МРНТИ 81.93.29
УДК 004.056.5

https://doi.org/10.51889/2022-1.1728-7901.09

А.С. Амирова[1], А.Т. Тохметов[1]*

[1]Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Нұр-Сұлтан қ., Қазақстан
**e-mail: whitesilk@mail.ru*

ЗАТТАР ӨНЕРКӘСІПТІК ИНТЕРНЕТІНДЕГІ ҚАУІПТІ АНЫҚТАУДЫҢ АРАЛАС МОДЕЛІ

Аңдатпа

Өнеркәсіптік заттар интернетінің (IIoT) қарқынды дамуымен жылдам әрекет ету, өнеркәсіптік желіге енуді анықтау және алдын алу қажеттілігі туындады. IIoT желілерінің арнайы функциялары бар және кибершабуылдардан қорғануда бірегей қиындықтарға тап болады. Бұл проблемалар әсіресе өзекті болып табылады, өйткені IIoT-ге пайдаланушы сұранысының өсуі болжануда. Мақалада өнеркәсіптік заттар интернетінің қауіпсіздік мәселелері қарастырылады. Қазіргі уақытта мақалада талданған IIoT желілерінде ақпараттық қауіпсіздікті қамтамасыз етудің кейбір әдістері бар. Қолданыстағы жүйелердің артықшылықтары мен кемшіліктері де сипатталған. Индустриалды Интернет желілеріндегі шабуылдың типтік сценарийлері ұсынылды. Осы талдаудың негізінде сараптамалық жүйелерді және шешім ағашы, аңғал Байес классификаторы және k-ең жақын көршілер әдісі сияқты машиналық оқыту алгоритмдерін пайдаланатын біріктірілген қауіптерді анықтау моделі ұсынылады.

Түйін сөздер: заттар өнеркәсіптік Интернеті (IIoT), machine learning алгоритмдері, сараптамалық жүйелер, шабуыл.

Аннотация

А.С.Амирова [1], А.Т.Тохметов[1]
[1]Евразийский национальный университет им. Л. Н. Гумилева, г. Нур-Султан, Казахстан

КОМБИНИРОВАННАЯ МОДЕЛЬ ОБНАРУЖЕНИЯ УГРОЗ В СЕТЯХ ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ

Со стремительным развитием индустриального интернета вещей (IIoT) возникла необходимость быстрого реагирования, обнаружения и предотвращения вторжений в производственную сеть. Сети IIoT обладают особыми функциями и сталкиваются с уникальными проблемами при защите от кибератак. Эти проблемы являются особенно актуальными, поскольку прогнозируется рост потребности пользователей в IIoT. В статье рассматриваются вопросы безопасности промышленного интернета вещей. На данный момент имеются некоторые методики обеспечения информационной безопасности в сетях IIoT, которые были проанализированы в статье. Также были описаны достоинства и недостатки существующих систем. Были предложены типовые сценарии атак в сетях промышленного интернета вещей.

На основе данного анализа предложена комбинированная модель обнаружения угроз с использованием экспертных систем и таких алгоритмов машинного обучения, как дерево решений, наивный байесовский классификатор, метод k- ближайших соседей.

Ключевые слова: промышленный интернет вещей (IIoT), алгоритмы machine learning, экспертные системы, атака.

Abstract

COMBINED MODEL OF THREAT DETECTION IN INDUSTRIAL INTERNET OF THINGS

Amirova A.S.[1], Tohmetov A.T.[1]
[1]L.N. Gumilyov Eurasian national University, Nur-Sultan, Kazakhstan

With the rapid development of the Industrial Internet of Things (IIoT), the need for rapid response, detection and prevention of intrusions into the industrial network has arisen. IIoT networks have special functions and face unique challenges in defending against cyberattacks. These problems are especially urgent as the growth of user demand for IIoT is predicted. The article deals with the security issues of the industrial Internet of things. At the moment, there are some methods of ensuring information security in IIoT networks, which were analyzed in the article. The advantages and disadvantages of existing systems have also been described. Typical attack scenarios in industrial Internet of Things networks were proposed. Based on this analysis, a combined threat detection model using expert systems and such machine learning algorithms as a decision tree, a naive Bayesian classifier, and the k-nearest neighbors method is proposed.

Keywords: industrial Internet of things (IIoT), machine learning algorithms, expert systems, attack.

