ҒТАМР 28.23.01

Н.М. Жунисов[1] – *негізгі автор*, ©
А.Б. Абен[2], **Д. Исаков**[3]

[1]*PhD, аға оқытушы,* [2]*Докторант,* [3]*Магистрант*

ORCİD [1]*https://orcid.org/0000-0001-7127-3987* [2]*https://orcid.org/0000-0001-8534-3288*

[1,2,3]*Қожа Ахмет Ясауи атындағы Халықаралық қазақ-түрік университеті, Түркістан қ., Қазақстан*

@ [1]*nurseit.zhunissov@ayu.edu.kz*

https://doi.org/10.55956/ZCJD4515

МАШИНАЛЫҚ ОҚЫТУ АЛГОРИТМДЕРІН САЛЫСТЫРА ОТЫРЫП ЖЕЛІЛІК ШАБУЫЛДАРДЫ АНЫҚТАУ

Аңдатпа. Заманауи ақпараттық жүйелердің дамуы желілік шабуылдардың күрделілігін арттырып, қауіпсіздік мәселелерінің өзектілігін көтерді. Бұл мақалада машиналық оқыту (МО) алгоритмдерінің желілік шабуылдарды анықтаудағы тиімділігі салыстырылады. Әртүрлі МО әдістері, оның ішінде нейрондық желілер, шешім ағаштары, терең оқыту және қарсыласушы машиналық оқыту, желілік шабуылдарды анықтаудағы дәлдігі мен жылдамдығын зерттеу объектісі ретінде алынады.

Зерттеу нәтижелері желілік қауіпсіздікті қамтамасыз ету үшін машиналық оқытудың адаптивті және инновациялық шешімдерінің маңыздылығын көрсетеді. Сонымен қатар, келешек зерттеулер үшін бағыттар мен ұсыныстар беріледі, осылайша, машиналық оқыту алгоритмдерінің желілік шабуылдарға қарсы тұрудағы әлеуеті мен тиімділігі арта түседі.

Бұл мақалада желілік шабуылдарды анықтауда қолданылатын машиналық оқыту алгоритмдері талданады. Дәстүрлі әдістер бұл қауіптерге қарсы тұруда жеткіліксіз болып отыр, сондықтан машиналық оқыту технологиялары тиімді балама ретінде қарастырылады. Мақалада бақыланатын оқыту, бақылаусыз оқыту және жартылай бақылаулы оқыту әдістері зерттеледі. Бақыланатын оқыту әдістерінің арасында логистикалық регрессия, шешім ағаштары, кездейсоқ ормандар, қолдау вектор машиналары және нейрондық желілер қарастырылады. Бақылаусыз оқыту әдістері ретінде K-Means кластерлеу, автоэнкодерлер және негізгі компоненттерді талдау әдістері талқыланады.

Жартылай бақылаулы оқыту әдістері ретінде белгілерді тарату және өздігінен оқыту әдістері зерттеледі. Әрбір алгоритмнің артықшылықтары мен кемшіліктері салыстырылып, олардың желілік шабуылдарды анықтаудағы тиімділігі талданады.

Тірек сөздер: машиналық оқыту, желілік шабуыл, алгоритм, DDoS, логистикалық регрессия, Random Forest моделі.

Жунисов, Н.М. Машиналық оқыту алгоритмдерін салыстыра отырып желілік шабуылдарды анықтау [Мәтін] / Н.М. Жунисов, А.Б. Абен, Д. Исаков //Механика және технологиялар / Ғылыми журнал. – 2024. – №4(86). – Б.430-439. https://doi.org/10.55956/ZCJD4515

Кіріспе. Желілік қауіпсіздік біздің заманымыздағы ақпараттық технологиялар саласындағы маңызды мәселелердің бірі. Шабуылдардың жаңа түрлері мен кибершабуыл әдістері үнемі дамып келе жатқандықтан,

желілік шабуылдарды анықтаудың тиімді әдістері қажет. Мұнда машиналық оқыту алгоритмдері маңызды рөл атқарады (Machine Learning – ML). Машиналық оқыту алгоритмдері салыстырылады және олардың желілік шабуылдарды анықтаудағы тиімділігі талқыланады. Желілік шабуылдарды анықтаудағы машиналық оқыту алгоритмдерінің тиімділігін салыстыра отырып, олардың нақты қолдану жағдайында қалай жұмыс істейтінін түсінуге болады. Бұл зерттеу желілік қауіпсіздік мамандарына машиналық оқыту әдістерін таңдауда және қолдануда көмек көрсетуге бағытталған. Машиналық оқыту алгоритмдерінің әртүрлі түрлері бар, олардың әрқайсысы ерекше артықшылықтар мен кемшіліктерге ие. Бақыланатын оқыту (Supervised Learning) әдістері алдын ала таңбаланған деректер жиынтығына негізделеді. Бұл әдістер нақты шабуыл түрлерін дәл анықтауға мүмкіндік береді. Бақылаусыз оқыту (Unsupervised Learning) әдістері таңбаланбаған деректерді пайдаланады және желідегі қалыпты және аномалды әрекеттерді автоматты түрде айыруға негізделген. Жартылай бақылаулы оқыту (Semi-supervised Learning) әдістері аз мөлшерде таңбаланған және көп мөлшерде таңбаланбаған деректерді бірге пайдаланып, шабуылдарды анықтаудың тиімділігін арттырады.

