ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

«ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫ» РҚБ

ҚАЙЫРЫМДЫЛЫҚ ҚОРЫ HALYK CHARITY FOUNDATION

«ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫ» РҚБ
«ХАЛЫҚ» ЖҚ

ХАБАРЛАРЫ

ИЗВЕСТИЯ

РОО «НАЦИОНАЛЬНОЙ
АКАДЕМИИ НАУК РЕСПУБЛИКИ
КАЗАХСТАН»
ЧФ «Халық»

NEWS

OF THE ACADEMY OF SCIENCES
OF THE REPUBLIC OF
KAZAKHSTAN
«Halyk» Private Foundation

SERIES
PHYSICS AND INFORMATION TECHNOLOGY

1 (349)

JANUARY – MARCH 2024

PUBLISHED SINCE JANUARY 1963
PUBLISHED 4 TIMES A YEAR

ALMATY, NAS RK

ЧФ «ХАЛЫҚ»

В 2016 году для развития и улучшения качества жизни казахстанцев был создан частный Благотворительный фонд «Халык». За годы своей деятельности на реализацию благотворительных проектов в областях образования и науки, социальной защиты, культуры, здравоохранения и спорта, Фонд выделил более 45 миллиардов тенге.

Особое внимание Благотворительный фонд «Халык» уделяет образовательным программам, считая это направление одним из ключевых в своей деятельности. Оказывая поддержку отечественному образованию, Фонд вносит свой посильный вклад в развитие качественного образования в Казахстане. Тем самым способствуя росту числа людей, способных менять жизнь в стране к лучшему – профессионалов в различных сферах, потенциальных лидеров и «великих умов». Одной из значимых инициатив фонда «Халык» в образовательной сфере стал проект Ozgeris powered by Halyk Fund – первый в стране бизнес-инкубатор для учащихся 9-11 классов, который помогает развивать необходимые в современном мире предпринимательские навыки. Так, на содействие малому бизнесу школьников было выделено более 200 грантов. Для поддержки талантливых и мотивированных детей Фонд неоднократно выделял гранты на обучение в Международной школе «Мирас» и в Astana IT University, а также помог казахстанским школьникам принять участие в престижном конкурсе «USTEM Robotics» в США. Авторские работы в рамках проекта «Тәлімгер», которому Фонд оказал поддержку, легли в основу учебной программы, учебников и учебно-методических книг по предмету «Основы предпринимательства и бизнеса», преподаваемого в 10-11 классах казахстанских школ и колледжей.

Помимо помощи школьникам, учащимся колледжей и студентам Фонд считает важным внести свой вклад в повышение квалификации педагогов, совершенствование их знаний и навыков, поскольку именно они являются проводниками знаний будущих поколений казахстанцев. При поддержке Фонда «Халык» в южной столице был организован ежегодный городской конкурс педагогов «Almaty Digital Ustaz.

Важной инициативой стал реализуемый проект по обучению основам финансовой грамотности преподавателей из восьми областей Казахстана, что должно оказать существенное влияние на воспитание финансовой грамотности и предпринимательского мышления у нового поколения граждан страны.

Необходимую помощь Фонд «Халык» оказывает и тем, кто особенно остро в ней нуждается. В рамках социальной защиты населения активно проводится работа по поддержке детей, оставшихся без родителей, детей и взрослых из социально уязвимых слоев населения, людей с ограниченными возможностями, а также обеспечению нуждающихся социальным жильем, строительству социально важных объектов, таких как детские сады, детские площадки и физкультурно-оздоровительные комплексы.

В копилку добрых дел Фонда «Халык» можно добавить оказание помощи детскому спорту, куда относится поддержка в развитии детского футбола и карате в нашей стране. Жизненно важную помощь Благотворительный фонд «Халык» оказал нашим соотечественникам во время недавней пандемии COVID-19. Тогда, в разгар тяжелой борьбы с коронавирусной инфекцией Фонд выделил свыше 11 миллиардов тенге на приобретение необходимого медицинского оборудования и дорогостоящих медицинских препаратов, автомобилей скорой медицинской помощи и средств защиты, адресную материальную помощь социально уязвимым слоям населения и денежные выплаты медицинским работникам.

В 2023 году наряду с другими проектами, нацеленными на повышение благосостояния казахстанских граждан Фонд решил уделить особое внимание науке, поскольку она является частью общественной культуры, а уровень ее развития определяет уровень развития государства.

Поддержка Фондом выпуска журналов Национальной Академии наук Республики Казахстан, которые входят в международные фонды Scopus и Wos и в которых публикуются статьи отечественных ученых, докторантов и магистрантов, а также научных сотрудников высших учебных заведений и научно-исследовательских институтов нашей страны является не менее значимым вкладом Фонда в развитие казахстанского общества.

С уважением,
Благотворительный Фонд «Халык»!

«ҚР ҰҒА Хабарлары. Физика және информатика сериясы».
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)
Меншіктеуші: «Қазақстан Республикасының Ұлттық ғылым академиясы» РҚБ (Алматы қ.). Қазақстан Республикасының Ақпарат және қоғамдық даму министрлігінің Ақпарат комитетінде 14.02.2018 ж. берілген **No 16906-Ж** мерзімдік басылым тіркеуіне қойылу туралы куәлік.
Тақырыптық бағыты: *физика және ақпараттық коммуникациялық технологиялар сериясы.*
Қазіргі уақытта: *«ақпараттық технологиялар»бағыты бойынша ҚР БҒМ БҒСБК ұсынған журналдар тізіміне енді.*
Мерзімділігі: *жылына 4 рет.*
Тиражы: *300 дана.*
Редакцияның мекен-жайы: *050010, Алматы қ., Шевченко көш., 28, 219 бөл., тел.: 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

«Известия НАН РК. Серия физика и информатики».
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)
Собственник: *Республиканское общественное объединение «Национальная академия наук Республики Казахстан» (г. Алматы).*
Свидетельство о постановке на учет периодического печатного издания в Комитете информации Министерства информации и общественного развития Республики Казахстан **No 16906-Ж** выданное 14.02.2018 г.
Тематическая направленность: *серия физика и информационные коммуникационные технологии.*
В настоящее время: *вошел в список журналов, рекомендованных ККСОН МОН РК по направлению «информационные коммуникационные технологии».*
Периодичность: *4 раз в год.*
Тираж: *300 экземпляров.*
Адрес редакции: *050010, г. Алматы, ул. Шевченко, 28, оф. 219, тел.: 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

News of the National Academy of Sciences of the Republic of Kazakhstan.
Series of physics and informatics.
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)
Owner: RPA «National Academy of Sciences of the Republic of Kazakhstan» (Almaty). The certificate of registration of a periodical printed publication in the Committee of information of the Ministry of Information and Social Development of the Republic of Kazakhstan **No. 16906-Ж,** issued 14.02.2018
Thematic scope: *series physics and information technology.*
Currently: *included in the list of journals recommended by the CCSES MES RK in the direction of «information and communication technologies».*
Periodicity: *4 times a year.*
Circulation: *300 copies.*
Editorial address: *28, Shevchenko str., of. 219, Almaty, 050010, tel. 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