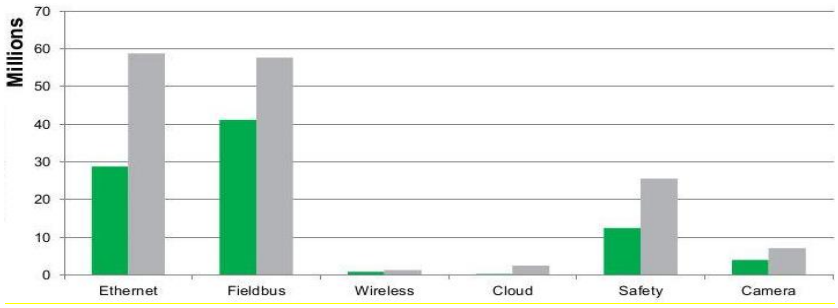
Кіріспе

IIoT өнеркәсіптік ортада IoT технологияларын қолдануды білдіреді. Оны «Индустрия 4.0» деп те атайды, ол - цифрлық және физикалық салаларды біріктіру мүмкіндігіне байланысты неміс тілінде пайда болған термин. IIoT немесе 4.0 индустриясы бұлтты, үлкен деректерді, кибер-физикалық өзара байланыстарды және т.б. қамтиды. Мұнда АТ өнеркәсіптік заттар интернеті шеңберінде физикалық және виртуалды әлемдер бір-бірімен зияткерлік нысандар ретінде үздіксіз әрекеттеседі және байланысады. IIoT – бұл өнеркәсіптік мүмкіндіктерді өзгерте бастайтын көптеген деректерді ұсынатын, барлығы когнитивті құрылғылар мен заттардың желісі. Бұл өндірісті ұлғайту ғана емес, сонымен қатар нақты уақыт режимінде тәулік бойы деректерді беру, ол дұрыс пайдаланылған кезде барлығын өзгертеді.

Positive Technologies баяндамасына сәйкес, 2020 жылы өнеркәсіптік және энергетикалық компанияларға жасалған шабуылдар саны артқан. Осы салалардың кәсіпорындарына қарсы 239 шабуыл жасалды, бұл 2019 жылмен салыстырғанда 91%-ға көп (125 шабуыл). Өнеркәсіпке жасалған әрбір он шабуылдың тоғызында шабуылдаушылар зиянды бағдарламаны пайдаланды. Олардың ішінде төлемдік бағдарламалық қамтамасыз ету шабуылдардың 41%-ын құраса, 25%-да шпиондық бағдарламалар байқалған [1].

Kaspersky компаниясының есебін талдағаннан кейін 2021 жылдың бірінші жартыжылдығында ICS компьютерлерінің шабуылға ұшырау пайызы 33,8%, ол 2020 жылдың екінші жартыжылдығына қарағанда 0,4 проценттік пункте көп екенін көруге болады. [2].

Интернетке қосылған құрылғылардың саны өсуде және озық IoT технологиясын қолдана отырып қосылған Интернетке қол жетімді түйіндердің саны артқан сайын, жақын арада IIoT деңгейі күрт өседі деп күтілуде. 2017 жылғы Өнеркәсіптік коммуникациялар есебіне сәйкес, Интернетке қосылған құрылғылардың саны тек өнеркәсіп секторында 2016 жылы 90 миллионнан аз ғана болады деп болжанған. Бұл жүйелердің көбісі желіге күнделікті қосылатындықтан, төмендегі 1-суретте көрсетілгендей бұл сан 2022 жылға қарай 150 миллионнан асады деп күтілуде [3].



Сурет 1. 2016 жылғы желілік технологиялар бойынша өнеркәсіптік коммуникациялардың әлемдік нарығы және 2022 жылға жоспарланған [3]

Бұл болжам IIoT қауіпсіздігін қамтамасыз етумен байланысты қиындықтарды одан әрі көрсетеді. Қауіпсіз байланыс әдістерінің артықшылығын пайдалану үшін өнеркәсіптік құрылғылардың көп саны тасымалданғанымен, бұл бұрынғы жүйелердің көпшілігі бұрынғыша бұрынғы протоколдарға сүйенеді. Бұл жағдай қоғамның қандай да бір сәйкестендіру немесе аутентификация талаптарының болмауына байланысты олардың тән осалдықтары туралы хабардар болуына қарамастан сақталады.

Дегенмен, IIoT жүйесінде бірқатар күрделі мәселелер бар. Жүйенің күрделілігі ең маңызды мәселе болып табылады, өйткені IIoT операциялары сараланған және құрылғылар арасында икемді интеграция жоқ. Дизайндары, орналастырулары және техникалық қызмет көрсетуі әртүрлі құрылғылар бар, сондықтан бағдарламалық жасақтамадағы немесе аппараттық құралдағы кез келген ақаулар елеулі проблемаларды тудыруы мүмкін. IIoT желісінде аутентификация және қол жеткізуді басқару проблемалары бар, өйткені смарт нысандар әртүрлі платформаларға (аппараттық құралдар мен желілер) негізделген гетерогенді құрылғылар болып табылады. Сонымен қатар, барлық құрылғылар басқа құрылғылармен әртүрлі желілер арқылы байланысуы керек. Осылайша, қауіпсіздік мәселелері ең өзекті мәселе болып табылады, өйткені барлық құрылғылар мен деректер барлық қауіптер мен шабуылдарға ұшырайды. Желіде ауыр зардаптарға әкелетін әртүрлі қауіптер мен шабуылдар бар.

