ХҒТАР 50.47.29

Ж.К. Абдугулова, А.М. Акбаракова

Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Нұр-Сұлтан, Қазақстан
(E-mail: janat_6767@mail.ru, rai.arai95@mail.ru)

Киберфизикалық жүйенің желілік инфрақұрылым объектілерінің жұмыс істеу сенімділігін қамтамасыз етуді модельдеу

Аңдатпа. Осы зерттеу шеңберінде базалық платформа ретінде бұлтты есептеулерді пайдаланатын өндірістік киберфизикалық жүйе архитектурасының құрылымдық моделі құрылған. Ұсынылған киберфизикалық жүйені абстракцияның төрт деңгейінде, мультиагенттік тәсіл негізінде барлық элементтерді біріктіреді. Мониторинг жүйесінің деректерін зияткерлік талдау әдістері негізінде ұсынылған тәсіл бұлтты платформа базасында орналасқан киберфизикалық жүйенің желілік инфрақұрылымының сенімділік тұрғысынан осал элементтерін іздестіруге және анықтауға мүмкіндік береді. Зерттеуде желі элементтерінің ағымдағы жай-күйіне шоғырландырылған бағалау жүргізу үшін мониторинг жүйесінен алынған деректерді жинау, талдау және верификациялау жоспарын қалыптастыратын өлшенген мультиграф түрінде ұсынылған желілік инфрақұрылым объектілерінің жұмыс істеу сенімділігін қамтамасыз ету моделі әзірленді. Бұл ретте, бағанның шыңы ретінде киберфизикалық жүйенің инфрақұрылымы мен бұлтты платформа үшін сенімділікті қамтамасыз ету параметрлері таңдалған. Доғалар ретінде баған деректердің айналмалы ағындарының ағымдағы параметрлерін ескере отырып, киберфизикалық жүйенің байланысқан тораптарының жұмыс жағдайы мен параметрлері арасындағы өзара байланысты көрсететін сенімділіктің белгіленген өлшемдері арасындағы байланыстар берілген. Бұл жүйе сегменттерін анықтауға мүмкіндік береді, бұл өзгерістер енгізу үшін қажетті үстеме шығыстарды қысқартады. Бұл ретте киберфизикалық жүйенің үздіксіз инфрақұрылымын болжау үшін нейрожелілік тәсіл қолданылады. Ұсынылған гибридті тәсілді пайдалану уақыт өте келе инфрақұрылымның мінез-құлқын болжауға және жекелеген компоненттер мен аса маңызды тораптардың жұмысындағы мүмкін болатын іркілістер туралы ескертуге мүмкіндік берді.

Түйін сөздер: Киберфизикалық жүйе, бұлтты платформа, нейрондық желі, сенімділік.

DOI: doi.org/10.32523/2616-7263-2021-137-4-88-97

Кіріспе

Киберфизикалық жүйелерді (КФЖ) пайдалану нұсқалары жыл сайын кеңеюде. Бүгінгі

таңда киберфизикалық жүйелер көптеген қосымшаларға, соның ішінде жоғары сенімділікті қажет ететін және маңызды инфрақұрылымның жұмыс істеуін қамтамасыз етуге қабілетті. Киберфизикалық жүйелердің ерекшелігі өңделген мәліметтердің едәуір мөлшері болып табылады. Бұл факт барлық негізгі инфрақұрылым элементтерінің архитектурасын ұйымдастырудың басқа тәсілдерін әзірлеуді талап етеді. Әдетте, киберфизикалық жүйе - бұл көптеген өзара байланысты элементтері бар көп деңгейлі есептеу платформасы. Сонымен қатар, оның элементтерін соңғы пайдаланушы да, оның контроллерінде іске асырылатын ақылды алгоритмдер арқылы да басқаруға болады. Әдетте, киберфизикалық жүйе интернет заттарының (Internet of Things, IoT) технологиялық базасына негізделген [1]. Бұл КФЖ-нің барлық элементтері бір-бірімен тығыз байланысты екендігіне байланысты. Бұл функция осындай инфрақұрылымды тиімді басқару және оның сенімділігін қамтамасыз ету жүйесін ұйымдастыру аясында шешілетін есептердің күрделілігінің экспоненциалды ұлғаюымен түсіндіріледі. Бұл мәселені шешу үшін көптеген әдістер мен тәсілдер бар.

Осындай тәсілдердің бірі бұлтты есептеу технологиясына негізделген зияткерлік басқару жүйелерін қолдану. Киберфизикалық жүйе аясында есептеулерді ұйымдастыру процесін басқарудың қолданыстағы әдістері әдетте тұтас ансамбльді қолданады. Олар негізінен иерархиялық, желілік-центрлік, матрицалық және ситуациялық басқаруды қолдануға негізделген. Алайда, олар бұлтты есептеу технологиясын қолдану кезінде туындайтын міндеттердің жоғары құрылымдық күрделілігі жағдайында жеткілікті тиімділікті қамтамасыз етпейді. Ақпараттың үлкен көлемін өңдеу мәселесі де маңызды мәселе болып табылады, бұл ақпараттың көлемінен басқа, сонымен қатар көптеген сілтемелер жасайды. Бұлтты жүйелер үшін контроллер деңгейінде тек интеллектуалды желіні басқаруды қолдану ең тиімді болып табылатындығын атап өткен жөн.