NEWS OF THE NATIONAL ACADEMY OF SCIENCESOF THE REPUBLIC OF KAZAKHSTAN
PHYSICO-MATHEMATICAL SERIES
ISSN 1991-346X
Volume 1. Namber 349 (2024). 121–135
https://doi.org/10.32014/2024.2518-1726.246

UDC 004-93

© T. Zhukabayeva[1,2,3], L. Zholshiyeva [1,4*], A. Adamova[1,3], Yerik Mardenov[1], N. Karabayev[1,3], 2024
[1]International Science Complex "ASTANA", Astana, Kazakhstan;
[2]Eurasian National University named after L.N. Gumilyov, Astana, Kazakhstan;
[3]Astana IT University, Astana, Kazakhstan;
[4]Astana IT College, Astana, Kazakhstan.
E-mail: lazzat.zhol.81@gmail.com

APPLICATION OF MACHINE LEARNING METHODS FOR ATTACK DETECTION IN WIRELESS SENSOR NETWORKS: PERFORMANCE ANALYSIS OF XGBOOST AND SGD

Zhukabayeva Tamara Kokenovna — PhD, assoc. Professor. International Science Complex "ASTANA", Astana IT University, L. Gumilyov Eurasian National University, Astana, Kazakhstan
E-mail: tamara_kokenovna@mail.ru. ORCID: 0000-0001-6345-5211;
Zholshiyeva Lazzat Zulpuharkyzy — International Science Complex "ASTANA", Astana IT College, Astana, Kazakhstan
E-mail: lazzat.zhol.81@gmail.com. ORCID: 0000-0002-2526-8471;
Adamova Aigul — PhD, International Science Complex "ASTANA", Department of Computer Engineering, Astana IT University, Astana IT University, Astana, Kazakhstan
E-mail: aigul.adamova@astanait.edu.kz. ORCID: 0000-0001-7773-9522;
Mardenov Yerik — International Science Complex "ASTANA", Astana, Kazakhstan
E-mail: emardenov@gmail.com. ORCID: 0000-0002-5982-8983
Karabayev Nurdaulet — International Science Complex "ASTANA", Astana IT University, Astana, Kazakhstan

E-mail: 222240@astanait.edu.kz.

Abstract. Wireless sensor networks are exposed to various threats and despite significant progress in security, there are a number of unsolved problems, such as creating algorithms, developing methods to detect and prevent attacks that provide a high degree of security with minimal computational and energy costs. An attack on a network, on a device can cause significant damage to data security and privacy. Machine learning techniques are effective in detecting various attacks. This paper presents an analysis of research on the most effective machine learning techniques used to prevent attacks by classifying and detecting distributed botnets in a stateless sensor network using efficient technology. Literature review was conducted on various scientific databases using PRISMA diagram and through inclusion and exclusion process 54 potential studies from last 5 years were selected. In this paper,

machine learning techniques, particularly Extreme Gradient Boosting (XGBoost) and Stochastic gradient descent (SGD), are reviewed and applied to detect botnet attacks on wireless sensor networks. By comparing these methods, 6 botnets were categorized into classes and the precision, recall and f1-score of their detection were obtained. Based on the comparison between the studied machine learning and attack detection methods, the highest precision, recall and f1-score of their detection was obtained. Based on the comparison between the studied machine learning and attack detection methods, a high score of 99.18% was obtained in XGBoost.

Keywords: Machine Learning, XGBoost, SGD, botnet, attack, wireless sensor network

Financing: *This research has been funded by the Science Committee of the Ministry of Education and Science of the Republic of Kazakhstan (Grant No. No AP19680345).*

Conflict of interest: *The authors declare that there is no conflict of interest.*

© Т. Жукабаева[1,2,3], Л. Жолшиева[1,4*], А. Адамова[1,3], Е. Марденов[1], Н. Карабаев[1,3], 2024

[1]«АСТАНА» халықаралық ғылыми кешені, Астана, Қазақстан;
[2]Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан;
[3]Astana IT University, Астана, Қазақстан;
[4]«Astana IT University» ЖШС колледжі, Астана, Қазақстан.
E-mail: lazzat.zhol.81@gmail.com

СЫМСЫЗ СЕНСОРЛЫҚ ЖЕЛІЛЕРГЕ ШАБУЫЛДАРДЫ АНЫҚТАУ ҮШІН МАШИНАЛЫҚ ОҚЫТУ ӘДІСТЕРІН ҚОЛДАНУ: XGBOOST ЖӘНЕ SGD ТИІМДІЛІГІН ТАЛДАУ

Жукабаева Тамара Кокеновна — PhD, қауымдастырылған профессор. «АСТАНА» халықаралық ғылыми кешені, Л.Н. Гумилев атындағы Евразия ұлттық университеті, Astana IT University, Астана, Қазақстан
E-mail: tamara_kokenovna@mail.ru. ORCID: 0000-0001-6345-5211;
Жолшиева Лаззат Зулпухаркызы — «АСТАНА» халықаралық ғылыми кешені, «Astana IT University» ЖШС колледжі, Астана, Қазақстан
E-mail: lazzat.zhol.81@gmail.com. ORCID: 0000-0002-2526-8471;
Adamova Aigul — PhD, «АСТАНА» халықаралық ғылыми кешені, Astana IT University, Астана, Қазақстан
E-mail: aigul.adamova@astanait.edu.kz. ORCID: 0000-0001-7773-9522;
Марденов Ерик — «АСТАНА» халықаралық ғылыми кешені, Астана, Қазақстан
E-mail: emardenov@gmail.com. ORCID: 0000-0002-5982-8983;
Карабаев Нурдаулет — «АСТАНА» халықаралық ғылыми кешені, Astana IT University, Астана, Қазақстан
E-mail: 222240@astanait.edu.kz.

Аннотация. Сымсыз сенсорлық желілер әртүрлі қауіп-қатерлерге бейім және оның қауіпсіздігін қамтамасыз етудегі елеулі прогреске қарамастан,

минималды есептеу шығындары мен энергия шығындарын есепке ала отырып, қауіпсіздіктің жоғары дәрежесін беретін алгоритмдерді құру және оны әзірлеу сияқты бірқатар шешілмеген мәселелер бар. Желіге немесе құрылғыға жасалған бір шабуылдың өзі деректердің қауіпсіздігі мен құпиялылығына айтарлықтай зиян келтіреді. Кез келген шабуылды анықтау үшін машиналық оқыту әдістерін қолданудың тиімділігі жоғары. Осыған байланысты, мақалада алдымен сымсыз сенсорлық желілерде жалпы ботнеттерді жіктеу және анықтау үшін машиналық оқытудың ең тиімді әдістеріне және тиімді алгоритмдерді пайдалана отырып, шабуылдардың алдын алуды зерттеуге шолу жасалды. Әртүрлі ғылыми дерекқорлар бойынша әдебиеттерге шолу жүргізіліп, PRISMA диаграммасы арқылы ғылыми жұмыстарады жіктеу арқылы соңғы 5 жылдағы ғылыми зерттеулер ішінен 54 ғылыми жұмыстар іріктелініп анықталды. Мақалада сымсыз сенсорлық желілерге ботнет шабуылдарын анықтау үшін машиналық оқыту әдістері, атап айтқанда Extreme Gradient Boosting (XGBoost) және Stochastic Gradient Descent (SGD) талқыланды және қолданылды. Әдістерді салыстыра отырып, ботнеттің 6 түрін классқа бөліп, оларды анықтаудың precision, recall және f1-score көрсеткіштері алынды. Машиналық оқыту мен шабуылды анықтау әдістерін салыстыру нәтижелері бойынша XGBoost 99,18 % жоғары көрсеткішке ие болды.