Машиналық оқыту алгоритмдері желілік шабуылдарды анықтаудың маңызды құралы болып табылады. Әр әдістің өзіндік ерекшеліктері бар, сондықтан нақты жағдайға байланысты дұрыс алгоритмді таңдау өте маңызды. Алдағы бөлімдерде осы әдістердің әрқайсысын жан-жақты қарастырып, олардың артықшылықтары мен кемшіліктері талқыланады.

Y.K. Saheed және әріптестері [1] өз зерттеуінде IoT желілеріндегі шабуылдарды анықтау үшін МО әдістерін қолданады. Зерттеу нәтижелері алгоритмдердің тиімділігі мен өнімділігі, әсіресе деректер жинағының сапасы мен көлеміне байланысты екенін көрсетеді. Авторлар IoT экожүйесіндегі шабуылдарға ерекше назар аударып, адаптивті модельдердің қажеттілігін атап өтеді. K. Ullah және командасы [2] SS7 протоколындағы осалдықтарды зерттеп, машиналық оқыту мен ереже негізіндегі әдістерді салыстырады. Нәтижелер машиналық оқыту әдістерінің ережелерге негізделген тәсілдерден тиімдірек екенін көрсетеді. Зерттеу SS7 желісіндегі шабуылдарды анықтауда МО-ның әлеуетін және оның жылдамдығы мен дәлдігін айқындайды. K. Не және басқалары [3] қарсыласушы машиналық оқытуды желілік қауіпсіздік контекстінде қарастырады. Зерттеу нейрондық желілердің шабуылдарға төзімділігін арттыруға арналған түрлі стратегияларды ұсынады. Авторлар алгоритмдердің әлсіз жақтарын атап өтіп, тиімдірек шешімдер әзірлеу қажеттілігін білдіреді. Y. Wu және оның серіктестері [4] терең оқыту әдістерін пайдалана отырып желілік шабуылдарды анықтауға арналған әдістерді зерттейді. Бұл зерттеуде терең нейрондық желілердің тиімділігі көрсетіліп, олардың ауқымды деректермен жұмыс істеу қабілеті талданады. A. Aljuhani [5] дистрибутталған шабуылдарға қарсы МО әдістерін талдайды. Зерттеу машиналық оқытудың DDoS шабуылдарын анықтаудағы мүмкіндіктерін көрсетеді, сонымен қатар деректерді өңдеу жылдамдығының шешуші рөлін атап өтеді. S. Wang және әріптестері [6] желідегі аномалияларды анықтау үшін МО әдістерінің әртүрлілігін зерттейді. Бұл шолу алгоритмдердің тиімділігін, сонымен қатар олардың аномалияларды анықтаудағы дәлдігін бағалайды.

Келтірілген зерттеулер машиналық оқыту алгоритмдерінің желілік шабуылдарды анықтаудағы көпқырлылығы мен тиімділігін көрсетеді. IoT желілеріндегі шабуылдарды анықтау, SS7 протоколының уязвимостары,

қарсыласушы машиналық оқыту және терең оқыту әдістері – бұл саладағы негізгі бағыттар. Алдағы уақытта машиналық оқыту әдістерінің әрі қарай дамуы желілік қауіпсіздік мәселелерін шешуде маңызды рөл атқара алады.

Желілік қауіпсіздік саласында машиналық оқыту (МО) әдістерінің дамуы, әсіресе, шабуылдарды анықтау мен алдын алуда жаңа мүмкіндіктер ашады. Бұл бөлімде қарсыласушы машиналық оқытудың, DDoS шабуылдарын анықтаудың және сымсыз сенсорлық желілердегі шабуылдарды анықтаудың тиімді әдістері мен шешімдері қарастырылады.