Киберфизикалық жүйелердің тағы бір ерекшелігі - деректерді сақтау мен өңдеуге жауапты инфрақұрылым элементтері мен ақпарат көздерінің арасындағы телекоммуникациялық өзара әрекеттесудің жоғары қарқындылығы, бұл ресурстарды уақтылы түзетуді және олардың жұмысының сенімділігін қамтамасыз етуді талап етеді. Осыған байланысты бұлтты платформаларға негізделген қолданыстағы шешімдердің де бірқатар кемшіліктері бар. Біріншіден, бұл инфрақұрылымның күрделілігі. Бұл аспект, әсіресе әртүрлі гетерогенді бұлтты платформалар әртүрлі бағдарламалық және аппараттық шешімдерді қолдана отырып өзара әрекеттескенде, сенімділік проблемаларын тудырады. Екіншіден, бір бұлтты платформадан екіншісіне деректерді беру кезінде қызмет көрсету сапасын қамтамасыз ету күрделілігі. Бұл киберфизикалық жүйелердің инфрақұрылым нысандарының жай-күйі туралы мониторинг деректерін алмасудың қол жетімді әдістері мен құралдарының жоқтығымен байланысты. Киберфизикалық жүйенің әртүрлі элементтерінің тиімді өзара әрекеттесуін қамтамасыз ету үшін уақыт өте келе ағымды болжау үшін желінің топологиясы мен параметрлері туралы сенімді ақпарат қажет.

Айта кету керек, қолданыстағы киберфизикалық жүйелер, негізінен, бағдарламалық жасақтамамен конфигурацияланған желілерде қолданылатын мәліметтер ағындарының байланыс сызбаларына адаптивті түзету механизмдерін пайдаланбайтын дәстүрлі желілерде жұмыс істеуге бағытталған. Негізінен, қолданыстағы шешімдер реактивті принципке сәйкес жұмыс істейтін дәстүрлі бағыттау әдістерін қолдануға бағытталған - деректер беру жолдары тораптар арасында деректер ағындарының пайда болу сәтіне қойылады [2, 3]. Бұл тәсіл деректерді тасымалдау маршрутын орнатудың белгілі бір кідірісін тудырады, сонымен қатар маршруттағы желілік құрылғылар немесе байланыс желілері істен шыққан жағдайда, арнаның жүктемесі өзгерген кезде оны өзгерту үшін уақыт қажет. 2.1 Experiment in the laboratory.

Сонымен қатар, желілердегі параллельді ағындар негізінен киберфизикалық немесе бұлтты жүйені тұрақсыз күйге келтіретін теріс фактор ретінде қарастырылады және нәтижесінде оның сенімділігі төмендейді.

Зерттеу әдістемесі

Қолданыстағы сенімділік жүйелерінің негізгі жетіспеушілігі - киберфизикалық жүйелердің инфрақұрылымын пайдалану кезінде болатын оқиғалар мен жағдайларды тиімді болжаудың болмауы. Сонымен қатар, қолданыстағы жүйелер инфрақұрылым нысандарының жай-күйі туралы қол жетімді мәліметтер негізінде өздігінен білім алу мүмкіндіктерін толық пайдаланбайды. Бұл өз кезегінде алынған деректердің эвристикалық талдауын пайдаланбайтын мониторинг жүйелерінің жеткіліксіз тиімді жұмыс істеуімен байланысты.

Осылайша, қазіргі уақытта киберфизикалық жүйелерді тиімді басқаратын және олардың сенімділігін қамтамасыз ететін әмбебап шешімдер жеткіліксіз екендігі анықталды. Ресурстар мен деректер ағындарын икемді басқаруға және жоспарлауға қабілетті бейімделетін және заманауи инфрақұрылымды құру үшін осы кластағы жүйелердің жұмысын ұйымдастырудың гибридті әдістері мен тәсілдерін дамыту қажет. Шешілетін мәселенің ғылыми маңыздылығы киберфизикалық жүйелер үшін телекоммуникациялар мен есептеу инфрақұрылымын ұйымдастырудың жаңа тәсілдерін сипаттайтын жаңа әдістер мен модельдерді жасауда, сонымен қатар оның сенімділігін қамтамасыз ететін әдістерді әзірлеуде жатыр.