Түйін сөздер: Machine Learning, XGBoost, SGD, botnet, attack, wireless sensor network

Қаржыландыру: *Бұл зерттеу Қазақстан Республикасы Ғылым және жоғары білім министрлігі, Ғылым комитетімен қаржыландырылған (Грант No AP19680345).*

Мүдделер қақтығысы: *Авторлар осы мақалада мүдделер қақтығысы жоқ деп мәлімдемейді.*

© Т. Жукабаева[1,2,3], Л. Жолшиева[1,4*], А. Адамова[1,3], Е. Марденов[1], Н. Карабаев[1,3], 2024

[1]Международный научный комплекс «АСТАНА», Астана, Казахстан;
[2]Евразийский национальный университет имени Л.Н. Гумилева, Астана, Казахстан;
[3]Astana IT University, Астана, Казахстан;
[4]Колледж ТОО «Astana IT University», Астана, Казахстан.
E-mail: lazzat.zhol.81@gmail.com

ПРИМЕНЕНИЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ОБНАРУЖЕНИЯ АТАК В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ: АНАЛИЗ ЭФФЕКТИВНОСТИ XGBOOST И SGD

Жукабаева Тамара Кокеновна — PhD, ассоц. профессор, Международный научный комплекс «АСТАНА», Евразийский национальный университет имени Л.Н. Гумилева, Astana IT University, Астана, Казахстан

E-mail: tamara_kokenovna@mail.ru. ORCID: 0000-0001-6345-5211;
Жолшиева Лаззат Зулпухаровна — Международный научный комплекс «АСТАНА», Колледж ТОО «Astana IT University», Астана, Казахстан
E-mail: lazzat.zhol.81@gmail.com. ORCID: 0000-0002-2526-8471;
Адамова Айгуль — PhD, Международный научный комплекс «АСТАНА», Департамент компьютерной инженерии, Astana IT University, Астана, Казахстан
E-mail: aigul.adamova@astanait.edu.kz. ORCID: 0000-0001-7773-9522;
Марденов Ерик — Международный научный комплекс «АСТАНА», Астана, Казахстан
E-mail: emardenov@gmail.com. ORCID: 0000-0002-5982-8983;
Карабаев Нурдаулет — Международный научный комплекс «АСТАНА», Astana IT University, Астана, Казахстан
E-mail: 222240@astanait.edu.kz.

Аннотация. Беспроводные сенсорные сети подвергаются различным угрозам и несмотря на значительный прогресс в области обеспечения безопасности, существует ряд нерешённых проблем, таких как создание алгоритмов, разработка методов обнаружения и предотвращения атак, которые обеспечат высокую степень безопасности при минимальных вычислительных и энергетических затратах. Атака на сеть, на устройство может нанести значительный ущерб безопасности и конфиденциальности данных. Методы машинного обучения эффективны для обнаружения различных атак. В работе представлен анализ исследований по наиболее эффективным методам машинного обучения используемых для предотвращения атак путем классификации и обнаружения расспространенных ботнетов в беспородной сенсорной сети с использованием эффективных технологии. Литературный обзор проводился по различным научным базам данных с помощью диаграммы PRISMA и в результате процесса включения и исключения были отобраны 54 потенциальных исследования за последние 5 лет. В статье рассмотрены и применены методы машинного обучения, в частности экстремальный градиентный бустинг (Extreme Gradient Boosting, XGBoost) и стохастический градиентный спуск (Stochastic gradient descent, SGD), для обнаружения ботнет атак на беспроводные сенсорные сети. Путем сравнения этих методов, шесть ботнетов были разделены на классы и получены показатели precision, recall и f1-score их обнаружения. По результатам сравнения между изученными методами машинного обучения и обнаружения атак был получен высокий показатель в XGBoost – 99,18 %.

Ключевые слова: машинное обучение, XGBoost, SGD, ботнет, атака, беспроводная сенсорная сеть

Финансирование: *данное исследование финансировалось Комитетом науки Министерства науки и высшего образования Республики Казахстан (Грант No AP19680345).*

Конфликт интересов: *авторы заявляют об отсутствии конфликта интересов.*

Кіріспе

Интернетке қосылған смарт құрылғылар күнделікті процестерді автоматтандыру және нақты уақытта ақпаратқа қол жеткізуді қамтамасыз ету арқылы өмірімізді жеңілдетеді. Алайда, сымсыз сенсорлық желлердің өсуімен қатар, ботнет шабуылдарының қаупі де пайда болды. Сонымен қатар, ботнеттер спам жіберу, фишингтік шабуылдар жасау, деректерді ұрлау, таратылған қызмет көрсетуден бас тарту (DDoS) шабуылдарына қатысу, веб-сайттар мен онлайн қызметтер жұмысын тоқтату секілді түрлі зиянды әрекеттерді жасайды (Dasari & Kaluri, 2024). Шабуылдармен күресу оңай мәселе емес, бірақ зақымдануды азайту үшін ерте уақытта анықтау өте маңызды. Ботнеттерді анықтау үшін әртүрлі тәсілдер қолданылады, соның ішінде: күдікті әрекетті іздеу үшін желілік трафикті талдау, ауытқуларды анықтау үшін құрылғы әрекетін бақылау және зиянды үлгілерді тану үшін машиналық оқыту мен жасанды интеллектті пайдалану. Ботнеттерді ерте анықтау жеке құрылғыларды сақтап қана қоймайды, сонымен қатар сандық инфрақұрылым мен құпиялылықты қорғай отырып, зиянды бағдарламаның кең ауқымда таралуын болдырмайды. Кең ауқымды шабуылдарға әкелген ең әйгілі ботнеттердің екеуі - Mirai және BASHLITE. Бұл ботнеттер DDoS шабуылдарын іске қосады, ал DDoS шабуылдары кәсіпорындар мен ұйымдарға айтарлықтай әсер етуі мүмкін. Соңғы уақытта IoT құрылғыларының саны бүкіл әлемде күрт өсуде және атап айтсақ, DDoS шабуыл трафигінің көлемі бұрын-соңды болмаған деңгейге жетуде.

