Инфокоммуникационные технологии и системы

УДК 62-51 DOI: 10.14529/ctcr180404

МОДЕЛИРОВАНИЕ ОБЕСПЕЧЕНИЯ НАДЕЖНОСТИ ФУНКЦИОНИРОВАНИЯ ОБЪЕКТОВ СЕТЕВОЙ ИНФРАСТРУКТУРЫ КИБЕР-ФИЗИЧЕСКОЙ СИСТЕМЫ

И.П. Болодурина, Д.И. Парфёнов

Оренбургский государственный университет, г. Оренбург, Россия

В рамках настоящего исследования построена структурная модель архитектуры производственной кибер-физической системы, использующей облачные вычисления в качестве базовой платформы. Представленная модель детализирует кибер-физическую систему на четырех уровнях абстракции, объединяя все элементы на основе мультиагентного подхода. Предложенный подход на основе методов интеллектуального анализа данных системы мониторинга позволяет осуществлять поиск и выявлять уязвимые с точки зрения надежности элементы сетевой инфраструктуры кибер-физической системы, расположенной на базе облачной платформы. Для проведения консолидированной оценки текущего состояния элементов сети в исследовании разработана модель обеспечения надежности функционирования объектов сетевой инфраструктуры, представленная в виде взвешенного мультиграфа, формирующего план сбора, анализа и верификации получаемых от системы мониторинга данных. При этом в качестве вершин графа выбраны параметры обеспечения надежности для отельных компонентов и узлов, как инфраструктуры кибер-физической системы, так и облачной платформы. В качестве дуг графа представлены связи между установленными критериям надежности, отражающие взаимосвязь между состоянием и параметрами работы связанных узлов инфраструктуры кибер-физической системы с учетом текущих параметров циркулирующих потоков данных. Это позволит определять сегменты системы, требующие реконфигурации, что сократит накладные расходы, необходимые для внесения изменений. При этом для прогнозирования бесперебойной инфраструктуры кибер-физической системы задействован нейросетевой подход. Использование предлагаемого гибридного подхода позволило предсказывать поведение инфраструктуры с течением времени и предупреждать о возможных сбоях в работе отдельных компонентов и критически важных узлов.

Ключевые слова: кибер-физическая система, облачная платформа, нейронная сеть, надежность.

Введение

Варианты использования кибер-физических систем (КФС) ежегодно расширяются. На сегодняшний день кибер-физические системы способны обслуживать множество приложений, в том числе требующих высокой надежности и обеспечивающих функционирование критически важной инфраструктуры. Отличительной особенностью кибер-физических систем является значительный объем обрабатываемых данных. Этот факт требует разработки иных подходов к организации архитектуры всех ключевых элементов инфраструктуры. Как правило, кибер-физическая система представляет собой многоуровневую вычислительную платформу с множеством взаимосвязанных элементов. При этом управление ее элементами может осуществляться как конечным пользователем, так и интеллектуальными алгоритмами, реализованными на ее контроллере. Как правило, кибер-физическая система основывается на технологической базе интернета вещей (Internet of Things, IoT) [1]. Это обуславливается тем, что все элементы КФС сильно связаны между собой. Эта особенность объясняет экспоненциальный прирост вычислительной трудоемкости задач, решаемых в рамках организации системы для эффективного управления подобной инфраструктурой и обеспечения ее надежности. Для решения данной проблемы существует достаточно много методов и подходов.

Одним из таких подходов является использование интеллектуальных управляющих систем, основанных на технологии облачных вычислений [2, 3]. Существующие методы управления процессом организации вычислений в рамках кибер-физической системы обычно используют целый ансамбль подходов. Главным образом они основываются на применении иерархического, сетецентрического, матричного и ситуационного управления [4]. Однако они не обеспечивают достаточную эффективность в условиях высокой структурной сложности задач, возникающих в результате применения технологии облачных вычислений. Не менее важным вопросом является проблема обработки больших потоков данных [5], которая кроме самих объемов информации создает так же значительное количество связей. Необходимо отметить, что для облачных систем наиболее эффективным является использование исключительно интеллектуального управления сетями на уровне контроллера.

Еще одной особенностью кибер-физических систем является высокая интенсивность телекоммуникационного взаимодействия между элементами инфраструктуры, отвечающими за хранение и обработку данных, а также источниками информации, что требует своевременной подстройки ресурсов и обеспечения надежности их работы. В этом плане существующие решения, основанные на облачных платформах, также обладают рядом недостатков. В первую очередь это сложность инфраструктуры. Этот аспект вызывает проблемы с надежностью, особенно при взаимодействии нескольких разнородных облачных платформ, построенных с применением различных программных и аппаратных решений. Во-вторых, сложность обеспечения качества обслуживания при передаче данных от одной облачной платформы в другую. Это вызвано отсутствием доступных методов и средств, позволяющих осуществлять обмен данными мониторинга о состоянии объектов инфраструктуры кибер-физических систем. Для обеспечения эффективного взаимодействия различных элементов кибер-физических систем необходима достоверная информация о топологии и параметрах сети для прогнозирования потоков с течением времени.