M. Khan мен L. Ghafoor [7] зерттеуінде қарсыласушы машиналық оқыту желілік қауіпсіздік контекстінде кездесетін негізгі мәселелер мен шешімдерді талдайды. Авторлар қарсыласушы шабуылдардың әсерін, олардың алгоритмдерге қауіп төндіру қабілетін және желілік қауіпсіздік жүйелеріндегі осалдықтарды қарастырады. Зерттеу қарсыласушы машиналық оқытудың жетілдірілген алгоритмдерін және олардың тиімділігін арттыру үшін қажет шараларды анықтайды, осылайша желілік шабуылдарға қарсы тұру үшін тиімді әдістерді ұсынады. H.M. Saleh және әріптестері [8] сымсыз сенсорлық желілердегі шабуылдарды анықтау үшін стохастикалық градиентті төмендету әдісін қолданатын зерттеу жүргізді. Бұл зерттеу сымсыз желілердегі шабуылдарды тиімді анықтау мақсатында машиналық оқыту алгоритмдерін пайдаланудың инновациялық тәсілдерін көрсетеді. Нәтижелер алгоритмнің жылдамдығы мен дәлдігін арттыруға мүмкіндік беретінін айқындайды, бұл сымсыз сенсорлық желілердегі қауіпсіздікті нығайту үшін маңызды болып табылады. M.S. Elsayed және оның командасы [9] DDoS шабуылдарын анықтауға арналған Ddosnet атты терең оқыту моделін таныстырады. Зерттеуде терең нейрондық желілердің DDoS шабуылдарын анықтаудағы тиімділігі және алгоритмнің жылдамдығы мен дәлдігі талқыланады. Ddosnet моделі DDoS шабуылдарын реальды уақытта анықтауға мүмкіндік беретін қуатты құрал ретінде қарастырылады, бұл желілік қауіпсіздікті қамтамасыз етуде маңызды рөл атқарады.

Аталған зерттеулер машиналық оқыту әдістерінің желілік шабуылдарды анықтаудағы әлеуетін айқындайды. Қарсыласушы машиналық оқыту, сымсыз сенсорлық желілердегі шабуылдарды анықтау және DDoS шабуылдарын алдын алу – бұл саланың дамуына үлкен әсер етеді. Болашақта осы бағыттағы зерттеулер машиналық оқыту әдістерінің тиімділігін арттыру мен желілік қауіпсіздікті қамтамасыз етуге көмектеседі.

Зерттеу шарттары мен әдістері. Желілік шабуылдар – бұл компьютерлік желілерге рұқсатсыз кіру немесе бүліну мақсатында жасалатын әрекеттер. Мұндай шабуылдар желілік инфрақұрылымның қауіпсіздігіне үлкен қауіп төндіреді, өйткені олар деректердің ұрлануына, бүлінуіне немесе жойылуына әкелуі мүмкін. Желілік шабуылдар ұйымдардың қызметіне айтарлықтай зиян келтіруі және экономикалық шығындар мен беделдің төмендеуіне әкелуі мүмкін. Сондықтан желілік қауіпсіздік шараларын тиімді ұйымдастыру және шабуылдарды уақтылы анықтау өте маңызды.

Желілік шабуылдардың әртүрлі түрлері бар, олардың кейбіреулері төменде келтірілген:

– DOS және DDoS шабуылдары (Denial of Service және Distributed Denial of Service): бұл шабуылдардың мақсаты-жүйені немесе қызмет көрсету желісін жою. Шабуылдар жүйені шамадан тыс жүктеу арқылы жүзеге асырылады, нәтижесінде жүйе пайдаланушылардың сұраныстарына жауап бере алмайды. DDoS шабуылдары көптеген компьютерлерге бір уақытта шабуыл жасау арқылы жүзеге асырылады;

– Фишинг (Phishing): шабуылдың бұл түрі пайдаланушыларды алдау арқылы олардың жеке ақпаратын (парольдер, несие карталарының нөмірлері) алуға бағытталған. Фишингтік шабуылдар көбінесе электрондық пошта немесе жалған веб-сайттар арқылы жасалады;

– Зиянды бағдарламалар (зиянды бағдарламалар): бұл санатқа вирустар, Трояндар және басқа зиянды бағдарламалар кіреді. Олар компьютерлерге немесе желілерге еніп, деректерді ұрлауға, бүлдіруге немесе жоюға қабілетті;

– MitM шабуылдары (man-in-the-Middle): бұл шабуыл кезінде шабуылдаушы екі тарап арасындағы байланысты өз пайдасына ұстап, пайдаланады. Бұл әдіс арқылы шабуылдаушы құпия деректерді ұстай алады;

– SQL инъекциясы: бұл шабуыл зиянды SQL сұрауларын веб-қосымшалар базасына енгізу арқылы жүзеге асырылады. Нәтижесінде шабуылдаушы дерекқордағы деректерге рұқсатсыз қол жеткізе алады.

