https://doi.org/10.53360/2788-7995-2025-3(19)-14

МРНТИ: 81.93.29

Н.А. Бажаев[1,2], А.К. Шайханова[1*], Д.Ж. Сатыбалдина[1], К.С. Бакенова[1]
[1]Л.Н. Гумилев атындағы Еуразия ұлттық университеті,
010000, Қазақстан Республикасы, Астана қ., Қ. Сәтпаев көшесі, 2
[2]«Мемлекеттік техникалық қызмет» акционерлік қоғамы,
010000, Қазақстан Республикасы, Астана қ., Мәңгілік Ел даңғылы, 55 В
*e-mail: shaikhanova_ak@enu.kz

IEEE 802.15.4 ЖЕЛІЛЕРІНДЕ ҚАУІПСІЗДІКТІ ҮЗДІКСІЗ МОНИТОРИНГІЛЕУДІҢ ЗИЯТКЕРЛІК ӘДІСІ АДАПТИВТІ АНОМАЛИЯЛАР ТАЛДАУЫ НЕГІЗІНДЕ

Аңдатпа: *IEEE 802.15.4 стандарты бойынша сымсыз желілердің қауіпсіздігін қамтамасыз ету – Заттар интернетін (IoT) дамытудың негізгі міндеттерінің бірі болып табылады. IoT құрылғыларының есептеу ресурстары шектеулі болғандықтан, криптографиялық механизмдерге және детерминирленген шектерге негізделген дәстүрлі шабуылдарды анықтау әдістері әрдайым қажетті қорғаныс деңгейін қамтамасыз ете бермейді.*

Осы зерттеуде трафикті желілік мониторингтеудің жаңа бейімделмелі әдісі ұсынылады. Бұл әдіс үлгі көлемін ескеретін түрлендірілген Z-бағалауды және шабуыл ықтималдығын динамикалық түрде түзететін бейімделмелі Байес классификаторын біріктіреді. NS-3 ортасында генерацияланған деректер негізінде жүргізілген эксперименттік сынақтар ұсынылған әдістің шабуылдарды анықтау дәлдігі бойынша дәстүрлі тәсілдерден асып түсетінін көрсетті: жалған іске қосу көрсеткіші 10.9%-дан 3.8%-ға дейін төмендеді.

Ұсынылған гибридтік модель 94.7% классификация дәлдігін және 91.8% шабуылды анықтау толықтығын қамтамасыз етеді, бұл стандартты Байес классификаторымен салыстырғанда 6.3%-ға жоғары. Алынған нәтижелер IoT желілерінің қауіпсіздігін нақты уақыт режимінде бақылау жүйелерінде бұл әдісті қолданудың болашағы зор екенін көрсетеді. Дамытылған тәсіл желілік ортаның өзгеруіне бейімделуге мүмкіндік береді және кездейсоқ флуктуациялардың әсерін азайтады, бұл оны энергияны аз тұтынатын желілерді қорғауға арналған тиімді шешім етеді.

Түйін сөздер: *Ақпараттық қауіпсіздік, дербес желілер, IEEE 802.15.4, IoT, шабуылды анықтау, Z-бағалау, Байес классификаторы, машиналық оқыту, желіні мониторингтеу.*

1 Кіріспе

Қазіргі заманғы Заттар интернеті (IoT) технологиялары қарқынды дамып келеді, бұл көптеген зияткерлік құрылғылардың сымсыз өзара әрекеттесуін қамтамасыз етеді. Энергияны аз тұтынатын IoT-желілерінің негізінде жатқан негізгі стандарттардың бірі – ZigBee, 6LoWPAN және WirelessHART сияқты протоколдарда қолданылатын IEEE 802.15.4 стандарты. Бұл технологиялар өнеркәсіптік автоматтандыруда, ақылды қалаларда, қашықтан бақылау жүйелерінде және денсаулық сақтау саласында кеңінен қолданылады [1]. Алайда құрылғылар санының өсуі мен желі топологиясының күрделене түсуі ақпараттық қауіпсіздік саласында айтарлықтай сын-қатерлер туындатады.

IoT сымсыз желілерінің қауіпсіздігін қамтамасыз етудегі ең маңызды аспектілердің бірі – мәліметтердің құпиялылығын, тұтастығын және қолжетімділігін (CIA) қорғау болып табылады. Құрылғылардың жеткіліксіз қорғалуы мен сенімді мониторинг механизмдерінің болмауы IEEE 802.15.4 желілерін қызмет көрсетуден бас тарту (DoS), жалған пакеттерді енгізу, сәйкестендіру деректерін қолдан жасау және трафикті талдау сияқты түрлі шабуылдарға осал етеді [2]. Мұндай шабуылдар IoT-инфрақұрылымының жұмысын бұзып қана қоймай, сонымен қатар құпия ақпараттың таралуына әкелуі мүмкін, бұл әсіресе өнеркәсіптік және медициналық қолданбалар үшін өте маңызды.