Следует заметить, что существующие кибер-физические системы ориентированы в основном на работу в традиционных сетях, которые не используют адаптивные механизмы подстройки под коммуникационные схемы потоков данных, применяемые в программно-конфигурируемых сетях. В основном существующие решения ориентированы на использование традиционных методов маршрутизации, работающих по реактивному принципу – пути передачи данных прокладываются в момент возникновения потоков данных между узлами. Такой подход вызывает определенную задержку при установке маршрута передачи данных, а также требуется время для его изменения при возникновении отказов сетевых устройств или линий связи на маршруте, изменении загрузки каналов. При этом параллельные потоки в сетях в основном рассматриваются как негативный фактор, приводящий кибер-физическую или облачную систему в нестационарное состояние, и как следствие, снижает ее надежность.

Ключевым недостатком существующих систем обеспечения надежности является отсутствие эффективного прогнозирования инцидентов и событий, возникающих в процессе функционирования инфраструктуры кибер-физических систем. Кроме того, существующие системы не в полной мере используют возможности самообучения на основе имеющихся данных о состояниях объектов инфраструктуры. В свою очередь это связано с недостаточно эффективной работой систем мониторинга, не использующих методы эвристического анализа получаемых данных.

Таким образом, установлено, что на сегодняшний день нет достаточно универсальных решений, позволяющих эффективно эксплуатировать кибер-физические системы и обеспечивать их надежность. Для проектирования адаптивной и современной инфраструктуры, способной осуществлять гибкое управление и планирование ресурсов и потоков данных, необходима разработка более совершенных гибридных методов и подходов к организации работы систем данного класса. Научная значимость решаемой проблемы состоит в разработке новых методов и моделей, позволяющих описать новые подходы к организации телекоммуникационной и вычислительной инфраструктуры для кибер-физических систем, а также в разработке методов обеспечения ее надежности.

1. Обзор исследований

Современные методы для достижения высокой надежности требуют значительных накладных расходов на инфраструктуру. Так в исследовании Israel Koren отмечается, что кибер-

физические системы часто остаются уязвимыми к угрозам безопасности. Это негативно сказывается на надежности их работы. Автор предлагает использовать данные о состоянии устройств для обеспечения требуемого уровня надежности. Для классификации состояния устройств автор предлагает использовать различные методы машинного обучения [6].

Исследователи Quanyan Zhu и Tamer Basar отмечают, что решения, связанные с безопасностью систем управления должны строиться на основе понимания компромисса между безопасностью системы и её доступностью. Авторы предложили унифицированный фреймворк для решения проблем безопасности в кибер-физических системах. В исследовании проведено моделирование архитектуры безопасности с помощью сетей Джексона и устройств безопасности в тандемных сетях массового обслуживания. В качестве метрик системы управления исследовались два ключевых параметра: задержка и скорость передачи пакетов [7].

Группа ученых под руководством Tamoghna Ghosh в своем исследовании освещает вопрос использования данных событий для построения модели прогнозирования неисправностей устройств. Авторы совместили в своем исследовании метод стратифицированной выборки с новым методом анализа технических характеристик, использующим скользящие окна для получения данных о событиях [8].

Учеными Массачусетского университета предложен метод активной реновации программного обеспечения, позволяющий строить динамическое дерево возможных ошибок в работе ПО и анализировать критерии их возникновения в процессе эксплуатации облачных сервисов и приложений [9]. Это позволяет обеспечивать надежность функционирования приложений еще до момента запуска на кибер-физических системах.

Исследователями технического университета Луизианы предложен подход, обеспечивающий эффективное использование кибер-физических систем. В модели оценки надежности ученые предлагают использовать среднее время до отказа, а также частоту отказов на основе логов доступа к вычислительным узлам и виртуальным машинам. Однако такой подход не позволяет отслеживать доступность сервисов прикладного уровня виртуализации, упакованных в контейнеры [10].

Ряд исследователей затрагивают вопросы маршрутизации. Так в исследовании Ouzhou Dong et al. обращают внимание на уязвимые места в маршрутизации в кибер-физической энергетической системе (CPPS). Существующие решения являются слишком централизованными, что приводит к увеличению риска отказа в обслуживании в сети. В целях снижения влияния рисков они предлагают подход к восстановлению маршрутизации услуг, основанный на балансе риска. В исследовании раскрывается модель оценки риска, а также приводится усовершенствованный генетический алгоритм для решения проблемы реконструкции маршрутизации и восстановления сервиса [11].

Исследователи Lee и Seshia используют кибер-физический подход к встроенным системам. Основное внимание они уделяют моделированию, проектированию и анализу кибер-физических систем, которые объединяют вычислительные, сетевые и физические процессы [12].