Желілік шабуылдардың салдары. Желілік шабуылдардың салдары өте ауыр болуы мүмкін, олардың кейбіреулері:

– Деректерді жоғалту немесе ұрлау: құпия деректерді ұрлау ұйымдар мен жеке тұлғаларға үлкен зиян келтіруі мүмкін;

– Қызметті тоқтату: DOS және DDoS шабуылдары компаниялардың қызметін тоқтатып, экономикалық шығындарға әкелуі мүмкін;

– Қаржылық шығындар: жүйені қалпына келтіру және шығындарды өтеу үлкен қаржылық ресурстарды қажет етеді;

– Беделдің төмендеуі: қауіпсіздік оқиғалары ұйымдардың беделіне нұқсан келтіруі және клиенттердің сенімін жоғалтуы мүмкін [10].

Желілік шабуылдарды анықтау қажеттілігі. Желілік шабуылдарды уақтылы анықтау және алдын алу ұйымдардың киберқауіпсіздігін қамтамасыз етудің маңызды бөлігі болып табылады. Желілік шабуылдарды ерте анықтау үшін желіге үнемі мониторинг жүргізіп, тиімді қорғаныс шараларын қабылдау қажет. Мұнда машиналық оқыту алгоритмдері үлкен рөл атқара алады, өйткені олар заңдылықтарды тануға және ауытқуларды анықтауға қабілетті. Машиналық оқыту әдістерін қолдана отырып, желілік шабуылдарды анықтаудың тиімділігін арттыруға және қауіпсіздікті арттыруға болады. Келесі бөлімде біз желілік шабуылдарды анықтауда қолданылатын машиналық оқыту алгоритмдерін талқылаймыз.

Машиналық оқыту алгоритмдерін қолдана отырып, желілік шабуылдарды зерттеу өте өзекті сала болып табылады, әсіресе киберқауіпсіздік жағдайында. Қазіргі қауіп-қатерлерге қарсы тиімсіз болуы мүмкін шабуылдарды анықтаудың дәстүрлі әдістерінің орнына Машиналық оқыту алгоритмдері деректердің үлкен көлемін талдауға және шабуылдың болуын көрсететін жасырын заңдылықтарды анықтауға мүмкіндік береді [11]. Деректерді жүктеуден бастап, соның ішінде әртүрлі белгілер туралы ақпарат (мысалы, IP мекенжайлары, пакет түрлері және т.б.) және бұл шабуыл ма, жоқ па екенін көрсететін белгі. Содан кейін деректерден ең маңызды белгілерді таңдау үшін selectkbest деп аталатын әдісті қолданылады. Шабуыл белгілерімен тығыз байланысты ең жақсы 10 белгіні таңдалуы керек. chi2 деп аталатын статистикалық тест арқылы әрбір белгіні және оның шабуыл белгілерімен байланысын талдалынады. Әрбір белгінің маңыздылығын бағалағаннан кейін компьютерлік желілердегі шабуылдарды болжау қабілетімізге ең үлкен әсер ететін үздік 10 белгіні қарастырылады. Сайып келгенде, бұл процесс желідегі шабуылдарды дәлірек болжау үшін

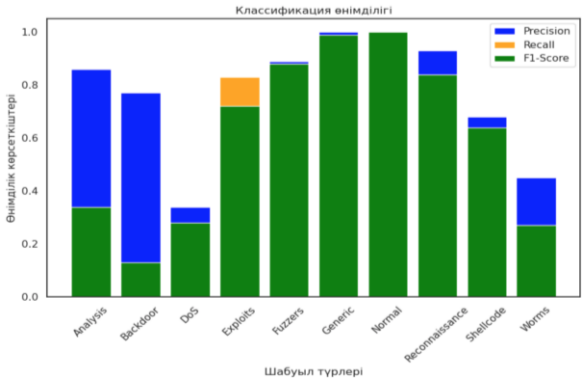
пайдалануға болатын деректеріміздегі ең маңызды белгілерді анықтауға көмектеседі.