Қауіпсіздікті қамтамасыз етуге арналған қазіргі қолданыстағы тәсілдер, оның ішінде криптографиялық әдістер, желілік мінез-құлықты талдау және машиналық оқыту алгоритмдері бірқатар шектеулерге ие. Атап айтқанда, трафикті мерзімді талдау шабуылдарды дер кезінде анықтауға әрдайым мүмкіндік бермейді, ал есептеу шығындарының жоғары болуы ресурстары шектеулі құрылғылардың жұмыс істеу қабілетіне кері әсерін тигізуі мүмкін [3]. Бұдан бөлек, статикалық қауіпсіздік саясаты желідегі динамикалық өзгерістерді ескермейді, бұл олардың тиімділігін төмендетеді [4].

Осы зерттеуде IEEE 802.15.4 желісінің жағдайын тұрақты бақылауға арналған әдістеме ұсынылады. Бұл әдіс трафик параметрлерін статистикалық талдауға және құрылғылар арасындағы өзара әрекеттестікке мінез-құлықтық аналитика жүргізуге негізделген. Әзірленіп жатқан модель деректерді беру процесіндегі ауытқуларды анықтауға бағытталған, бұл ықтимал қауіптерді көрсетуі мүмкін. Зерттеудің негізгі мақсаты – аномалияларды бейімделмелі түрде анықтай алатын және нақты уақыт режимінде жұмыс істей алатын, бірақ көп есептеу ресурстарын қажет етпейтін механизм құру арқылы IoT-желілерінің шабуылдарға төзімділігін арттыру [5].

2 Міндет қою

Зерттеу IEEE 802.15.4 желілерін қорғаудың қолданыстағы механизмдерінің тиімділігінің төмендігі мәселесін шешуге бағытталған. Бұл мәселе желілік белсенділіктегі өзгерістерді жеткілікті деңгейде бақылаудың болмауымен байланысты. Ғылыми шешімді қажет ететін негізгі сын-қатерлерге шабуылдарды дер кезінде анықтау қажеттілігі, жалған іске қосылуларды азайту, желінің динамикалық жағдайларына бейімделу және IoT тораптарындағы есептеу жүктемесін төмендету жатады [6].

Қойылған мақсатқа қол жеткізу үшін келесі міндеттерді орындау қажет:

IEEE 802.15.4 желілеріндегі бар осалдықтарды егжей-тегжейлі талдау, ең жиі кездесетін шабуыл түрлерін анықтау және бұзушылар жүйені бұзу үшін қолданатын трафиктің негізгі параметрлерін айқындау [7].

Желілік белсенділікті талдауға арналған әдістеме әзірлеу, ол деректер ағынының статистикалық сипаттамаларына және желі тораптарының мінез-құлқына негізделіп, қалыпты жұмыс істеуден ауытқуларды анықтауға мүмкіндік береді.

Желілік трафиктің ықтималдық сипаттамаларын және құрылғылар арасындағы өзара әрекеттестіктерді ескере отырып, аномалияларды анықтауға арналған математикалық модель құру [8].

Ұсынылған әдісті нақты IoT құрылғыларында эксперименттік зерттеу, оның тиімділігін, шабуылдарды анықтау дәлдігін және есептеу күрделілігін бағалау.

IoT-тың қолданыстағы қауіпсіздік жүйелеріне ұсынылған әдісті біріктіру бойынша ұсыныстар әзірлеу, бұл олардың киберқауіптерге төзімділігін арттыруға мүмкіндік береді.

Зерттеудің күтілетін нәтижесі – есептеу шығындарын айтарлықтай арттырмай, нақты уақыт режимінде қауіптерді анықтай алатын IEEE 802.15.4 желілерін мониторингтеудің бейімделмелі механизмін жасау. Дайындалған модель шабуылдарды анықтау дәлдігі мен жалған іске қосылу деңгейінің төмендігі арасындағы теңгерімді қамтамасыз етуі тиіс, бұл оны IoT қолданбаларының кең ауқымында қолдануға мүмкіндік береді.

3 Ұсынылатын әдіс

IEEE 802.15.4 стандарты бойынша сымсыз желілердің қауіпсіздік деңгейін арттыру үшін осы жұмыста модификацияланған Z-бағалау мен бейімделмелі Байес классификаторы негізіндегі гибридті шабуылдарды анықтау әдісі ұсынылады. Ұсынылған тәсілдерді қолдану аномалияларды анықтау дәлдігін арттырып, жалған іске қосылулар санын минимизациялауға және желідегі динамикалық өзгерістерге жүйені бейімдеуге мүмкіндік береді.

1. Модификацияланған Z-бағалау аномальды пакет-терді анықтау үшін:

Z-бағалау – деректердегі статистикалық ауытқушылықтарды анықтаудың негізгі құралы. Классикалық тұр-де (1) ол былай есептеледі:

$$Z = \frac{X-\mu}{\sigma} \quad (1)$$

мұндағы: X – ағымдағы өлшенген мән,
μ – таңдаманың орташа мәні,
σ – стандартты ауытқу.

