

**ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ**

**«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ**

**Студенттер мен жас ғалымдардың  
«GYLYM JÁNE BILIM - 2023»  
XVIII Халықаралық ғылыми конференциясының  
БАЯНДАМАЛАР ЖИНАҒЫ**

**СБОРНИК МАТЕРИАЛОВ  
XVIII Международной научной конференции  
студентов и молодых ученых  
«GYLYM JÁNE BILIM - 2023»**

**PROCEEDINGS  
of the XVIII International Scientific Conference  
for students and young scholars  
«GYLYM JÁNE BILIM - 2023»**

**2023  
Астана**

**УДК 001+37**  
**ББК 72+74**  
**G99**

**«GYLYM JÁNE BILIM – 2023» студенттер мен жас ғалымдардың XVIII Халықаралық ғылыми конференциясы = XVIII Международная научная конференция студентов и молодых ученых «GYLYM JÁNE BILIM – 2023» = The XVIII International Scientific Conference for students and young scholars «GYLYM JÁNE BILIM – 2023». – Астана: – 6865 б. - қазақша, орысша, ағылшынша.**

**ISBN 978-601-337-871-8**

Жинаққа студенттердің, магистранттардың, докторанттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

**УДК 001+37**  
**ББК 72+74**

**ISBN 978-601-337-871-8**

**©Л.Н. Гумилев атындағы Еуразия  
ұлттық университеті, 2023**

7. Gazaliyev, A. M., Portnov, V. S., Kamarov, R. K., Maussymbayeva, A. D., & Yurov, V. M. (2015). Geophysical research of areas with increased gas content of coal seams. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu*, (6), 24-29.

8. Portnov, V., Kamarov, R., Mausymbaeva, A., & Yurov, V. (2014). Link of specific electric resistance with qualitative and strength characteristics of ores. *Progressive technologies of coal, coalbed methane, and ores mining* (pp. 65-70).

9. Shakhatova, A., Shishlenin, M., Mirgalikyzy, T., & Portnov, V. (2021). Application of GPR research for the diagnosis of decompaction zones of coal massif of shubarkol field. Paper presented at the SIST 2021 - 2021 IEEE International Conference on Smart Information Systems and Technologies, doi:10.1109/SIST50301.2021.9465955

ӘОК 004.83

## БАҒДАРЛАМАЛЫҚ ЖАСАҚТАМАМЕН АНЫҚТАЛҒАН ЖЕЛІГЕ ҚАУІП-ҚАТЕРДІ АНЫҚТАУ АЛГОРИТМДЕРІН ҚОЛДАНУ ӘДІСТЕРІНЕ ШОЛУ

Шырын Бексұлтан Андасұлы

[bexultan.shyryn@gmail.com](mailto:bexultan.shyryn@gmail.com)

Ақпараттық технологиялар факультетінің 3 курс докторанты

«Л.Н. Гумилев атындағы Еуразия ұлттық университеті» КеАҚ, Астана, Қазақстан

Ғылыми жетекшісі – техника ғылымдарының кандидаты А.К. Жумадилаева

**Аңдатпа.** Телекоммуникациялық желі абоненттерінің көбеюі дәстүрлі желілерді қиындатты, бірақ бағдарламалық жасақтамамен анықталған желілер (SDN) шешім ұсынады. SDN икемді желі конфигурациясын, орталықтандырылған басқаруды және виртуализацияны қамтамасыз етеді. Олар орталықтандырылған басқаруды қолдайтын деректер орталығының желілері үшін өте қолайлы. Бұл құжат SDN архитектурасын сипаттайды, дәстүрлі желілермен салыстырады және қауіпсіздік мәселелерін талқылайды. Мақалада SDN-де машиналық оқытуды (ML) қолдану талданады және SDN жұмысын оңтайландыруға арналған практикалық қосымшалар келтірілген.

**Түйінді сөздер:** программаланған анықталған желілер, SDN, машиналық оқыту, ML.

**Кіріспе.** Байланыс желілерін оңтайландыру үшін машиналық оқытуды (ML) пайдалану идеясы көптеген жылдар бойы болды, бірақ бұған дәстүрлі желілердің орталықтандырылмаған құрылымы кедергі болды. Бағдарламалық жасақтамамен анықталған желілердің (SDN) пайда болуымен және машиналық оқыту технологияларының дамуымен ML негізіндегі шешімдер өте мүмкін болды. SDN желінің күйін орталықтан бақылауға және бақылауға мүмкіндік береді, бұл ML тапсырмалары үшін қажетті деректерді жинауды жеңілдетеді. ML алгоритмдерін қауіпсіздікті қамтамасыз ету, желінің кептелуін болжау және т.б. үшін пайдалануға болады. SDN бағдарламалануы нақты уақыт режимінде оңтайлы ML шешімдерін қолдануға мүмкіндік береді.