Компьютерлік желілерде қандай шабуылдар болғанын болжауға тырысатын Машиналық оқыту моделін жасалады. Деректер екі бөлікке бөлінеді: бір бөлігі модельді үйрету үшін, ал екіншісі оның қаншалықты жақсы жұмыс істейтінін тексеру үшін қолданылады. Модельді оқытқаннан кейін оның бұрын көрмеген деректерге шабуыл түрлерін қаншалықты дәл болжайтынын тексеріледі. Модельдің шабуылдардың әр түрі үшін болжамдарды қаншалықты жақсы орындайтынын көрсететін есеп шығарылады. Бұл процесс модельдің өнімділігін бағалауға және оның компьютерлік желілердегі шабуылдарды қаншалықты жақсы анықтап, жіктей алатынын түсінуге мүмкіндік береді [12]. Модель кейбір класстар үшін жоғары мәндермен жақсы нәтиже көрсетеді (мысалы, «жалпы» және «қалыпты»), ал басқалары үшін төмен (мысалы, «Backdoor» және «Worms»). Бұл деректердегі сыныптардың біркелкі бөлінбеуіне немесе кейбір сыныптарды басқаларға қарағанда болжау қиынырақ болуына байланысты болуы мүмкін. 1-суреттегі код компьютерлік желілердегі әрбір шабуыл сыныбы үшін дәлдік (дәлдік), толықтық (recall) және (F1-score) мәндерін көрсететін бағаналы диаграмма жасайды.

```
import matplotlib.pyplot as plt
classes = ['Analysis', 'Backdoor', 'DoS', 'Exploits', 'Fuzzers', 'Generic', 'Normal
precision = [0.86, 0.77, 0.34, 0.64, 0.89, 1.00, 1.00, 0.93, 0.68, 0.45]
recall = [0.21, 0.07, 0.23, 0.83, 0.88, 0.98, 1.00, 0.76, 0.61, 0.19]
f1_score = [0.34, 0.13, 0.28, 0.72, 0.88, 0.99, 1.00, 0.84, 0.64, 0.27]
plt.figure(figsize=(10, 6))
plt.bar(classes, precision, color='blue', label='Precision')
plt.bar(classes, recall, color='orange', label='Recall')
plt.bar(classes, f1_score, color='green', label='F1-Score')
plt.xlabel('Шабуыл түрлері')
plt.ylabel('Өнімділік көрсеткіштері')
plt.title('Классификация өнімділігі')
plt.xticks(rotation=45)
plt.legend()
plt.show()
```

Сурет 1. Шабуыл мәндерін көрсететін бағаналы диаграмма жасау коды

Әрбір шабуыл класы X осі бойынша, ал метрикалық мәндер Y осі бойынша белгіленеді. 2-суреттегі график әртүрлі шабуыл сыныптары үшін модельдің өнімділігін салыстыруға және модельдің әр шабуыл түрін болжауда қаншалықты жақсы жұмыс істейтінін түсінуге көмектеседі (Көк бағандар әр сынып үшін дәлдікті білдіреді, Қызғылт сары бағандар әр сынып үшін толықтығын білдіреді, Жасыл бағандар әр сынып үшін F1 өлшемін білдіреді).



Сурет 2. Кибершабуыл түрлерінің классфикация өнімділігі

Зерттеу нәтижелері және оларды талқылау. *Алгоритмдерді қолдану.* Суреттегі код scikit-learn (sklearn) кітапханасынан шешім ағашы (Decision Tree Classifier) классификатор нысанын жасайды.Содан кейін классификатор оқу деректер жиынтығында (X_train және y_train) оқытылады және соңында сынақ деректер жиынына (X_test) жауаптарды болжау үшін пайдаланылады.

```
from sklearn.metrics import accuracy_score, precision_score, recall_score, f1_score

# Calculate accuracy
accuracy = accuracy_score(y_test, y_pred)
print("Accuracy:", accuracy*100)

# Calculate precision
precision = precision_score(y_test, y_pred)
print("Precision:", precision*100)

# Calculate recall (sensitivity)
recall = recall_score(y_test, y_pred)
print("Recall (Sensitivity):", recall*100)

# Calculate F1-score
f1 = f1_score(y_test, y_pred)
print("F1-Score:", f1*100)
```

```
Accuracy: 93.63147137202142
Precision: 95.08528417943063
Recall (Sensitivity): 94.96039443905593
F1-Score: 95.0227982731951
```

Сурет 3. Visualizing the rules дәлдікті бағалау

3-суреттегі код дәлдік (accuracy), дәлдік (precision), толықтық (recall) сияқты жіктеу моделінің өнімділігін бағалау үшін бірнеше көрсеткіштерді есептейді [13]. Олардың әрқайсысын қарастырайық:

– Дәлдік (Accuracy): бұл сынақ жинағындағы барлық үлгілер арасында дұрыс жіктелген үлгілердің пайызы;

– Дәлдік (precision): бұл модель оң деп болжаған барлық үлгілер арасында дұрыс жіктелген оң үлгілердің үлесі;

– Толықтығы (Recall) немесе сезімталдығы: бұл барлық жарамды оң үлгілер арасында дұрыс жіктелген оң үлгілердің үлесі;

– F1-Өлшем (F1-Score): бұл дәлдік пен толықтық арасындағы гармоникалық орта. Ол дәлдік пен толықтық арасындағы тепе-теңдікті қамтамасыз етеді және көбінесе теңгерімсіз сыныптар үшін жалпы өнімділік көрсеткіші ретінде қолданылады.