Дегенмен дәстүрлі Z-бағалау таңдаманың көлемі N-ді ескермейді, бұл оны шағын деректер пакеттерін талдағанда тұрақсыз етеді. IEEE 802.15.4 сымсыз желілерінде берілетін деректер көлемі жүктеме мен белсенді тораптардың санына байланысты айтарлықтай өзгеруі мүмкін. Осы факторларды ескеру үшін модификацияланған (2) Z-бағалау енгізіледі:

$$Z' = \frac{X-\mu}{\sigma} \times \frac{1}{1+\frac{1}{\sqrt{N}}} \quad (2)$$

Бұл әдістемелік тәсіл мына мүмкіндіктерді береді:

– Шағын таңдамалардың әсерін азайту – N аз болған жағдайда түзету коэффициенті $\frac{1}{1+\frac{1}{\sqrt{N}}}$ Z-бағалаудың кенет өзгерістерін төмендетеді.

– Динамикалық түрде өзгеретін IoT-желілерінде аномалияларды тұрақты анықтауды қамтамасыз ету.

– Кішкентай таңдамалардағы статистикалық ауытқулардан туындайтын жалған дабылдар санын азайту.

Классикалық статистикада Z-бағалау мәндері 2 немесе 3-тен жоғары болса, олар аномалия деп есептеледі. Алайда біздің әдістемемізде шек желідегі деректердің өзгергіштігіне байланысты динамикалық түрде орнатылады. Бұл құрылғылардың мінез-құлқын нақты уақыт режимінде ескере отырып, қате дабылдардың пайда болу ықтималдығын төмендетеді.

2. Шабуыл ықтималдығын бағалау үшін бейімделмелі Байес классификаторы: Байес классификаторы келіп түсетін деректер негізінде шабуыл ықтималдығы P(A|X) есептеу үшін қолданылады. Классикалық түрде (3) формуласын қолданады:

$$P(A|X) = \frac{P(X|A)P(A)}{P(X)} \quad (3)$$

мұндағы: *P(A/X)* – байқалған аномалияның шабуылмен байланыстылығы ықтималдығы,
P(X/A) – Шабуыл болған жағдайда X бақылау ықтималдығы,
P(A) – Шабуылдың апріогі ықтималдығы,
P(X) – Деректерде X-тің пайда болу ықтималдығы.

Алайда бұл модель ауытқулардың маңыздылығын есепке алмайды, сондықтан ол маңызды шабуылдарға әлсіз сезімтал болады [9]. Осы кемшілікті жою үшін бейімделмелі салмақ енгізіледі (4):

$$P(A|X) = \frac{P(X|A)P(A)}{P(X)} \times W(X) \quad (4)$$

мұндағы: *W(X)* – Z-бағалауға байланысты салмақ коэффициенті.

2.1 Салмақтардың динамикалық жаңартылуы: W(X) мәні ауытқушылық дәрежесі Z-ге байланысты түзетіледі (5):

$$W(X)\begin{cases} 1, \text{ егер } |Z'| < 2, \\ 1.5, \text{ егер } 2 \le |Z'| < 3, \\ 2, \text{ егер } |Z'| \ge 3. \end{cases} \quad (5)$$

Бұл механизм:

Маңызды ауытқулардың шабуыл ықтималдығына әсерін күшейтуге мүмкіндік береді.

Трафиктің елеусіз тербелістеріне сезімталдықты төмендетеді.

IoT-желісінің өзгермелі орта жағдайларына бейімделуді қамтамасыз етеді [10].

IEEE 802.15.4 желісінде қауіп-қатерлерді анықтау алгоритмі:

Өзіміз ұсынған шабуылдарды анықтау әдісі желілік трафикті статистикалық талдау мен бейімделмелі Байес классификаторы негізінде нақты уақыт режимінде жұмыс істейді және келесі кезеңдерді қамтиды:

– Деректерді жинау. Белгіленген уақыт аралығында желілік трафик мониторингі жүргізіледі. Әр пакет үшін көлемі, уақыт таңбалары, жіберушілер мен алушылар және қолданылатын протоколдар секілді негізгі параметрлер тіркеледі.

– Модификацияланған Z-бағалауды есептеу. Әр пакеттің желінің қалыпты мінез-құлқынан ауытқуын, таңдаманың көлеміне бейімделген түзету коэффициенті арқылы анықтаймыз. Бұл ықтимал аномалияларды көрсетіп, кездейсоқ флуктуациялардың әсерін азайтуға мүмкіндік береді.

– Шабуыл ықтималдығын бағалау. Алынған Z-бағалау негізінде пакет аномалия дәрежесіне сәйкес шабуыл ықтималдығын түзететін бейімделмелі Байес классификаторы қолданылады.