Ряд исследователей затрагивают вопросы качества обслуживания в CPS. Например, исследователи Lin Gu et al. рассматривают медицинские кибер-физических системы (MCPS). Интеллектуальное взаимодействие между элементами таких систем и медицинскими устройствами организовано с помощью облачных систем. Облачные ресурсы также необходимы для обработки чувствительных данных от медицинских устройств. Медицинские кибер-физические системы требуют высокого качества обслуживания. Для борьбы с этой проблемой используют промежуточное решение на базе туманных вычислений (Fog computing) [13].

Как отмечают авторы, технология Fog computing обладает большей устойчивостью и ненадежностью по сравнению с технологией облачных вычислений. Вычисления, основанные на технологии fog computing, могут решать эти проблемы, предоставляя более гибкие вычислительные ресурсы и сетевые услуги конечным пользователям на границе сети, в то время как технология облачных вычислений ориентирована на предоставлении ресурсов, распределенных внутри сети [14, 15]. В своих исследованиях O.A. Osanaiye и E. Baccarelli описывают архитектуру туманных вычислений и рассматривают ее различные сервисы и приложения. Особое внимание исследователи уделяют вопросам безопасности и доступности услуг и ресурсов области туманных вычислений [16, 17].

Таким образом, проведенный обзор исследований показывает, что в настоящее время проблема обеспечения надежности кибер-физической инфраструктуры является достаточно актуальным вопросом и необходима разработка новых решений ее обеспечения, основанных на современных методах и подходах. В частности, для обеспечения надежности необходимо в комплексе решать следующий перечень задач:

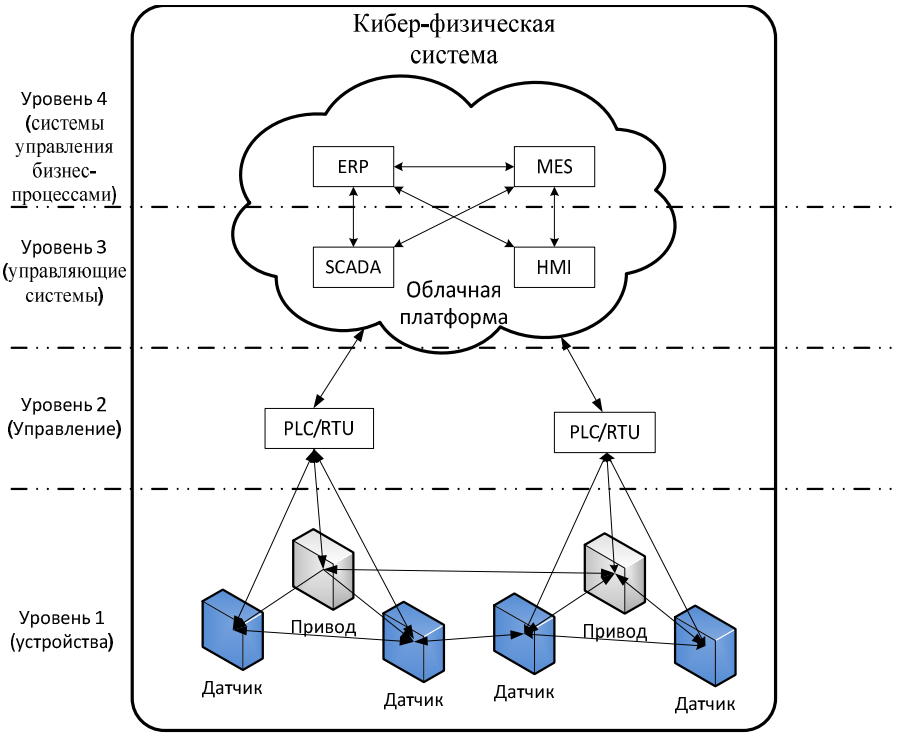
– организовать эффективную маршрутизацию потоков данных в рамках программно-конфигурируемых сегментов сети кибер-физической инфраструктуры, в том числе с использованием проактивного принципа;

– обеспечить адаптивность изменения параметров системы управления ресурсами кибер-физических систем;

– обеспечить устойчивость к отказам и динамическим изменениям требований на уровне каждого элемента кибер-физической системы.

2. Модель архитектуры кибер-физической системы

Для того чтобы перейти к разработке методики обеспечения надежности в CPS необходимо построить модель инфраструктуры и оценить влияние ее элементов на стабильность работы. В рамках настоящего исследования будем рассматривать производственную кибер-физическую систему, использующую облачные вычисления в качестве базовой платформы. Архитектура кибер-физической системы, использующей облачные технологии для обеспечения надежности, представлена на рисунке.