Аномалияны анықтау сымсыз сенсорлық желілер (WSN) жүйесіндегі өзекті мәселе болып табылады, өйткені ол деректердегі әдеттен тыс оқиғаларды және қалыптан тыс әрекетті анықтауға көмектеседі. Аномалиялар жүйе датчиктеріндегі ақауды, жабдықтың істен шығуын немесе дереу және тиісті түрде шешілуі қажет ықтимал қауіпсіздік қатерлерін көрсетуі мүмкін. Дегенмен, ережеге негізделген аномалияларды анықтаудың дәстүрлі әдістері WSN үшін жарамсыз болуы мүмкін, өйткені олар жоғары өлшемді деректері бар күрделі WSN жүйелері үшін жобалау қиын болатын алдын ала анықталған ережелерді талап етеді.

Мақалада WSN-ге шабуылды анықтау саласындағы зерттеулер мен оларды классификациялап, анықтайтын машиналық оқыту әдістеріне шолу жасалған. Сымсыз сенсорлық желілерге ботнет шабуылдарын анықтау үшін машиналық оқыту әдістері, XGBoost және SGD зерттеледі.

Зерттеудің мақсаты – WSN-ге шабуылдарды машиналық оқыту алгоритмдері арқылы анықтау.

Зерттеу барысында жасалған жұмыстар:

- Соңғы 5 жылдағы WSN-ге шабуылды зерттейтін ғылыми жұмыстарға PRIZMA әдісі бойынша ғылыми әдебиеттерге шолу жасау;

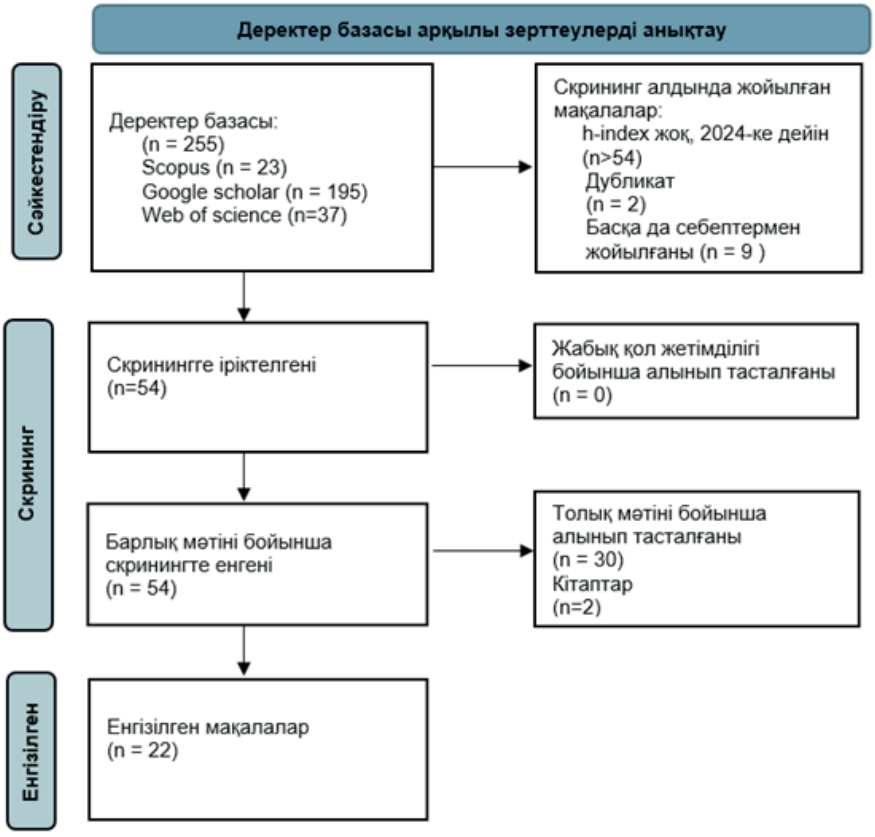
- Машиналық оқыту алгоритмедрі бойынша кең таралған шабуылдарды анықтау;

- Таңдалған алгоритмдерді салыстыру.

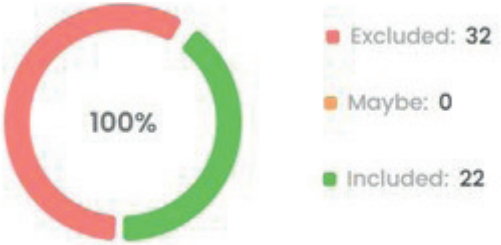
Бірінші бөлімде кіріспе, зерттеудің мақсаты мен зерттеу барысында жасалған жұмыстар жазылған, ал екінші бөлімде зерттеу тақырыбы бойынша әдебиеттерге шолу мен методология жасалған. Зерттеудің жалпы нәтижелері XGBoost және SGD алгоритмдері ретінде үшінші бөлімде келтірілген. Төртінші бөлімде қорытынды жазылған.

Әдебиетке шолу және методология

Бұл бөлімде ғылыми әдебиеттерге шолу PRISMA методологиясы арқылы жасалған. Зерттеудің бастапқы және маңызды сатысында XGBoost, SGD, botnet, attack, wireless sensor network кілттік сөздері анықталды. Аталған кілттік сөздер арқылы сәйкес ғылыми еңбектерді табу үшін Scopus, Google Scholar, Web of Science базалары қарастырылып, қажетті мақалалар PRISMA (Moher, D., 2009) диаграммасы бойынша іріктеп алынды (1-сурет). Олардың ішінен h-индексі жоғары және 2020–2024 жылдар аралығындағы мақалалар таңдалып алынды. Арықарай, Rayan ортасы арқылы таңдалған жұмыстар дубликатқа тексеріліп, толық мәтіні бойынша зерттелді. Нәтижесінде 32 мақалана алынып тасталып, 22 мақала зерттеуге іріктеп алынды (2-сурет).



1-сурет. Әдебиеттерді PRISMA бойынша іріктеу блок-схемасы



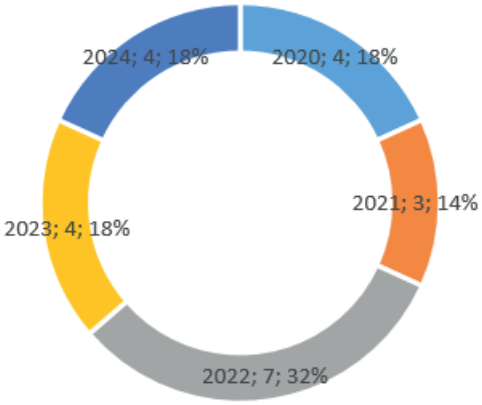
2-сурет. Әдебиеттерді Rayan ортасы арқылы іріктеу

Методология нәтижесінде 54 мақала зерттеліп, PRISMA блок-схемасынан кейін 22 мақала іріктеліп алынды. Ол төмендегі 1-кестеде жинақталған. Әр жылдардан таңдалған мақалалар саны да пайыздық шамамен көрсетілген (3-сурет).