– Шешім қабылдау. Егер апостериорлық шабуыл ықтималдығы P(A|X)P(A | X)P(A|X) алдын ала орнатылған шек *T*-дан асса, жүйе шабуыл бар екенін тіркеп, тиісті жауап шараларын іске қосады. Әйтпесе, мониторингті жалғастырып, дабыл шығармайды.

– Параметрлерді бейімдеу. Жүйе жұмыс барысында шекті мәндер мен классификатор салмақ коэффициенттерін динамикалық түрде жаңартып, желі ортасының өзгеруіне бейімделеді.

Ұсынылған алгоритм жоғары шабуылдарды анықтау дәлдігі мен төмен жалған дабылдар деңгейін қамтиды [11], бұл оны IEEE 802.15.4 сымсыз желілерін қорғауда тиімді шешім етеді.

3. Ұсынылған әдістің артықшылықтары:

Дәстүрлі шабуылды анықтау әдістерімен салыстырғанда, әзірленген тәсіл бейімделгіштігі, жоғары дәлдігі және желідегі динамикалық өзгерістерге төзімділігі арқасында бірқатар маңызды артықшылықтарға ие.

Икемділік. Әдіс таңдаманың көлемін және трафик сипаттамаларының өзгеруін ескере отырып, шабуылды анықтау параметрлерін нақты уақыт режимінде түзетуге мүмкіндік береді.

Бейімделгіштік. Динамикалық салмақ коэффициенті бар Байес классификаторы пакеттердегі аномалия дәрежесіне қарай шабуыл ықтималдығын реттеп, қауіп-қатерді дәл анықтауды қамтамасыз етеді.

Жалған дабылдарды азайту. Z-бағалауға түзеткіш көбейткіш енгізу желілік трафиктің кездейсоқ флуктуацияларының әсерін төмендетеді, бұл жоғары вариативті деректері бар сымсыз IoT-желілерінде аса маңызды.

Жоғары сезімталдық. Бейімделгіш Байес классификаторы критикалық шабуылдардың маңыздылығын күшейтіп, жүйеге есептеу ресурстарын айтарлықтай арттырмай-ақ ықтимал қауіп-қатерлерге дер кезінде әсер етуге мүмкіндік береді.

4. Қазіргі заманғы машиналық оқыту әдістерімен байланысы:

Әзірленген әдістемелік амал аномалияларды анықтау және желілік қауіпсіздік жүйелерінде қолданылатын қазіргі заманғы интеллектуалды деректерді талдау әдістерімен тығыз байланысты:

– Адаптивті кездейсоқ ормандар (Adaptive Random Forests). Шабуылдарды анықтау параметрлерін динамикалық түрде жаңартып отыруға қолданылады, бұл өзгермелі орта жағдайларын ескеруге мүмкіндік береді..

– Градиенттік бустинг (Gradient Boosting). Желі трафигінің өзгерістерімен байланысты белгілердің маңыздылығын автоматты түрде түзету үшін қолданылады; бұл біздің бейімделмелі Байес классификаторындағы салмақты түзетуге ұқсас.

– Уақыттық қатарларды статистикалық сүзу әдістері. Таңдаманың көлемін ескере отырып, шынымен тыс мәндерді түзету жұмысын қамтиды, бұл модификацияланған Z-бағалаудағы тәсілге параллель.

Желілік қауіпсіздік аясында осындай әдістерді пайдалану модельді жиі қайта оқытпай-ақ жаңа шабуылдарға бейімделетін интеллектуалды қорғаныс механизмдерін жасауға мүмкіндік береді. Әзірленген тәсіл адаптивті статистикалық әдістер мен ықтималдық моделдеудің артықшылықтарын үйлестіріп, жоғары дәлдік, сенімділік және есептеу тиімділігін қамтамасыз етеді, бұл оны нақты сымсыз IoT-желілерінде қолдануға үмітті етеді [12].

4 Эксперимент жүргізу

Эксперимент ұсынылған шабуылдарды анықтау әдісінің IEEE 802.15.4 сымсыз желілерінде тиімділігін тексеруге бағытталды. Зерттеу барысында анықтау дәлдігі, толықтық (recall), ерекшелік (specificity) және жалған срабатываниелер коэффициенті талданды.

Ұсынылған тәсілді верификациялау үшін IEEE 802.15.4 желілерін модельдеу үшін бейімделген NS-3 симуляциялық ортасы құрылды. Симуляцияға 50 торап қатысты, AODV протоколы қолданылды, орташа беру жылдамдығы 250 Кбит/с болды. Аномалияларды бағалау үшін қарастырылған терезе ұзындығы – 1000 пакет. Шабуылдарды модельдеу үшін желінің тұтастығына, құпиялылығына және қолжетімділігіне бағытталған ең таралған сценарийлер қолданылды: селективті глушение, флудинг және кадрларды подмена [13]. Жалпы 50 000 пакет өңделді, оның 15%-ында әдісті сынау мақсатында енгізілген шабуылдар болды.