Архитектура кибер-физической системы

Установлено, что для данного типа систем можно выделить 4 уровня абстракции компонентов кибер-физической системы. На базовом уровне (уровень 1) располагаются непосредственно устройства (Sensors, Actuators) , отвечающие за непосредственный сбор данных с производственного оборудования. На следующем уровне (уровень 2) располагаются промежуточные контроллеры (например, PLCs, RTUs и др.), осуществляющие управление и взаимодействие с конечными устройствами кибер-физической системы, расположенными на 1 уровне. На уровне 3 располагаются управляющие системы, реализующие целостный контроль в рамках производственного процесса (SCADA, HMI). На самом высоком уровне располагаются системы, отвечающие за управление бизнес-процессами, ERP и другие. Последние два уровня, как правило, размещают

внутри облачной платформы. Это позволяет сократить издержки и повысить надежность работы кибер-физической системы за счет масштабирования ресурсов и централизации управления. В свою очередь реализация кибер-физических систем в рамках этого контекста означает внедрение передовых цифровых технологий, а именно использование современных средств для организации подключения устройств и выделения вычислительных ресурсов для обеспечения эффективности и надежности сбора данных от физических устройств в режиме реального времени.

Надежность и доступность приложений и сервисов играют важную роль в оценке производительности кибер-физических систем. В связи с этим для обеспечения высокой надежности инфраструктуры необходимо обеспечить эффективное управление жизненным циклом размещаемого программного обеспечения. Основные сбои в работе облачного программного обеспечения происходят из-за истощения ресурсов системы, фрагментации данных и накопления ошибок.

Восстановление системы после сбоя является неотъемлемой частью обеспечения надежности как самой кибер-физической системы, так всей инфраструктуры в целом. При этом основой должна служить возможность автономной работы такой системы за счет самоорганизации управления. Поэтому в рамках настоящего исследования ресурсы кибер-физической системы рассматриваются как автономные единицы (агенты), которые выступают в роли потребителей и поставщиков друг для друга. Каждый объект кибер-физической системы можно представить в виде следующего множества параметров:

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

где $p_{i,1}$ – определяет тип объекта инфраструктуры кибер-физической системы; $p_{i,2}$ – консолидированный показатель надежности конкретного экземпляра объекта инфраструктуры кибер-физической системы; $p_{i,3}, \ldots, p_{i,n}$ – индивидуальные параметры объекта инфраструктуры кибер-физической системы, влияющие на надежность. Опишем модель обеспечения надежности инфраструктуры кибер-физической системы более детально.

3. Модель обеспечения надежности инфраструктуры кибер-физической системы

Для проведения консолидированной оценки текущего состояния элементов сети в исследовании разработана модель обеспечения надежности функционирования объектов сетевой инфраструктуры, представленная в виде взвешенного мультиграфа G, формирующего план сбора, анализа и верификации получаемых от системы мониторинга данных:

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

При этом в качестве вершин (V) графа выбраны параметры обеспечения надежности для отдельных компонентов и узлов как инфраструктуры кибер-физической системы, так и облачной платформы. В качестве дуг графа (A) представлены связи между установленными критериям надежности, отражающие взаимосвязь между состоянием и параметрами работы связанных узлов инфраструктуры кибер-физической системы с учетом текущих потоков данных.

Остановимся более подробно на показателях надежности. Основной проблемой в рамках взаимодействия между объектами кибер-физической системы является организация стабильного канала связи между узлами. Поэтому под надежностью телекоммуникационного обмена данными будем понимать доступность отдельных узлов кибер-физической системы в каждый момент времени и их безотказную совместную работу в течение заданного интервала времени.

Ввиду того, что кибер-физические системы являются структурно сложными и многоуровневыми объектами, определим уровни, от которых зависит надежность каналов связи:

Уровень инфраструктуры определяет надежность аппаратных компонентов датчиков и устройств опорной сети передачи данных.

Уровень архитектуры определяет надежность как отельных компонентов кибер-физической системы, так и их совместной работы по предоставлению и распределению сетевых и вычислительных ресурсов между программными системами, развернутыми внутри облачной платформы.

Уровень приложений определяет надежность и устойчивость корпоративной информационной системы к сбоям и отказам на уровнях архитектуры и инфраструктуры облачной платформы.

Таким образом, каждый из перечисленных уровней оказывает влияние на надежность всей

кибер-физической системы, размещенной на базе облачной платформы. Следовательно, доступность такой системы (*Cs*) определяется как произведение показателей всех уровней:

$$Cs = \prod_{i=1}^{n} C_i, \tag{3}$$

где *Cs* – суммарная доступность всей кибер-физической системы; C_i – доступность каждого из уровней, определяемая в зависимости от выполняемой роли в кибер-физической системе и в соответствии с индивидуальными показателями; *n* – число уровней, выделенных в ходе анализа надежности системы.

Как правило, уровень инфраструктуры кибер-физической системы обладает достаточным резервированием основных компонентов, включая запасные каналы связи, вычислительные узлы в холодном и горячем резерве. Однако такой подход требует использования дополнительных ресурсов, что в рамках решаемой нами задачи физически не всегда возможно.