IIoT дамыту үшін киберқауіпсіздіктің деңгейін қамтамасыз ету мәселесі бірден-бір маңызды кедергі болып тұр. Осыған байланысты қызметтерді желілік шабуылдардың әртүрлі түрлерінен қорғау құралдарында қолдануға болатын ең тиімді әдістемені анықтау өзекті мәселе болып табылады. IIoT желілерінде ақпараттық қауіпсіздікті және қауіпті анықтауды қамтамасыз ету үшін қолданылатын бірнеше жүйелер бар. Келесі бөлімде бұл жүйелер толығырақ қарастырылады.

Әдебиет талдау

Бұл бөлімде бар әдебиеттерге шолу жасалады және IIoT қауіпсіздік жүйелері санаттарға бөлінеді. Талдау негізінде мыналарды ажыратуға болады:

- Шабуылдарды анықтау жүйелері (IDS) және шабуылға қарсы шаралар (IPS).
- Машиналық оқыту алгоритмдеріне негізделген жүйелер.
- Сараптамалық жүйелер.
- Қолтаңба әдісіне негізделген жүйелер.

Бастапқыда өнеркәсіптік заттар интернеті, қауіпсіздік, қауіптер, шабуылды анықтау жүйелері (IDS), шабуылға қарсы жүйелер (IPS), машиналық оқыту, сараптамалық жүйелер, қолтаңба әдісі сияқты кілт сөздерді іздеу жүргізілді және жетекші журналдар мен конференциялардағы соңғы мақалаларды жүктеп алынды. Мақала келесі шарттарға сай болуы керек:

- 2015 және 2021 жылдар аралығында жарияланған (қоса алғанда);
- IIoT байланысты қауіпсіздік қатерлерін талдайды.

Шабуылды анықтау және алдын алу жүйелері, сәйкесінше IDS және IPS бүкіл әлем бойынша мыңдаған компьютерлік желілерде орналастырылған жетілген желілік деңгей қорғанысы болып табылады. Шабуылды анықтау жүйелері (IDS) – зиянды әрекет немесе саясат опциялары үшін желіні және/немесе жүйе әрекетін бақылайтын құрылғы немесе бағдарламалық құрал. Шабуылды алдын алу жүйелері (IPS) IDS сияқты талдауды орындайды, бірақ IPS датчиктері басқа желі құрамдастары арасындағы тізбекке ортантылады, олар зиянды әрекетті анықтайды, көрсетілген әрекет туралы ақпаратты журналға түсіреді және әрекетті блоктауға тырысады және хабарлайды. IDS және IPS «брандмауэрден» айырмашылығы – брандмауэр шабуылды болдырмау үшін сырттан бақылайды. Брандмауэрлер шабуылды алдын алу үшін желілер арасындағы қатынасты шектейді және желі ішіндегі шабуыл туралы сигнал бермейді [3].

SIEM жүйелері негізінен корпоративтік желіде орналастырылған әртүрлі желілік қауіпсіздікті қорғау технологиялары (мысалы, шабуылды анықтау жүйелері, брандмауэрлер, меншікті құрылғы шешімдері, операциялық жүйе сислогтары және т.б.) хабарлаған оқиғаларды корреляциялау үшін қауіпсіздік саласында қолданылады. Оқиға корреляциясының нәтижелері қауіпсіздік бар-жоғын көрсетеді.

[4] мақалада DDoS шабуылдарын анықтау және азайту үшін SIEM негізіндегі жүйе ұсынылды. Ұсынылған жүйе пакеттердің белгілі бір түрлерін, соның ішінде осы құрылғылардан келетін TCP SYN, ICMP және DNS пакеттерін бақылау арқылы бұзылған IoT құрылғыларынан DDoS трафигін анықтайды және блоктайды.

[5] мақаласында авторлар SIEM (Қауіпсіздік туралы ақпарат және оқиғаларды басқару), IDS (шабуылды анықтау жүйелері), IPS (шабуылдың алдын алу жүйелері) және ICS брандмауэрлерін жүзеге асыратын IIoT тек желі деңгейіндегі қауіпсіздікке ықпал ететінін айтады. Олар шектік процестер жылдамдық пен қолжетімділікке байланысты болатын OT шабуылдарына қарсы тұрмайды, өйткені мұны осы деңгейлерде жүзеге асыру арқылы шектік процестер арасындағы кідірісті арттыруға болады. Бұзушылықтар орын алғаннан кейін де оларды анықтау, бағалау және түзету тағы бір қиындық.

Ұйым ішіндегі ішкі қауіпті толығымен жоя алатын шешім жоқ сияқты. Бұған қоса, техникалық тәсіл зиянды ішкі қауіптердің алдын алудың және/немесе анықтаудың ең тиімді жолы болмауы мүмкін. SIEM жүйелерінің тиімділігі мен нәтижелігін арттырудың перспективалы тәсілдерінің бірі машиналық оқыту әдістерін пайдалану болып табылады.