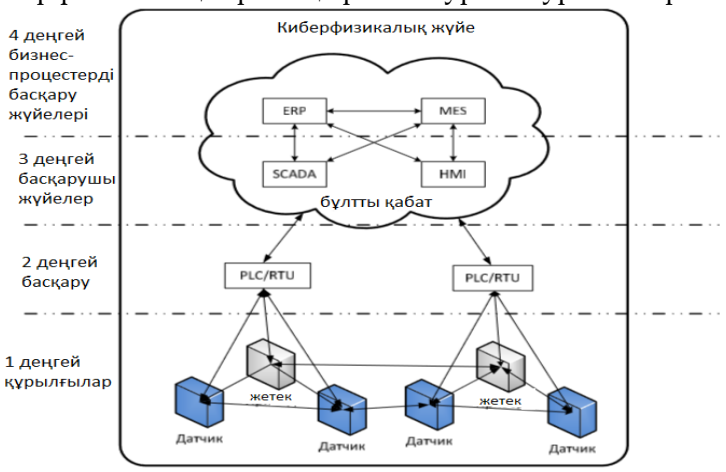
Зерттеулерге шолу қазіргі уақытта киберфизикалық инфрақұрылымның сенімділігін қамтамасыз ету проблемасы өте өзекті мәселе болып табылады және қазіргі заманғы әдістер мен тәсілдерге сүйене отырып, оны қамтамасыз етудің жаңа шешімдерін әзірлеу қажет. Атап айтқанда, сенімділікті қамтамасыз ету үшін кешендегі келесі мәселелер тізбесін шешу қажет:

- белсенді қағиданы қолдана отырып, киберфизикалық инфрақұрылым желісінің бағдарламаланатын сегменттері шеңберінде деректер ағындарының тиімді бағыттауын ұйымдастырады;

- киберфизикалық жүйелердің ресурстарын басқару жүйесінің параметрлерін өзгертуге бейімділікті қамтамасыз ету;

- киберфизикалық жүйенің әр элементі деңгейіндегі талаптардың сәтсіздікке және динамикалық өзгерістерге тұрақтылығын қамтамасыз ету [3].

Киберфизикалық жүйелердегі сенімділікті қамтамасыз етудің әдіснамасын жасауға кірісу үшін инфрақұрылым моделін құру және оның элементтерінің жұмыс тұрақтылығына әсерін бағалау қажет. Осы зерттеу аясында бұлттық есептеуді базалық платформа ретінде пайдаланатын өндірістік киберфизикалық жүйені қарастырамыз. Сенімділікті қамтамасыз ету үшін бұлтты технологияны қолданатын киберфизикалық жүйенің архитектурасы суретте көрсетілген.



Сурет 1- Киберфизикалық жүйенің архитектурасы

Жүйенің бұл түрі үшін киберфизикалық жүйенің компоненттерін абстракциялаудың 4 деңгейін бөлуге болатындығы анықталды. Базалық деңгейде (1 деңгей) өндірістік құрылғылардан мәліметтерді тікелей жинауға жауап беретін құрылғылар (сенсорлар, қоздырғыштар) тікелей орналасқан. Келесі деңгейге (2-деңгей) 1 деңгейде орналасқан киберфизикалық жүйенің соңғы құрылғыларымен басқаратын және өзара әрекеттесетін аралық бақылаушылар (мысалы, PLC, RTU және т.б.) жатады. 3 деңгейде өндіріс процесінде кешенді бақылауды жүзеге асыратын басқару жүйелері бар (SCADA, HMI). Жоғары деңгейде бизнес-процестерді басқаруға, ERP және басқаларға жауапты жүйелер бар. Соңғы екі деңгей әдетте бұлтты платформаның ішінде орналасады. Бұл ресурстарды масштабтау және басқаруды орталықтандыру арқылы шығындарды азайтуға және киберфизикалық жүйенің сенімділігін арттыруға мүмкіндік береді. Өз кезегінде, осы контексте киберфизикалық жүйелерді енгізу алдыңғы қатарлы цифрлық технологияларды енгізуді, атап айтқанда нақты уақыт режимінде физикалық құрылғылардан деректерді жинаудың тиімділігі мен сенімділігін қамтамасыз ету үшін құрылғылардың қосылуын ұйымдастырудың және есептеу ресурстарын бөлудің заманауи құралдарын қолдануды білдіреді.

Киберфизикалық жүйелердің жұмысын бағалауда қосымшалар мен қызметтердің сенімділігі мен қол жетімділігі маңызды рөл атқарады. Осыған байланысты инфрақұрылымның жоғары сенімділігін қамтамасыз ету үшін орналастырылған бағдарламалық жасақтаманы өмірлік циклді тиімді басқаруды қамтамасыз ету қажет. Бұлтты бағдарламалық жасақтаманың жұмысындағы негізгі сәтсіздіктер жүйелік ресурстардың сарқылуына, деректердің үзіндісі мен қателіктердің жиналуына байланысты болады.

Ақаудан кейін жүйені қалпына келтіру киберфизикалық жүйенің де, бүкіл инфрақұрылымның да сенімділігін қамтамасыз етудің ажырамас бөлігі болып табылады. Бұл жағдайда негіз өзін-өзі басқаруға байланысты мұндай жүйенің автономды жұмыс істеу мүмкіндігі болуы керек. Сондықтан, осы зерттеу аясында киберфизикалық жүйенің ресурстары бір-біріне тұтынушылар мен жеткізушілер ретінде әрекет ететін автономды бірліктер (агенттер) ретінде қарастырылады. Киберфизикалық жүйенің әрбір объектісі келесі параметрлер жиынтығы ретінде ұсынылуы мүмкін:

$$Obj_i = \{p_{i,1}, \dots, p_{i,n}\} \quad (1)$$

мұнда, $p_{i,1}$ - киберфизикалық жүйенің инфрақұрылым объектісінің түрін анықтайды; $p_{i,2}$- киберфизикалық жүйенің инфрақұрылым объектісінің нақты данасының сенімділігінің жиынтық көрсеткіші; $p_{i,1}, \dots, p_{i,n}$- сенімділікке әсер ететін киберфизикалық жүйенің инфрақұрылым объектісінің жеке параметрлері. Киберфизикалық жүйенің сенімділігін қамтамасыз ету моделін толығырақ сипаттайық.

