9 Utilizacija tverdyh othodov: ispol'zovanie ugol'noj zoly v kachestve syr'ja dlja proizvodstva teploizoljacionnogo betona [Tekst] / R. Rana [i dr.] // Ogneupory i tehnicheskaja keramika. - 2013. - № 4-5. - S. 74-80.
10 Fosfornoshlakovye vjazhushhie i betony [Tekst] / Z.A. Estemesov [i dr.] - Almaty: Nauka, 1997. - 456 s.
17 Rjabov, A.V. Raschet processa jelektroplavki: ucheb. posobie [Tekst] / A.V. Rjabov, I.V. Chumanov. - Cheljabinsk: JuUrGU, 2005. - 175 s.
18 Ivanova, L.I. Indukcionnye kanal'nye pechi: ucheb. posobie [Tekst] / L.I. Ivanova, L.S. Grobova, B.A. Sokunov. - 2-e izd., dop. - Ekaterinburg: UGTU-UPI, 2002. - 105 s.

РЕЗЮМЕ

В Экибастузской ГРЭС-2 по исследуемым параметрам и показателей соотношении шлаковая пыль состоит из таких показателей и при этом показывает, что удельная поверхность равна 300 м^2/кг, истинная плотность = 1,9 г/см^3, насыпная плотность ~780 кг/м^3.

По химическим показателям SiO_2 (56,7 %) и Al_2O_3 (28,6 %), фазовый состав – муллитом (38 %), кварцом (32 %), силлиманитом (12 %), гематитом (5 %), стеклофазой (10 %) и несгоревшим углеродом (3 %); модуль основности составляет 0,02, а модуль активности – 0,5.

По данным описания можно извлечь то, что эта шлаковая пыль насколько кислотная, что ее составляющая по минералам может быть таковым, что состоящая в составе золы стеклофаза (10 %) может иметь высокую активность (и может быть в пределах 10 %), наибольшее составляющая кремнезема (в пределах 26 %).

Показатели распространения структур по объёму определили, что:

- несгоревший углерод в основном сосредоточен в составе крупных фракций, а стеклофаза, преимущественно, находится среди мельчайших частиц;
- частицы муллита, силлиманита и кварца несколько однородно присутствуют по фракциям.

Шлаковая пыль или летучая зола - это остатки сгораемого топлива. которая может содержаться в дымовых газах и может находиться в котельных трубопроводах и дымососах и может загрязнять атмосферу.

В данной работе исследуется зола, где есть возможность использования продукта для производства строительных материалов.

ӘӨЖ 004.056.53 ***DOI 10.52578/2305-9397-2023-2-3-180-190***
ҒТАХР 50.37.23

Курмашева Д.Н., педагогика ғылымдарының магистрі, **негізгі автор**, https://orcid.org/0009-0007-9755-231
М.Өтемісов атындағы Батыс Қазақстан университеті, 090000, Н.Назарбаев көш., 162, Орал қ., Қазақстан Республикасы, kurmashevadin@mail.ru
Куангалиев Т.Г., техникалық ғылым магистрі, https://orcid.org/0000-0002-0849-5875
«Жәңгір хан атындағы Батыс Қазақстан аграрлық-техникалық университеті» КеАҚ, 090009, Жәңгір хан көш., 51, Орал қ., Қазақстан Республикасы, ttimurkuan@gmail.com
Мұхамбетов А.А., техника ғылымдарының магистрі, https://orcid.org/0000-0002-3022-4086
«Жәңгір хан атындағы Батыс Қазақстан аграрлық-техникалық университеті» КеАҚ, Жәңгір хан көш., 51, Орал қ., Қазақстан Республикасы, amangeldy.abatovish@gmail.com
Гусманова А.С., техникалық ғылым магистрі, https://orcid.org/0000-0001-7730-051X
«Жәңгір хан атындағы Батыс Қазақстан аграрлық-техникалық университеті» КеАҚ, 090000, Жәңгір хан көш., 51, Орал қ., Қазақстан Республикасы, alida_the_best@mail.ru
Аманкулова Г.М., техникалық ғылым магистрі, https://orcid.org/0000-0002-5566-5814 «Жәңгір хан атындағы Батыс Қазақстан аграрлық-техникалық университеті» КеАҚ, 090009, Жәңгір хан көш., 51, Орал қ., Қазақстан Республикасы, gulfayrus.amankulova@bk.ru

Kurmasheva D.N., master, **the main author**, https://orcid.org/0009-0007-9755-231X

Makhambet Utemisov West Kazakhstan University, 090000, 162 N.Nazarbaev Str., Uralsk, Republic of Kazakhstan, kurmashevadin@mail.ru
Kuangaliev T.G., master, https://orcid.org/0000-0002-0849-5875
«Zhangir Khan West Kazakhstan Agrarian-Technical University» NPJSC, 090000, 51 Zhangir Khan Str., Uralsk, Republic of Kazakhstan, gaisiyevich@gmail.com
Mukhambetov A.A., master, https://orcid.org/0000-0002-3022-4086
«Zhangir Khan West Kazakhstan Agrarian-Technical University» NPJSC, 090000, 51 Zhangir Khan Str., Uralsk, Republic of Kazakhstan, amangeldy.abatovich@gmail.com
Gusmanova A.S., master, https://orcid.org/0000-0001-7730-051X
«Zhangir Khan West Kazakhstan Agrarian-Technical University» NPJSC, 090000, 51 Zhangir Khan Str., Uralsk, Republic of Kazakhstan, alida_the_best@mail.ru
Amankulova G.M., master, https://orcid.org/0000-0002-5566-5814
«Zhangir Khan West Kazakhstan Agrarian-Technical University» NPJSC, 090000, 51 Zhangir Khan Str., Uralsk, Republic of Kazakhstan, gulfayrus.amankulova@bk.ru

БАҒДАРЛАМАЛЫҚ ШАБУЫЛДЫҢ ҚАУІПТІЛІГІН АЗАЙТУДА IOT-та TCP ПАКЕТІН БАҚЫЛАУ ТИІМДІЛІГІ
EFFICIENCY OF TCP PACKET MONITORING IN IOT IN REDUCING THE THREAT OF A SOFTWARE ATTACK

Аннотация

В последнее время современные системы Интернета вещей внедрили открытые стандарты протокола управления передачей (TCP), чтобы учесть разнородность приложений и устройств от различных продавцов. Цель исследования - понять эффективность слежки за TCP-пакетами в IoT для снижения риска атак программ-вымогателей. Более конкретно, исследование сосредоточено на определение эффективности наблюдения за TCP-пакетом, используемым в IOT. Между тем, изучение эффективности снижения риска атак программ-вымогателей с помощью протокола наблюдения TCP в IOT также было одной из целей настоящего расследования.

Результаты исследования свидетельствуют о том, что IoTSDN-RAN зарекомендовал себя как эффективный метод наблюдения, используемый для снижения риска атак программ-вымогателей. Этот метод был признан эффективным при сравнении с методами IoT SVM и IoT ML. С точки зрения обнаружения, точности и безошибочности, этот метод был доказан как эффективный по сравнению с другими наиболее часто используемыми методами. Задача в SVM состоит в том, чтобы найти опорные векторы, классифицировать неизвестный трафик для атак.