Әрбір метрика пайыздық форматта ұсынылған. Бұл көрсеткіштер модельдің тестілік деректер жиынтығындағы сыныптарды болжауда қаншалықты жақсы жұмыс істейтінін бағалау үшін қолданылады.

4-суреттегі код бұрын жүктелген деректер жиынтығы болуы мүмкін data айнымалысын пайдаланады. Ол осы деректер жиынтығының «attack_cat» бағанынан бірегей мәндерді шығарады және оларды экранға шығарады.

```
# 'attack_cat' sütunundaki benzersiz değerleri kontrol edin
unique_attack_categories = data['attack_cat'].unique()
print(unique_attack_categories)
```

```
['Normal' 'Reconnaissance' 'Backdoor' 'DoS' 'Exploits' 'Analysis'
 'Fuzzers' 'Worms' 'Shellcode' 'Generic']
```

Сурет 4. «attack_cat» мәндері

Бұл кодтың міндеті – деректер жиынтығының "attack_cat" бағанында болатын шабуылдардың бірегей санаттарын анықтау. Бұл деректерде берілген шабуыл түрлерінің әртүрлілігін түсіну және тапсырманың нақты

қажеттіліктеріне байланысты әрі қарай талдау немесе өңдеу үшін пайдалы болуы мүмкін [14-15].

5-суретте жаңа new_data деректер жинағы үшін шабуыл санатын болжау үшін оқытылған Random Forest (rf_classifier) үлгісін пайдаланады.

```
# Yeni verileri girin (bu örnekte varsayılan olarak bir örnek kullanılmıştır)
new_data = pd.DataFrame({
    'dur': [1.0],
    'proto': [0],
    'service': [1],
    'state': [1],
    'spkts': [20],
    'dpkts': [20],
    'sbytes': [500],
    'dbytes': [250],
    'rate': [100.0],
    'sttl': [300],
    'ct_state_ttl': [1],
    'ct_dst_ltm': [0],
    'ct_src_dport_ltm': [1],
    'ct_dst_sport_ltm': [1],
    'ct_dst_src_ltm': [0],
    'is_ftp_login': [0],
    'ct_ftp_cmd': [0],
    'ct_flw_http_mthd': [0],
    'ct_src_ltm': [1],
    'ct_srv_dst': [1],
    'is_sm_ips_ports': [0]
})

# Random Forest modeli
predicted_attack_cat = rf_classifier.predict(new_data)

print("Болжалды шабуыл түрі:", predicted_attack_cat)
```

Сурет 5.Шабуыл түрін болжау коды

new_data – жіктеуге арналған жаңа деректерді қамтитын DataFrame. Бұл жағдайда сөздік түрінде берілген жаңа деректердің бір мысалы қолданылады.

predicted_attack_cat = rf_classifier.predict (new_data) – random Forest моделі жаңа деректер үшін шабуыл санатын болжау үшін қолданылады. Predict () әдісі жаңа деректерді қабылдайды және шабуылдың болжамды санатын қайтарады.

print ("Болжалды шабуыл түрі:", predicted_attack_cat) – шабуылдың болжамды санаты экранға шығарылады.

Бұл кодты оқытылған Random Forest моделін қолдана отырып, жаңа деректерді шабуыл түріне қарай жіктеу үшін пайдалануға болады.

Машиналық оқыту алгоритімдерінің нәтижелері 1-кестеде келтірілген.

Кесте 1

Машиналық оқыту алгоритімдерінің нәтижелері

Model	Accuracy	Precision	Recall (Sensitivity)	F1-Score
Шешім ағашы	93,55	95,04	94,88	94,96
Логистикалық регрессия	80,73	78,78	95,66	86,40
k-ең жақын көрші (kNN)	85,05	86,70	90,54	88,57
Қосымша ағаштар	94,68	96,32	95,34	95,82
Кездейсоқ орман	94,99	96,41	95,73	96,07
Градиентті Күшейтетін Классификатор	93,26	94,53	94,97	94,75
Көпқабатты перцептрон (MLP) нейрондық желі	81,83	82,89	90,25	86,41

Random Forest моделі UNSW-NB15 деректер жиынында ең жоғары дәлдікке (94,99%) қол жеткізіп, деректерді ең тиімді жіктейтін модель ретінде ерекшеленеді. Бұл модельден кейін Қосымша ағаштар (94,68%) және Шешім ағашы (93,55%) әдістері келеді. P дәлдік мәндерін талдау кезінде де Random Forest ең жоғары нәтижені көрсетіп отыр (96,41%), одан кейін Қосымша ағаштар (96,32%) және Шешім ағашы (95,04%) модельдері орналасқан.