Желілік элементтердің ағымдағы жай-күйін шоғырландырылған бағалауды жүргізу үшін, мониторинг жүйесінен алынған мәліметтерді жинау, талдау және тексеру жоспарын құра отырып, өлшенген G мультиграф түрінде ұсынылған желілік инфрақұрылым объектілерінің жұмысының сенімділігін қамтамасыз ету моделі жасалды:

$$G = \{V, A\}. \quad (2)$$

Сонымен қатар, кестенің шыңдары (V) ретінде киберфизикалық жүйенің және бұлтты платформаның жеке құрамдас бөліктері мен тораптарының сенімділігін қамтамасыз ету параметрлері таңдалды. (A) бағанының доғалары ретінде ағымдағы мәліметтер ағынын ескере отырып, киберфизикалық жүйенің инфрақұрылымының қосылған түйіндерінің күйі мен жұмыс параметрлері арасындағы байланысты көрсететін сенімділіктің белгіленген өлшемдері арасындағы қатынастар ұсынылған.

Сенімділік көрсеткіштері туралы толығырақ тоқталайық. Киберфизикалық жүйе объектілерінің өзара әрекеттесуі аясындағы басты мәселе - түйіндер арасында тұрақты байланыс арнасын ұйымдастыру. Сонымен, телекоммуникациялық деректермен алмасудың сенімділігі бойынша,

біз киберфизикалық жүйенің жеке түйіндерінің әр сәтте әр уақытта болуы және олардың белгілі бір уақыт аралығында проблемасыз өзара әрекеттесуін айтамыз.

Киберфизикалық жүйелер құрылымдық жағынан күрделі және көп деңгейлі нысандар болғандықтан, байланыс арналарының сенімділігі байланысты болатын деңгейлерді анықтаймыз:

Инфрақұрылым деңгейі деректер базасының датчиктері мен құрылғыларының аппараттық құрамдас бөліктерінің сенімділігін анықтайды.

Сәулет деңгейі киберфизикалық жүйенің жеке құрамдас бөліктерінің де сенімділігін, сондай-ақ бұлтты платформада орналастырылған бағдарламалық қамтамасыз ету жүйелері арасында желілік және есептеу ресурстарын ұсыну және тарату бойынша бірлескен жұмысын анықтайды.

Қосымшалар деңгейі бұлтты платформаның сәулеті мен инфрақұрылым деңгейлеріндегі сәтсіздіктер мен ақауларға қатысты корпоративтік ақпараттық жүйенің сенімділігі мен тұрақтылығын анықтайды.

Осылайша, аталған деңгейлердің әрқайсысы бұлтты платформа негізінде орналасқан бүкіл киберфизикалық жүйенің сенімділігіне әсер етеді. Сондықтан мұндай жүйенің болуы (Cs) барлық деңгейдегі көрсеткіштердің көбейтіндісі ретінде анықталады:

$$Cs = \prod_{i=1}^{n} C_i \qquad (3)$$

мұндағы Cs - бүкіл киберфизикалық жүйенің жалпы қол жетімділігі; C_i - киберфизикалық жүйеде атқаратын рөліне байланысты және жеке индикаторларға сәйкес анықталған деңгейлердің әрқайсысының қол жетімділігі; n - жүйенің сенімділігін талдау кезінде анықталған деңгейлер саны.

Әдетте, киберфизикалық жүйенің инфрақұрылымында негізгі компоненттердің, соның ішінде қосалқы байланыс каналдарының, суық және ыстық резервтегі есептеу түйіндерінің жеткілікті мөлшерде болуы. Алайда бұл тәсіл қосымша ресурстарды қолдануды талап етеді, бұл біз шешетін проблема аясында әрдайым мүмкін емес.

Киберфизикалық жүйеде сәтсіздіктердің пайда болу процесі кездейсоқ және тәуелсіз болғандықтан, оны кездейсоқ шаманы бөлу функциясы ретінде қарастыруға болады. Киберфизикалық жүйенің архитектурасының кез-келген деңгейі үшін тарату заңдарды қолдана аламыз, өйткені сәтсіздік мәліметтер ағынының қарқындылығына байланысты болады. Қателіктер киберфизикалық жүйенің белгілі бір деңгейіне келіп түсетін мәліметтер ағынымен бірдей таралу заңына ие делік. Содан кейін біз киберфизикалық жүйенің жұмысын параметрлердің жұп тізбегі ретінде елестетеміз

$$(X_i, Q_i), \qquad (4)$$

мұнда X_i- бұл жұмыс уақыты, Qi - қызмет көрсетуден бас тартудың ұзақтығы.

