Об управлении гетерогенными доверенными блокчейн-средами нового технологического уклада

О. Л. Головин
Российский экономический университет им. Г.В. Плеханова
mifioleg@gmail.com

Е. Г. Андрианова[1], Р. Г. Болбаков[2], А. Н. Миронов[3]
Московский технологический университет
[1]andrianova@mirea.ru, [2]bolbakov@mirea.ru,
[3]amironov1993@yandex.ru

***Аннотация*. Рассмотрены некоторые вопросы управления в реальном времени доверенными средами, формируемыми в рамках нового технологического уклада. Эти среды могут включать различные компоненты сетей вещей и машин IoT/IIoT/M2M. В подобных сложных распределенных системах для обеспечения эффективности, безопасности и интероперабельности обосновано применение блокчейн-алгоритмов частного и публичного распределенного реестра, программно-конфигурируемых сетей SDN/SD-WAN с виртуализацией сетевых функций и неразрывным резервированием, а также гиперконвергентных дата-центров. Для адаптивного управления средой предлагается контроллер, включающий экспертную систему управления, рекуррентную многослойную нейросеть глубокого обучения и квазианалоговое нейроядро, обеспечивающие в реальном времени принятие оптимального решения при неполных и искаженных данных.**

Ключевые слова: новый технологический уклад; доверенная блокчейн-среда; нейрокомпьютинг; программно-конфигурируемая сеть; сети вещей и машин IoT/IIoT/M2M; обработка данных в реальном времени

I. Введение

При переходе к новому технологическому укладу (6-й техноуклад, Индустрия 4.0) значительно возрастает сложность информационно-телекоммуникационных распределенных систем, включающих различные неоднородные компоненты бытового и индустриального интернета вещей и машин IoT/IIoT/M2M [1]. Архитектура, состав и параметры этих компонентов могут меняться при реализации конкретных задач. Такие гетерогенные системы включают, как правило, значительное количество разнотипных датчиков и других источников измерительной информации разной степени точности и достоверности. Это также требует локальной и глобальной обработки неполных и искаженных данных с принятием и исполнением решений в реальном времени, в том числе в критически последний допустимый момент времени.

Важнейшим для обеспечения надежности и безопасности таких систем является создание среды с высоким и управляемым уровнем доверенности, соответствующим поставленными перед системой задачам [2]. В качестве одного из инструментов создания такой доверенной среды возможно использование блокчейн-алгоритмов частного и публичного распределенного реестра [3, 4]. Оптимальный состав гетерогенной доверенной среды также включает облачные инструменты и ресурсы гиперконвергентных дата-центров.

Для сложных распределенных доверенных сред возникает проблема управления и распознавания ситуации для адекватного принятия решения в реальном времени на основе неполных и/или искаженных данных. Для таких задач оптимальными представляются нейросетевые алгоритмы [5–7]. В качестве управляющего центра предлагается контроллер на основе рекуррентных многослойных нейронных сетей глубокого обучения с ядром реального времени на квазианалоговом нейрокомпьютинге.

II. Подход к формированию гетерогенной доверенной среды с IoT/IIoT/M2M

Доверенные гетерогенные среды должны обеспечивать надежное и эффективное функционирование совокупности неоднородных объектов в условиях стохастических процессов, меняющихся параметров и элементов среды, возможных критических ситуаций, с учетом большого потока данных, возможно неполных и/или искаженных. Такие большие данные генерируются входящими в среду устройствами и машинами IoT/IIoT/M2M, например, датчиками с различными характеристиками точности и соотношения сигнал/шум, затухания с учетом потерь в передающей сети. В доверенной среде решения должны приниматься на основе обработки и интеллектуального анализа этих больших данных с выделением определяющей информации в реальном времени.

Важнейшими функциями доверенной среды должны быть идентификация повреждений и изменений в телекоммуникационной сети, поиск и выбор оптимального пути для потоков данных, а также определение наиболее эффективного вычислительного ресурса с учетом характеристик и доступности дата-центров. Эти требования к доверенной среде нового технологического уклада определяют её структуру, технологии и порядок функционирования. Эти же требования определяют инструментарий разработки и оперативное изменение программной поддержки среды – непосредственное макетирование.