Сезімталдық тұрғысынан қарастырғанда, Random Forest үлгісінің ең жоғары мәнге ие болғаны анық (95,73%). Сонымен қатар, Extra Trees (95,34%) және Decision Tree (94,88%) үлгілері де сезімталдық көрсеткіштері бойынша жоғары нәтижелер көрсетуде. F1-Score метрикасына сәйкес те, Random Forest моделі ең жоғары көрсеткішке (96,07%) ие, бұл басқа модельдер арасынан Extra Trees (95,82%) және Decision Tree (94,96%) үлгілерін де ерекше атап өтуге мүмкіндік береді.

Қорытынды. Желілік шабуылдарды анықтау үшін әртүрлі машиналық оқыту алгоритмдерін қолдануға болады. Әрбір алгоритмнің артықшылықтары мен кемшіліктері бар, және олардың тиімділігі нақты жағдайға байланысты өзгереді. Қазіргі таңда ең тиімді шешім – бірнеше әдісті біріктіріп қолдану, яғни гибридтік жүйелерді құру болып табылады. Мұндай тәсілдер желілік шабуылдарды дәлірек және тиімдірек анықтауға мүмкіндік береді.

Ең сенімді жіктеуіш деректердің ерекшелігіне және жіктеу тапсырмасына байланысты. Бір классификатор басқаларға қарағанда белгілі бір деректер түрлеріне немесе шарттарға жақсырақ сәйкес келуі мүмкін. Мысалы, Random Forest деректердегі шығарындылар мен шуды жақсы басқара алады, Gradient Boosting үлкен деректер жиынында жақсы нәтиже бере алады, ал MLP белгілер мен мақсатты айнымалы арасында сызықтық емес тәуелділіктер бар жоғары күрделілік тапсырмалары үшін тиімді болуы мүмкін.

Белгілі бір тапсырма үшін ең сенімді жіктеуішті анықтау үшін көбінесе әртүрлі модельдермен эксперименттер жүргізу, гиперпараметрлерді таңдау және олардың өнімділігін кросс-валидация немесе модельді бағалаудың басқа әдістері арқылы бағалау қажет.

Қорытындылай келе, берілген нәтижелерге сәйкес, Random Forest моделі UNSW-NB15 деректер жиынында ең жоғары өнімділікке қол жеткізіп, тиімді машиналық оқыту модельдерінің бірі ретінде киберқауіпсіздік саласындағы қолданбалар үшін оңтайлы таңдау бола алатыны көрінеді.

Әдебиеттер тізімі

1. Saheed Y.K. et al. A machine learning-based intrusion detection for detecting internet of things network attacks //Alexandria Engineering Journal. – 2022. – Vol. 61. – No. 12. – P. 9395-9409.
2. Ullah K. et al. SS7 vulnerabilities – a survey and implementation of machine learning vs rule based filtering for detection of SS7 network attacks //IEEE Communications Surveys & Tutorials. – 2020. – Vol. 22. – No. 2. – P. 1337-1371.
3. He K., Kim D.D., Asghar M.R. Adversarial machine learning for network intrusion detection systems: A comprehensive survey //IEEE Communications Surveys & Tutorials. – 2023. – Vol. 25. – No. 1. – P. 538-566.
4. Kumar A., Glisson W. B., Benton R. Network attack detection using an unsupervised machine learning algorithm. – Proceedings of the 53rd Hawaii International Conference on System Sciences, 2020.

5. Wu Y., Wei D., Feng J. Network attacks detection methods based on deep learning techniques: a survey //Security and Communication Networks. – 2020. – Vol. 2020. – No. 1. – P. 8872923.
6. Aljuhani A. Machine learning approaches for combating distributed denial of service attacks in modern networking environments //IEEE Access. – 2021. – Vol. 9. – P. 42236-42264.
7. Khan M., Ghafoor L. Adversarial Machine Learning in the Context of Network Security: Challenges and Solutions //Journal of Computational Intelligence and Robotics. – 2024. – Vol. 4. – No. 1. – P. 51-63.
8. Saleh H.M., Marouane H., Fakhfakh A. Stochastic gradient descent intrusions detection for wireless sensor network attack detection system using machine learning //IEEE Access. – 2024.
9. Wang S. et al. Machine learning in network anomaly detection: A survey //IEEE Access. – 2021. – Vol. 9. – P. 152379-152396.
10. Elsayed M.S. et al. Ddosnet: A deep-learning model for detecting network attacks //2020 IEEE 21st International Symposium on" A World of Wireless, Mobile and Multimedia Networks" (WoWMoM). – IEEE, 2020. – P. 391-396.
11. Bout E., Loscri V., Gallais A. How machine learning changes the nature of cyberattacks on IoT networks: A survey //IEEE Communications Surveys & Tutorials. – 2021. – Vol. 24. – No. 1. – P. 248-279.
12. Injadat M.N., Moubayed A., Shami A. Detecting botnet attacks in IoT environments: An optimized machine learning approach //2020 32nd International Conference on Microelectronics (ICM). – IEEE, 2020. – P. 1-4.
13. Magán-Carrión R. et al. Towards a reliable comparison and evaluation of network intrusion detection systems based on machine learning approaches //Applied Sciences. – 2020. – Vol. 10. – No. 5. – P. 1775.
14. Haji S.H., Ameen S.Y. Attack and anomaly detection in iot networks using machine learning techniques: A review //Asian J. Res. Comput. Sci. – 2021. – Vol. 9. – No. 2. – P. 30-46.
15. Furdek M. et al. Machine learning for optical network security monitoring: A practical perspective //Journal of Lightwave Technology. – 2020. – Vol. 38. – No. 11. – P. 2860-2871.