Сонымен қатар, $X_i \geq 0$ және $Qi \geq 0$, $i = 1, 2, \ldots$ шамалары.

Жалпы, сәтсіздік деңгейі келесідей анықталады

$$\lambda(x) = \frac{f(x)}{R(x)} \qquad (5)$$

мұндағы $f\ (x)$ - бөлу тығыздығы; $R\ (x) = 1 - F\ (x)$ - киберфизикалық жүйенің немесе оған кіретін желілік инфрақұрылымның берілген деңгейі үшін тарату заңымен анықталған сенімділік функциясы.

Киберфизикалық жүйенің барлық объектілері стационарлық режимде қарастырылатындықтан, дайындық коэффициентін келесідей көрсетуге болады:

$$K = \frac{EX}{EX+EQ} \qquad (6)$$

мұндағы EX және EQ - математикалық күтулер.

Графиктің әр күйі оқиғаның P_n ықтималдығымен өлшенеді.

Оқиғаның басталу қарқындылығы келесі параметрлермен анықталады: қалпына келтіру күйі үшін λ және сәтсіздік күйіндегі μ. Негізгі ықтималдық сипаттамалары уақыт бойынша тұрақты болған кезде киберфизикалық жүйенің тұрақты жұмыс режимін қарастыруға бел буамыз. Сонда әр мемлекет үшін ағынның қарқындылығы теңестіріледі:

$$P_0 * \lambda = P_1 * \mu \,. \quad (7)$$

Сондықтан киберфизикалық жүйенің жұмысын сипаттайтын теңдеулерді келесідей

көрсетуге болады:

$$\begin{cases} P_0 * \lambda - P_1 * \mu = 0; \\ P_0 + P_1 = 1. \end{cases} \quad (8)$$

Сонда ақпараттық жүйенің тоқтап қалу ықтималдығы келесідей көрініс табады:

$$P_1 = P_0 * \lambda/\mu. \quad (9)$$

P_0 дайындығының ықтималдығын анықтау үшін (8) теңдеулер жүйесінен өрнекті түрлендіреміз:

$$P_0 + P_0 * \frac{\lambda}{\mu} = 1; \quad P_0 = \frac{1}{(1+\lambda/\mu)} \quad (10)$$

Киберфизикалық жүйенің тоқтап қалу ықтималдығын келесі өрнек арқылы анықтауға болады

$$P_1 = 1 - P_0 = 1 - \frac{\mu}{(\mu+\lambda)} \quad (11)$$

Киберфизикалық жүйенің барлық элементтері тәуелсіз агенттер ретінде жұмыс істейтіндіктен, архитектураның әр деңгейіне есеп жүргізуге болады. Аналитикалық есептеуді әр ақпараттық жүйенің жұмысы туралы статистикалық мәліметтерді пайдалана отырып жүргізуге болады. Біз келесі белгіні енгіземіз:

$$\bar{X} = \frac{1}{n}\sum_{j=1}^{n} X_j, \quad \bar{Q} = \frac{1}{n}\sum_{j=1}^{n} Q_j \quad (12)$$

Сонда К қол жетімділік коэффициентін өрнектің көмегімен алуға болады

$$\widehat{K} = \frac{\bar{X}}{\bar{X}+\bar{Q}} \quad (13)$$

Қол жетімділік коэффициентін есептеу әдістемесі осы сыныптың жүйелерін құруда қолданылатын стандартты құралдармен салыстыру арқылы сенімділікті қамтамасыз ету үшін әзірленген алгоритмдік шешімдердің тиімділігін бағалауға мүмкіндік береді.

Сенімділіктің қажетті деңгейін қамтамасыз ету және киберфизикалық жүйенің үздіксіз жұмыс істеуін қамтамасыз ету үшін сәтсіздікке неғұрлым сезімтал тораптар мен байланыс арналарын анықтау қажет. Оны орындау үшін (1) –ші формулада сипатталған белгілер жиынтығына сәйкес жүйенің барлық элементтерін жіктеуге мүмкіндік беретін тәсілді қолданамыз.

Талқылау

Киберфизикалық жүйенің желілік инфрақұрылымының объектілерін жіктеу үшін біз көп қабатты перцептрондық архитектурасы бар нейрондық желіні қолданамыз. Нейрондық желінің кірісіне біз (1)-ші тізімде көрсетілген параметрлерді жібереміз. Шығару кезінде нейрондық желі барлық киберфизикалық жүйенің ағымдағы жағдайын ескере отырып, қол жетімділік коэффициентін есептеу негізінде объектілердің әрқайсысына сенімділік класын тағайындайды. Бұл қайта құруды қажет ететін жүйенің сегменттерін анықтауға мүмкіндік береді және өзгерістер енгізуге қажет шығындарды азайтады.

1-қадам. Желілік топологияны бастаңыз және Дейкстр алгоритмін қолданып, киберфизикалық жүйенің әр элементі үшін негізгі жол ретінде кідіріспен жолды таңдаңыз.

2-қадам. Киберфизикалық жүйе зерттелген элементінің сенімділігін сипаттайтын нейрондық желі параметрлерін енгізіңіз.