Бұл мақалада SDN орнату және пайдалану мәселелерін шешу үшін машиналық оқыту алгоритмдерін пайдалану мүмкіндігі қарастырылады. Ол проблемалардың әртүрлі түрлерін және оларды шешу үшін пайдалануға болатын әртүрлі ML алгоритмдерін қарастырады. Сондай-ақ, мақалада SDN-ге арналған ml құралдарының қолданыстағы қосымшалары қарастырылады және болашақ зерттеулердің нәтижелері мен ықтимал бағыттары ұсынылады.

**Негізгі бөлім.** ML алгоритмдері арқылы шешілетін бағдарламалық жасақтама желілерінің міндеттері. Бұл бөлімде SDN пайдалану және конфигурациялау процесінде пайда болатын және ML көмегімен шешілуі мүмкін бар тапсырмалар тобы толығырақ қарастырылады. Жалпы, оларды келесі бес топқа бөлуге болады:

1. *Трафикті жіктеу* - трафиктің әртүрлі түрлерін анықтау арқылы желіні егжей-тегжейлі басқаруды қамтамасыз ететін функция. Трафикті жіктеу желілік операторларға қызметтерді ұсынуға және желілік ресурстарды тиімдірек бөлуге мүмкіндік береді. Трафикті жіктеу үшін терең пакеттік инспекция (DPI) және машиналық оқыту кеңінен қолданылады [3].

2. *Маршруттауды оңтайландыру* - SDN-де контроллер маршрутизатордың ағындық кестесін өзгерту, трафик ағындарын әр түрлі маршруттарға тастау немесе қайта бағыттау арқылы

трафик ағындарының бағытын басқара алады. Маршруттауды тиімді басқару өте маңызды, әйтпесе желілік арна шамадан тыс жүктеліп, деректер кідірістері артуы мүмкін. Сондықтан SDN-де трафикті бағыттауды оңтайландыру басым міндеттердің бірі болып табылады. Пакеттерді бағыттау үшін әдетте қысқа жол алгоритмдері мен эвристикалық Алгоритмдер қолданылады. SPF алгоритмі қарапайым көрсеткіштерді қолданады, бірақ желілік ресурстарды тиімді пайдаланбайды.

3. *QoS/QoE болжау* - жоғалту коэффициенті, кідіріс, діріл және өткізу қабілеттілігі сияқты QoS параметрлері желі өнімділігін бағалау үшін желілік операторлар жиі қолданатын желілік көрсеткіштер болып табылады. Мультимедиялық технологияларды тарату және енгізу процесінде соңғы пайдаланушының қанағаттануы желілік қызмет провайдерлері үшін өте маңызды болды. QoE клиенттердің көрсетілетін қызметтерге қаншалықты қанағаттанатынын бағалауға көмектеседі; QoS/QoE болжамдарына сүйене отырып, провайдерлер клиенттердің кетуіне жол бермеу немесе олардың санын көбейту үшін белгілі бір қадамдар жасай алады. QoS және KPI параметрлері Пакеттің өлшемі, деректер жылдамдығы және кезек ұзындығы сияқты желі өнімділігінде тығыз байланысқа ие. Бұл қатынасты регрессиялық талдау арқылы QoS басқаруды болжау және жақсарту үшін пайдалануға болады, өйткені QoS параметрлері үздіксіз деректер болып табылады. Сол сияқты, бақыланатын оқытуды QoE болжау үшін қолдануға болады, өйткені QoE мәндері субъективті және дискретті деректер болып табылады және QoS параметрлеріне тәуелді.

4. *Ресурстарды басқару* - желілік ресурстарды тиімді басқару желінің өнімділігін арттыру үшін өте маңызды және SDN бұл процесті жеңілдетеді. Ресурстарды басқаруға қатысты әртүрлі тапсырмалар деректер жазықтығы үшін де, басқару жазықтығы үшін де бар, соның ішінде ресурстарды бөлу, қосылымдарды бақылау және контроллерлерді орналастыру. Әрбір тапсырма үшін көптеген шешімдер бар болса да, олардың ең жақсысы әлі де анықтау процесінде. ML әдістері келесі бөлімде қарастырылған оңтайлы шешімдерді табуға көмектеседі.