1-кесте. PRISMA методологиясы бойынша зерттеуге іріктелген мақалалар

Мақала авторлары	Жылы	Мақала атауы	Жарияланған орны
Alothman Z., Alkasassbeh M. & Al-Haj Baddar S	2020	An efficient approach to detect IoT botnet attacks using machine learning	Journal of High Speed Networks, 26(3), 241-254.
Waqas M., Kumar K., Laghari A.A., Saeed U., Rind M.M., Shaikh A.A. & Qazi A.Q.	2020	Botnet attack detection in Internet of Things devices over cloud environment via machine learning	Concurrency and Computation: Practice and Experience, 34(4), e6662.
Kim J., Shim M., Hong S., Shin Y. & Choi E.	2020	Intelligent detection of IoT botnets using machine learning and deep learning	Applied Sciences, 10(19), 7009.
Churcher A., Ullah R., Ahmad J., Ur Rehman S., Masood F., Gogate M. & Buchanan W.J.	2022	An experimental analysis of attack classification using machine learning in IoT networks	Sensors, 21(2), 446.
Jeyabharathi, Alphonse A.S., Priya E.D. & Kowsigan M.	2022	Review of Machine Learning Techniques Used for Intrusion and Malware Detection in WSNs and IoT Devices	Design and Development of Efficient Energy Systems, 57–65.
Wazirali R. & Ahmad R.	2022	Machine Learning Approaches to Detect DoS and Their Effect on WSNs Lifetime	Computers, Materials & Continua, 70(3).
Tyagi H. & Kumar R.	2021	Attack and Anomaly Detection in IoT Networks Using Supervised Machine Learning Approaches	Revue d'Intelligence Artificielle, 35(1)
Faysal J.A., Mostafa S.T., Tamanna J.S., Mumenin K.M., Arifin M.M., Awal M.A. & Mostafa S.S.	2022	XGB-RF: A hybrid machine learning approach for IoT intrusion detection	In Telecom (Vol. 3, No. 1, pp. 52–69). MDPI
Saied M., Guirguis S. & Madbouly M.	2023	A comparative analysis of using ensemble trees for botnet detection and classification in IoT.	Scientific Reports, 13(1), 21632

Awotunde J.B., Folorunso S.O., Imoize A.L., Odunuga J.O., Lee C.C., Li C.T. & Do D.T.	2023	An Ensemble Tree-Based Model for Intrusion Detection in Industrial Internet of Things Networks	Applied Sciences, 13(4), 2479
Li P.H., Xu J., Xu Z. Y., Chen S., Niu B. W., Yin J. & Chen L.L.	2022	Automatic Botnet Attack Identification Based on Machine Learning	Computers, Materials & Continua, 73(2)
Dener M., Okur C., Al S. & Orman A.	2023	Wsn-bfsf: A new dataset for attacks detection in wireless sensor networks	IEEE Internet of Things Journal
Saleh H.M., Marouane H. & Fakhfakh A	2024	Stochastic Gradient Descent Intrusions Detection for Wireless Sensor Network Attack Detection System Using Machine Learning	IEEE Access
Azimjonov J. & Kim T.	2024	Stochastic gradient descent classifier-based lightweight intrusion detection systems using the efficient feature subsets of datasets	Expert Systems with Applications, 237, 121493
Baydoğmuş G.K.	2021	The Effects of Normalization and Standardization an Internet of Things Attack Detection	Avrupa Bilim ve Teknoloji Dergisi, (29), 187–192
Aljabri M., Aljameel S.S., Mohammad R. M.A., Almotiri S.H., Mirza S., Anis F.M. & Altamimi, H.S.	2021	Intelligent techniques for detecting network attacks: review and research directions	Sensors, 21(21), 7070
Inayat U., Zia M.F., Mahmood S., Khalid H.M. & Benbouzid M.	2022	Learning-based methods for cyber-attacks detection in IoT systems: A survey on methods, analysis, and future prospects	Electronics, 11(9), 1502
Tahaei H., Afifi F., Asemi A., Zaki F. & Anuar N.B.	2020	The rise of traffic classification in IoT networks: A survey	Journal of Network and Computer Applications, 154, 102538
Shukla A.K. & Dwivedi S	2022	Discovery of Botnet Activities in Internet-of-Things System Using Dynamic Evolutionary Mechanism.	New Generation Computing, 40(1), 255–283
Natarajan R., Ranjith, C.P., Mohideen M. S.K., Gururaj H.L., Flammini F. & Thangarasu N.	2024	Utilizing a machine-learning algorithm to choose a significant traffic identification system	International Journal of Information Management Data Insights, 4(1), 100218
Dasari S. & Kaluri R.	2024	An Effective Classification of DDoS Attacks in a Distributed Network by Adopting Hierarchical Machine Learning and Hyperparameters Optimization Techniques	IEEE Access.
Batchu R.K. & Seetha H.	2023	A hybrid detection system for DDoS attacks based on deep sparse autoencoder and light gradient boost machine	Journal of Information & Knowledge Management, 22(01), 2250071



3-сурет. PRISMA ююйынша іріктелген 22 мақаланың жылға шаққандағы пайыздық үлесі

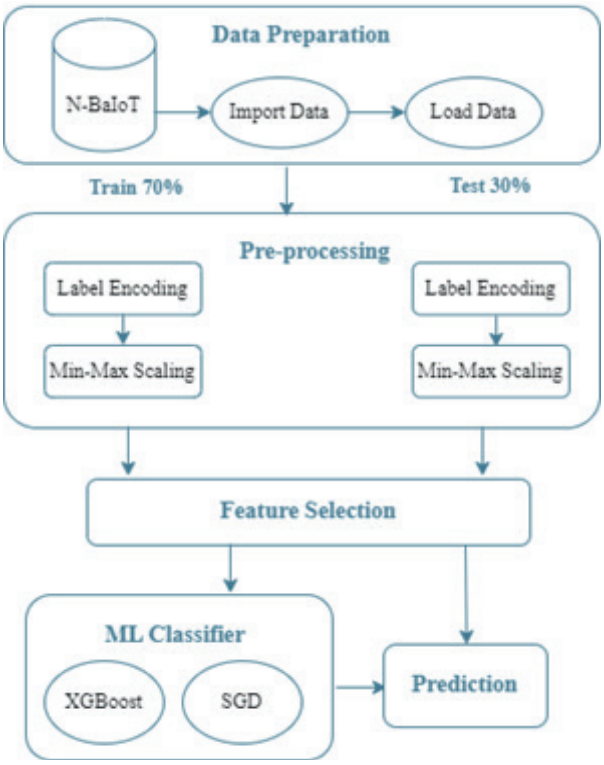
WSN осалдықтарының мәселелері бойынша талдауды Жукабаева Т.К. және басқалар (Жукабаева, 2023) қарастырған, WSN желілеріндегі желілік шабуылдарды анықтаудың белгілі тәсілдерін, әдістерін және механизмдерін жүйелеу үшін әдебиеттерге шолу жасаған. Авторлар Haq, Rahim Khan (Haq, 2022) XGBoost алгоритмі мен конволюциялық нейрондық желі негізінде IoT ботнеттерін анықтауға арналған келесі жұмыс CIC-IDS2017 деректер жинағын пайдаланып 99,4 % дәлдікке қол жеткізді. Saleh H. және басқалар (Saleh, 2024) авторлары IoT шабуылдарын анықтауға арналған SGD моделін зерттеді. WSNS-ге шабуылды анықтау технологиясы үш негізгі бөліктен тұрады: алу, анықтау және жауап беру (Saleh, 2024). Сымсыз сенсорлық желілердегі аномалияларды анықтау процесі желілік жүйелердің қауіпсіздігін және шабуылдардан қорғауды қамтамасыз етеді. Алдымен сенсор деректері жиналады және өңделетін базалық станцияға жіберіледі. Содан кейін деректер кез келген ықтимал енуді анықтау үшін талдау процесінен өтеді, ол үшін машиналық оқыту алгоритмдерін пайдалану тиімді. Кез келген күдікті әрекет немесе шабуыл анықталса, жүйе кіруді блоктау немесе желі әкімшісін ескерту үшін дереу әрекет ете алады.