Надежность на более высоких уровнях значительно ниже, чем на инфраструктурном уровне. Это связано с устойчивостью к сбоям отдельных компонентов и их программной составляющей. Однако применение инженерных подходов на уровне алгоритмов оптимизации, учитывающих инфраструктурные и архитектурные особенности кибер-физической системы, позволяет повысить устойчивость системы к сбоям и, тем самым, улучшить надежность системы за счет ее масштабируемости. Кроме того, преимуществом программной реализации является время реакции системы. В отличие от физической инфраструктуры, время на изменение параметров отдельных программных компонентов значительно ниже.

Для определения индивидуальных требований к системе распределения потоков информации в сети передачи данных следует установить показатели надежности для каждого из выделенных ранее уровней архитектуры кибер-физической системы. Как правило, оценка надежности производится путем расчета коэффициента готовности *K*. При этом отказы системы принято рассматривать в виде потоков событий. Для кибер-физических систем потоки отказов характеризуются следующими особенностями:

- отказы происходят не по одному, то есть вероятность отказа двух и более элементов объекта в один момент времени достаточно велика, следовательно, поток требований неординарный;
- вероятность наступления последующих отказов объекта в любой момент времени не зависит от предыдущих отказов – поток отказов без последействия;
- поток отказов стационарный, т. е. не зависит от расположения рассматриваемого интервала времени.

Учитывая данные характеристики, поток отказов кибер-физической системе не является простейшим.

Так как процесс возникновения отказов в кибер-физической системе является случайным и независимым, его можно рассматривать как функцию распределения случайной величины. Для каждого из уровней архитектуры кибер-физической системы можно применить собственные законы распределения, так как отказы зависят от интенсивности потоков данных. Предположим, что отказы имеют тот же закон распределения, что и входящий поток данных, поступающих на заданный уровень кибер-физической системы. Тогда представим работу кибер-физической системы в виде последовательности пар параметров

$$(X_i, Q_i), \tag{4}$$

где X_i – продолжительность безотказной работы, Q_i – продолжительность отказа в обслуживании. При этом значения $X_i \geq 0$ и $Q_i \geq 0$, $i = 1, 2, \ldots$.

В общем случае интенсивность отказов определяется как

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

где $f(x)$ – плотность распределения; $R(x) = 1 - F(x)$ – функция надежности, определяемая законом распределения для данного уровня кибер-физической системы или входящего в его состав объекта сетевой инфраструктуры.

Так как все объекты кибер-физической системы рассматриваются в стационарном режиме, то коэффициент готовности можно представить в виде:

$$K = \frac{EX}{EX + EQ}, \tag{6}$$

где EX и EQ – математические ожидания.

Каждое состояние в графе количественно оценивается вероятностью P_n наступления события. При этом интенсивность наступления события определяется следующими параметрами: λ для состояния восстановления и μ состояния отказа.

Ограничимся рассмотрением установившегося режима работы кибер-физической системы, когда основные вероятностные характеристики постоянны во времени. Тогда интенсивности потоков для каждого состояния будут сбалансированы:

$$P_0 \cdot \lambda = P_1 \cdot \mu. \tag{7}$$

Следовательно, уравнения, описывающие работу кибер-физической системы, можно представить в виде:

$$\begin{cases} P_0 \cdot \lambda - P_1 \cdot \mu = 0; \\ P_0 + P_1 = 1. \end{cases} \tag{8}$$

Тогда вероятность простоя (отказа) информационной системы можно представить в виде:

$$P_1 = P_0 \cdot \lambda / \mu. \tag{9}$$

Для определения вероятности готовности P_0 преобразуем выражение из системы уравнений (8):

$$\begin{aligned} &P_0 + P_0 \cdot \lambda / \mu = 1; \\ &P_0 = 1/(1 + \lambda / \mu). \end{aligned} \tag{10}$$

Тогда вероятность простоя кибер-физической системы можно определить следующим выражением

$$P_1 = 1 - P_0 = 1 - \frac{\mu}{\mu + \lambda}. \tag{11}$$

Так как все элементы кибер-физической системы работают как независимые агенты, можно провести расчет для каждого из уровней архитектуры. Аналитически расчет может быть выполнен с использованием статистических данных о работе каждой из информационных систем. Введем обозначения:

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

Тогда коэффициент готовности K можно получить, используя выражение

$$\hat{K} = \frac{\bar{X}}{\bar{X} + \bar{Q}}. \tag{13}$$

Представленная методика расчета коэффициента готовности позволит оценить эффективность разработанных алгоритмических решений по обеспечению надежности путем сравнения со стандартными средствами, применяемыми при построении систем данного класса.

4. Алгоритм обеспечения надежности на базе нейронной сети

Для обеспечения требуемого уровня надежности и обеспечения бесперебойной работы кибер-физической системы необходимо определить узлы и каналы связи,наиболее подверженные сбою. Для этого применим подход, позволяющий классифицировать все элементы системы согласно набору признаков описанному в (1).