5. *Қауіпсіздік* - желілік қызмет провайдерлері үшін өте маңызды, ал кіруді анықтау желілік қауіпсіздіктің маңызды құрамдас бөлігі болып табылады. Интрузияны анықтау жүйесі (IDS) - бұл желілік жүйедегі оқиғаларды бақылайтын және зиянды болдырмау және азайту үшін ықтимал шабуылдарды анықтайтын құрылғы немесе Бағдарламалық құрал[6]. IDS талдау әдістері бойынша екі түрге бөлуге болады: қолтаңбаға негізделген IDS және ауытқуларға негізделген IDS.

6. *SDN IoT-те* - денсаулық сақтау, көлік және энергетикалық жүйелер сияқты интеллектуалды жүйелердің дамуын қолдау үшін қолданылады. Бұл жүйелер Машиналық оқыту арқылы талданатын деректердің үлкен көлемін жасайды. Дегенмен, бұл деректерді орталықтандырылған SDN контроллерімен тасымалдау желінің айтарлықтай өткізу қабілеттілігін қажет етеді. Бұл мәселені шешу үшін деректерді алдын ала өңдеу және жүйенің жауап беру уақытын жақсарту үшін шекаралық есептеу шешімдері қолданылады. Содан кейін оқытылған модельдер IoT қызметтерінің жауап беру уақытын жақсарту үшін шекаралық серверлерге орналастырылады. Машиналық оқыту және SDN гибриді әдістері маршруттарды оңтайландыру, деректерді талдау, оқиғаларды анықтау, хост кластері, локализация, IoT қолданбалары үшін кірулер мен ақауларды анықтау сияқты әртүрлі тапсырмаларды шешу үшін қолданылады.

Енді біз SDN пайдалану және орнату шеңберінде шешілуі керек және ML көмегімен шешуге болатын негізгі тапсырмаларды қарастырдық, біз бірнеше нақты мысалдарды қарастыруымыз керек.

*Машиналық оқыту әдістерін қолданатын қолданыстағы шешімдерді ұсынатын әдебиеттерге шолу.* Трафикті жіктеу үшін [1] ұсынылған шешу әдістері қолданылады. Бұл мақалада SVM (Support Vector Machine Method) сияқты Машиналық оқыту әдістері, жіктеу және регрессиялық талдау тапсырмалары үшін қолданылатын ұқсас бақыланатын оқыту алгоритмдерінің жиынтығы және бақыланбайтын оқытуға арналған кластерлеу әдісі K-means әдісі қарастырылады. әдістері. Ол трафикті тікелей пакет тақырыбынан алынған мәліметтерге негізделген қолданбалы сыныптарға бөлу үшін пайдаланылуы мүмкін (сегмент өлшемі, пакет кірістері арасындағы уақыт). Нәтижелер анықтамалық векторлық машина барлық трафик кластары үшін 98% дейін жіктеу дәлдігін қамтамасыз ететінін көрсетеді.

Мақалада [2] әр түрлі мобильді қосымшаларға тиесілі трафик терең нейрондық желі арқылы анықталды, ал 8 қабатты модельге арналған нұсқаулық ретінде трафик ағынының бес параметрі таңдалды, мысалы, тағайындалған мекен-жай, порт, хаттама түрі, пакет мөлшері және өмір сүру уақыты. Модельдеу нәтижелері 200 мобильді қосымшаны анықтауға арналған дайындалған модель 93,5% дәлдікке жеткенін көрсетті.

Маршруттауды оңтайландыру үшін [3] мақалада сипатталған әдістерді қолдануға болады. Бұл мақалада DDPG (Deep Deterministic Policy Gradient) тереңдетіп оқытудың жаңа техникасын қолдана отырып, машиналық оқытуға негізделген жолды іздеуді оңтайландыру схемасы ұсынылған. Бұл құрылым желіні нақты уақыт режимінде басқаруға мүмкіндік береді және қолданыстағы оңтайландыру шешімдерімен салыстырғанда желінің өнімділігін арттырады. [4] мақала авторлары neuroute деп аталатын динамикалық маршруттау құрылымын ұсынады. NeuRoute желінің болашақ трафигін бағалау үшін қайталанатын LTE нейрондық желісінің архитектурасын (ұзақ мерзімді қысқа мерзімді жады) пайдаланады. Нейрондық желінің кірісі желінің күйі мен күтілетін желілік трафик туралы, сондай-ақ қолайлы маршруттау шешімдері туралы ақпарат береді, мұның бәрі нейрондық желіні оқыту үшін қолданылады. Оқытудан кейін нақты уақыт режимінде эвристикалық нәтижелерге қол жеткізу үшін оқытылған модельді қолдануға болады.