Yao және т.б. IIoT үшін жаңа гибридті IDS архитектурасын ұсынды, онда жаңа машиналық оқыту алгоритмі және сәйкесінше төменгі деңгейлі желіде және жоғарғы деңгейлі желіде терең оқыту алгоритмі қолданылады. Олар LightGBM1 машиналық оқытудың жаңа алгоритмін өңделмеген деректердің енуін анықтау және жылдам, бөлінген және жоғары өнімді шешім ретінде қарастырылатын уақытты ұлғайтуға негізделген анықтау дәлдігін жақсарту үшін пайдаланды. градиент өсетін ағаш құрылымы [6].

Aboelwafa және т.б. жалған деректер шабуылдарын (FDI) анықтау үшін қолданылатын машиналық оқыту әдісін ұсынды. Бұл әдіс ауытқуларды анықтауда өте тиімді екендігі дәлелденген нейрондық желінің бір түрі болып табылатын автокодерлерді қолдануға негізделген. Ұсынылған анықтау әдісі SVM негізіндегі әдістермен салыстырғанда жақсырақ анықтау өнімділігін ұсынады [7].

Zolanvari және басқалар өз жұмыстарында қазіргі заманғы машиналық оқыту алгоритмдері қауіпсіздіктің қажетті деңгейін қамтамасыз етпейтін жағдайларды зерттеді, атап айтқанда, IIoT-те теңгерімсіз деректер жинағы мәселесін қарастырды [8]. Қолданыстағы жүйелердің артықшылықтары мен кемшіліктері де сипатталды (Кесте 1).

Кесте 1. Қолданыстағы жүйелердің артықшылықтары мен кемшіліктері

Әдістеме	*Артылықшылықтар*	*Кемшіліктер*
Шабуылдарды анықтау жүйелері (IDS) және шабуылға қарсы шаралар (IPS)	*рұқсатсыз кіру фактілерін анықтау*	*жалған әсер етудің көп болуы*
Машиналық оқыту алгоритмдеріне негізделген жүйелер	*жалған дабылдардың санын азайтады, нәтижелерді түсіндіруді жақсартады*	*ML-модельдерді дұрыс оқыту үшін деректер жиынтығының жеткілікті санының болмауы*
Сараптамалық жүйелер	*осы мақсаттар үшін арнайы әзірленген жаңа математикалық аппаратты тарту арқылы күрделі есептерді шешу мүмкіндігі, жұмыстың жоғары жылдамдығы*	*белгісіз шабуылдарды анықтай алмау, жүйенің білім базасында бекітілген ережелердің толықтығына, дұрыстығына және өзектілігіне тәуелділігі, деректер көлемінің ұлғаюымен жұмыс тиімділігінің төмендеуі*
Қолтаңба әдісіне негізделген жүйелер	*аномальды оқиғалардың белгілі заңдылықтарын анықтау мүмкіндігінше тиімді жүзеге асырылады*	*қолтаңбалардың үлкен дерекқорын пайдалану анықтау жүйесінің жұмысына кері әсер етеді*

Шабуылдың типтік сценарийлерін әзірлеу

Автоматтандырылған процестерді басқару жүйелерінің ақпараттық қауіпсіздігі саласындағы стандарттарды талдау негізінде IIoT-те келесі шабуыл сценарийлері ұсынылды.

1. Контроллер (мысалы, DCS, PLC) мен жетектер арасындағы байланысқа қарсы

Шабуылдың бұл түрі шабуылдаушы кодты енгізген және орындаған немесе бақыланбайтын желіні пайдаланып бұзылған жүйе арқылы деректерді жіберген (манипуляцияланған) кезде орын алады.

Әсері: басқаруды манипуляциялау немесе жоғалту, партияның/өнімнің және инфрақұрылымның зақымдануы.

Қатысты қауіптер: ішкі және сыртқы диверсия, аппараттық және бағдарламалық жасақтаманы манипуляциялау, басқару құрылғысының конфигурациясын манипуляциялау.

2. Датчиктерге қарсы (өлшенген мәндерді/күйлерді өзгерту, оларды қайта конфигурациялау және т.б.)

Өлшеу деректері соңғы құрылғыларда өңделеді, мысалы, сенсорға кіру және оның микробағдарламасын немесе конфигурациясын өзгерту, мысалы, өлшемдерді реттеу, т.б.

Әсері: өңделген деректер негізінде қате оператор шешімдерін қабылдау. Дұрыс емес өлшемдер негізінде процесті жүргізу. Регламентпен қамтылған өлшемдер дұрыс бағаланбайды.

Қатысты қауіптер: ақпаратты өзгерту, саботаж, аппараттық және бағдарламалық құралдарды манипуляциялау, жіберілген сенсор деректерін манипуляциялау.

3. Жетектерге қарсы (олардың күйін басу, конфигурациясын өзгерту)

Жетектердің конфигурациясын/параметрлерін бұрмалау, оларды қате конфигурацияларды, шектерді немесе деректерді пайдалануға, сондықтан олардың қалыпты жұмыс параметрлерін бұзу арқылы олардың қалыпты әрекетіне әсер етеді.

Әсері: ол әсер ететін жетектерге байланысты өзгереді. Ол өндірістік процестерге әсер етуі мүмкін.