Пользователи должны понимать, что IoT имеет тенденцию быть сложным, и, следовательно, им необходимо лучше разбираться в атаках TCP и программ-вымогателей и избегать их с помощью последствий TCP. Значение TCP для ИТ-пользователей важно для обеспечения эффективности всей системы и отсутствия риска атак программ-вымогателей.

ANNOTATION

In recent times, up-to-date IoT systems have implemented the open standards of Transmission Control Protocol (TCP) practices in order to accommodate the heterogeneity of applications and devices from various sellers. The study aims to understand the efficiency of surveillance of TCP packets in IoT in reducing the risk of ransomware attacks. More specifically, the study is focused on

determining the efficiency of surveillance of TCP packet used in IOT. Meanwhile, investigating the effectiveness in reducing the risk of ransomware attacks through surveillance TCP in IOT has also been one of the present investigation's objectives.

The findings of the study suggests that IoTSDN-RAN is proven as effective surveillance technique used in reducing the risk of ransomware attacks. The technique has been considered as efficient when is compared with the IoT SVM and IoT ML techniques. In terms of detection, precision and accuracy, the technique was proven as efficient in comparison to the other most frequently utilised techniques. The challenge in SVM is to find the support vectors, to classify unknown traffic to the attacks.

The users need to understand that IoT tends to be a complex and thus, they need to have a better understanding with regards to the TCP and ransomware attacks and avoid them through the TCP implications.The implications of TCP by the IT users is important to ensure that there is effectiveness and efficiency addressed among the entire system and there pertains no risk of ransomware attacks.

Түйін сөздер: *TCP пакеті, Ransomware шабуылдары, Iotsdn -RAN, Iot SVM, Iot ML, интернет, әлеуметтік желілер, интернетке тәуелділік, мазасыздық, стресс, шабуыл, кибер шабуыл, агрессия, халықаралық қылмыс.*

Key words: TCP Packet, Ransomware Attacks, Iotsdn-RAN, Iot SVM, Iot ML, Internet, social networks, Internet addiction, anxiety, stress, cyber attack, attack, aggression, international crime.

Кіріспе. IoT жүйелері әртүрлі сатушылар қолданбалары мен құрылғыларының біркелкі еместігін қамтамасыз ету үшін Transmission Control Protocol (TCP) тәжірибелерінің ашық стандарттарын енгізді. Бірнеше дәуірден астам уақыт бұрын бұл сымды жаһандық Интернет үшін де құрылған[2]. Дегенмен, IoT желілерінің құбылысы ескірген сымды компьютерлік желілерден негізгі тәсілдермен ерекшеленеді. Трансмиссияны басқару протоколы (TCP) ғаламдық интернет ортасында ұшты-соңды сапаны қамтамасыз ететін ең кең тараған транспорттық деңгей протоколдарының бірі ретінде танылғаны талданған. Әдетте, сымдар ортасында, әдетте, ұқсас арнадағы үлкен жүктемеге байланысты кептелістің жоғары ықтималдығы бар. IoT желісінің дизайнында TCP түсінігі шартты түрде еленбегені анықталды. Дегенмен, қазіргі заманғы үрдістер TCP IoT параметрлерінде кең таралған позицияға ие болатындығын болжайды. [3] зерттеуден белгілі болғандай, TCP құрылымы сегмент өлшемін өзгерту және диспетчерге монотонды растауларды бағыттау арқылы кептеліс жағдайларын өте қалыпты түрде өңдеуге қабілетті.

Арнаның сымсыз ортадағы өнімділігі қабылдағышқа жетпестен және деректерді тарату үшін жіберушіге растауды бағыттамай-ақ, қатты және қатал түрде өзгертеді және деректердің зақымдалуына әкеледі. Бұл энергетикалық жағдай сымсыз желіде модельденген кептеліс ортасын тудырады. Бұған қоса, [4] зерттеуі TCP сымсыз желілердің қарқынды әрекетін қате есептейтінін және жағдайды әдеттегі сценарийлердегі кептеліс жағдайы ретінде шығаратынын көрсетеді. Дегенмен, [5] зерттеуі TCP кептеліс алгоритмі сымсыз байланыстарды белгілемейтінін көрсетеді, өйткені олар қате есептеуден және пакеттің зақымдану жылдамдығынан зардап шегеді, және нәтижесінде олар әлі де еліктірер түрде болжау мүмкін емес. [9] жүргізген тағы бір зерттеуде TCP протоколы сымсыз бағдарламадағы кез келген пакеттің жоғалуын жаңылыспен өлшейді, өйткені терезенің өлшемін бір секцияға дейін азайту және кейіннен жылдамдықты төмендету үшін кептеліс алгоритмін ынталандыратын кептеліс салдарынан. беру және пакеттік шығыс. Бұған қоса, Jutila (2016) жүргізген зерттеу TCP жүйесі пакеттер тұтынатын маршрутқа қарамастан қосылудың кез келген келісімі бар деген болжам бойынша жұмыс істеуін жалғастыруы керек деп бағалады. Үстем жүйелердің IoT құрылғыларына қосылу перспективасы көліктің, әсіресе мультимедиялық көліктің әсері болып табылады. Сонымен қатар, TCP ең үлкен мақсаттарының бірі жолдың соңында күрделі технологиялар массасы бойынша мультимедиялық қызметтерге/қолданбаларға өлшенетін түпкілікті QoS кепілдіктерін ұсыну екені анықталды. Бұған қоса, заттарды интернетке байланыстыру IoT құрылғылары мен ұқсас жүйеде орнатылған басқа процессорлар арасында үздіксіз қосылуға мүмкіндік беретіні даусыз. [14] жүргізген зерттеу жоғалтқан сымсыз желілерде жұмыс істегенде, TCP ретті жеткізу және қайта жіберу құрылғысы қажетсіз үзіліспен таныстыратын желілік блоктауға әкелуі мүмкін екенін көрсетеді. Сонымен қатар, TCP компьютерлердің бір-біріне деректер пакеттерін жіберу жолын сипаттайтын Интернет протоколымен (IP) жұмыс істейтіні түсінілді. TCP және Internet Protocol (IP) екеуі де Интернетті анықтайтын қарапайым нұсқаулар болып табылады. Сонымен қатар, TCP стегі файлды пакеттерге бөледі, нөмірлейді, содан кейін оларды жеткізу үшін IP деңгейіне жеке жібереді.