[5] машиналық оқыту әдістері, атап айтқанда қысқа мерзімді жады бар нейрондық желілер, перспективалы байланыс желілерінің трафигінің кешігуі мен көлемін болжау үшін қолданылады. Авторлар IoT қосымшаларына назар аударғанымен, дәл осындай әдістерді басқа перспективалы байланыс қосымшаларына да қолдануға болады.

[6] мақалада машиналық оқыту әдістері QoS көрсеткіштеріне негізделген QoE негізгі факторларын бағалау және болжау үшін қолданылады. Авторлар QoE айнымалыларынан маңызды заңдылықтарды тапты және Байес желісінің моделін құру арқылы болжаудың жоғары дәлдігін қамтамасыз етті. Сондай-ақ, барлық қарастырылған QoE детерминанттары үшін жасырын айнымалылар бойынша аралық болжамдар арқылы тәсілдің тиімділігін арттыруға болатындығы көрсетілген.

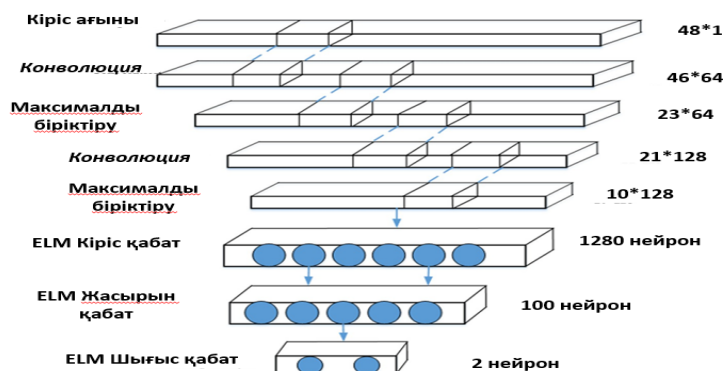
[7] мақала авторлары бейне сапасын бағалау параметрлеріне негізделген QoE мәндерін болжау үшін машиналық оқытудың төрт алгоритмін (Decision Tree, нейрондық желі, k-nearest neighbor және Random Forest әдісі) пайдаланады (құрылымдық ұқсастық индексі (SSIM) және бейне сапасының индексі (VQM)). Бұл алгоритмдердің тиімділігін бағалау үшін Пирсонның корреляция коэффициенті және RMS қолданылады.

[8] автор DDoS SDN-ді нашар анықтау мәселесін қарастырады және желілік трафиктің сипаттамаларын алу үшін CNN қолданатын және жіктеу үшін ELM алгоритмдерін қолданатын CNN-ELM терең оқытудың гибриді моделін ұсынады. Бұл анықтау дәлдігін жақсартып қана қоймайды, сонымен қатар анықтау тиімділігін жақсартады. Аномальды трафикпен күресу үшін бұл техникалық құжат аномальды трафиктің IP көзін бақылау, шабуыл көзін дәл анықтау және құрбандардан барынша пайда алу үшін жаһандық, орталықтандырылған SDN бақылау мен басқарудың артықшылықтарын пайдаланады. DDoS шабуылдарын бейтараптандыру. іргелі. SDN қауіпсіздік жүйесінің тиімділігін тексеру үшін біз Mininet платформасында Имитациялық эксперимент жүргіздік. Эксперимент нәтижелері ұсынылған сурет 1 көрсетілген CNN-ELM моделі жақсы анықтау тиімділігіне ие екенін және гипотезаны тексеру кезінде алынған дәлдік CICIDS-2017 деректер жиынтығы үшін 98,92% және InSDN деректер жиынтығы үшін 99,91% екенін көрсетеді. Екінші жағынан, ұсынылған SDN негізіндегі IP бақылау әдісі шабуылдардың көзін тиімді қадағалап, DDoS шабуылдарының әсерін азайта алады.

