lumotlarni umumiy yoki kam uchraydigan xususiyatlariga ko‘ra guruhlash usulidir. Ushbu jarayonning oxirida belgilanmagan ma’lumotlar turli ma’lumotlar guruhlariga saralanadi. Klasterlash algoritmlarini eksklyuziv, bir-birining ustiga chiqadigan, ierarxik va ehtimolli deb pastki toifalarga bo‘lish mumkin. Eksklyuziv klasterlashda guruhlangan ma’lumotlar faqat bitta klasterga tegishli bo‘lishi mumkin. Bir-biriga o‘xshash klasterlar ma’lumotlarning turli toifalarga tegishli bo‘lishi mumkin bo‘lsa, yanada ko‘proq ma’lumotga modelga ega bo‘lish uchun ma’lumotlarning bir nechta klasterlarga tegishli bo‘lishiga imkon beradi. Misol uchun, videoni tahlil qilish uchun bir-biriga o‘xshash klasterlash talab qilinadi, chunki video bir nechta toifalarga ega bo‘lishi mumkin.

Assotsiatsiya (Association) - bu kirish ma’lumotlari o‘rtasidagi munosabatlarni topadigan usul. Assotsiatsiya ko‘pincha marketing maqsadlarida mahsulotlar o‘rtasidagi munosabatlarni topish va shu tariqa mijozlar xaridlari asosida boshqa mahsulotlarni taklif qilish uchun ishlatiladi. Umumiy assotsiatsiya algoritmi Apriori algoritmidir.

O‘lchovlarni qisqartirish (Dimensionality reduction) - bu ma’lumotlar to‘plamidagi xususiyatlar sonini qayta ishlashni osonlashtirish uchun kamaytirish uchun ishlatiladigan usul. Hozirgi vaqtda foydalaniladigan ma’lumotlar to‘plamining hajmi o‘sib borayotganligi sababli, ma’lumotlar to‘plamiga ma’lum

ISSN 3030-3907

bir mashinani o‘rganish algoritmini qo‘llashdan oldin o‘lchovni kamaytirish usulidan foydalanish odatiy holdir. Ma’lumotlar to‘plamining o‘lchamini kamaytirishning ikkita asosiy usuli mavjud. Birinchisi, xususiyatni yo‘q qilishdir. Bu tadqiqotchilar bashorat qilish uchun foydali bo‘lmagan xususiyatlarni olib tashlashdan iborat. Ikkinchisi - xususiyatni ajratib olish. Xususiyatlarni ajratib olish ma’lumotlar to‘plamida mavjud bo‘lgan bir xil miqdordagi xususiyatlarni yaratadi. Ushbu yangi xususiyatlar eski xususiyatlarning kombinatsiyasi. Bu xususiyatlar mustaqil va ahamiyatiga qarab tartiblangan. Shunday qilib, tadqiqotchilar eng kam muhim yangi xususiyatlarni olib tashlashlari mumkin. Ushbu yondashuvning afzalligi shundaki, tadqiqotchilar har bir asl xususiyatning muhim qismini saqlab qolgan holda ma’lumotlar to‘plamini kamaytiradi. Xususiyatlarni ajratib olishning eng ko'p qo‘llaniladigan usullaridan biri bu asosiy komponentlar tahlili hisoblandi. Boshqa samarali o‘qitish toifalar tasodifiy o‘rmon va qaror daraxti algoritmlaridir. Nazorat ostidagi o‘qitishdan foydalangan holda botnetni aniqlashga qanday qilib yuqori aniqlik bilan erishish mumkinligini o‘rganishdi. Birinchidan, ular botnetlarni aniqlash vositasi sifatida oqimga asoslangan trafik tahlili va boshqariladigan mashinalarni o‘rganishdan foydalanadigan botnetlarni aniqlash tizimini taklif qildi. Keyin ular botnetlar trafigini aniqlash uchun sakkizta eng muhim mashinani o‘rganish algoritmlarining (MLA) ishlashini sinab ko‘rishga kirishadilar. Muvaffaqiyatli algoritimlar uchun qancha trafik kuzatilishi kerakligini o‘rganishdi. Trafik tahlili iz boshidan oxirigacha kuzatiladigan "**to‘plamli**" tahlil yoki vaqt oralig‘i va paket raqamlari cheklangan tahlil orqali amalga oshirildi. Tajribalar zararli va zararli bo‘lmagan yozuvlarni o‘z ichiga olgan ISOP ma’lumotlar to‘plamidan foydalangan holda o‘tkazildi. Natijalar shuni ko‘rsatdiki, tasodifiy o‘rmon algoritmi botnetni aniqlashning eng yuqori aniqligiga ega bo‘lsada, tasodifiy daraxt algoritmi aniqlik va aniqlash vaqti o‘rtasidagi eng yaxshi muvozanatga ega bo‘lgani uchun optimal deb hisoblanadi.Mashinani o‘qitishda (ML) modelining muvaffaqiyati amalaga oshishi uchun Domen nomi, xizmatining ustunligi va eng yaxshi ko‘rsatkichga ega algoritmdan foydalanishni tanlandi. Natijalar tasodifiy o‘rmon algoritmi yordamida botnetni aniqlashda 90% umumiy aniqlikni ko‘rsatdi.Shuningdek, botnetlarni aniqlash uchun DNS yordamida tadqiqot olib borilmoqda. DNS jurnallari asosida botnet domen trafigining oltita maxsus xususiyati tanlanadi.DNS trafigidan zararli domenlarni tanlash uchun uchta mashhur ML klassifikatoridan foydalanildi. Ishlatilgan tasniflagichlar Adaboost, Bagging va NB edi. Natijalar barcha algoritmlar uchun 90% dan yuqori aniqlik yaxshi ishlashi ko‘zlangan, ular orasida faqat kichik farqlar mavjud bo‘lishi mumkin. Bunday natijalar domen nomlari trafikda paydo bo‘lganda zararli botnet xatti-harakatlarini aniqlash va to‘xtatish muvaffaqiyatini aniq ko‘rsata oladi.