АТ барлық TCP түсінігі тақырыптың үстеме шығынының жоғарылауы, жоғалтуға төзімді қолданбалар үшін икемділіктің болмауы және көп таратуға сәйкес келмеуі сияқты ерекше кемшіліктерді қамтитыны бағаланды. Сонымен қатар, бірқатар зерттеулер TCP феномені заттардың Интернеті үшін жақсы қабылданған unicast endways консистенциясы

механизмдеріне ұқсас әрекет ету мүмкіндігіне ие екенін бөлісті. Сонымен қатар, Ransomware қатерлерінің шеңбері IoT жалпы идеологиясында маңызды мәселе болды. Ағымдағы зерттеудің авторы TCP пакеттерінің тұжырымдамасына, оның архитектурасына, оған енгізілген қиындықтарға жарық түсіретін бірқатар зерттеулерді таба алды. Дегенмен, төлемдік бағдарламалық жасақтама шабуылдарының қаупін азайту үшін IoT жүйесінде TCP пакетін бақылаудың тиімділігіне жарық түсіретін үйлесімді зерттеулер көп емес. Сондықтан, қазіргі зерттеудің авторы осы олқылықты атап көрсетеді және зерттеудің мақсаты мен мәселелерін назарда ұстай отырып, тиімді нәтиже береді. Осыны ескере отырып, зерттеудің мақсаты төлемдік бағдарлама шабуылдарының қаупін азайту үшін IoT жүйесінде TCP пакетін бақылаудың тиімділігін түсіну болып табылады. Нақтырақ айтқанда, зерттеу қадағалаудың тиімділігін анықтауға бағытталған

IoT жүйесінде TCP пакетін қадағалаудың тиімділігі. TCP – пайдаланушыға желілік процесс арқылы жылдам қосылуға және байланысуға мүмкіндік беретін толық протокол. Осыған ұқсас зерттеуде автор TCP-нің Интернеттегі заттардың маңызды рөлі бар екенін түсіндіре отырып, өз нәтижелерін одан әрі нақтылады, өйткені ол пайдаланушыға бұлтпен қосылуға және сәйкесінше байланыс орнатуға мүмкіндік береді. Сол сияқты [6] өз зерттеулерінде қазіргі дәуірде жылдам дамып келе жатқан желі қосылымдары жылдам, қол жеткізу оңай және қауіпсіз кеңістікті талап ететінін атап өтті. Осылайша, TCP тиімді қауіпсіздікке ие интернет протоколы болып табылады, өйткені ол пайдаланушыларға олардың қарым-қатынасы мен идеяларына кедергі келтірместен байланысуға мүмкіндік береді.

Бұдан басқа, [7] ұсынған зерттеу TCP арқылы қауіпсіздік пен бақылау интернет порталы үшін жоғарылайтынын түсіндіреді, өйткені TCP пайдаланушыға байланыс жасамас бұрын қосылым жасауға мүмкіндік береді, сондықтан ол интернет үшін тиімді бақылау платформасы болып саналады. пайдаланушылар.

Сонымен қатар, [8] TCP IoT- те қауіпсіздік пен бақылаудың толық пакетін қамтамасыз ете алады, өйткені ол қосылған желіні талдайды және одан әрі байланысты төмен деректермен қамтамасыз етеді. TCP жүйесінде бақылаудың тиімділігінің тағы бір ерекшелігі интернет-порталда әдетте қауіпсіздік мәселелері болады, себебі ол кейбір нәрселерді бұзу және бағалау оңайырақ болды. Дегенмен, TCP пакеті пайдаланушыға деректерді жылдам түрлендіруге көмектеседі, ол пайдаланушыға деректерге қол жеткізуге және өзінің тұтастығын сақтау арқылы басқа пайдаланушыны қосуға мүмкіндік береді, өйткені ол қосылу үшін құпиялылық мүмкіндігін қамтамасыз етеді. Бұдан басқа, Нати мен Сутар өз зерттеулерінде интернет-портал пайдаланушыларға қауіпсіздік сенімділігімен байланысты байланыстыруға көмектесетін осындай жүйеге мұқтаж екенін атап өтті, осылайша бұл TCP бақылауының ерекшелігі болып табылатын қиын тапсырмалардың біріне айналды. IoT тиімді өсуіне көмектеседі [9]. Интернет-порталда осындай жіберуді басқару элементтері мен хаттама талап етілетіні анықталды, бұл бүкіл байланыс пен желі жүйесін қосу мен қадағалауды тиімді етеді. Желі мен байланыс жолының тиімділігі интернет-порталдағы қауіпсіздіктің тиімділігін сақтауға көмектеседі.

Зерттеулер [21] IOT ML әдістерінің шектеулерін ұсынады. Оларды рұқсатсыз араласуды анықтау үшін компьютерлік желі қауіпсіздік өрісінде пайдалануға болады. Екінші жағынан, күдікті әрекет болған жағдайда, IOT ML талдауының нәтижелері келесіден ауытқиды. Күтілетін қалыпты желілік белсенділіктің және күдікті әрекеттің анықтамасы айқын болады. Сонымен қатар, SVM IoT желілік трафигіндегі шабуылдарды анықтау және тіпті желі периметрі шегінде бұзушының физикалық болуын анықтау үшін пайдаланылды. SVM-тің анықталған міндеті белгісіз трафикті зиянды немесе зиянсыз деп жіктей алатын қолдау векторларын табу болып табылады [22].

IOT жүйесіндегі TCP пакетіне қатысты қиындықтар. Davoli, Protskaya және Veltri зерттеуі талқылауда TCP пакеті максималды тасымалдау бірлігін қажет ететінін айтады, бірақ IoT азырақ тасымалдау блогымен жүреді [16]. Автор IoT үшін IoT TCP пакетінде максималды деңгейде талап етілетін мұндай жылдам тасымалдау бірліктерін қажет етпейтінін түсіндіре отырып, негізгі мәселені одан әрі нақтылады. Doshi, Apthorpe және Feamster пікірінше, TCP пайдалану бұлтпен қосылуға және IoT -де байланысты қолдауға мүмкіндік береді, бірақ ол әрқашан онымен байланысты көптеген мәселелерге ие. Автор әрі қарай IoT жүйесіндегі TCP қиындықтары Басқару хаттамасын пайдалануды шектейтінін түсіндіреді [10] TCP пакетімен байланысты тағы бір қиындықты тудырады, автор көп сілтемелі ішкі желі тағы бір маңызды

мәселе екенін түсіндіреді. Бұл негізінен екі түйінге бір сілтеме бойынша бір уақытта екі пайдаланушы қол жеткізе алады деген болжам қабылданған кезде. Демек, IoT қабаттарда жұмыс істейді, онда бір сілтемеде бірнеше түйіндердің бірге жұмыс істеуі ең қиын тапсырмалардың бірі болып табылады және оны шектеу ретінде қарастыруға болады. Көп тарату тиімділігін [11] басқа мәселе ретінде анықтайды, себебі мультикаст пайдаланушылардан бір уақытта екіден көп функцияға қол жеткізуді талап ететіні түсіндіріледі. Одан әрі зерттеуде мультикастқа қатысты негізгі мәселе IoT бір-бірімен байланыстырылған қабаттарда жұмыс істейтіні түсіндірілді, сондықтан пайдаланушыға қабаттар бір-бірімен байланыстырылған желіде қалпына келтіру немесе кіру қиынға соғады..