Для классификации объектов сетевой инфраструктуры кибер-физической системы будем использовать нейронную сеть с архитектурой многослойный персептрон. На вход нейронной сети будем подавать параметры, перечисленные в (1). На выходе нейронная сеть будет присваивать каждому из объектов класс надежности на основании расчета коэффициента готовности, с учетом текущего состояния всей кибер-физической системы в целом. Это позволит определять сегменты системы, требующие реконфигурации, что сократит накладные расходы, необходимые для внесения изменений.

Подробные шаги алгоритма показаны ниже.

Шаг 1. Инициализация топологии сети и использование алгоритма Дейкстры для настройки пути с наименьшей задержкой в качестве основного пути для каждого элемента КФС.

Шаг 2. Подать на вход нейронной сети параметры, характеризующие надежность исследуемого элемента КФС.

Шаг 3. Вычислить выход сети $y(x)$.

Шаг 4. Вычислить разность между выходом сети и требуемым значением для данного вектора $E(w) = \frac{1}{2}(d-y)^2$.

Шаг 5. Если была допущена ошибка при классификации выбранного вектора, то подкорректировать последовательно веса сети сначала между выходным и скрытым слоями

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

затем между скрытым и входным

$$\Delta w_{ji} = \eta \left[(d-y) f'(\sum_{i=0}^{H} v_i z_i) v_j \right] f'(\sum_{t=0}^{p} w_{jt} x_t) x_i .$$

Шаг 6. Повторять шаги с 3 по 6 для каждого вектора обучающего множества до тех пор, пока ошибка на всем множестве не достигнет приемлемого уровня.

На основании присвоенного класса надежности для элемента сетевой инфраструктуры применяется одна из следующих последовательностей действий, позволяющих повысить надежность работы кибер-физической системы.

1. Если элемент сетевой инфраструктуры кибер-физической системы признан не надежным на момент проверки, то для повышения надежности инфраструктуры данный элемент выводится в резерв. О данном инциденте происходит запись в базе данных с указанием параметров объекта и его характеристик, отвечающих за надежность. Все потоки данных с данного объекта перемаршрутизируются согласно разработанному ранее алгоритму выбора оптимальных путей [16]. В базе данных также устанавливается новая временная метка следующей проверки данного объекта.

2. Если элемент сетевой инфраструктуры кибер-физической системы признан надежным на момент проверки, то для него вносится соответствующая отметка в базу данных системы контроля надежности и устанавливается новая временная метка следующей проверки.

Использование предлагаемого нейросетевого подхода позволит в дальнейшем предсказывать поведение элементов инфраструктуры кибер-физической системы с течением времени и предупреждать о возможных сбоях в работе отдельных компонентов и критически важных узлов.

5. Экспериментальные исследования

Для экспериментального исследования разработанной методики обеспечения надежности нами выбрана часть сетевой инфраструктуры кибер-физической системы одного из предприятий Оренбургского региона. Исследуемая кибер-физическая система использует в своей работе облачную платформу, построенную на базе OpenStack. В выделенном сегменте сети CPS насчитывается 50 сетевых узлов и 140 каналов связи.

Используя методику расчета коэффициента готовности, приведенную в разделе 4, проведем оценку эффективности работы компонентов кибер-физической системы. При этом будем учитывать неоднородность поступающих запросов и различную интенсивность обращения к различным элементам сетевой инфраструктуры кибер-физической системы. Зададим интенсивность входного потока в диапазоне от 1 до 500 при времени исследования 60 мин.

Экспериментальное исследование было в два этапа. На первом этапе проведено исследование параметров сети с целью получения исходных данных. В соответствии с заданными параметрами получены коэффициенты готовности для каждого из уровней архитектуры кибер-физической системы. Также проведено измерение времени отклика в выбранном сетевом сегменте. На втором этапе исследование повторялось, но уже с использованием алгоритма обеспечения надежности на базе нейронной сети. Результаты исследования представлены в таблице.

Результаты экспериментального исследования

Исследуемый параметр		Этап 1	Этап 2
Коэффициенты готовности	Уровень 1	$K = 0{,}40$	$K = 0{,}45$
	Уровень 2	$K = 0{,}45$	$K = 0{,}65$
	Уровень 3	$K = 0{,}82$	$K = 0{,}95$
	Уровень 4	$K = 0{,}90$	$K = 0{,}98$
Время отлика в сети, мс		60	30

Исследование показало, что в зависимости от уровня архитектуры предлагаемый подход позволяет повысить надежность кибер-физической системы от 5 до 13 %. Низкая эффективность на первом уровне обусловлена ввиду аппаратных ограничений конечных устройств, используемых в экспериментальной сети. При этом высокая эффективность на третьем уровне обуславливается применением высокоэффективных решений на базе облачных технологий. Сокращение времени отклика в сети на 50 % обусловлено оптимизацией маршрутов в процессе диагностирования сетевых элементов на надежность.