3-қадам. Желінің шығысын $y\,(x)$ есептеңіз.

4-қадам. Берілген вектор үшін желі шығысы мен қажетті мән арасындағы айырманы есептеңіз:

$E(w) = 1/2\ (d-y)^2$

5-қадам. Егер таңдалған векторды жіктеу кезінде қате пайда болса, онда алдымен желінің салмағын шығыс пен жасырын қабаттар арасындағы рет-ретімен түзетіңіз:

$\Delta w_{ji} = -\eta \frac{\partial E}{\partial w_{ji}} = -\eta \frac{\partial E}{\partial y} \frac{\partial y}{\partial z_j} \frac{\partial z_j}{\partial w_{ji}}$,

содан кейін жасырын және кіріс арасындағы

$\Delta w_{ji} = \eta \left[(d-y) f`(\sum_{i=0}^{H} v_i z_i) v_j\right] f`(\sum_{t=0}^{p} w_{jt} x_t) x_i$.

6-қадам. Барлық жиынтықтағы қателік рұқсат етілген деңгейге жеткенше жаттығулар жиынтығының әр векторы үшін 3-6 қадамдарды қайталаңыз. Желілік инфрақұрылым элементі үшін берілген сенімділік класына сүйене отырып, киберфизикалық жүйенің сенімділігін арттыру үшін келесі әрекеттер тізбегінің бірі қолданылады.

1. Егер киберфизикалық жүйенің желілік инфрақұрылымының элементі тексеру кезінде сенімді емес деп танылса, онда инфрақұрылымның сенімділігін арттыру үшін бұл элемент резервке қойылады. Бұл оқиға объектінің параметрлері мен сенімділігіне жауап беретін сипаттамаларын көрсете отырып, мәліметтер базасында тіркеледі. Осы объектінің барлық ағындары оңтайлы жолдарды таңдаудың алдын-ала жасалған алгоритміне сәйкес қайта бағытталады [5]. Деректер базасы осы нысанды келесі қарап шығудың жаңа уақыт белгісін орнатады.

2. Егер киберфизикалық жүйенің желілік инфрақұрылымының элементі тексеру кезінде сенімді деп саналса, онда ол үшін сенімділікті басқару жүйесінің деректер базасында тиісті белгі қойылады және келесі тексеруге жаңа уақыт белгісі тағайындалады.

Нәтижелер

Ұсынылған нейрондық желіні қолдану уақыт өткен сайын киберфизикалық жүйенің инфрақұрылымы элементтерінің әрекетін болжайды және жекелеген компоненттер мен критикалық тораптардың жұмысындағы мүмкін болатын сәтсіздіктер туралы ескертеді.

Сенімділікті қамтамасыз етудің әзірленген әдістемесін тәжірибелік зерттеу үшін біз IntelliSense интеллектуалды шешім технологиясын Қазақстанда танымал алтын құймаларын өндіруші, модельдік цифрлық фабрикалар арасында көшбасшылардың бірі болып табылатын «Алтын Алтыналмас» АҚ Ақтоғай филиалының алтын өндіретін фабрикасында енгізу технологиялық процесті және үлкен деректерді басқаруды болжамды талдау үшін нейрондық желілердің күрделі моделін құруға мүмкіндік береді. Ақтоғайдағы алтынды байыту фабрикасы - бұл Қазақстанда жасанды интеллект технологияларын қолдану арқылы шардың жүктелу деңгейін және ішкі төсемдердің тозуын болжауға мүмкіндік беретін, сондай-ақ диірмен кешенінің шамадан тыс жүктелуін болдырмайтын, өндіріс процесінің мөлдірлігінің артуына және диірменнің тоқтап қалуының азаюына алып келетін алғашқы өндіріс болып табылады. Сонымен бірге магистральді тау-кен өндірісін цифрландыру жобаларын іске асыру шеңберінде «Казцинк» ЖШС, «Eurasian Resources Group» және «Өскемен титан-магний комбинаты» АҚ Pitram, ERP, персоналды басқарудың мобильді жүйесі, балансты есептеу және жобаны Качарский карьерінде жүзеге асырды. Бұл жобаларда озық технологиялар қолданылды: ERP датчиктері, борттық компьютерлер, спутниктік орналастыру, барлығы нақты уақыт режимінде. Питрам өндірісті жедел басқару мәселелерін шешеді. Борттық компьютерлер LHD кабиналарында орнатылған, оған жүргізушілер нақты уақыт режимінде кенді тиеу, тасымалдау және түсіру туралы мәліметтерді енгізеді. Жүйе автоматты түрде драйвердің өнімділігін бір ауысымда есептейді және ақпаратты Wi-Fi кіру нүктесі арқылы серверге жібереді, содан кейін оны өңдейді. Персоналды сәйкестендіру жүйесі өз кезегінде қызметкерлер мен жабдықтардың қозғалысын нақты уақыт режимінде бақылауға мүмкіндік береді.