XGBoost және SGD алгоритмдерін жүзеге асыру

Бұл бөлімде шабуылдарды анықтау кезінде қолданылатын датасет, аномалияларды анықтау, мәліметтерді дайындау, модельдерді таңдау және оқыту, машиналық оқыту алгоритмдерін жүзеге асыру, модельдердің алгоритмі қарастырылған.

IoT ботнет-шабуылдарын анықтауға арналған бұл әдіс келесі негізгі қадамдардан тұрады: деректерді жинау, мүмкіндіктерді шығару, аномалия детекторын оқыту.

Машиналық оқыту моделін әзірлеу процестерді оңтайландыруға, жеке тәжірибелерді ұсынуға, ауқымды деректерді өңдеуге және тиімділікті арттыруға мүмкіндік береді. 4-суретте ұсынылған модельдің толық сипаттамасы көрсетілген.



4-сурет. Ұсынылған модельдер алгоритмі

XGBoost - градиент негізіндегі оңтайландыру алгоритмін және артық бағалаумен күресу үшін реттеу әдісін пайдаланатын GBM нұсқасы. Ал ботнеттерді анықтауда XGBoost желілік трафиктерді классификациялау үшін қолданылады, яғни IoT трафик деректерінен алынған мүмкіндіктерге негізделген желілік трафикті қалыпты немесе зиянды деп жіктеу үшін пайдаланылады.

SGD – барлық деректер жиынына қарағанда оқу деректерінің кездейсоқ жиынындағы үлгі параметрлерін жаңарту үшін пайдаланылатын итеративті оңтайландыру алгоритмі. SGD терең нейрондық желілер сияқты үлкен масштабты машиналық оқыту үлгілерін үйрету үшін кеңінен қолданылады. IoT ботнеттерін анықтау саласында XGBoost-пен қатар, трафик деректерінен алынған мүмкіндіктерді пайдаланып, желілік трафикті қалыпты немесе зиянды деп жіктеу үшін де қолданылады.

Датасет

Датасет машиналық оқыту үлгілерін бағалауда маңызды рөл атқарады. Жақсы таңдалған деректер жинағы үлгінің өнімділігін оқыту, тексеру және сынауға негіз болады. Деректер жиыны модельдің белгісіз деректер негізінде дәл болжау жасау қабілетін, белгісіз деректер негізінде дәл болжам жасау қабілетін бағалауда маңызды рөл атқарады.

IoT құрылғылары үшін жиі қолданылатын деректер жинағы N-BaIoT деректер жинағы болып табылады, ол Mirai және BASHLITE ботнеттері арқылы бұзылған тоғыз коммерциялық IoT құрылғыларынан жиналған нақты трафик деректерін сенімді түрде ұсынады.

IoT құрылғыларындағы осалдықтарды Mirai және BASHLITE ботнеттері DDoS шабуылдарын іске қосу үшін жиі пайдаланады. 116 мүмкіндікті қамтитын деректер жинағы үлкен көлемде ақпарат береді (Merdan, 2018). Зерттеу үшін үшін және ұсынылып модельді мұқият бағалау үшін тоғыз құрылғының бірінші IoT құрылғысынан үлгілер алынып, бірқатар деректер жиынтығы пайдаланылды.

Аномалияны анықтау

Ең алдымен аномалияларды анықтау әдістерін арқылы зиянсыз трафик деректері зиянды трафик деректерінен ажыратылды. Әрбір сынақ жинағында аномалия детекторы ретінде терең автокодер қолданылды. Аномалияны анықтау 100 %-ға қол жеткізді (Merdan, 2018). benign, g-jank, g-combo, g-scan, g-tcp және g-udp ботнеттерін классификациялау үшін (N-BaIoT) деректер жинағы қолданылды. Әрбір сынақ жинағы аномалия детекторы ретінде сәйкес оқытылған терең автокодерді пайдаланады. Аномалияны анықтау 100 % көрсеткішпен аяқталды.

Мәліметтерді дайындау

Модельдерді құруға арналған бақылау деректерін дайындау үшін алдымен жазу кітапшасындағы деректер тексеріліп, модельді оқыту және сынауға арналған деректерді біріктіру үшін барлық қалыпты трафик пен зиянды бағдарлама трафигінің бірдей көлемі таңдалды.

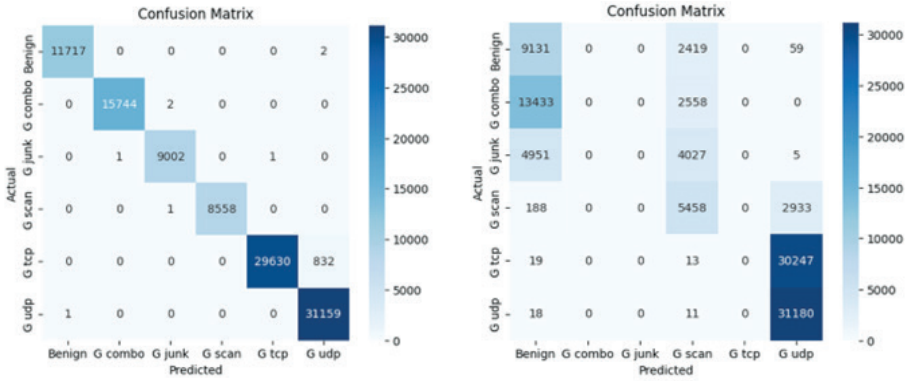
Модельді таңдау

XGBoost және SGD машиналық оқыту модельдері ботнеттерді классификациялау және анықтау үшін пайдаланылды. Үлгілердің өнімділігін салыстыру үшін метрика ретінде «precision» және «recall» таңдалды (2-кесте). Precision - ең маңызды көрсеткіш, recall модельдің жалпы өнімділігін көрсетеді.