ISSN 3030-3907

Hujumlarni aniqlash tizimlari uchun Naive Bayesning takomillashtirilgan yechimini taklif qildi. Naive Bayes algoritmi Bayes tenglamasiga asoslanadi:

$$P(H|U) = \frac{P(U|H) * P(H)}{P(U)}$$

Bu yerda:

- U – klassga ega bo‘lmagan ma’lumotlar
- H - U ning gipotezasi
- P () - ehtimollik

Naive Bayes algoritmida ehtimolliklardan biri 0 bo‘lganda muammo bor. Bu ishlatilganda uning past aniqligiga olib keladi.Naive Bayes algoritmiga ikkita modifikatsiyani taklif qildi. Birinchisi, ehtimolligi 0 ga teng bo‘lgan har bir o‘zgaruvchini olib tashlashdir. Ikkinchi modifikatsiya esa, ehtimollik 0 ga teng bo‘lganda, ko‘paytirish amalini qo‘shish amali bilan o‘zgartirishdir. Ularning yechimida ular birinchi navbatda korrelyatsiyaga asoslangan xususiyatlarni tanlashni amalga oshirdilar.

Xulosa

Maqolada mashinani o‘qitishning yangi texnologiyalaridan foydalangan holda botnet yoki zararli trafik faoliyatini aniqlash taklif qilingan. Ushbu ishda mashinani o‘qitishning nazorat ostida hamda nazoratda bo‘lmagan algoritmlar haqida va Naive Bayes,tasodisiy o‘rmon hamda qaror daraxtlari algoritmlari haqida ma’lumotga ega bo‘lishingiz mumkin. Eksperimental natijalar shuni ko‘rsatdiki, qarorlar daraxti modeli boshqa algoritm modellariga qaraganda yaxshiroq ishlagan, shuningdek, ilgari ko‘rib chiqilgan adabiyotlarda eslatib o‘tilgan modellar biroz yaxshilangan. Nazariy jihatdan, ushbu model bir nechta botnet hujumlarini va boshqa turdagi zararli tarmoq faoliyatini aniqlash uchun ishlatilishi mumkin.

Bundan tashqari, klasterlash hamda nazoratsiz o‘qitish usullarini tekshirish va ushbu maqolada qo‘llaniladigan nazorat ostida o‘qitish usullari bilan solishtirish mumkin. Bundan tashqari, ushbu natijalarni yanada takomillashtirish uchun xususiyatlarni tanlashning boshqa usullarini tekshirish mumkin. Nihoyat, mashinani o‘qitish modeli real vaqt rejimida boshqariladigan muhitda sinovdan o‘tkazilishi mumkin, bu modelning ishlashini aniq o‘lchash va u turli xil tahdidlarga, masalan, nol kunlik tahdidlarga qanday munosabatda bo‘lishini aniqlaydi.

FOYDALANILGAN ADABIYOTLAR

1. Checkpoint. What Is an Intrusion Detection System? Available online: https://www.checkpoint.com/cyber-hub/network-security/what-is-an-intrusion-detection-system-ids/ (accessed on 19 May 2022).