Көп тапсырма тиімділігінің тағы бір маңызды мәселесі [12] бірнеше протоколдар бірге жұмыс істейтіндіктен түсіндіріледі, сондықтан ол IoT- де мүмкін емес қол жеткізудің бірнеше жылдамдығын көрсетеді. IoT желісі пайдаланушыға жұлдыз топологиясы және тең дәрежелі топология болып табылатын екі топологияны ортақ пайдалануға мүмкіндік береді, осылайша [13] TCP-ге қол жеткізу үшін деректер мен түйіндер оңай ортақ пайдаланылатын және оларға қол жеткізуге болатын торлы топологияға қол жеткізу қажет екенін айтады. жылдам. Бұдан басқа, тор желісі заттардың Интернеті үшін күрделі аспект болып табылады, өйткені ол түйіндердің кең ауқымда қосылуын талап етеді және IoT қолдамайтын жан-жақты тропологияны жасау үшін портал жиі қосылуы керек. Осылайша, ол TCP пакетіне қол жеткізу үшін IoT үшін қиын факторлардың бірі ретінде қарастырылады. [14] атап өткен тағы бір қиын нәрсе - IoT TCP жағдайында жасалмайтын әртүрлі байланыс үлгілерін қолдайды, өйткені ол оны қолдауға жеткілікті күшті емес энергияны шектейтін құрылғылардан тұрады. Сол сияқты, TOP мүмкіндіктері негізінен IoT үшін күрделі фактор болып табылады, өйткені ол пайдаланушыларды шектейді және оларға шектеулі мүмкіндіктермен қамтамасыз етеді, бұл деректерге қол жеткізудің және пайдаланушы мен ұсынылған платформа арасындағы байланыстың шектелуіне әкеледі. [10] ұсынған зерттеу интернет-порталдағы түйіндер қосылу үшін қол жетімді қабаттар арқылы заңды түрде тасымалданбайтындықтан қол жеткізу үшін үлкен қиындыққа айналатынын тұжырымдады. Қабаттар негізінен пайдаланушы үшін операциялар мен желіні шектейтіні әрі қарай өңделді, бұл шешу үшін үлкен қиындыққа айналады.

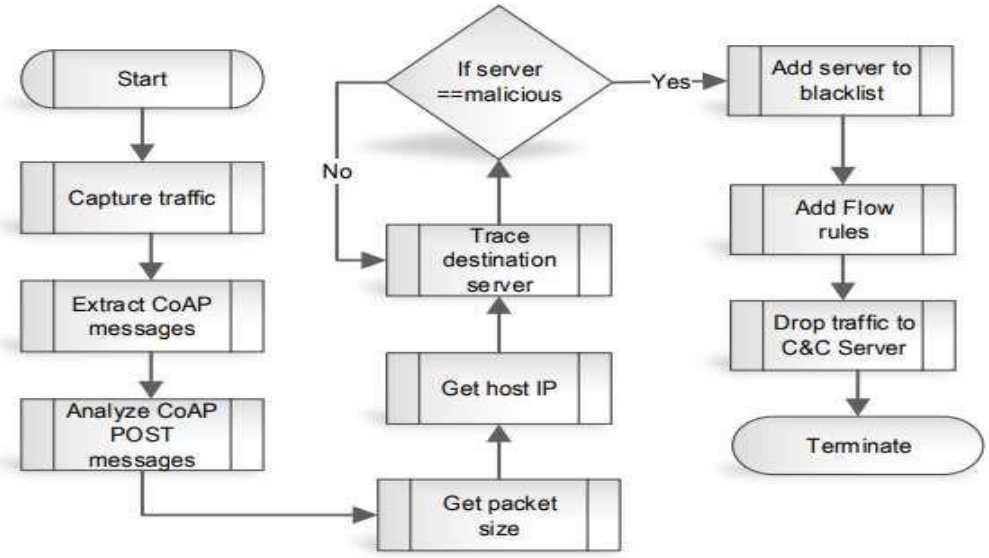
IOT жүйесіндегі Ransomware шабуылдарының түсінігі. Ransomware шабуылы - құрбанның деректерін кодтайтын және төлем төленгенге дейін рұқсатты болдырмайтын зиянды бағдарлама шабуылының бір түрі [14]. Төлем шабуылдарына қатысқан шабуылдаушылар әдетте құрбанның ортасына рұқсат алу үшін фишинг сияқты әлеуметтік инженерия әдістерін пайдаланады. Әдетте, төлемдік бағдарламалық құрал шабуылдары құрылғыға немесе компьютерге кіру, содан кейін ондағы сақталған деректерге тыйым салу және шифрлау арқылы жүзеге асады [3]. Бүкіл процедурадағы ең үлкен кемшілік - пайдаланушы деректерінің сақталатынына кепілдік жоқ. бұл төлемді төлеуге қарамастан қалпына келтірілді. Қауіптілер ешқашан иесіне шифрды шешу кілтін бермеген бірқатар жағдайлар болды. Бұдан басқа, IoT ұйымға қауіпсіздікті қамтамасыз ету үшін қажет болатын шабуылдың бетін қорқынышты түрде қайта анықтау мүмкіндігіне ие екендігі бағаланды. Бұл қорқыныш сонымен қатар смарт машиналар мен маршрутизаторлар сияқты әдеттегі IoT құрылғыларын қамтиды.

Дегенмен, бұл күнделікті құрылғыларды төлемдік бағдарламалық құралдың жүйеге енуіне мүмкіндік беру үшін теріс пайдалану қаупі бар екені анықталды [15]. Технологияның соңғы уақытында IoT құбылысы адамдардың өмір салты мен жұмыс істеу тәсілін өзгертеді. Ол күнделікті адам әрекеттері мен технологияларының бірнеше қолдану салаларын бір бетте біріктіру арқылы маңызды рөл атқарады. Дегенмен, IoT жүйесі кибералаяқтық режимінде бірқатар қиындықтарды бастан өткеруі мүмкін және өте маңызды төлем бағдарламалық қамтамасыз ету шабуылдары. Зиянды ransomware шабуылдары қандай да бір жолмен динамикалық ақпаратқа рұқсат беруді шектейді және осы ақпаратты қабылдау үшін өтемақы талап етеді. Төлемдік бағдарламалық жасақтаманың шабуылы күн сайын өте ауқымды болып келе жатқаны және күрделі деректердің зақымдануынан, өндірістік деректердің жойылуынан, беделді жоғалтудан және бизнестің үзілуінен тұратын жойқын мәндерге ие болатыны анықталды. Одан әрі, өкінішке орай, бұл тоқтап қалу салдарынан күнделікті миллиардтаған доллар шығынға әкеледі..