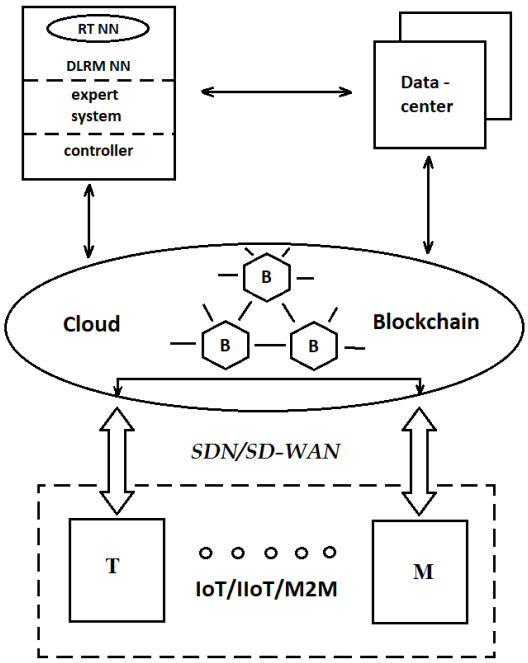

Рис. 1. Пример общей компоновки доверенной блокчейн-среды и структуры контроллера среды с Real-Time – нейроядром

На рис. 1 представлена компоновка гетерогенной доверенной среды, включающая блокчейн-реализации, сети SDN/SD-WAN, облачные решения с функциями фильтрации данных и оперативного выбора вычислительных ресурсов, гиперконвергентные дата-центры на основе микросерверов, сети вещей и машин IoT/IIoT/M2M с возможным изменением состава и параметров и средства ассиметричной криптографии. Интеллектуальным центром среды является её контроллер.

Блокчейн-технологии обеспечивают доверие, определяют уровень защиты и ограничивают риски в среде. Выбор типа блокчейна зависит от задач среды. От выбора характеристик блокчейна также зависят требования к контроллеру среды, в который могут быть включены инструменты распознавания критических ситуаций с доверием, а также блокировки манипуляций. В случае ограниченного набора пользователей-заказчиков распределенной сети машин может применяться частный реестр. В то же время, например, при общегородском интернете вещей публичный реестр предпочтителен, однако может быть ограничен квалифицированными участниками. Вместе с тем, ограничения участников могут создать возможность манипуляции с блокчейном, включая откаты действий и псевдоконсенсусы, что может породить кризис доверия в среде, в том числе в отношении смарт-контрактов.

При организации взаимодействия нескольких доверенных сред, в том числе пересекающихся по компонентам, доверие можно делегировать в виде обмена хэшей текущих блоков. В этом случае возможна и более сложная, уже не одноранговая, топология блокчейн-системы и дополнительные требования к контроллеру среды.

В существенно распределенных доверенных средах эффективно применение программно-конфигурируемых сетей SDN/SD-WAN с виртуализацией сетевых функций [8,9]. Опыт показывает, что SDN (software-defined network) сети наиболее пригодны для обеспечения гиперконвергентности, гибкости и адаптивности доверенных сред, включающих виртуальные ресурсы облачных сервисов и центры обработки данных. В гетерогенных средах, включающих сети вещей и машин IoT/IIoT/M2M, технологии SDN обеспечивают необходимый набор функций и гибкость при взаимодействии объектов друг с другом и с внешней средой, а также поддерживает интероперабельность компонент [10].

Для дополнительной защиты и повышения доверенности, особенно в корпоративных средах, интересны SD-WAN сети (software-defined - wide area network; программно конфигурируемая – глобальная компьютерная сеть), изначально основанные на идеях и базовой архитектуре SDN, однако имеющие отличия, важные для гетерогенной среды. В частности, SD-WAN по сравнению с SDN отличается более сложной аппаратной и программной реализацией. Целью усложнений в основном является дополнительная защита (безопасность) и самонастраивающиеся сети (особая сетевая аналитика). Механизмы повышения быстродействия в SD-WAN при реализации доверенных блокчейн-сред могут быть выполнены в том числе, например, на базе масштабируемых многопротокольных MPLS – решений (multiprotocol label switching – многопротокольная коммутация по меткам). Для доверенных сред перспективны возможности SDN/SD-WAN по работе с квантовыми роутерами, а также реализации на базе SDN/SD-WAN защищенных сетевых решений поверх общедоступных публичных телекоммуникационных сетей – «туннелирование».