Таңдаманың параметрлері (1 сурет):

Timestamp – пакетті жіберу уақыт таңбасы.

Packet_Size – пакет көлемі (байтпен).

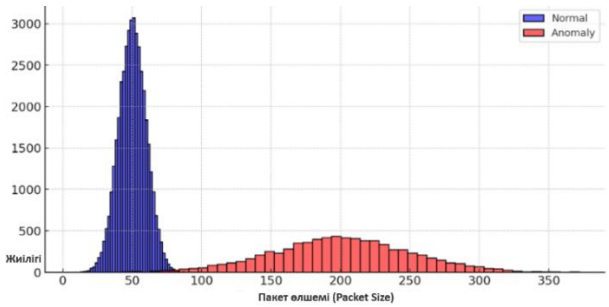
Source_IP – жіберушінің IP-мекенжайы.

Destination_IP – алушының IP-мекенжайы.

Protocol – протокол түрі (TCP, UDP, ZigBee).

Anomaly_Score – аномалия дәрежесінің көрсеткіші (модификацияланған Z-бағалау).

Label – пакет түрі («Normal» немесе «Anomaly»).



Сурет 1 – Қалыпты және аномальды трафик үшін пакет көлемдерінің таралымы

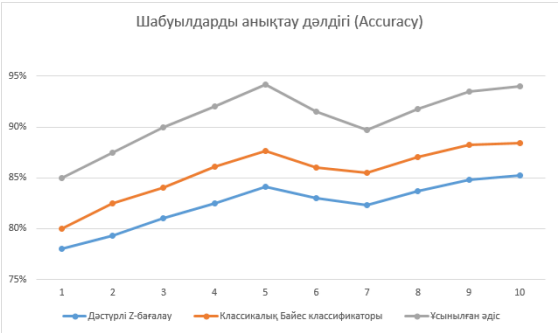
– Пакет өлшемдерінің таралуы – аномальды пакеттердің (қызыл) өлшемі қалыпты пакеттерге (көк) қарағанда әлдеқайда үлкен екенін көрсетеді.

– Трафикті салыстыруға арналған Boxplot – қалыпты және аномальды пакеттер арасындағы медиандық мәндер мен шеткі мәндердің айырмашылығын көрсетеді.

– Протоколдардың таралуы – деректер жиынтығындағы TCP, UDP және ZigBee протоколдарының қолданылу жиілігін көрсетеді.

– Трафиктегі аномалиялардың үлесі – пакеттердің 15%-ы аномальды деп белгіленген (қызыл сектор).

Ұсынылған әдістің тиімділігін бағалау дәстүрлі Z-бағалауымен және бейімделусіз классикалық Байес классификаторымен салыстыру арқылы жүргізілді. Әрбір тәсіл үшін дәлдік, толықтық, спецификалық және жалған іске қосылу коэффициенті есептелді. Эксперимент барысында 10 минут бойы желілік трафик тіркеліп, әрбір пакет үшін динамикалық түзетуді ескеретін модификацияланған Z-бағалау есептелді, адаптивті Байес классификаторы негізінде шабуыл ықтималдығы анықталды және болжанған мәндердің нақты деректер белгілеріне сәйкестігі тексерілді (2 сурет).



Сурет 2 – Тарификтегі аномалиялардың ұсынылған әдісті қолданғанда жіктеудің дәлдігі

Алынған нәтижелерді талдау көрсеткендей, ұсынылған шабуылдарды анықтау әдісі базалық тәсілдермен салыстырғанда жоғары көрсеткіштер көрсетті. Эксперименттік деректерге сәйкес, ұсынылған әдісті қолдану кезінде классификация дәлдігі 94.7% құрады, бұл классикалық Байес классификаторынан 6.3%-ға және дәстүрлі Z-бағалауынан 9.5%-ға жоғары. Шабуылдарды анықтау толықтығы 91.8% болды, бұл әдістің желілік түйіндердің мінез-құлқындағы ауытқуларға жоғары сезімталдығын көрсетеді. Әдістің спецификалығы 96.2%-ға жетті, бұл жалған дабылдарды барынша азайту қабілетін білдіреді. Сонымен қатар, жалған іске қосылу коэффициенті дәстүрлі Z-бағалаудағы 10.9%-дан ұсынылған әдісте 3.8%-ға дейін төмендеді (1-кесте), бұл оның кездейсоқ ауытқуларға төзімділігін дәлелдейді.