Yaqoob зерттеуі қауіпсіздік зерттеушілері жеке тұлғалар мен ұйымдарды төлемдік бағдарламалық жасақтама шабуылдарынан қорғау үшін көптеген түсініктемелер мен шешімдер ұсынуға көп күш салғанын көрсетеді. Дегенмен, Захра зерттеуі IoT прогрессімен ерекше өмір кәсіби өмірмен қатар адамдар мен есептеуіш құрылғылар арасындағы өзара байланыс пен интернетке толығымен тәуелді болатынын көрсетеді. Жаңа аспектілері мен технологиялары бар нарықтағы хакерлердің әсері өте қауіпті болды деп саналады және осыған байланысты әрбір жеке тұлға мен ұйым өздерінің активтеріне, жеке және ұйымдық, олар мүмкін болмайтындай қамқорлық жасауы міндетті болып табылады. төлем бағдарламасының құрбаны болыңыз. Захра зерттеуі есептеу ортасын қорғау үшін қазіргі уақытта қолданыстағы бірқатар бағдарламалық қамтамасыз ету және алдын алу шаралары бар екенін бағалайды, дегенмен жеке адамдар мен кәсіпкерлердің қауіпсіздік бағдарламалық жасақтамасын уақтылы жаңарту негізгі жауапкершілігі болып табылады.

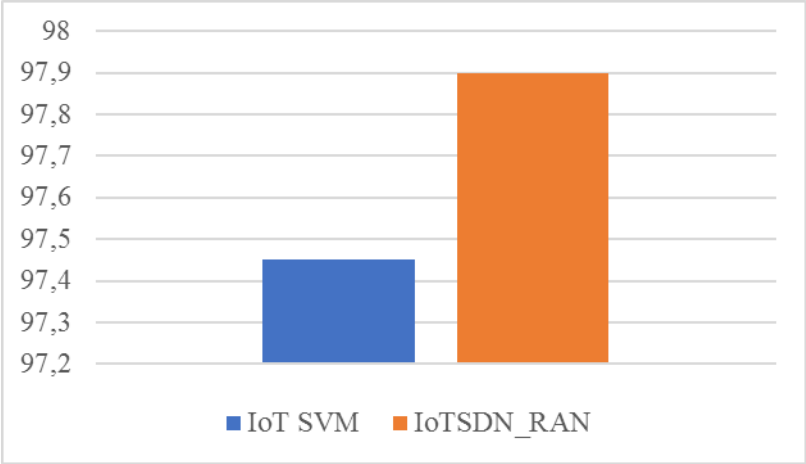
Құпиялылық және төлемдік бағдарлама шабуылдарына қарсы TCP пакеттерін қадағалаудың негізгі әдістері. Интернет-провайдер тұрғысынан пакетті жоғалту коэффициенті (PLR) желілердің өнімділігі мен қауіпсіздігін өлшеудің ең негізгі параметрлерінің бірі болып табылады [1]. Ол үшін қосылған маршрутизаторлардан барлық желілер бойынша пакеттердің жоғалуының статистикасы жиналады, бұл ISP-ге ықтимал күшейтілген пакет жоғалуы туралы жергілікті көріністі қамтамасыз етеді. Мұндай жоғарылатылған жоғалту қандай да бір қате немесе төлемдік бағдарлама шабуылына байланысты болуы мүмкін. Дегенмен, бұл әдіс негізінен екі аспектіде елеулі проблемаларды тудырады. Біріншіден, деректер жоғалтуларының қосындысы әр секунд негізіндегі жоғалтуларды әрқашан толық көрсетпейді [2]. Екіншіден, интернет-провайдер желіні толық қорғауды қамтамасыз ету үшін олардың басқару доменін шектейтін кең ұшынан аяғына дейінгі қосылымның автономды жүйесі сияқты тар сегменттер желісіне ғана қол жеткізе алады. Ұсынылған әдістеме эвристикаға негізделген, ол екі тасымалдаушы эндхалардағы ең ықтимал TCP күй машина мысалы жолын анықтауға бағытталған. Әдебиеттер осы эвристиканы толық түсіндіру үшін үлгілерді пайдаланады. Эвристика жиі жан-жақты тексеруді қамтамасыз ете алмайтындықтан, біз іргелі қолданылатын мемлекеттік кеңістіктің үлкен бөлігін зерттеу үшін рекреацияларды пайдаланамыз. Сонымен қатар, есептеу сынақ алаңында бағаланады. Әрбір конфигурация үшін своптардың көп санын модельдеу арқылы есептеудің дұрыстығын тексереміз. Бағалаулар көрсеткендей, есептің екі мәнді бөліктер үшін де бақытсыздықтардың позициясына тәуелсіз, жоғары дәлдікпен байламдық бақытсыздық пропорциясын есептеу үшін қолайлы. TCP, Интернеттің ең танымал протоколы ақаулы арналар арқылы сенімді деректерді жеткізуді қамтамасыз ететін күрделі бейімделу механизмін ұсынады. Біз осы эвристиканы толық түсіндіру үшін үлгілерді қолданамыз. Эвристика жиі жан-жақты тексеруді қамтамасыз ете алмайтындықтан, біз іргелі қолданылатын мемлекеттік кеңістіктің үлкен бөлігін зерттеу үшін рекреацияларды пайдаланамыз [2]. Сонымен қатар, есептеу сынақ алаңында бағаланады. Зерттеушілер әр конфигурация үшін своптардың көп санын модельдеу арқылы есептеудің дұрыстығын тексереді. Бағалаулар көрсеткендей, есептің екі мәнді бөліктер үшін де бақытсыздықтардың позициясына тәуелсіз, жоғары дәлдікпен байламдық бақытсыздық пропорциясын есептеу үшін қолайлы. IOT ортасында төлемдік бағдарламалық қамтамасыз ету шабуылдарына қарсы тұру механизмдері IOT құрылғыларының гетерогенді архитектурасын, сондай-ақ төлемдік бағдарламалық құралдың әртүрлі сипатын ескеруі керек. Сондықтан, IOT құрылғыларының кез келген қауіпсіздік механизмдері төлемдік бағдарламалық құрал мен желіні жүйелі түрде тексере алды. Бұл үшін Wani et al. IoTSDNRAN деп аталатын төлемдік бағдарламаны азайту үшін SDN негізіндегі крипто әдісін ұсынды. Қарсыластың Command and Control (C&C) серверінен шифрлау кілтін алу үшін төлем бағдарламалық құралының кез келген түрі бірдей механизмді пайдаланады [3]. Төлемдік бағдарламаның болуы зиянды бағдарлама мен C&C сервері арасындағы байланыс ағынымен анықталады. Делдалдық серверді пайдалана отырып, қарсылас мақсатты IoT құрылғысының IP мекенжайын алады. Алынған IP мекенжайы, сондай-ақ сәйкестендіру C&C серверінен жіберіледі. Ransomware шабуылы C&C сервері арқылы іске қосылады. C&C IoT құрылғысымен байланысады және оған шифрлау кілтін енгізеді. IoT құрылғысын кодтаудан кейін C&C сервері төлем үшін бұзылған IoT құрылғысының иесіне төлем бағдарламасының онлайн интерфейсінің мәліметтерін береді. Бұл әдісте төлем бағдарламалық құралын анықтау үшін Principal

Component Analysis және Naïve Bayes комбинациясы қолданылады. Төмендегі схема 1 сурет жоғарыда аталған процестің негізгі кезеңдерін бейнелеуге арналған.