III. Контроллер гетерогенной доверенной среды

Управление гетерогенной доверенной средой осложняется наличием значительного количества частично взаимодействующих стохастичных процессов. Необходимо распознавать и оценивать явления и ситуации в реальном времени на основе неполных и/или недостоверных (искаженных) больших массивов данных, изменений в компонентах среды и в реализуемых задачах. Также управленческие решения необходимо принимать, имея в виду историю и прогнозы прохождения процессов.

Оптимальным представляется реализация основных функций управления средой в контролере, использующем различные типы нейронных сетей и разделенном на три следующие основные взаимодействующие части:

- система управления экспертного типа, включая контроль телекоммуникационных сетей, поддержку протоколов управления и базовых функций коммутации, общий контроль потоков данных, технические аспекты;
- интеллектуальная система на основе технологии рекуррентных многослойных нейронных сетей глубокого обучения (DLRM NN – deep learning recurrent multilayer neural network), обеспечиваю-

щей обратную связь, исторический анализ и прогнозирование событий, а также поведение компонентов среды, кластеризацию объектов, событий и процессов;

- нейроядро реального времени на квазианалоговом нейрокомпьютинге (RT NN – real time neural network), определяющее время отклика и участвующее в распознавании критических ситуаций совместно с другими частями контроллера. Нейроядро имеет собственную периодическую динамику и внутреннее время, задаваемое возможными событиями и кризисными ситуациями в управляемой доверенной среде, отклик на которые являются задачами нейроядра. Именно принятие решения о времени отклика, последнего допустимого времени отклика в кризисных ситуациях, является основной задачей нейроядра. Фактически нейроядро минимизирует риски неоправданной задержки отклика на кризисную ситуацию и неточности отклика при некорректных данных.

Предлагаемый нами подход к реализации основных функций управления на основе нейронных сетей позволяет разрешать конфликты и обеспечивать безопасность в пересекающихся по компонентам IoT/IIoT/M2M и телекоммуникационным сетям доверенных сред, создавая распределенное управление этими средами.

IV. Динамика RT – нейроядра

Динамика нейроядра в простых случаях определяется только изменением состояний нейронов, например, для i-го нейрона

$$\frac{\partial \Theta_i}{\partial t} = \omega_{o_i} - k(t,i) \cdot \frac{1}{N} \cdot \sum_{j=1, j\neq i}^{N} T_{ij} \cdot \varphi(\Theta_i - \Theta_j)$$

где N – число нейронов; ω_{o_i} – собственная периодическая динамика i-го нейрона с недетерминированным числом состояний; θ_i и θ_j – состояния (фазы в случае нейронов-осцилляторов) i-го и j-го нейрона соответственно, $0 \leq \theta_i, \theta_j \leq 2\pi \; \forall i,j$, а совокупность состояний (фаз) нейронов представляют матрицу кратковременной памяти STM (short term memory); $k(t,i)$ – распределение силового поля по времени (постоянное, импульсное и пр.) и пространству нейронов – позволяет, в частности, оперативно реагировать на внешние вызовы, в том числе менять топологию сети; T_{ij} – матрица долговременной памяти LTM (long term memory), определяемая при настройке нейронной сети;

Вариант для нейронов-осцилляторов $\varphi(\theta_\text{i} - \theta_j) = sin(\theta_\text{i} - \theta_j)$, то есть $-1 \leq \varphi(\theta_\text{i} - \theta_j) \leq 1$.

Подобные алгоритмы были ранее разработаны авторами этой статьи для возможной реализации на оптических и гибридных нейрокомпьютерах, в том числе с использованием когерентного и некогерентного излучения различных частотных диапазонов, а также фотонного эха, и могут быть исполнены в квазианалоговом, аналоговом или гибридном виде [11]. В таком нейроядре с собственной периодической динамикой путем настройки устанавливается количество распознаваемых ситуаций, точность, время отклика на различные ситуации. Нейроядро вместе с рекуррентной нейросетью прогнозирует и определяет типы, время, источники кризисных ситуаций, выдает адекватные отклики в реальном времени, что позволяет контроллеру принять меры предупреждения и/или реагирования.