Заключение

В рамках проведенного исследования построены модель, описывающая архитектуру кибер-физической системы, развернутой с использованием облачной платформы. Разработана методика оценки надежности элементов сетевой инфраструктуры кибер-физической системы. Синтезировано алгоритмическое решение, позволяющее повысить надежность кибер-физической системы за счет эффективного распределения потоков данных и анализа состояния устройств. Предложенный подход позволяет определить потенциальные «узкие» места для оптимизации маршрутов в сетевой инфраструктуре кибер-физической системы. Основными достоинства разработанных решений являются:

– учет коммуникационной составляющей и сетевой конкуренции – принимаются во внимание задержки в передаче пакетов между сетевыми устройствами;

– учет виртуальной и физической топологии кибер-физической системы;

– обеспечение выбора маршрутов в зависимости от типа и интенсивности потоков данных, загруженности и надежности сетевых ресурсов.

Работа выполнена при поддержке РФФИ (научные проекты № 16-07-01004 и № 18-47-560016) и гранта Президента Российской Федерации для государственной поддержки молодых российских ученых – кандидатов наук (МК-1624.2017.9).

Литература/References

1. Xia F., Yang L.T., Wang L., Vinel A. Internet of Things. *International Journal of Communication Systems*, 2012, vol. 25 (9), p. 1101. DOI: 10.1002/dac.2417

2. Цветков, В.Я., Алпатов А.Н. Проблемы распределённых систем. Перспективы науки и образования. 2014. № 6. С. 31–36. [Tsvetkov V.Ya., Alpatov A.N. [Problems of the Distributed Systems]. *Prospects of Science and Education*, 2014, no. 6, pp. 31–36. (in Russ.)]

3. Bolodurina I., Parfenov D. Development and Research of Models of Organization Distributed Cloud Computing Based on the Software-Defined Infrastructure. *Procedia Computer Science*, 2017, vol. 103, pp. 569–576. DOI: 10.1016/j.procs.2017.01.064

4. Тихонов А.Н., Иванников А.Д., Соловьёв И.В., Цветков В.Я., Кудж С.А. Концепция сетецентрического управления сложной организационно-технической системой. М.: МаксПресс, 2010. 136 с. [Tikhonov A.N., Ivannikov A.D., Solov'yov I.V., Tsvetkov V.Ya., Kudzh S.A. *Kontseptsiya setetsentricheskogo upravleniya slozhnoy organizatsionno-tekhnicheskoy sistemoy*. [Concept of Network-Centric Management of Difficult Organizational and Technical System]. Moscow, MaksPress Publ., 2010. 136 p.]

5. Чехарин Е.Е. Большие данные: большие проблемы. Перспективы науки и образования. 2016. № 3 (21). С. 7–11. [Chekharin E.E. [Big Data: Big Problems]. *Prospects of Science and Education*, 2016, no. 3 (21), pp. 7–11. (in Russ.)]

6. Koren I. Detecting and Counteracting Benign Faults and Malicious Attacks in Cyber Physical Systems, *Proc. of 2018 7th Mediterranean Conference on Embedded Computing* (MECO), 2018, June 10–14, p. 1.

7. Zhu Q., Basar T. Towards a Unifying Security Framework for Cyber-Physical Systems. *Proc. of the Workshop on the Foundations of Dependable and Secure Cyber-Physical Systems* (FDSCPS-11), 2011, Dec. 15–18, pp. 47–50.

8. Ghosh T., Sarkar D., Sharma T., Bali R., Desai A. Reliability-Based Software Rejuvenation Scheduling for Cloud-Based Systems. *Proc. of the 2016 IEEE International Conference on Internet of Things (iThings)*, 2016, Dec. 15–18, pp. 822–827. DOI: 10.1109/iThings-GreenCom-CPSCom-SmartData.2016.171

9. Rahme J., Xu H. Reliability-Based Software Rejuvenation Scheduling for Cloud-Based Systems. *Proc. of the 27th International Conference on Software Engineering and Knowledge Engineering*, 2015, July 15, pp. 1–6. DOI: 10.18293/SEKE2015-233

10. Jing Li, Mingze Li, Gang Wang , Xiaoguang Liu, Zhongwei Li, R., Huijun Tang. Global Reliability Evaluation for Cloud Storage Systems with Proactive Fault Tolerance. *Algorithms and Architectures for Parallel Processing Lecture Notes in Computer Science*, 2015, vol. 9531 (3), pp. 189–203. DOI: 10.1007/978-3-319-27140-8_14

11. Dong O., Yu P., Liu H., Feng L., Li W., Chen F., Shi L. The Impact of Information Visualization on Human Problem-Solving Performance in a Complex Business Domain. *Proc. of NOMS 2018 – 2018 IEEE/IFIP Network Operations and Management Symposium*, 2018, April 23–27, pp. 1–6. DOI: 10.1109/NOMS.2018.8406294

12. Lee E.A., Seshia S.A. *Introduction to Embedded Systems – A Cyber-Physical Systems Approach*. MIT Press, 2017, 585 p.