2-кесте. XGBoost, SGD моделдерінің precision, recall және f1-score көрсеткіштері

	precision		recall		f1-score		support	
0	1.00	0.33	1.00	0.79	1.00	0.46	11664	11609
1	1.00	0.00	1.00	0.00	1.00	0.00	15819	15991
2	1.00	0.00	1.00	0.00	1.00	0.00	8867	8983
3	1.00	0.38	1.00	0.64	1.00	0.47	8430	8579
4	1.00	0.00	0.97	0.00	0.99	0.00	30596	30279
5	0.97	0.48	1.00	1.00	0.99	0.65	31274	31209
accuracy					0.99	0.43	106650	106650
macro avg	1.00	0.20	1.00	0.40	1.00	0.26	106650	106650
weighted avg	0.99	0.21	0.99	0.43	0.99	0.28	106650	106650
	XGBoost	SGD	XGBoost	SGD	XGBoost	SGD	XGBoost	SGD

Модельді оқыту және тестілеу кезінде тестілеу және валидация құрылғыларының әрбір жиынтығы үшін шатастыру матрицасы (5-сурет) құрылды.



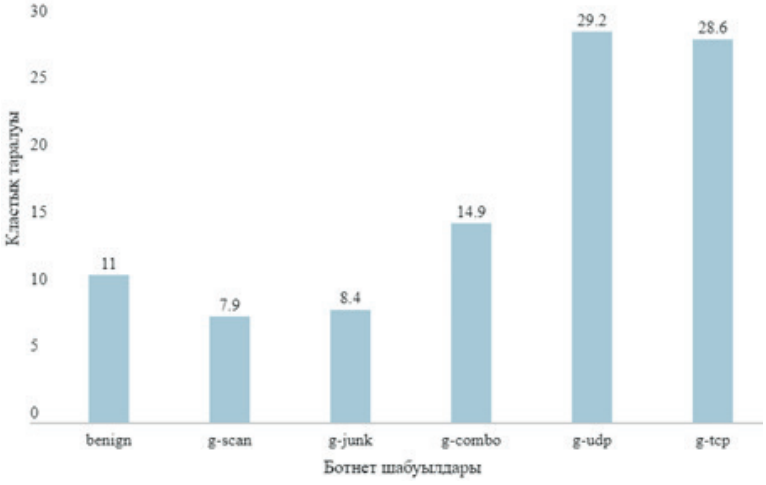
a b

5-сурет. XGBoost (a) және SGD (b) үлгілерінің шатастыру матрицасы

Ботнет шабуылдарының класстық таралуы 3-кесте мен 6-суретте диаграмма арқылы көрсетілді.

3- Кесте. Ботнет шабуылдарының класстық таралуы

Ботнет шабуылдары	*Кластық таралуы, %*
benign	*11*
g-scan	*7.9*
g-junk	*8.4*
g-combo	*14.9*
g-udp	*29.2*
g-tcp	*28.6*



6-сурет. Ботнет шабуылдарының класстық таралу диаграммасы

Үлгілерді қолданудың жалпы алгоритмі

4-кестедегі алгоритмде бақыланатын әрекетті бағалау үшін зерттелген әдістерді пайдаланатын шабуылды анықтау модулі көрсетілген.

4-кесте. XGBoost және SGD-ді қолданып, ұсынылған модуль алгоритмі

Input: Import and load N-BaIoT dataset Output: Detecting attacks
Start Step 1: Split data into x and y Step 2: Split data into training and testing sets with 0.3 70% train, 30% test Step 3: Converting string labels to numerical labels: For 6 class: Converting string labels to numerical string with Label Encoder Step 4: Define the model with 'multi: softmax' 6 classes Step 5: Training the models 1) Training XGBoost model based on training data 2) Training SGD: For max iteration=1000: - Repeat each training data in a shuffled order - Fit model on a training data Step 6: Make predictions on test data 1) Make predictions using XGBoost 2) Make predictions using SGD Step 7: Calculate the accuracy for models Step 8: Create and print the classification reports of models Evaluate the accuracy, precision, recall and F1 score 1) XGBoost 2) SGD End.

Жұмыс нәтижелері

Ұсынылған сымсыз сенсорлық желілерге шабуылды анықтау үшін XGBoost және SGD машиналық оқыту әдістері пайдаланылды. Ең алдымен N-BaIot деректері базасы жүктелді. Деректер базасын оқыту және тестілеуге бөлініп, 70% оқыту және 30% сынақ деректерін қамтыды.

Бағалау

Екі үлгіні салыстыру барысында XGBoost үлгісі жақсы болжау өнімділігіне ие болды, SGD үлгісінің пайыздық көрсеткіші төмен болғандықтан, тиімді үлгі ретінде XGBoost таңдалды. Зерттеу нәтижесінде XGBoost әдісі жоғары 99,18 % дәлдік көрсетті, алайда SGD әдісі 42,92 % төменгі көрсеткішке ие болды.

Қорытынды

Бұл мақалада сымсыз сенсорлық желідегі шабуылдарды жіктеу және анықтау арқылы шабуылдардың алдын алу үшін қолданылатын машиналық оқыту әдістері бойынша зерттеулердің талдауы ұсынылған. PRISMA диаграммасы арқылы әртүрлі ғылыми әдебиеттер бойынша әдебиеттерге

шолу жүргізілді. Зерттеу нәтижесінде сымсыз сенсорлық желілердегі шабуылдарды анықтау үшін XGBoost және SGD қолданылады, 6 ботнет анықталып, дәлдік көрсеткіші бойынша XGBoost алгоритмі тиімді алгоритм болып табылды. Зерттеу нәтижесінің қорытындысы бойынша сымсыз сенсорлық желілерге шабуылды анықтап, табу үшін тиімділікті жоғарылату мақсатында машиналық оқыту әдістерінің басқа да алгоритмдерін қолдану арқылы зерттеуді жалғастыру қажеттігі ұсынылады.

REFERENCES

Aljabri M., Aljameel S.S., Mohammad R.M.A., Almotiri S.H., Mirza S., Anis F.M. & Altamimi H.S. (2021). Intelligent techniques for detecting network attacks: review and research directions. — *Sensors*, — *21*(21), — 7070.

Alothman Z., Alkasassbeh M. & Al-Haj Baddar S. (2020). An efficient approach to detect IoT botnet attacks using machine learning. — *Journal of High Speed Networks*, — *26*(3), — 241–254.

Awotunde J.B., Folorunso S.O., Imoize A.L., Odunuga J.O., Lee C.C., Li C.T. & Do D.T. (2023). An Ensemble Tree-Based Model for Intrusion Detection in Industrial Internet of Things Networks. — *Applied Sciences*, — *13*(4), — 2479.

Azimjonov J. & Kim T. (2024). Stochastic gradient descent classifier-based lightweight intrusion detection systems using the efficient feature subsets of datasets. — *Expert Systems with Applications*, — *237*, —121493.

Batchu R.K. & Seetha H. (2023). A hybrid detection system for DDoS attacks based on deep sparse autoencoder and light gradient boost machine. — *Journal of Information & Knowledge Management*, — *22*(01), 2— 250071.

BAYDOĞMUŞ G.K. (2021). The Effects of Normalization and Standardization an Internet of Things Attack Detection. *Avrupa Bilim ve Teknoloji Dergisi*, — (29), — 187–192.