Қатысты қауіптер: Аппараттық және бағдарламалық жасақтаманы манипуляциялау, сенсордың/жетегінің істен шығуы немесе дұрыс жұмыс істемеуі, басқару жүйесінің істен шығуы немесе дұрыс жұмыс істемеуі (PLC, RTU, DCS).

4. Желі арқылы берілетін ақпаратқа қарсы

Шабуыл желілік деңгейдегі деректермен манипуляциялауға бағытталған (2,3,4 OSI үлгісінің деңгейі). OSI моделінің 5,6,7 деңгейі деңгейінде, яғни контроллер және басқару жүйесі (DCS, SCADA) деректер мәндері дұрыс болып көрінеді. Манипуляцияны желілік деңгейдегі трафикті бақылау арқылы анықтауға болады.

Әсері: Ол өңделген деректерге байланысты өзгереді. Ол өндіріс процесіне әсер етуі немесе процеске зақым келтіруі мүмкін, мысалы: жарылыс тудыруы мүмкін пеш температурасының манипуляциясы.

Қатысты қауіптер: APT, Man-in-the-Middle шабуылы, саботаж, зиянды бағдарлама.

5. IIoT шлюздеріне қарсы

Шабуылдаушы IIoT шлюзін бұзуға тырысады, бұл бүкіл ортаны бұзуы мүмкін. Әлсіз/осал протоколдар немесе әдепкі құпия сөздер немесе хаттамалар пайдаланылса, бұл өте сәтті болуы мүмкін. Шабуылдың бұл түрі әртүрлі кезеңдерден/фазалардан тұрады және әдетте жасырын түрде іске қосылады. Айта кету керек, шабуылдың бұл түрі құрылғының бүкіл өмірлік циклінде ескерілуі керек.

Әсері: шабуылдаушы желіге және деректерге, соның ішінде құрылғыларға, жүйелерге және желілік жабдыққа қол жеткізе алады. Бұл бүкіл жүйені және оның құрамдас бөліктерін пайдаланудың бірінші кезеңі болуы мүмкін.

Қатысты қауіптер: пароль шабуылдары, эксплуат жинақтары, жеке деректерді теріс пайдалану, зиянды бағдарлама және DDoS.

6. Қашықтан басқару құралының құрылғыларымен манипуляциялау (мысалы, операциялық панельдер, смартфондар)

Шабуылдаушы басқару жүйесінен (үлестірілген орта) алыс орналасқан құрылғыны бұза алады. Көбінесе мұндай құрылғылар жергілікті бақылауға арналған және тұрақты түрде бақыланбайды. Мұндай құрылғыны сатып алу бүкіл желіге ену мүмкіндігіне үлкен қауіп төндіреді, сондай-ақ жабдыққа зақым келтіруі мүмкін, бұл ақпаратты алу үшін көп уақыт қажет, сондықтан зақымдануды ұлғайта алады.

Әсері: жүйеге қол жеткізу және басқару деңгейіне, сонымен қатар инженерлік құралдарға және толық қол жеткізу өзгерістер. Ол IoT ортасына қауіпті өзгерістер тудыруы мүмкін.

Қатысты қауіптер: Құпия сөз шабуылдары, бағдарламалық жасақтаманың осалдықтарын пайдалану, сеанстарды ұрлау, ақпаратты ашу.

7. Қауіпсіздік құралдарының жүйелеріне қарсы (SIS)

Ең қауіпті шабуылдардың бірі, сайып келгенде, қоршаған ортаны, адам өмірін және/немесе компанияларды үлкен қаржылық шығындардан қорғауға тиіс жүйелерге қарсы. Басқару жүйесін иемдену немесе осы жүйемен кез келген манипуляция орнатудың бұзылуына немесе ең аз қауіпті жағдайда әкелуі мүмкін. Мұндай шабуылдың мысалы - жақында болған Тритон шабуылы.

Әсері: SIS жүйесін бұзу, SIS жүйесін манипуляциялау немесе үзу көптеген адамдарға әсер етуі, қоршаған ортаны қорғау мәселелерін тудыруы және тіпті басқа жүйелерге таралуы, олардың жұмысына әсер етуі немесе оларды тіпті өшіруі мүмкін.

Қатысты қауіптер: зиянды бағдарлама, диверсия, қашықтан басқару құралының құрылғыларын манипуляциялау, APT.

8. Зиянды бағдарлама

Бұл шабуылдар желіге таралатын зиянды код арқылы жүзеге асырылады. Ол жәбірленушінің деректеріне қол жеткізуге мүмкіндік береді. Бұл шабуылдар зиянды бағдарламаға негізделгендіктен, осал құрылғыларды жаңарту/патчинг арқылы оларды болдырмауға болады. Мұны IIoT экожүйесінен тыс жерде де жасауға болады. IIoT-ге қатысты мәселе әртүрлі құрылғыларды жаңарту/патч жасау қиындығы болып табылады - олардың кейбіреулері жаңарту немесе түзету мүмкіндігін ұсынбайды.