ISSN 3030-3907

2. IBM Cloud Education. Supervised Learning. Available online: https://www.ibm.com/cloud/learn/supervised-learning (accessed on 19 May 2022).
3. Seldon. Machine Learning Regression Explained. Available online: https://www.seldon.io/machine-learning-regression-explained (accessed on 19 May 2022).
4. Terence, S. All Machine Learning Models Explained in 6 Minutes. Available online: https://www.ibm.com/cloud/learn/unsupervised-learning (accessed on 19 May 2022).
5. IBM Cloud Education. Unsupervised Learning. Available online: https://www.ibm.com/cloud/learn/unsupervised-learning (accessed on 19 May 2022).
6. Ben n'cir, C.-E.; Cleuziou, G.; Nadia, E. Overview of Overlapping Partitional Clustering Methods. In Partitional Clustering Algorithms; Springer: Cham, Switzerland, 2015; pp. 245–275.
7. Joos, K. The Apriori Algorithm. Available online: https://towardsdatascience.com/the-apriori-algorithm-5da3db9aea95 (accessed on 22 June 2022).
8. Matt, B. A One-Stop Shop for Principal Component Analysis. Available online: https://towardsdatascience.com/a-one-stop-shop-for-principal-component-analysis-5582fb7e0a9c (accessed on 28 June 2022).
9. Ashiku, L.; Dagli, C. Network Intrusion Detection System using Deep Learning. Procedia Comput. Sci. 2021, 185, 239–247.
10. Tavallaee, M.; Bagheri, E.; Lu, W.; Ghorbani, A.A. A detailed analysis of the KDD CUP 99 data set. In Proceedings of the 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, Ottawa, ON, Canada, 8–10 July 2009; pp. 1–6.
11. Protic, D. Review of KDD Cup '99, NSL-KDD and Kyoto 2006+ Datasets. Vojnoteh. Glas. 2018, 66, 580–596.
12. Moustafa, N. The UNSW-NB15 Dataset. Available online: https://research.unsw.edu.au/projects/unsw-nb15-dataset (accessed on 28 February 2022).
13. Sharafaldin, I.; Lashkari, A.H.; Ghorbani, A. Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization; Canadian Institute for Cybersecurity (CIC): Fredericton, NB, Canada, 2018; pp. 108–116.
14. Chen, L.; Kuang, X.; Xu, A.; Suo, S.; Yang, Y. A Novel Network Intrusion Detection System Based on CNN. In Proceedings of the 2020 Eighth International Conference on Advanced Cloud and Big Data (CBD), Taiyuan, China, 5–6 December 2020; pp. 243–247.

ISSN 3030-3907

15. Gautam, R.K.S.; Doegar, E.A. An Ensemble Approach for Intrusion Detection System Using Machine Learning Algorithms. In Proceedings of the 2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 11–12 January 2018; pp. 14–15.
16. Al-Yaseen, W.L.; Othman, Z.A.; Nazri, M.Z.A. Multi-level hybrid support vector machine and extreme learning machine based on modified K-means for intrusion detection system. Expert Syst. Appl. 2017, 67, 296–303.
17. Kanimozhi, P.; Victoire, T.A.A. Oppositional tunicate fuzzy C-means algorithm and logistic regression for intrusion detection on cloud. Concurr. Comput. Pract. Exp. 2022, 34, e6624.
18. Chen, Y.; Yuan, F. Dynamic detection of malicious intrusion in wireless network based on improved random forest algorithm. In Proceedings of the 2022 IEEE Asia-Pacific Conference on Image Processing, Electronics and Computers (IPEC), Dalian, China, 14–16 April 2022; pp. 27–32.
19. Jabez, J.; Muthukumar, B. Intrusion Detection System (IDS): Anomaly Detection Using Outlier Detection Approach. Procedia Comput. Sci. 2015, 48, 338–346.
20. Kurniawan, Y.; Razi, F.; Nofiyati, N.; Wijayanto, B.; Hidayat, M. Naive Bayes modification for intrusion detection system classification with zero probability. Bull. Electr. Eng. Inform. 2021, 10, 2751–2758.
21. Chauhan, N. Naïve Bayes Algorithm: Everything You Need to Know. Available online: https://www.kdnuggets.com/2020/06/naive-bayes-algorithm-everything.html#:~:text=One%20of%20the%20disadvantages%20of,all%20the%20probabilities%20are%20multiplied (accessed on 9 September 2022).
22. Gu, J.; Lu, S. An effective intrusion detection approach using SVM with naïve Bayes feature embedding. Comput. Secur. 2021, 103, 102158.
23. Pan, J.-S.; Fan, F.; Chu, S.C.; Zhao, H.; Liu, G. A Lightweight Intelligent Intrusion Detection Model for Wireless Sensor Networks. Secur. Commun. Networks 2021, 2021, 1–15.
24. Xiao, Y.; Xing, C.; Zhang, T.; Zhao, Z. An Intrusion Detection Model Based on Feature Reduction and Convolutional Neural Networks. IEEE Access 2019, 7, 42210–42219.
25. Zhang, X.; Chen, J.; Zhou, Y.; Han, L.; Lin, J. A Multiple-Layer Representation Learning Model for Network-Based Attack Detection. IEEE Access 2019, 7, 91992–92008.
26. Yu, Y.; Bian, N. An Intrusion Detection Method Using Few-Shot Learning. IEEE Access 2020, 8, 49730–49740.

ISSN 3030-3907

27. Gao, X.; Shan, C.; Hu, C.; Niu, Z.; Liu, Z. An Adaptive Ensemble Machine Learning Model for Intrusion Detection. IEEE Access 2019, 7, 82512–82521.

ISSN 3030-3907