Датчиктер тау-кен фонарларына орнатылған. «Алтын алмас» кәсіпорындарының бірінің киберфизикалық жүйесінің желілік инфрақұрылымының бір бөлігін таңдадық. Зерттеліп жатқан киберфизикалық жүйе өз жұмысында OpenStack негізінде құрылған бұлтты платформаны пайдаланады. Киберфизикалық жүйе таңдалған сегментінде 50 желілік торап және 140 байланыс каналы бар.

Қорытынды

Тәжірибелік зерттеу екі кезеңде болды. Бірінші кезеңде бастапқы мәліметтерді алу үшін желі параметрлері зерттелді. Берілген параметрлерге сәйкес киберфизикалық жүйенің архитектурасының әр деңгейіне дайындық коэффициенттері алынған. Таңдалған желі сегментіндегі жауап уақыты өлшенді. Екінші кезеңде зерттеу қайталанды, бірақ нейрондық желі негізінде сенімділікті қамтамасыз ету алгоритмі қолданылуда. Киберфизикалық жүйенің инфрақұрылымы 1-ші кестеде келтірілген.

Кесте 1

Зерттелетін параметр	1-Кезең	2-Кезең
1-деңгей	K=0,40	K=0,45
2-деңгей	K=0,45	K=0,65
3-деңгей	K=0,82	K=0,95
4-деңгей	K=0,90	K=0,98
Желіге жауап беру уақыты, м/с	60	30

Зерттеу көрсеткендей, ұсынылған тәсіл сәулет деңгейіне байланысты киберфизикалық жүйенің сенімділігін 5-тен 13% -ға дейін жақсартады. Бірінші деңгейдегі тиімділіктің төмендігі тәжірибелік желіде қолданылатын соңғы құрылғылардың аппараттық шектеулеріне байланысты. Сонымен қатар, үшінші деңгейдегі жоғары тиімділік жоғары тиімді бұлтқа негізделген шешімдерді қолдану арқылы анықталады. Желіде жауап беру уақытын 50% қысқарту сенімділік үшін желінің элементтерін диагностикалау процесінде маршрутты оңтайландыруға байланысты.

Осылайша, зерттеу аясында бұлтты платформаның көмегімен орналастырылған киберфизикалық жүйенің архитектурасын сипаттайтын модель жасалды. Киберфизикалық жүйенің желілік инфрақұрылымы элементтерінің сенімділігін бағалау әдістемесі жасалды. Алгоритмдік шешім синтезделеді, бұл мәліметтер ағындарын тиімді тарату және құрылғылардың жағдайын талдау арқасында киберфизикалық жүйенің сенімділігін арттыруға мүмкіндік береді. Ұсынылған тәсіл киберфизикалық жүйенің желілік инфрақұрылымында маршруттарды оңтайландыру үшін мүмкін болатын қиындықтарды анықтауға мүмкіндік береді. Әзірленген шешімдердің негізгі артықшылықтары:

- байланыс компоненттерін және желілік бәсекелестікті есепке алу;
- желілік құрылғылар арасындағы пакеттерді таратудың кешігуі ескеріледі;
- киберфизикалық жүйенің виртуалды және физикалық топологиясын есепке алу;
- мәліметтер ағынының түріне және қарқындылығына, желілік ресурстардың жиналуы мен сенімділігіне байланысты бағыттарды таңдауды қамтамасыз ету.

Әдебиеттер тізімі

1. Ся Ф., Янг Л.Т., Ванг Л., Винель А. Заттардың ғаламторы // Байланыс жүйелерінің халықаралық журналы. – 2012. - Т. 25. - № 9. - Б. 1101. DOI: 10.1002 / dac.2417.

2. Цветков В.Я., Алпатов А.Н. Таратылған жүйелер мәселелері // Ғылым мен білімнің болашағы. - 2014. - № 6. - С. 31–36.

3. Болодурина И., Парфенов Д. Бағдарламалық жасақтамаға негізделген инфрақұрылым негізінде таратылған бұлтты есептеулерді ұйымдастыру модельдерін жасау және зерттеу // Процедура Информатика. - 2017. – Т. 103. - С. 569-576. DOI: 10.1016 / j.procs.2017.01.01.064.

4. Тихонов А.Н., Иванников А.Д., Соловьев И.В., Цветков В.Я., Куж С.А. Күрделі ұйымдық-техникалық жүйені желілік-центрлік басқару түсінігі. - М .: MaxPress, 2010. - 136 с.

5. Чехарин Е.Е. Үлкен деректер: үлкен мәселелер // Ғылым мен білімнің болашағы. - 2016. – Т. 21. - № 3. - С. 7–11.