Сурет-1. Крипто қорғау схемасы

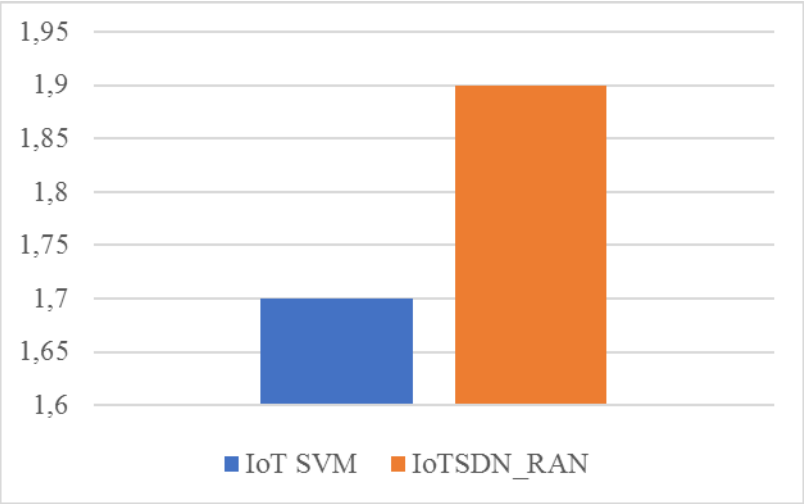
Талқыланғандай, TCP пакеттерін тиімді қадағалау үшін қолданылатын көрнекті әдістердің немесе тәсілдердің бірі IoTSDN -RAN болып табылады. Басқалармен салыстырғанда осы бақылау әдісінің орындылығы мен тиімділігін арттырудың кейбір негізгі себептері. Мысалы, ransomware бағдарламасының болуы тұрғысынан бұл әдіс батареяны тұтыну негізінде оның болуы туралы есеп бермейді. Сонымен қатар, бұл әдіс шынайы болып саналады, өйткені есеп беру кезінде белгілі бір батареяның жұмыс күшінің жоғары сағаттарында жұмысы тоқтап қалуы немесе тұтынылуы немесе DDoS сияқты шабуылдар кезінде оның жұмысын тоқтату мүмкіндігі бар. Дегенмен, IoTSDN -RAN төлем бағдарламалық құралын анықтау үшін мүдделі CoAP тақырыптары үшін тиісті CoAP тақырыптарынан маңызды ақпаратты алуға бейім екенін атап өткен жөн. Бұл сонымен қатар CoAP IoT байланысының ажырамас хаттамаларының бірі ретінде қарастырылуына байланысты болды.



Сурет-2: Салыстыру Iotsdn -RAN Iot SVM көмегімен.

Ешқандай ерекшеліксіз, дәлдік бақылау әдісінің тиімділігіне қол жеткізу кезінде көп ескерілетін басқа маңызды параметрлердің бірі болып саналады деп айтуға негіз бар. Осыған байланысты жоғары анықтау және дәлдік тұрғысынан тиімді деп саналатын 3-суретте көрсетілген IoTSDN -RAN дәл деп саналатын тәсілдердің біріне жататын IoT -SVM-мен салыстыру үшін орнатылды. Алайда, оны IoTSDN -RAN- мен салыстырған кезде, IoTSDN -

RAN анықтау және дәлдік тұрғысынан ғана тиімді емес екені анықталды, бірақ сонымен бірге бұл әдіс жоғары дәлдікке ие, сондықтан бұл әдісті басқалардан басым етеді. әдістер.



Сурет-3: Салыстыру Iotsdn -RAN Iot SVM көмегімен

Әрі қарай, FNR тұрғысынан әдістерді салыстыру қажет болды, өйткені SNR сонымен қатар төлемдік бағдарламалық жасақтама шабуылдарының қаупін азайту үшін қолданылатын бақылау әдісінің тиімділігін анықтау кезінде ажырамас факторлардың бірі болып саналады. IoT SVM мен IoTSDNRAN салыстырылған кезде, IoTSDN -RAN әлі де IOT SVM қарағанда айтарлықтай жоғары тиімді FNR болатыны анықталды. Бұл басқа әдістермен барлық салыстыруларда IoTSDN -RAN төлемдік бағдарлама шабуылдарының қаупін азайту мақсатында тиімді әдістердің бірі ретінде табылғанын көрсетеді.

Қорытынды және ұсыныстар. Интернет заттарының (IoT) құрылымы немесе моделі әдетте бақылау қолданбаларының бірнеше түрлерін қолдау мақсатында есептеулерге қатысты құрылғылардың бірнеше түрін өзара байланыстыруды белгілейді. Соңғы кездері қазіргі заманғы IoT жүйелері әртүрлі сатушылар қолданбалары мен құрылғыларының біркелкі еместігін қанағаттандыру үшін Transmission Control Protocol (TCP) тәжірибесінің ашық стандарттарын ашты деп бағаланды. Бұл зерттеудің мақсаты IOT-та қолданылатын TCP пакетін қадағалаудың тиімділігін анықтау, IOT-тегі TCP бақылауы арқылы төлемдік бағдарламалық құрал шабуылдарының қаупін азайту тиімділігін зерттеу және деректер қауіпсіздігіндегі TCP қадағалауының тиімділігін зерттеу. TCP - пайдаланушыларға қосылуға, сонымен қатар желілік процедура арқылы кең және жылдам байланысуға мүмкіндік беретін толық протокол. TCP заттардың интернетіне жатады, өйткені ол пайдаланушыға бұлтпен қосылуға және сәйкесінше байланыс орнатуға мүмкіндік береді. Сонымен қатар, TCP тиімді қауіпсіздікке ие интернет протоколы болып табылады, өйткені ол пайдаланушыларға олардың қарым-қатынасына және ұсынатын идеяларына кедергі келтірместен байланысуға мүмкіндік береді. Сонымен қатар, TCP арқылы қауіпсіздік пен бақылау интернет порталы үшін жоғарылайды, өйткені TCP пайдаланушыға байланыс жасамас бұрын қосылымды дамытуға мүмкіндік береді, сондықтан ол интернет пайдаланушылары үшін тиімді бақылау платформасы болып саналады. Бұған қоса, TCP қосылған желіні талдау немесе бағалау кезінде IoT арасында қауіпсіздік пен бақылаудың толық пакетін шешу мүмкіндігіне ие. Сонымен қатар, TCP-де бақылау тиімділігінің тағы бір ерекшелігі, интернет-порталда әдетте қауіпсіздік мәселелері бар, өйткені ол кейбір нәрселерді бұзу және бағалау оңайырақ болды, осылайша TCP пакеті пайдаланушыға деректерді жылдам түрлендіруге көмектеседі, ол пайдаланушыға қол жеткізуге мүмкіндік береді. деректер мен басқа пайдаланушыны өзінің тұтастығын сақтау арқылы байланыстырады, себебі ол қосылу үшін құпиялылық мүмкіндігін береді. Сонымен қатар, IoT астында TCP пакетіне қатысты кейбір қиындықтар бар. TCP пайдалану бұлтпен қосылуға және IoT -де байланысты қолдауға мүмкіндік береді, бірақ ол әрқашан онымен сәйкес келетін көптеген мәселелерге ие. Бұған қоса, тағы бір қиындық көп буынды ішкі желі болып табылады, ол негізгі қиындыққа айналады, өйткені бұл негізінен екі түйінге бір сілтемеде бір уақытта екі

пайдаланушы қол жеткізе алады деген болжам қабылданған кезде, осылайша ол TCP үшін қиындыққа айналады.