Материал редакцияға 02.10.24 түсті.

Н.М. Жунисов[1], А.Б. Абен[1], Д. Исаков[1]

[1]Международный казахско-турецкий университет им. Ходжи Ахмеда Ясави, г. Туркестан, Казахстан

ОБНАРУЖЕНИЕ СЕТЕВЫХ АТАК С ПОМОЩЬЮ СРАВНЕНИЯ АЛГОРИТМОВ МАШИННОГО ОБУЧЕНИЯ

Аннотация. Развитие современных информационных систем повысило сложность сетевых атак и повысило актуальность вопросов безопасности. В этой статье сравнивается эффективность алгоритмов машинного обучения (МО) при обнаружении сетевых атак. Различные методы МО, включая нейронные сети, деревья решений, глубокое обучение и противоборствующее машинное обучение, принимаются в качестве объекта исследования точности и скорости обнаружения сетевых атак.

Результаты исследования подчеркивают важность адаптивных и инновационных решений машинного обучения для обеспечения сетевой безопасности. Кроме того, будут даны направления и рекомендации для будущих исследований, что повысит потенциал и эффективность алгоритмов машинного обучения в борьбе с сетевыми атаками.

В этой статье анализируются алгоритмы машинного обучения, используемые для обнаружения сетевых атак. Традиционные методы становятся недостаточными для противодействия этим угрозам, поэтому технологии машинного обучения рассматриваются как эффективная альтернатива. В статье исследуются методы контролируемого обучения, неконтролируемого обучения и частично контролируемого обучения. Среди методов контролируемого обучения рассматриваются логистическая регрессия, деревья решений, случайные леса, вспомогательные векторные машины и нейронные сети. Обсуждаются кластеризация K-Means, автоэнкодеры и методы анализа ключевых компонентов как методы неконтролируемого обучения.

В качестве частично контролируемых методов обучения изучаются методы распространения признаков и самообучения. Сравниваются преимущества и недостатки каждого алгоритма и анализируется их эффективность в обнаружении сетевых атак.

Ключевые слова: машинное обучение, сетевая атака, алгоритм, DDoS, логистическая регрессия, модель Random Forest.

N.M. Zhunissov[1], A.B. Aben[1], D. Isakov[1]

[1]Akhmet Yassawi International Kazakh-Turkish University, Turkistan, Kazakhstan

DETECTING NETWORK ATTACKS BY COMPARING MACHINE LEARNING ALGORITHMS

Abstract. The development of modern information systems has increased the complexity of network attacks and increased the relevance of security issues. This article compares the effectiveness of machine learning (ML) algorithms in detecting network attacks. Various ML methods, including neural networks, decision trees, deep learning, and adversarial machine learning, are accepted as the object of research on the accuracy and speed of detecting network attacks.

The results of the study highlight the importance of adaptive and innovative machine learning solutions for network security. In addition, directions and recommendations for future research will be given, which will increase the potential and effectiveness of machine learning algorithms in combating network attacks.

This article analyzes the machine learning algorithms used to detect network attacks. Traditional methods are becoming insufficient to counter these threats, so machine learning technologies are considered an effective alternative. The article examines the methods of supervised learning, unsupervised learning and partially supervised learning. Among the methods of supervised learning, logistic regression, decision trees, random forests, auxiliary vector machines and neural networks are considered. K-Means clustering, autoencoders, and key component analysis methods as unsupervised learning methods are discussed.

Methods of feature propagation and self-learning are being studied as partially controlled learning methods. The advantages and disadvantages of each algorithm are compared and their effectiveness in detecting network attacks is analyzed.

Keywords: machine learning, network attack, algorithm, DDoS, logistic regression, Random Forest model.