Жүктемені теңестіру алгоритмдері мақалада сипатталған [9] желілік ресурстарды тиімді пайдалануды қамтамасыз ету мақсатында бағдарламалық жүктемелердің таралуын бақылау және үйлестіру. Авторлар MRBS (Multiple Regression Based Searching) алгоритмін ұсынды. Алгоритм сұраныстарды трафиктің көлемі мен сипаттамалары (белсенділіктің жоғарылауы және әртүрлі хабарлама жиілігі) сияқты әртүрлі жүктеме көрсеткіштеріне негізделген қосылымдары аз және трафик ағыны аз серверлерге қайта бағыттау қажеттілігін бағалайды және оларды ең аз шығынды

маршрут бойынша бағыттайды. Бұл алгоритм өткізу қабілеттілігін жақсартады, кідірісті азайтады және кластердегі серверлер арасында жүктемені бөледі.

Дегенмен, осы мақалада ұсынылған аномальды бизнесті анықтау жүйесі бақыланатын сауаттылық жүйесіне негізделген, оның кемшілігі бар, қажетті деректерді таңбалау құны шынымен жоғары.



Сурет 1 – CNN-ELM терең оқытудың гибриді модельдері.

Дегенмен, осы мақалада ұсынылған аномальды бизнесті анықтау жүйесі бақыланатын сауаттылық жүйесіне негізделген, оның кемшілігі бар, қажетті деректерді таңбалау құны шынымен жоғары.

[10] openflow контроллеріндегі қызметтік хабарламалар ағынының қарқындылығын болжауды ұсынады. Болжау үшін кәдімгі нейрондық желі қолданылады. Нәтижелер көп контроллерлі SDN-дегі ағындарды интеллектуалды басқаруға, сондай-ақ контроллерлерге жүктемені болжауға мүмкіндік береді.

[11] мақалада орталық процессордың (процессордың) ресурстарды тұтынуы мен басқару хабарламаларының пайда болу жиілігі арасындағы сәйкестікті табуға арналған үш түрлі регрессиялық модель сипатталған. Модельдерді оқыту үшін желілік гипервизордың орталық процессорының жүктелуі және басқару хабарламаларының пайда болу жиілігі туралы жиналған мәліметтер қолданылады. Сонымен қатар, модельді басқарушы хабарламалардың өлшенген жиілігіне байланысты желілік гипервизордың шамадан тыс жүктелу дәрежесін бағалау үшін нақты уақыт режимінде пайдалануға болады. Бұл өте маңызды, өйткені желілік гипервизордың шамадан тыс жүктелуі әр клиент үшін басқару хабарламаларын өңдеуге айтарлықтай әсер етеді.

[12] машиналық оқыту алгоритмдерін (MLP, SVM, Decision Tree және Random Forest) DDoS шабуылдарының үш санатын (өткізу қабілеттілігі шабуылдары, контроллерге шабуылдар және ағындар кестесіне шабуылдар) анықтау үшін ұсынды. Эксперимент нәтижелері Decision Tree ең аз өңдеу уақытына ие екенін және жалпы алғанда ең жақсы алгоритм ретінде танылғанын және Random Forest ең жоғары дәлдікке ие екенін көрсетті. Аномалияларды жіктеу үшін ең маңызды сипаттама порттың шығу тегі, содан кейін қосылыстың өмір сүру уақыты болып табылады. Алынған нәтижелер DDoS шабуылдарының әсерін бейтараптандыратын жүйелерді құру үшін пайдаланылуы мүмкін.

Кеңінен қолданылатын тағы бір классификатор-SVM (қолдау векторы машинасы - тірек векторы машинасының әдісі). Бұл әдіс сонымен қатар өте жоғары дәлдікті және жалған позитивтердің төмен санын көрсетеді. Жұмыста [13] SVM классификаторы талданады және оның тиімділігі басқа классификаторлармен салыстырылады (RBF, Naive Bayes, J48, Random Forest). Эксперимент нәтижелері SVM ең жоғары дәлдікке және жалған позитивтердің ең төмен санына ие екенін көрсетеді.

SDN шабуылдарын анықтау үшін терең нейрондық желілерді де пайдалануға болады. [14] авторлар Gru-RNN (Gated Recurrent Unit recurrent Neural Network) пайдаланады. Ұсынылған тәсіл NSL-KDD деректер жиынтығының көмегімен тексерілді. Эксперименттердің нәтижелері

анықтаудың жоғары дәлдігін көрсетті-89%. Авторлар ұсынылған GRU-RNN тиімді жұмыс істейді және желі өнімділігін нашарлатпайды деген қорытындыға келді.