Сонымен қатар, зерттеу нәтижелері желілердің өнімділігін және олардың қауіпсіздігін өлшеудің ең іргелі параметрлерінің бірі болып табылатын пакеттік жоғалту коэффициентінің (PLR) әсеріне байланысты болды. Ол үшін қосылған rs маршруттарынан барлық желілер бойынша пакеттердің жоғалуларының статистикасы жиналады, бұл ISP-ге ықтимал күшейтілген пакет жоғалуы туралы жергілікті көріністі қамтамасыз етеді. Дегенмен, бұл әдіс екі аспектіде маңызды проблемаларды тудырады. Біріншіден, деректер жоғалтуларының қосындысы әр секіру негізіндегі жоғалтуларды әрқашан толық көрсетпейді. Екіншіден, интернет-провайдер желіні толық қорғауды қамтамасыз ету үшін олардың басқару доменін шектейтін кең ұшынан аяғына дейінгі қосылымның автономды жүйесі сияқты тар сегменттер желісіне ғана қол жеткізе алады. Сонымен қатар, ұсынылған әдістеме эвристикаға негізделген, ол екі тасымалдаудың соңында ең ықтимал TCP күй машинасының мысалы жолын анықтауға бағытталған. Бұдан басқа, бағалаулар жоғары дәлдікпен бақытсыздықтардың позициясына тәуелсіз екі мәнді бөліктер үшін дестенің бақытсыздық пропорциясын есептеу үшін қолайлы екенін көрсетті. Зерттеудің бірінші тарауы зерттеудің фонына, зерттеу мақсаттары мен міндеттеріне және проблемалық қойылымға негізделген. Зерттеудің екінші тарауы зерттеу контекстімен байланысты әдебиеттерге шолуды суреттейді. Сонымен қатар, үшінші тарауда зерттеудің әдістемесі суреттеледі, ал келесі төртінші тарауда зерттеу нәтижелері түсіндіріледі. Соңында тарау қорытынды мен ұсыныстармен аяқталады. Сонымен қатар, TCP пакеті пайдаланушыларға деректерді жылдам түрлендіруге көмектеседі, ол пайдаланушыға деректерге қол жеткізуге және өзінің тұтастығын сақтау арқылы басқа пайдаланушыны қосуға мүмкіндік береді, өйткені ол қосылу үшін құпиялылық мүмкіндігін береді. Кейбір ұсыныстар төлемдік бағдарламалық қамтамасыз ету шабуылдарының қаупін азайту үшін IoT жүйесінде TCP пакетін қадағалау тиімділігі контекстінде қарастырылды.

ӘДЕБИЕТТЕР ТІЗІМІ

1 Hashemi, S. Fuzzy, Dynamic and Trust Based Routing Protocol for IoT [Text]. / F. Shams Aliee // Journal of Network and Systems Management. -2020. 28(4), pp.1248-1278.

2 Duffield, N. "Multicast topology inference from measured end-to-end loss" [Text] / J. Horowitz, F. Lo Presti and D. Towsley // IEEE Transactions on Information Theory. -2002. vol. 48, no. 1, pp. 26-45.

3 Wani, A "Ransomware protection in IoT using software defined networking" [Text] / S. Revathi // International Journal of Electrical and Computer Engineering (IJECE). -2020. vol. 10, no. 3, p. 3166.

4 Na, W. "DLTCP: Deep Learning-Based Transmission Control Protocol for Disaster 5G mmWave Networks" [Text] / B. Bae, S. Cho and N. Kim // IEEE Access. -2019. vol. 7, pp. 145134-145144.

5 Vatsala, B. "Performance Evaluation of TCP Variants for IoT Built on Visible Light Communication" [Text] / C. Vidya Raj // Ransomware protection in loT using software defined networking. Int. J. Electr. Comput. Eng. -2020. 10(3), pp.3166-3175.

6 Javanmardi, S. A security driven task scheduling approach for SDN-based IoT– Fog networks / M. Shojafar, R. Mohammadi, A. Nazari, V. Persico, A. Pescapè [Text] // Journal of Information Security and Applications. -2021. 60, p.102853.

7 Trabelsi, Z. IoT based Smart Home Security Education using a Hands-on Approach. [Text] // In 2021 IEEE Global Engineering Education Conference (EDUCON). -2021. (pp. 294-301). IEEE.

8 Yazdinejad, A., Enabling drones in the internet of things with decentralised blockchain-based security [Text] / R.M. Parizi, A. Dehghantanha, H. Karimipour, G. Srivastava, M. Aledhari, // IEEE Internet of Things Journal. -2021. 8(8), pp.6406-6415.

9 Nathi, R.A. Object Secured TCP Socket for Remote Monitoring IoT Devices / D. Zutar // In 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT). -2019. (pp. 1-5). IEEE.

10 Jutila, M. An adaptive edge router enabling internet of things [Text] // IEEE Internet of Things Journal, 3(6). -2016. pp.1061-1069.

11 Shang, W. Challenges in IoT networking via TCP/IP architecture [Text] / Y. Yu, R. Droms, L. Zhang // NDN Project. -2016. (pp. 29-35).

12 Rad, P. Implementation of deep packet inspection in smart grids and industrial Internet of Things: Challenges and opportunities [Text] / K.K.R. Choo // Journal of Network and Computer Applications. -2019. 135, pp.32-46.

13 Ahmad, M. Intrusion detection in internet of things using supervised machine learning based on application and transport layer features using UNSW-NB15 data-set [Text] / Q. Riaz, M. Zeeshan, H. Tahir, S.A. Haider // EURASIP Journal on Wireless Communications and Networking. -2021(1), pp.1-23.

14 Al-Hawawreh, M. Leveraging deep learning models for ransomware detection in the industrial internet of things environment [Text] / E. Sitnikova // In 2019 Military Communications and Information Systems Conference (MilCIS). -2019. (pp. 1-6). IEEE.

15 Davoli, L. An anonymisation protocol for the internet of things [Text] / Y. Protskaya, L. Veltri // In 2017 International Symposium on Wireless Communication Systems (ISWCS). -2019. (pp. 459464). IEEE.

16 Doshi, R. Machine learning ddos detection for consumer internet of things devices [Text] / N. Apthorpe, N. Feamster // In 2018 IEEE Security and Privacy Workshops (SPW). -2016. (pp. 29-35). IEEE.

REFERENCES

1 Hashemi, S. Fuzzy, Dynamic and Trust Based Routing Protocol for IoT [Text]. / F. Shams Aliee // Journal of Network and Systems Management. -2020. 28(4), pp.1248-1278.