13. Lin Gu, Deze Zeng, Song Guo, Ahmed Barnawi, Yong Xiang. Cost Efficient Resource Management in Fog Computing Supported Medical Cyber-Physical System. *IEEE Transactions on Emerging Topics in Computing*, 2017, vol. 5 (1), pp. 108–119. DOI: 10.1109/TETC.2015.2508382

14. Yi S., Li C., Li Q. The Impact of Information Visualization on Human Problem-Solving Performance in a Complex Business Domain. *Proc. of the 2015 Workshop on Mobile Big Data (Mobidata '15)*, 2015, June 21, pp. 37–42. DOI: 10.1145/2757384.2757397

15. Osanaiye O.A., Chen S., Yan Z., Lu R., Kim-Kwang R. Choo, Dlodlo M.E. From Cloud to Fog Computing: A Review and a Conceptual Live VM Migration Framework. *IEEE Access*, 2017, vol. 5, pp. 8284–8300. DOI: 10.1109/ACCESS.2017.2692960

16. Bolodurina I., Parfenov D. The Development and Study of the Methods and Algorithms for the Classification of Data Flows of Cloud Applications in the Network of the Virtual Data Center. *International Journal of Computer Networks and Communications*, 2018, vol. 10 (2), pp. 15–22. DOI: 10.5121/ijcnc.2018.10202

17. Baccarelli E., Gabriela P., Naranjo V., Scarpiniti M., Shojafar M., Abawajy J.H. Fog of Everything: Energy-Efficient Networked Computing Architectures, Research Challenges, and a Case Study. *IEEE Access*, 2017, vol. 5, pp. 9882–9910. DOI: 10.1109/ACCESS.2017.2702013

Болодурина Ирина Павловна, д-р техн. наук, профессор, зав. кафедрой прикладной математики, Оренбургский государственный университет, г. Оренбург; prmat@mail.osu.ru.

Парфёнов Денис Игоревич, канд. техн. наук, начальник отдела программно-технической поддержки дистанционного обучения, Оренбургский государственный университет, г. Оренбург; parfenovdi@mail.ru.

Поступила в редакцию 20 августа 2018 г.

DOI: 10.14529/ctcr180404

MODELING OF RELIABILITY OF RELIABILITY OF FUNCTIONING OF OBJECTS OF NETWORK INFRASTRUCTURE OF CYBER-PHYSICAL SYSTEM

***I.P. Bolodurina**, prmat@mail.osu.ru,*
***D.I. Parfenov**, parfenovdi@mail.ru*
Orenburg State University, Orenburg, Russian Federation

In the framework of this study, a structural model of an industrial cyber-physical system architecture was constructed using cloud computing as a basic platform. The presented model details the cyber-physical system on four levels of abstraction, combining all the elements on the basis of the multi-agent approach. The proposed approach based on the data mining methods of the monitoring system allows searching and identifying vulnerable from the point of view of reliability elements of the network infrastructure of a cyber-physical system based on the cloud platform. To conduct a consolidated assessment of the current state of network elements, the study developed a model for ensuring the reliability of network infrastructure facilities, presented in the form of a weighted multigraph forming a plan for collecting, analyzing and verifying data received from the monitoring system. At the same time, the parameters of ensuring reliability for hotel components and nodes, both the infrastructure of the cyber-physical system and the cloud platform, are selected as the vertices of the graph. As arcs of the graph, the relations between the established reliability criteria are presented, reflecting the relationship between the state and the operating parameters of the associated nodes of the infrastructure of a cyber-physical system, taking into account the current parameters of circulating data flows. This will allow you to identify system segments that require reconfiguration, which will reduce the overhead required to make changes. At the same time, the neural network approach is used to predict the uninterrupted infrastructure of the cyber-physical system. The use of the proposed hybrid approach made it possible to predict the behavior of the infrastructure over time and warn of possible failures in the operation of individual components and critical nodes.

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

Received 20 August 2018

ОБРАЗЕЦ ЦИТИРОВАНИЯ

Болодурина, И.П. Моделирование обеспечения надежности функционирования объектов сетевой инфраструктуры кибер-физической системы / И.П. Болодурина, Д.И. Парфёнов // Вестник ЮУрГУ. Серия «Компьютерные технологии, управление, радиоэлектроника». – 2018. – Т. 18, № 4. – С. 41–51. DOI: 10.14529/ctcr180404

FOR CITATION

Bolodurina I.P., Parfenov D.I. Modeling of Reliability of Reliability of Functioning of Objects of Network Infrastructure of Cyber-Physical System. *Bulletin of the South Ural State University. Ser. Computer Technologies, Automatic Control, Radio Electronics*, 2018, vol. 18, no. 4, pp. 41–51. (in Russ.) DOI: 10.14529/ctcr180404