**Қорытынды.** Бұл мақалада SDN-ге қатысты мәселелерді шешу үшін машиналық оқыту алгоритмдерін қолдану жолдары қарастырылды. Қарастырылған жұмыстарда машиналық оқытудың әртүрлі алгоритмдері қолданылады, мысалы, тірек векторлық машина әдісі, k-nearest көршісі әдісі, кездейсоқ Орман және басқалары, ал кейбір мақалалар олардың негізінде өздерінің алгоритмдерін ұсынады. Алайда, осы алуан түрлі шешімдерде SDN құру кезінде болашақта қолдануға болатын ең жақсысын табу керек. Терең оқыту әдістерін егжей-тегжейлі қарастырған жөн, өйткені олар болжамдардың жоғары дәлдігін қамтамасыз ете алады және желі процесінде жиналатын деректердің үлкен көлемін тиімдірек пайдалана алады.

## LIST OF REFERENCES

- [1] A. Orłowski, R. Kozik, M. Karwatowski, "Traffic classification using machine learning methods", *Journal of Telecommunications and Information Technology*, 2017.
- [2] Li, J., Li, Y., Zhang, H., Yu, F.R., & Leung, V.C.M. (2018). Traffic classification of mobile applications using deep neural network. *Journal of Network and Computer Applications*, 103, 40-47.
- [3] D. Liu, Y. Cheng, Y. Huang, J. Zhang, X. Xue, "A Pathfinding Optimization Scheme Based on Machine Learning for Network Routing", *IEEE Access*, vol. 6, pp. 41494-41504, 2018.
- [4] A. Khosravi, M. Saberi, H. Hajimirsadeghi, M. Rasti, "NeuRoute: A Deep Learning Framework for Dynamic Routing in Communication Networks", *IEEE Transactions on Neural Networks and Learning Systems*, vol. 30, no. 10, pp. 3155-3166, Oct. 2019.
- [5] R. Abbas, M. Atiquzzaman, "Machine learning techniques for predicting latency and traffic volume in promising communication networks", *International Journal of Communication Systems*, vol. 31, no. 2, 2018.
- [6] P. Zwickl, D. K. Sharma, K. H. Johansson, "QoE estimation for multimedia services: A machine learning approach", *Computer Networks*, vol. 135, pp. 42-58, 2018.
- [7] C. Wang, Y. Zhang, X. Zhou, S. Xiang, "Video QoE prediction based on machine learning algorithms", *IEEE Transactions on Consumer Electronics*, vol. 64, no. 4, pp. 463-470, Nov. 2018.
- [8] X. Li, Y. Li, H. Li, S. Liu, "A CNN-ELM hybrid deep learning model for poor SDN DDoS detection", *IEEE Access*, vol. 7, pp. 73368-73379, 2019.
- [9] Y. Liu, L. Chen, W. Li, C. Chen, "Load balancing algorithms for distributed software systems: A survey", *Journal of Systems and Software*, vol. 120, pp. 76-90, Oct. 2016.
- [10] K. Zimny, "Predicting the Intensity of Service Message Flow on OpenFlow Controller with Neural Network", in *Proceedings of the International Conference on Computer Networks (CN 2017)*, pp. 127-136, June 2017.
- [11] M. Bekisz, K. Szwarc and M. Bukowiec, "Regression Models for Estimating CPU Usage of Network Hypervisor," in *IEEE Access*, vol. 8, pp. 169087-169101, 2020, doi: 10.1109/ACCESS.2020.3025282.
- [12] Wang, L., Su, S., Zhang, Y., Sun, L., & Xu, T. (2019). A Detection Method of SDN-Based DDoS Attacks Using Multiple Machine Learning Algorithms. *Symmetry*, 11(2), 245. doi: 10.3390/sym1102024
- [13] B. Liu, J. Zhu, and Y. Zhang, "A comparison of SVM, RBF, Naive Bayes, J48, and Random Forest with applications to spam filtering," in *Proceedings of the 2004 International Conference on Machine Learning and Cybernetics, Shanghai, China, August 2004*, vol. 1, pp. 525-530.
- [14] M. A. Alsheikh, W. Liu, M. N. Al-Kahtani, and X. Hu, "Intrusion detection in software-defined networking using deep learning approach," in *2017 IEEE Symposium on Computers and Communication (ISCC)*, Heraklion, Greece, 2017, pp. 412-417, doi: 10.1109/ISCC.2017.8024591.