2 Duffield, N. "Multicast topology inference from measured end-to-end loss" [Text] / J. Horowitz, F. Lo Presti and D. Towsley // IEEE Transactions on Information Theory. -2002. vol. 48, no. 1, pp. 26-45.

3 Wani, A "Ransomware protection in IoT using software defined networking" [Text] / S. Revathi // International Journal of Electrical and Computer Engineering (IJECE). -2020. vol. 10, no. 3, p. 3166.

4 Na, W. "DLTCP: Deep Learning-Based Transmission Control Protocol for Disaster 5G mmWave Networks" [Text] / B. Bae, S. Cho and N. Kim // IEEE Access. -2019. vol. 7, pp. 145134-145144.

5 Vatsala, B. "Performance Evaluation of TCP Variants for IoT Built on Visible Light Communication" [Text] / C. Vidya Raj // Ransomware protection in loT using software defined networking. Int. J. Electr. Comput. Eng. -2020. 10(3), pp.3166-3175.

6 Javanmardi, S. A security driven task scheduling approach for SDN-based IoT– Fog networks / M. Shojafar, R. Mohammadi, A. Nazari, V. Persico, A. Pescapè [Text] // Journal of Information Security and Applications. -2021. 60, p.102853.

7 Trabelsi, Z. IoT based Smart Home Security Education using a Hands-on Approach. [Text] // In 2021 IEEE Global Engineering Education Conference (EDUCON). -2021. (pp. 294-301). IEEE.

8 Yazdinejad, A., Enabling drones in the internet of things with decentralised blockchain-based security [Text] / R.M. Parizi, A. Dehghantanha, H. Karimipour, G. Srivastava, M. Aledhari, // IEEE Internet of Things Journal. -2021. 8(8), pp.6406-6415.

9 Nathi, R.A. Object Secured TCP Socket for Remote Monitoring IoT Devices / D. Zutar // In 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT). -2019. (pp. 1-5). IEEE.

10 Jutila, M. An adaptive edge router enabling internet of things [Text] // IEEE Internet of Things Journal, 3(6). -2016. pp.1061-1069.

11 Shang, W. Challenges in IoT networking via TCP/IP architecture [Text] / Y. Yu, R. Droms, L. Zhang // NDN Project. -2016. (pp. 29-35).

12 Rad, P. Implementation of deep packet inspection in smart grids and industrial Internet of Things: Challenges and opportunities [Text] / K.K.R. Choo // Journal of Network and Computer Applications. -2019. 135, pp.32-46.

13 Ahmad, M. Intrusion detection in internet of things using supervised machine learning based on application and transport layer features using UNSW-NB15 data-set [Text] / Q. Riaz, M. Zeeshan,

H. Tahir, S.A. Haider // EURASIP Journal on Wireless Communications and Networking. -2021(1), pp.1-23.

14 Al-Hawawreh, M. Leveraging deep learning models for ransomware detection in the industrial internet of things environment / E. Sitnikova // In 2019 Military Communications and Information Systems Conference (MilCIS). -2019. (pp. 1-6). IEEE.

15 Davoli, L. An anonymisation protocol for the internet of things [Text] / Y. Protskaya, L. Veltri // In 2017 International Symposium on Wireless Communication Systems (ISWCS). -2019. (pp. 459464). IEEE.

16 Doshi, R. Machine learning ddos detection for consumer internet of things devices [Text] / N. Apthorpe, N. Feamster // In 2018 IEEE Security and Privacy Workshops (SPW). -2016. (pp. 29-35). IEEE.

ТҮЙІН

Соңғы уақытта заманауи IoT жүйелері әртүрлі сатушылардан қосымшалар мен құрылғылардың біркелкі еместігіне сәйкестендіру үшін Transmission Control Protocol (TCP) тәжірибелерінің ашық стандарттарын енгізді. Зерттеу төлемдік бағдарлама шабуылдарының қаупін азайту үшін IoT жүйесінде TCP пакеттерін қадағалау тиімділігін түсінуге бағытталған. Нақтырақ айтқанда, зерттеу IOT-та қолданылатын TCP пакетін қадағалау тиімділігін анықтауға бағытталған. Сонымен қатар, IOT-те TCP бақылау арқылы төлемдік бағдарламалық жасақтама шабуылдарының қаупін азайту тиімділігін зерттеу де осы тергеудің мақсаттарының бірі болды.

Зерттеу нәтижелері IoTSDN-RAN төлемдік бағдарламалық жасақтама шабуылдарының қаупін азайту үшін қолданылатын тиімді бақылау әдісі ретінде дәлелденгенін көрсетеді. Бұл әдіс IoT SVM және IoT ML әдістерімен салыстырғанда тиімді деп танылды. Анықтау, дәлдік және дәлдік тұрғысынан әдіс басқа жиі қолданылатын әдістермен салыстырғанда тиімді екендігі дәлелденді. SVM-дегі міндет қолдау векторларын табу, шабуылдарға белгісіз трафикті жіктеу болып табылады.

IoT күрделі болатынын түсінуі керек, сондықтан олар TCP және төлемдік бағдарламалық жасақтама шабуылдарына қатысты жақсырақ түсінікке ие болуы және TCP салдары арқылы оларды болдырмауы керек. AT пайдаланушыларының TCP салдары маңызды. Бүкіл жүйеде тиімділік пен тиімділікті қамтамасыз ету және төлемдік бағдарламалық жасақтамаға шабуыл жасау қаупі жоқ.

ӘОЖ 658.562.3 ***DOI 10.52578/2305-9397-2023-2-3-190-202***
ҒТАХР 68.75.01

Даутканов Н.Б., техника ғылымдарының кандидаты, **негізгі автор,** https://orcid.org/0000-0001-7864-0217
«Қазақ өңдеу және тамақ өнеркәсібі ғылыми-зерттеу институты» ЖШС, Алматы қ., Гагарин даңғылы, 238 «Г», 050060, Қазақстан, ndautkanov@yandex.ru
Мухаметов А.Е., PhD, https://orcid.org/0000-0002-3615-1869
«Қазақ ұлттық аграрлық зерттеу университеті» КеАҚ, Алматы қ., Абай к., 8, 050010, Қазақстан myhametov_almas@mail.ru
Даутканова Д.Р., техника ғылымдарының докторы**,** https://orcid.org/0000-0002 - 9766-9039
«Қазақ өңдеу және тамақ өнеркәсібі ғылыми-зерттеу институты» ЖШС, Алматы қ., Гагарин даңғылы, 238 «Г», 050060, Қазақстан, dida09@yandex.ru

Dautkanov N.B., candidate of technical science, **the main author**, https://orcid.org/0000-0001-7864-0217
"Kazakh Research Institute of Processing and Food Industry" LLP, Almaty, Gagarin Avenue, 238 "G", 050060, Kazakhstan, ndautkanov@yandex.ru
Mukhametov A.E., PhD, https://orcid.org/0000-0002-3615-1869
Kazakh National Agrarian Research University, Almaty, st. Abay, 8, 050010, Kazakhstan, myhametov_almas@mail.ru
Dautkanova D.R., doctor of technical science, https://orcid.org/0000-0002 - 9766-9039