Әсері: IIoT ішінде зиянды бағдарламалардың көптеген ықтимал мақсаттары бар – шабуылдаушы қыстың ортасында смарт термостатты басқара алады және жылуды қоспай алады немесе ол электр желілерін немесе аурухана жүйелерін және т.б. ұстай алады. адамдардың қауіпсіздігіне қауіп төнеді.

Қатысты қауіптер: пайдалану жинақтары, зиянды бағдарламалар, DDoS, құпия сөз шабуылдары.

9. (IoT) ботнеттерімен DDoS шабуылы

Шабуылдың бұл түрі IIoT құрылғыларының өздеріне бағытталған емес, оның орнына оларды IIoT құрылғыларына емес, басқа құрылғыларға шабуыл жасау үшін пайдаланады. Біріншіден, зиянды бағдарлама осал заттар Интернеті құрылғыларын автоматты түрде тауып, оларды жұқтырады және

оларды ботнетке шақырады, содан кейін оны DDoS шабуылдарын орнату үшін пайдалануға болады, бұл мақсатты серверлерді зиянды трафикпен толтырады.

Әсері: мақсатты құрылғы немесе қызмет зиянды трафикке толып, оны өшіреді.

Қатысты қауіптер: пайдалану жинақтары, DDoS және зиянды бағдарламалар.

10. Бастапқы шабуылдар (мысалы, бұлтқа қарсы)

Шабуылдың бұл түрі жасырын шабуылдарды бастаудың кең таралған тәсілі болып табылады. Оларды жиі желі бұзушылары өздерінің жеке басын жасыру үшін пайдаланады, өйткені олар шабуылдарды өздерінің компьютерлерінен емес, бұрын бұзылған делдалдық хосттардан жасайды.

Әсер ету: Егер шабуылдаушы қадамдық шабуылды бастаса, ол шабуыл командаларын беру үшін оларды баспалдақ ретінде пайдалана отырып, хосттар жиынтығын бұзуы мүмкін.

Қатысты қауіптер: APT, DDoS, зиянды бағдарламалар.

Ұсынылған модель

Әзірленген модель шеңберінде сараптамалық жүйелер мен машиналық оқыту алгоритмдерін біріктіріп пайдалану ұсынылады. Қойылған функционалдық талаптар негізінде әзірленген жүйе қауіпті анықтаудың бірнеше сәтті тәсілдерін біріктіруі керек. Бұған қауіпті анықтаудың әртүрлі алгоритмдерін төмендегідей біріктіру арқылы қол жеткізуге болады. Жиынтықтармен жұмыс істеу тұрғысынан нәтижелерді біріктірудің 4 кең таралған тәсілі бар, бірақ біз 2 негізгісін қарастырамыз, өйткені қалған екеуі ескірген. Ұсынылған модель үшін стандарттар мен сала мамандарының пікірлері негізінде сараптамалық ережелер әзірленді (Кесте 2).

Кесте 2. Сараптамалық ережелер

Ереже	*Ережеге сәйкестік критерийі*	*Сыншылдық дәрежесі*
Құпиялылықты қамтамасыз ету	*Құрылғы өңдейтін деректер көлемінен асып кету*	*Тыйым салынған*
	IIoT ортасында берілетін шифрланбаған жеке деректерді беру	*Тыйым салынған*
Активтерді табу, басқару, бақылау және қызмет көрсету	*Ұйымдық емес және өндірістік активтерді табу және анықтау*	*Тыйым салынған*
	Алынбалы құрылғылар мен USB порттарын пайдалану	*Тыйым салынған*
	IIoT құрылғыларын қауіпсіз/шифрланған әдістерді қолданбай басқарылады (мысалы, HTTPS, SSH)	*Тыйым салынған*
Деректер мен құрылғылардың тұтастығы мен сенімділігін қамтамасыз ету	*Сенімсіз көзден бағдарламалық құралды орнату*	*Тыйым салынған*
	Автоматты жаңарту процедурасын орындау	*Күдікті*
	Стандартты емес қосылу порттарын пайдаланатын жалған IIoT құрылғыларының пайда болуы	*Тыйым салынған*
	Қосымшаның ақ тізіміне қосылмаған қосымшалардың болуы	*Тыйым салынған*
	Басқару немесе өндіріс деңгейіне үшінші тараптың бақылаусыз қол жеткізуі	*Тыйым салынған*
	Жеткізушінің басқару немесе өндіріс деңгейінде жүйеге тікелей қосылуы	*Тыйым салынған*
Қашықтан қол жеткізуді, аутентификацияны, артықшылықтарды, есеп жазбалары және физикалық қол жеткізуді басқаруды қамтамасыз ету	*3-тен астам сәтсіз аутентификацияны орындау*	*Күдікті*
	10-нан астам сәтсіз аутентификацияны орындау	*Тыйым салынған*

Машиналар арасындағы байланыс қауіпсіздігі	*Хосттарға сұраныстардың үлкен санын құру (қысқа уақыт ішінде – 1 минут ішінде – шамамен 1000 хабарлама).*	*Тыйым салынған*
	Минутына шамамен 1000 сұраныс көлемінде типтік емес сұраныстардың үлкен санын құру (TCP Reset, SYN, SYN + FIN жалауларымен).	*Тыйым салынған*
	Сеанстың қалыпты емес аяқталуы.	*Тыйым салынған*

Машиналық оқытудың келесі әдістерін қарастырыңыз: шешім ағаштары (DT) әдістері, аңғал Байес классификаторы (NB) әдісі, k-ең жақын көршілер (k-NN) әдісі.