V. Обсуждение результатов

Управление гетерогенной доверенной блокчейн-средой контроллером с рекуррентной многослойной нейросетью глубокого обучения и квазианалоговым нейроядром с собственной периодической динамикой способно обеспечить эффективное функционирование среды. В дополнении к этому, такое управление позволяет в реальном времени принимать оптимальные решения на основе неполных и/или искаженных данных.

Обсуждаемая в данной публикации гетерогенная доверенная среда предполагает значительное количество компонентов, относящихся к новому технологическому укладу и имеющих тенденцию к существенным изменениям. Очевидно, что новые типы компонентов безусловно будут частью таких сред. Прогресс неизбежен и в телекоммуникационных решениях и в обработке неполных и искаженных больших данных. Поэтому следует ожидать появления новых подходов к формированию и управлению гетерогенных доверенных сред, включающих элементы реального времени. Кроме того, нам представляется перспективным создание средств автоматизации проектирования и конструирования управляющих механизмов, контроллеров для конкретных гетерогенных доверенных сред, включая подбор видов и настройку интеллектуальных составляющих таких управленческих решений. Ещё одним потенциально интересным направлением, с нашей точки зрения, является применение аналоговых или гибридных компонент в системах управления гетерогенными доверенными средами в реальном времени.

Список литературы

[1] Жданов С.Е. Глобальная промышленная революция. Международный опыт стандартизации интернета вещей в рамках деятельности международного союза электросвязи // Электронный научный журнал «ИТ-Стандарт». 2016. №1, С.13-22. [Электронный ресурс] – Режим доступа: http://www.itstandard.ru (дата обращения: 08.02.2018).

[2] Андрианова Е.Г., Головин О.Л. Концептуальные аспекты построения доверенных неоднородных блокчейн-сред нового технологического уклада // Электронный научный журнал «ИТ-Стандарт». 2017. № 3. С.1-6. [Электронный ресурс] – Режим доступа: http://www.itstandard.ru (дата обращения: 12.02.2018).

[3] Melanie Swan. Blockchain: Blueprint for a New Economy.O'Reilly Media. 2015. 152 p.

[4] Gilbert H., Handschuh H. Security Analysis of SHA-256 and Sisters // Selected Areas in Cryptography: 10th Annual International Workshop, SAC 2003. Ottawa. Canada. 2003.

[5] Milos Miljanovic. Comparative analysis of Recurrent and Finite Impulse Response Neural Networks in Time Series Prediction //Indian Journal of Computer and Engineering. 2012. Vol.3, No 1. pp. 180-191.

[6] Yoshua Bengio. Learning Deep Architectures for AI // Foundations and Trends in Machine Learning. 2009, Vol. 2, No.1 pp. 1–127.

[7] Hopfield J.J. Neural networks and physical systems with emergent collective computational abilities // Proceedings of National Academy of Sciences. 1982. Vol. 79, No.8. pp. 2554–2558.

[8] Головин О.Л., Полторак А.В. О подходе к обеспечению надежности и безопасности в информационно-коммуникационных системах промышленного и бытового интернета вещей и объектов IoT/IIoT/M2M // XVI Научно-практическая конференция «Современные информационные технологии в управлении и образовании». 2017. С. 124-130.

[9] Андрианова Е.Г., Головин О.Л., Коняев Г.Б., Полторак А.В. Программно-конфигурируемые сети SD-WAN для интернета вещей и машин IoT/IIoT/M2M // VIII Международная конференция «ИТ-Стандарт 2017». 2017. С. 243-249.

[10] Андрианова Е.Г., Головин С.А., Гудкова О.К., Лаптев А.Н. Методика формирования профилей стандартов информационных технологий в интересах обеспечения интероперабельности сложных распределенных систем // Журнал радиоэлектроники. 2014. №12. С.25.

[11] Oleg L. Golovin. An artificial network based on unfixed states number oscillators // International Joint Conference on Neural Networks IJCNN’91 Singapore. Paper NO: S0163, Session: Hybrid system. 1991.