Кесте 1 – Ұсынылған әдіс пен салыстырылған әдістердің нәтижелері

Әдіс	Шабуылдарды анықтау дәлдігі (Accuracy)	Толықтық (Recall)	Ерекшелік (Specificity)	Жалған іске қосылу коэффициенті (FPR)
Дәстүрлі Z-бағалау	85.2%	78.6%	89.1%	10.9%
Классикалық Байес классификаторы	88.4%	82.1%	90.5%	9.5%
Ұсынылған әдіс	94.7%	91.8%	96.2%	3.8%

Бейімделетін салмақ коэффициентін Байес классификаторына енгізу шабуылдарды анықтау сапасын жақсартуға ықпал ететіні қосымша талдау нәтижесінде анықталды, себебі бұл әдіс ауытқулардың маңыздылығын ескере отырып, ықтималдықтарды динамикалық түрде түзетуге мүмкіндік береді. Таңдаманың көлеміне тәуелділікті модификацияланған Z-бағалауға қосу шудың деңгейін төмендетіп, болжамдардың дәлдігін арттырды [14].

Осылайша, эксперимент нәтижелері ұсынылған тәсілдің тиімділігін растайды. Модификацияланған Z-бағалау мен бейімделетін Байес классификаторына негізделген гибридті модель шабуылдарды анықтаудың жоғары дәлдігін, жалған іске қосылу деңгейінің төмендігін және желінің өзгермелі жұмыс жағдайларына бейімделу қабілетін көрсетеді. Әзірленген әдіс IEEE 802.15.4 желілерінің қауіпсіздігін бақылау үшін келешегі зор шешім болып табылады және деректердің құпиялылығына, тұтастығына және қолжетімділігіне қауіп төндіретін шабуылдардан сымсыз Интернет заттар жүйелерін қорғауға қолданылуы мүмкін.

5 Қорытынды

Осы жұмыста IEEE 802.15.4 стандарты бойынша сымсыз желілердегі шабуылдарды анықтауға арналған әдіс әзірленді. Бұл әдіс модификацияланған Z-бағалау мен бейімделетін Байес классификаторын біріктіреді. Ұсынылған тәсілдің басты артықшылығы – желілік трафик параметрлерінің өзгеруіне динамикалық бейімделу қабілеті, бұл қауіптерді анықтау дәлдігін арттыруға және жалған дабылдардың санын азайтуға мүмкіндік береді [15]. Z-бағалауға таңдаманың көлеміне байланысты түзетуді енгізу кездейсоқ ауытқулардың әсерін азайтады, ал Байес классификаторындағы салмақ функциясы жүйенің маңызды аномалияларға реакциясын күшейтеді.

Эксперименттік нәтижелер ұсынылған әдістің стандартты тәсілдерден артықшылығын көрсетті. Орташа классификация дәлдігі – 94,7%, шабуылды анықтау толықтығы – 91,8%, ерекшелігі – 96,2%, ал жалған іске қосылу коэффициенті 3,8%-ға дейін төмендеді, бұл дәстүрлі Z-бағалауға қарағанда 2,5 есе жақсы. Графикалық талдау қалыпты және аномальды трафиктің мінез-құлқындағы айтарлықтай айырмашылықты растады, бұл таңдалған талдау әдістерінің тиімділігін дәлелдейді.

Әзірленген әдістеме IoT-желілердің қауіпсіздігін бақылау жүйелерінде қолдануға жарамды, бұл жерде шабуылдарды жоғары дәлдікпен және минималды есептеу шығындарымен анықтау аса маңызды. Болашақта бұл модельді машиналық оқыту әдістерін қолдана отырып кеңейтуге болады, бұл шекті мәндерді автоматты түрде реттеуге және күрделі шабуылдарды болжауға мүмкіндік береді.

Әдебиеттер тізімі

1. Security and Privacy in the Industrial Internet of Things: Current Standards and Future Challenges / T. Gebremichael et al // IEEE Access. – 2020. – Vol. 8. – P. 152351-152366.
2. Sadikin F. ZigBee IoT Intrusion Detection System: A Hybrid Approach with Rule-based and Machine Learning Anomaly Detection / F. Sadikin, S. Kumar // Proc. of Int. Conf. on Security. – 2020. – P. 57-68.
3. Choudhary S. Internet of Things: Protocols, Applications and Security Issues / S. Choudhary, G. Meena // Procedia Computer Science. – 2022.
4. Kampourakis V. A systematic literature review on wireless security testbeds in the cyber-physical realm / V. Kampourakis, V. Gkioulos, S. Katsikas // Computers & Security. – 2023. – URL: https://www.sciencedirect.com/science/article/pii/S0167404823002936.
5. Ullah I. A two-level flow-based anomalous activity detection system for IoT networks / I. Ullah, Q.H. Mahmoud // Electronics. – 2020. – Vol. 9, № 3. – URL: https://www.mdpi.com/2079-9292/9/3/530.
6. Murugesan K.V.N. Comprehensive Security Analysis and DoS Attack Mitigation in Thread Networks / K.V.N. Murugesan, T. Master // Proc. IEEE WCNC. – 2025. – P. 1-7.
7. Morillo Fuetala D.G. Detecting targeted interference in the Internet of Things / D.G. Morillo Fuetala. – University College Cork, 2024.
8. Aljohani R. AI-Based Intrusion Detection for a Secure Internet of Things (IoT) / R. Aljohani, A. Bushnag, A. Alessa // Journal of Network and Systems Management. – 2024. – Vol. 32. – Art. 56.
9. A Survey on IoT Ground Sensing Systems for Early Wildfire Detection / C.C. Chan et al // IEEE Access. – 2024. – Vol. 12. – P. 172785-172819.
10. Kumari T.A. Tachyon: Enhancing stacked models using Bayesian optimization for intrusion detection / T.A. Kumari, S. Mishra // Egyptian Informatics Journal. – 2024. – Vol. 27. – Art. 100520.