Ж.К. Абдугулова, А.М. Акбаракова

Евразийский национальный университет им. Л.Н. Гумилева, Нур-Султан, Казахстан

Моделирование обеспечения надежности функционирования объектов сетевой инфраструктуры киберфизической системы

Аннотация. В рамках этого исследования была разработана структурная модель архитектуры промышленной кибер-физической системы, использующей облачные вычисления в качестве базовой платформы. Предложенная кибер-физическая система объединяет все элементы на четырех уровнях абстракции на основе многоагентного подхода. Предложенный подход, основанный на интеллектуальной системе анализа данных системы мониторинга, позволяет осуществлять поиск и идентификацию уязвимых элементов инфраструктуры кибер-физической сети на основе облачной платформы. В ходе исследования была разработана модель для обеспечения работы объектов сетевой инфраструктуры, представленная в виде измеренного мультиграфа, который формирует план сбора, анализа и проверки данных из системы мониторинга для обеспечения консолидированной оценки текущего состояния элементов сети. В то же время в качестве верхней части колонки были выбраны параметры для защиты инфраструктуры киберфизической системы и облачной платформы. В качестве дуг приведены взаимосвязи между фиксированными измерениями надежности, которые отражают взаимосвязь между операцией и параметрами подключенных узлов киберфизической системы с учетом текущих параметров столбцов потоков данных. Это позволяет идентифицировать системные сегменты, которые уменьшат накладные расходы, необходимые для внесения изменений. В то же время нейросетевой подход используется для прогнозирования непрерывной инфраструктуры киберфизической системы. Использование предложенного гибридного подхода позволило нам прогнозировать поведение инфраструктуры с течением времени и предупреждать о возможных сбоях в работе отдельных компонентов и критических узлов.

Ключевые слова: Киберфизическая система, облачная платформа, нейронная сеть, надежность.

Zh.K. Abdugulova, A.M. Akbarakova

L. N. Gumilyov Eurasian National University, Nur-Sultan, Kazakhstan

Modelization of reliability of functions of the network infrastructures of the cyberphysical systems

Abstract: Within the framework of this research, there has been developed a structural model of an industrial cyberphysical system architecture using cloud computing as a base platform has been developed. The proposed cyber-physical system integrates all elements in four levels of abstraction, based on a multi-agency approach. The proposed approach based on the Intelligent Data Analysis System of the Monitoring System allows searching and identifying vulnerable elements of the cyber-physical network infrastructure based on the cloud platform. The research has developed a model for securing the operation of network infrastructure facilities presented in the form of a measured multigraph, which forms a plan for collecting, analyzing and verifying data from the monitoring system to provide a consolidated assessment of the current state of the network elements. At the same time, the parameters for securing the infrastructure of the cyber-physical system and the cloud platform were selected as the top of the column. As arcs are given the relationships between the fixed dimensions of reliability, which reflect the

relationship between the operation and the parameters of the connected nodes of the cyber-physical system, taking into account the current parameters of the column data streams. This allows us to identify system segments that will reduce the overhead needed to make changes. At the same time, the neural network approach is used to predict the continuous infrastructure of the cyber-physical system. The use of the proposed hybrid approach allowed us to predict the behavior of the infrastructure over time and to warn of possible failures in the operation of individual components and critical nodes.

Keywords: Cyber-physical system, cloud platform, neural network, reliability.

References

1. Xia F., Yang L.T., Wang L., Vinel A. Internet veshchey. Mezhdunarodnyy zhurnal sistem svyazi [Internet of Things. International Journal of Communication Systems], 9(25), 1101 (2012). [in Russian]

2. Tsvetkov V.Ya., Alpatov A.N. Problemy raspredelennykh sistem. Perspektivy nauki i obrazovaniya [Problems of distributed systems. Prospects for science and education], 6, 31–36 (2014). [in Russian]

3. Bolodurina I., Parfenov D. Razrabotka i issledovaniye modeley organizatsii raspredelennykh oblachnykh vychisleniy na osnove programmno-opredelyayemoy infrastruktury. Protsedura Komp'yuternyye nauki [Development and Research of Models of Organization Distributed Cloud Computing Based on the Software-Defined Infrastructure. Procedia Computer Science], 103, 569-576 (2017). [in Russian]

4. Tikhonov A.N., Ivannikov A.D., Soloviev I.V., Tsvetkov V.Ya., Kuj S.A. Kontseptsiya setetsentricheskogo upravleniya slozhnoy organizatsionno-tekhnicheskoy sistemoy [Concept of Network-Centric Management of Difficult Organizational and Technical System] (Moscow: MaxPress, 2010, 136 p.). [in Russian]

5. Chekharin E.E. Bol'shiye dannyye: bol'shiye problemy. Perspektivy nauki i obrazovaniya [Big data: big problems. Prospects for science and education], 3 (21), 7–11 (2016). [in Russian]

Сведения об авторах:

Абдугулова Ж.К. *- экономика ғылымдарының кандидаты, жүйелік талдау және басқару кафедрасының доценті, Л. Н. Гумилев атындағы Еуразия ұлттық университеті, Нұр–Сұлтан, Казақстан.*

Акбаракова А.М. *- Жүйелік талдау және басқару кафедрасының оқытушысы, Л. Н. Гумилев атындағы Еуразия ұлттық университеті, Нұр–Сұлтан, Казақстан.*

Abdugulova Zh.K. *- Candidate of Economic Sciences, Associate Professor of the System Analysis and Management Department, L. N. Gumilyov Eurasian National University, Nur - Sultan, Kazakhstan.*

Akbarakova A.M. *- - Lecturer at the Department of the System Analysis and Control Department, L. N. Gumilyov Eurasian National University, Nur - Sultan, Kazakhstan.*