Churcher A., Ullah R., Ahmad J., Ur Rehman S., Masood F., Gogate M. & Buchanan W.J. (2021). An experimental analysis of attack classification using machine learning in IoT networks. — *Sensors*, — *21*(2), — 446.

Dasari S. & Kaluri R. (2024). An Effective Classification of DDoS Attacks in a Distributed Network by Adopting Hierarchical Machine Learning and Hyperparameters Optimization Techniques. — *IEEE Access*.

Dener M., Okur C., Al S. & Orman A. (2023). Wsn-bfsf: A new dataset for attacks detection in wireless sensor networks. — *IEEE Internet of Things Journal*.

Faysal J.A., Mostafa S.T., Tamanna J.S., Mumenin K.M., Arifin M.M., Awal M.A. & Mostafa S.S. (2022, January). XGB-RF: A hybrid machine learning approach for IoT intrusion detection. In *Telecom*. — Vol. 3. — No. 1. — Pp. 52–69). — MDPI.

Haq and Rahim Khan (2022). DNNBoT: Deep Neural Network-Based Botnet Detection and Classification, Computers, Materials & Continua Tech Science Press. — DOI:10.32604/cmc.2022.020938

Inayat U., Zia M.F., Mahmood S., Khalid H.M. & Benbouzid M. (2022). Learning-based methods for cyber attacks detection in IoT systems: A survey on methods, analysis, and future prospects. *Electronics*, — *11*(9), — 1502.

Irfan, Wildani I.M. & Yulita I.N. (2019, April). Classifying botnet attack on internet of things device using random forest. In *IOP Conference Series: Earth and Environmental Science*. — Vol. 248. — p. 012002. — IOP Publishing.

Jeyabharathi Alphonse A.S., Priya E.D. & Kowsigan M. (2022). Review of Machine Learning Techniques Used for Intrusion and Malware Detection in WSNs and IoT Devices. — *Design and Development of Efficient Energy Systems*, — 57–65.

Kim J., Shim M., Hong S., Shin Y. & Choi E. (2020). Intelligent detection of iot botnets using machine learning and deep learning. — *Applied Sciences*, — *10*(19), — 7009.

Li P.H., Xu J., Xu Z.Y., Chen S., Niu B.W., Yin J. & Chen L L. (2022). Automatic Botnet Attack Identification Based on Machine Learning. *Computers, Materials & Continua*, —*73*(2).

Meidan Yair, Bohadana Michael, Mathov Yael, Mirsky Yisroel, Breitenbacher Dominik, Asaf and Shabtai Asaf (2018). detection_of_IoT_botnet_attacks_N_BaIoT. UCI Machine Learning Repository. — https://doi.org/10.24432/C5RC8J.

Moher D., Liberati A., Tetzlaff J., Altman D.G. (2009). Prisma Group. Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. Ann. Intern. Med. — 151 (2009). — Pp. 264–269. — W64. — 10.7326/0003-4819-151-4-200908180-00135

Natarajan R., Ranjith C.P., Mohideen M.S.K., Gururaj H.L., Flammini F. & Thangarasu N. (2024). Utilizing a machine-learning algorithm to choose a significant traffic identification system. — *International Journal of Information Management Data Insights*, *4*(1), — 100218.

Sagirlar et al. (2018). G. Sagirlar, B. Carminati and E. Ferrari, "AutoBotCatcher: Blockchain-Based P2P Botnet Detection for the Internet of Things," 2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC), Philadelphia, PA, — USA, 2018. — Pp. 1–8, — doi: 10.1109/CIC.2018.00-46

Saied M., Guirguis S. & Madbouly M. (2023). A comparative analysis of using ensemble trees for botnet detection and classification in IoT. — *Scientific Reports*, — *13*(1), — 21632.

Saleh H.M., Marouane H. & Fakhfakh A. (2024). Stochastic Gradient Descent Intrusions Detection for Wireless Sensor Network Attack Detection System Using Machine Learning. — *IEEE Access*.

Samy A., Yu H. & Zhang H. (2020). Fog-based attack detection framework for internet of things using deep learning. —*IEEE Access*, — *8*, — 74571–74585.

Shukla A.K. & Dwivedi S. (2022). Discovery of Botnet Activities in Internet-of-Things System Using Dynamic Evolutionary Mechanism. — *New Generation Computing*, — *40*(1), — 255–283.

Tahaei H., Afifi F., Asemi A., Zaki F. & Anuar N.B. (2020). The rise of traffic classification in IoT networks: A survey. *Journal of Network and Computer Applications*, — *154*, —102538.

Tyagi H. & Kumar R. (2021). Attack and Anomaly Detection in IoT Networks Using Supervised Machine Learning Approaches. — *Revue d'Intelligence Artificielle*, — *35*(1).

Waqas M., Kumar K., Laghari A.A., Saeed U., Rind M.M., Shaikh A.A. & Qazi A.Q. (2022). Botnet attack detection in Internet of Things devices over cloud environment via machine learning. — *Concurrency and Computation: Practice and Experience*, — *34*(4), — e6662.

Wazirali R. & Ahmad R. (2022). Machine Learning Approaches to Detect DoS and Their Effect on WSNs Lifetime. — *Computers, Materials & Continua*, — *70*(3).

Zhukabayeva A. Adamova B. Khu Ven-Tsen Y. Mardenov L. Zholshiyeva (2023). Detection of Sybil And Wormhole Attacks In Wireless Sensor Networks. — *News Of The National Academy of Sciences of The Republic of Kazakhstan, Physico-Mathematical Series*, (4), — 171–183. — Https://Doi.Org/10.32014/2023.2518-1726.227

МАЗМҰНЫ

СОДЕРЖАНИЕ

CONTENTS

Publication Ethics and Publication Malpracticein the journals of the National Academy of Sciences of the Republic of Kazakhstan

For information on Ethics in publishing and Ethicalguidelines for journal publication see http://www.elsevier.com/publishingethics and http://www.elsevier.com/journal-authors/ethics.

Submission of an article to the National Academy of Sciences of the Republic of Kazakhstan implies that the described work has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see http://www.elsevier.com/postingpolicy), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any otherlanguage, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The National Academy of Sciences of the Republic of Kazakhstan follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/New_Code.pdf). To verify originality, your article may be checked by the Cross Check originality detection service http://www.elsevier.com/editors/plagdetect.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the National Academy of Sciences of the Republic of Kazakhstan.

The Editorial Board of the National Academy of Sciences of the Republic of Kazakhstan will monitor and safeguard publishing ethics.

Правила оформления статьи для публикации в журнале смотреть на сайтах:
www:nauka-nanrk.kz
http://physics-mathematics.kz/index.php/en/archive
ISSN2518-1726 (Online),
ISSN 1991-346X (Print)

Подписано в печать 28.03.2024.
Формат 60x881/8. Бумага офсетная. Печать–ризограф.
21,0 п.л. Тираж 300. Заказ 1.

РОО «Национальная академия наук РК» 050010,
Алматы, ул. Шевченко, 28, т. 272-13-19