11. Khayyat M.M. Improved bacterial foraging optimization with deep learning based anomaly detection in smart cities / M.M. Khayyat // Alexandria Engineering Journal. – 2023. – Vol. 75. – P. 407-417.
12. Sorostinean R. Anomaly Detection in Smart Industrial Machinery Through Hidden Markov Models and Autoencoders / R. Sorostinean, Z. Burghelea, A. Gellert // IEEE Access. – 2024. – P. 1-1.
13. Isong B. Insights into Modern Intrusion Detection Strategies for IoT Ecosystems / B. Isong, O. Kgote, A. Abu-Mahfouz // Electronics. – 2024. – Vol. 13. – Art. 2370.
14. Energy-aware and self-adaptive anomaly detection scheme based on network tomography / W. Wang et al // Information Sciences. – 2013. – Vol. 220. – P. 580-602.
15. Identification of Attacks against Wireless Sensor Networks Based on Behaviour Analysis / V. Korzhuk et al // Journal of Wireless and Ubiquitous Computing. – 2019. – Vol. 10, № 2. – P. 1-21.

Алғыс білдіру

Бұл зерттеу Қазақстан Республикасы Ғылым және жоғары білім министрлігінің Ғылым комитетінің қаржылық қолдауымен орындалды (грант № AP25794699).

Н.А. Бажаев[1,2], А.К. Шайханова[1*], Д.Ж. Сатыбалдина[1], К.С. Бакенова[1]
[1]Евразийский национальный университет им. Л.Н. Гумилева,
010000, Республика Казахстан, г. Астана, улица К. Сатпаева, 2
[2]АО «Государственная техническая служба»,
010000, Республика Казахстан, г. Астана, проспект Мангилик Ел, 55 В
*e-mail: shaikhanova_ak@enu.kz

ИНТЕЛЛЕКТУАЛЬНЫЙ МЕТОД ПОСТОЯННОГО МОНИТОРИНГА БЕЗОПАСНОСТИ В СЕТЯХ IEEE 802.15.4 НА ОСНОВЕ АДАПТИВНОГО АНАЛИЗА АНОМАЛИЙ

Обеспечение безопасности беспроводных сетей стандарта IEEE 802.15.4 является одной из ключевых задач в развитии Интернета вещей (IoT). Учитывая ограниченные вычислительные ресурсы IoT-устройств, традиционные методы обнаружения атак, основанные на криптографических механизмах и детерминированных порогах, не всегда обеспечивают достаточный уровень защиты. В данной работе предлагается новый метод адаптивного мониторинга сетевого трафика, который сочетает модифицированную Z-оценку с учетом размера выборки и адаптивный Байесовский классификатор с динамической корректировкой вероятности атаки. Экспериментальное тестирование на данных, сгенерированных в среде NS-3, показало, что предложенный метод превосходит традиционные подходы по точности обнаружения атак, снижая коэффициент ложных срабатываний с 10.9% до 3.8%. Гибридная модель обеспечивает 94.7% точности классификации и 91.8% полноты обнаружения атак, что на 6.3% выше, чем у стандартного Байесовского классификатора. Полученные результаты демонстрируют перспективность использования предложенного метода в системах реального времени для мониторинга безопасности IoT-сетей. Разработанный подход позволяет адаптироваться к изменяющейся сетевой среде, снижая влияние случайных флуктуаций, что делает его эффективным решением для защиты сетей с низким энергопотреблением.

Ключевые слова: *Информационная безопасность, персональные сети, IEEE 802.15.4, IoT, обнаружение атак, Z-оценка, Байесовский классификатор, машинное обучение, сетевой мониторинг.*

N. Bazhayev[1,2], A. Shaikhanova[1]*, D. Satybaldina[2], K. Bakenova[1]
[1]L.N. Gumilyov Eurasian National University,
010000, Republic of Kazakhstan, Satbayev Street, Astana,
[2]State Technical Service JSC,
010000, Republic of Kazakhstan, Astana, Mangilik El Avenue, 55 B
*e-mail: shaikhanova_ak@enu.kz