Шешім ағаштары (DT) әдісі. Әдіс – терминалды емес түйіндер түріндегі сандық атрибуттар мен предикаттарды және терминалдық түйіндер түріндегі класс белгілеулерін қамтитын иерархиялық құрылым. Ағашпен жүргенде векторлық компонент үшін кейбір предикаттың ақиқатына сүйене отырып, екі жолдың бірі таңдалады [9].

Аңғал Байес классификаторы (NB). Бұл бір болжамды қабылдайтын жіктеу әдістерінің тобы: жіктелген деректердің әрбір параметрі класстың басқа параметрлерінен тәуелсіз қарастырылады.

k-ең жақын көршілер (k-NN) әдісі талданатын векторды класс белгісімен байланыстыруға мүмкіндік береді, оның даналары берілген z векторына ең жақын барлық K оқыту нысандарының ішінде ең үлкен саны бар. Бұл әдіс алдын ала конфигурациялауды (жаттығуды) қажет етпейді деп айта аламыз. Оның жұмыс істеуі үшін бүкіл жаттығу үлгісін сақтау жеткілікті [10].

Кешеннің формальды анықтамасына сәйкес біз оның алгоритмдерінің жұмыс нәтижелерінің ықтимал комбинацияларын ұсынамыз:

1) NB классификаторын пайдалана отырып, сараптамалық ережелер мен машиналық оқыту әдістеріне негізделген алгоритмдердің нәтижелерін біріктіру

2) k-NN классификаторын пайдалана отырып, сараптамалық ережелер мен машиналық оқыту әдістеріне негізделген алгоритмдердің нәтижелерін біріктіру

3) DT классификаторын пайдалана отырып, сараптамалық ережелер мен машиналық оқыту әдістеріне негізделген алгоритмдер жұмысының нәтижелерін біріктіру

4) NB жіктеуішін пайдалана отырып, сараптамалық ережелер мен машиналық оқыту әдістеріне негізделген алгоритмдер нәтижелерінің қиылысуы

5) k-NN жіктеуішін пайдалана отырып, сараптамалық ережелер мен машиналық оқыту әдістеріне негізделген алгоритмдер жұмысының нәтижелерінің қиылысуы

6) DT классификаторын пайдалана отырып, сараптамалық ережелер мен машиналық оқыту әдістеріне негізделген алгоритмдер жұмысының нәтижелерінің қиылысуы

2 суретте көрсетілген диаграммаға сәйкес алгоритмдер кешені 4 кезеңнен тұрады:

1-кезең – КЖ желілік белсенділігі туралы деректерді енгізу, олар кейін сарапшылық ережелер мен машиналық оқыту әдістеріне негізделген алгоритмдер енгізуіне беріледі.

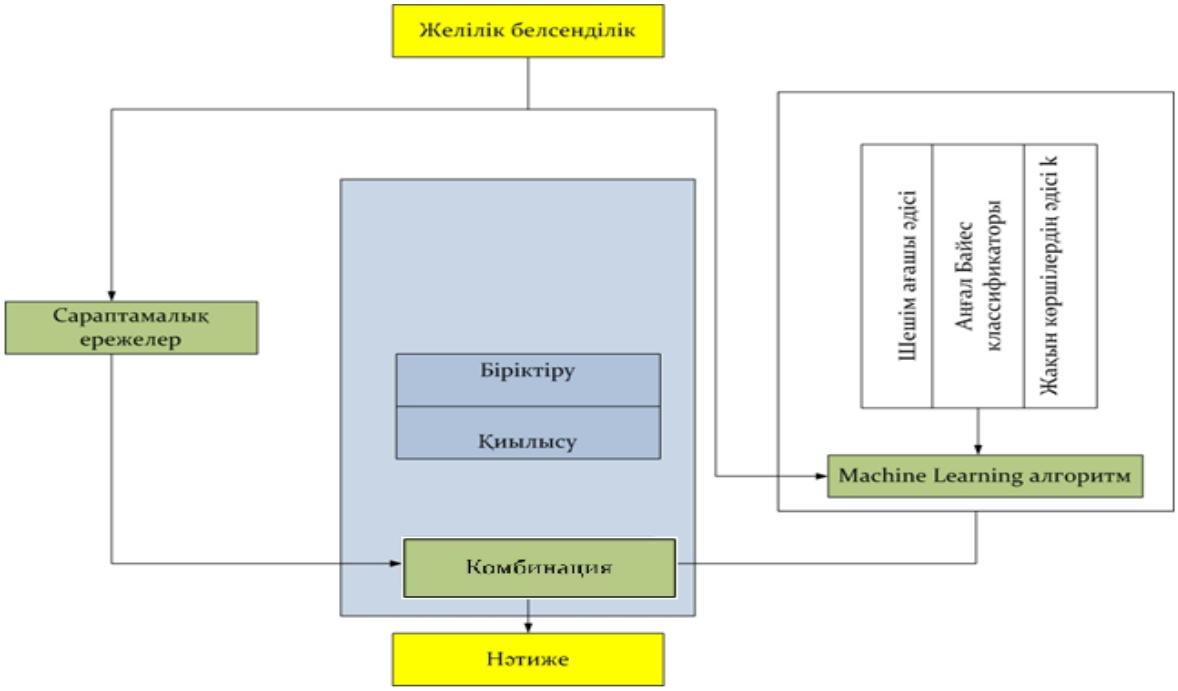
2-кезең – сарапшылық ережелерге негізделген алгоритмді параллель орындау және классификаторлардың әрқайсысы үшін машиналық оқыту әдістеріне негізделген алгоритм вариациялары (1-ші нұсқа).