INTELLIGENT METHOD OF CONTINUOUS SECURITY MONITORING IN IEEE 802.15.4 NETWORKS BASED ON ADAPTIVE ANOMALY ANALYSIS

Securing IEEE 802.15.4 wireless networks is one of the key challenges in the development of the Internet of Things (IoT). Given the limited computational resources of IoT devices, traditional attack detection methods based on cryptographic mechanisms and deterministic thresholds do not always provide a sufficient

level of protection. In this paper, we propose a novel method for adaptive network traffic monitoring that combines a modified Z-score with sample size consideration and an adaptive Bayesian classifier with dynamic attack probability adjustment. Experimental testing on data generated in an NS-3 environment shows that the proposed method outperforms traditional approaches in terms of attack detection accuracy, reducing the false positive rate from 10.9% to 3.8%. The hybrid model provides 94.7% classification accuracy and 91.8% attack detection completeness, which is 6.3% higher than the standard Bayesian classifier. The obtained results demonstrate the promising use of the proposed method in real-time systems for monitoring the security of IoT networks. The developed approach allows adapting to the changing network environment, reducing the influence of random fluctuations, which makes it an effective solution for protecting low-power networks.

Key words: *Information security, personal networks, IEEE 802.15.4, IoT, attack detection, Z-score, Bayesian classifier, machine learning, network monitoring*

Сведения об авторах

Нуржан Аманкулулы Бажаев – постдокторант; Евразийский национальный университет имени Л.Н. Гумилева; АО «Государственная техническая служба», г. Астана, Республика Казахстан; e-mail: nurzhan_nfs@hotmail.com. ORCID: https://orcid.org/0009-0009-4820-6132.

Айгуль Кайрулаевна Шайханова* – PhD, профессор кафедры «Информационная безопасность», Евразийский национальный университет имени Л.Н. Гумилева, г. Астана, Республика Казахстан; e-mail: shaikhanova_ak@enu.kz. ORCID: https://orcid.org/0000-0001-6006-4813.

Дина Жагыпаровна Сатыбалдина – кандидат физико-математических наук, ассоциированный профессор, Евразийский национальный университет имени Л.Н. Гумилева, г. Астана, Республика Казахстан; e-mail: dinasaty@gmail.com. ORCID: https://orcid.org/0000-0003-0291-4685.

Камила Сериковна Бакенова – докторант кафедры «Информационная безопасность», Евразийский национальный университет имени Л.Н. Гумилева, г. Астана, Республика Казахстан; e-mail: bakenova.ks@enu.kz. ORCID: https://orcid.org/0009-0004-2567-173X.

Авторлар туралы мәліметтер

Нуржан Аманкулулы Бажаев – постдокторант; Л.Н. Гумилев атындағы Еуразия ұлттық университеті, «Мемлекеттік техникалық қызмет» АҚ, Астана қ., Қазақстан Республикасы; e+mail: nurzhan_nfs@hotmail.com. ORCID: https://orcid.org/0009-0009-4820-6132.

Айгуль Кайрулаевна Шайханова* – PhD, «Ақпараттық қауіпсіздік» кафедрасының профессоры, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана қ., Қазақстан Республикасы; e-mail: shaikhanova_ak@enu.kz. ORCID: https://orcid.org/0000-0001-6006-4813.

Дина Жагыпаровна Сатыбалдина – физика-математика ғылымдарының кандидаты, қауымдастырылған профессор, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана қ., Қазақстан Республикасы; e-mail: dinasaty@gmail.com. ORCID: https://orcid.org/0000-0003-0291-4685.

Камила Сериковна Бакенова – «Ақпараттық қауіпсіздік» кафедрасының докторанты; Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана қ., Қазақстан Республикасы; e-mail: bakenova.ks@enu.kz. ORCID: https://orcid.org/0009-0004-2567-173X.

Information about the authors

Nurzhan Bazhayev – postdoctoral fellow; L.N. Gumilyov Eurasian National University, State Technical Service JSC; Astana, Republic of Kazakhstan; e-mail: nurzhan_nfs@hotmail.com. ORCID: https://orcid.org/0009-0009-4820-6132.

Aigul Shaikhanova* – PhD, Professor of the Information Security Department; L.N. Gumilyov Eurasian National University, Astana, Republic of Kazakhstan; e-mail: shaikhanova_ak@enu.kz. ORCID: https://orcid.org/0000-0001-6006-4813.

Dina Satybaldina – Candidate of Physical and Mathematical Sciences, Associate Professor, L.N. Gumilyov Eurasian National University, Astana, Republic of Kazakhstan; e-mail: dinasaty@gmail.com. ORCID: https://orcid.org/0000-0003-0291-4685.

Kamila Bakenova – PhD student of the Information Security Department, L.N. Gumilyov Eurasian National University, Astana, Republic of Kazakhstan; e-mail: bakenova.ks@enu.kz. ORCID: https://orcid.org/0009-0004-2567-173X.

Редакцияға енуі 22.07.2025
Өңдеуден кейін түсуі 14.08.2025
Жариялауға қабылданды 15.08.2025