3-кезең – екі алгоритмнің нәтижелерін әртүрлі тәсілдермен біріктіру (2-ші вариация).

4-кезең – вариациялардың әрқайсысы үшін алгоритмдердің нәтижелерінің жиынын көрсету.

Машиналық оқыту әдістеріне негізделген алгоритмнің дұрыс жұмыс істеуі сәйкес деректер жиынтығымен оқытуға негізделген. Ең қолайлы шешім - интеллектуалдық жүйеге оң және теріс мысалдар жиынтығын ұсынудан тұратын прецеденттерге оқыту болып табылады.

Сараптамалық жүйелер мен машиналық оқыту алгоритмдерін біріктіріп қолдану жалған позитивтердің санын азайтуға, нәтижелерді түсіндіруді жақсартуға және жұмыс жылдамдығын арттыруға тиіс.



Сурет 2. Аралас мөделдің алгоритмі

Қорытынды

Бұл мақалада өнеркәсіптік Интернет желілеріндегі шабуылдарды анықтаудың әртүрлі жүйелері талқыланып, артықшылықтары мен кемшіліктері талданады. Талдау негізінде сарапшылық ережелер мен машиналық оқыту алгоритмдерін біріктіріп қолдану үлгісі ұсынылды. Ұсынылған модель үшін машиналық оқытудың 3 алгоритмі таңдалды: шешім ағаштары (DT), аңғал Байес классификаторы (NB), k-ең жақын көршілер (k-NN).

References:

1 *Industrial IoT Market Research Report. Market Data Forecast, 2020*

2 *Beaumont M., Hopkins B., Newby T. Hardware Trojans – Prevention, Detection, Countermeasures (A Literature Review)// Command Control Communications and Intelligence Div. 2011. № 5, P.56–63.*

3 *Sklyar V., Krachenko V. ENISA Documents in Cybersecurity Assurance for Industry 4.0: IIoT Threats and Attacks Scenarios // 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS) – 2019. – P. 1046-1049, doi: 10.1109/IDAACS.2019.8924452.*

4 *Nakamura E. T., Ribeiro S. L. A Privacy, Security, Safety, Resilience and Reliability Focused Risk Assessment Methodology for IIoT Systems Steps to Build and Use Secure IIoT Systems// the Global Internet of Things Summit (GIoTS) – 2018. – P. 1-6, doi: 10.1109/GIOTS.2018.8534521.*

5 *Purdy M., Davarzan L. The Growth Game-Changer: How the Industrial Internet of Things can drive progress and prosperity// Accenture. 2015. №3. P. 21-26.*

6 *Yao H., Gao P., Zhang P. Hybrid Intrusion Detection System for Edge-Based IIoT Relying on Machine-Learning-Aided Detection. // IEEE Network. 2019. №5, P. 75-81.*

7 *Aboelwafa N., Seddik K. G., Eldefrawy M. H., Gadallah Y. A Machine-Learning-Based Technique for False Data Injection Attacks Detection in Industrial IoT. M // IEEE Internet of Things Journal. 2020. №9, P. 8462-8471.*

8 *Zolanvari M., Teixeira M. A., Jain R. Effect of Imbalanced Datasets on Security of Industrial IoT Using Machine Learningþ //IEEE International Conference on Intelligence and Security Informatics. 2018 P 112-117.*

9 *Navada A., Ansari A. N., Patil S., Sonkamble B. A. Overview of use of decision tree algorithms in machine learning// 2011 IEEE Control and System Graduate Research Colloquium. 2011. P. 37-42, doi: 10.1109/ICSGRC.2011.5991826.*

2 *Vallabh P., Malekian R., Ye N., Bogatinoska D. C. Fall detection using machine learning algorithms // 2016 24th International Conference on Software, Telecommunications and Computer Networks (SoftCOM). – 2016. – P. 1-9, doi: 10.1109/SOFTCOM.2016.7772142.*