ИССЛЕДОВАНИЕ ЭФФЕКТИВНЫХ АЛГОРИТМОВ ПОВЫШЕНИЯ ОТКАЗОУСТОЙЧИВОСТИ В СЕТЯХ SDN НА БАЗЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Г.М. Нурудинов, *Московский технический университет связи и информатики, g.nurudinov@mail.ru.*

УДК 004.855.5

Аннотация. В статье представлена разработка и исследование алгоритмов, направленных на повышение отказоустойчивости в сетях *SDN*, с использованием ИИ. Модель, предложенная в этой статье, учитывает способность ИИ обрабатывать большие объемы данных и принимать решения в режиме реального времени для эффективного управления сетевым трафиком и ресурсами. Также освещены гибридные подходы, которые интегрируют ИИ с традиционными сетевыми механизмами, демонстрируя возможность адаптации к динамичным условиям сети и предотвращения сбоев. Анализ эффективности предложенных алгоритмов осуществляется с применением симуляционных технологий.

Ключевые слова: *SDN*; ИИ; отказоустойчивость; алгоритмы; гибридные подходы; управление сетевым трафиком; динамическая оптимизация; симуляция; машинное обучение; централизованное управление.

RESEARCH OF EFFECTIVE ALGORITHMS FOR INCREASING FAULT TOLERANCE IN SDN NETWORKS BASED ON ARTIFICIAL INTELLIGENCE

Gasan Nurudinov, *Moscow Technical University of Communications and Informatics.*

Annotation. The article presents the development and research of algorithms aimed at improving fault tolerance in *SDN* networks using AI. The model proposed in this article takes into account the ability of AI to process large amounts of data and make real-time decisions for effective management of network traffic and resources. It also highlights hybrid approaches that integrate AI with traditional network mechanisms, demonstrating the capabilities to adapt to dynamic network conditions and prevent failures. Analysis of the effectiveness of the proposed algorithms is carried out using simulation technologies.

Keywords: *SDN*; *AI*; fault tolerance; algorithms; hybrid approaches; network traffic management; dynamic optimization; simulation; machine learning; centralized management.

Введение

С появлением *Software-Defined Networking* (*SDN*) сетевые архитектуры стали гораздо более гибкими и масштабируемыми, предоставляя возможности, которые были труднодоступны в традиционных сетевых конфигурациях. Основное преимущество *SDN* заключается в декомпозиции традиционных сетевых архитектур, а именно в разделении управления и передачи данных на два отдельных слоя. Это позволяет администраторам централизованно управлять сетевым трафиком и ресурсами, обеспечивая большую гибкость и контроль над сетевой инфраструктурой [1-4].

Тем не менее, с гибкостью и централизацией управления в *SDN* приходят и новые вызовы в области обеспечения надежности и отказоустойчивости. Так как управление сетью сконцентрировано в центральном контроллере, это может

создать узкие места и повысить риск сбоев или атак, что, в свою очередь, может оказать влияние на всю сетевую инфраструктуру.

В этом контексте, искусственный интеллект (ИИ) представляет огромный потенциал для повышения отказоустойчивости в *SDN*. Способность ИИ к обработке и анализу больших объемов данных в режиме реального времени, а также его способность обучаться и адаптироваться к изменяющимся условиям, делает его мощным инструментом для совершенствования сетевых систем.

С помощью ИИ можно реализовать механизмы прогнозирования для обнаружения потенциальных сбоев, прежде чем они произойдут, и принятия соответствующих мер. Кроме того, с применением алгоритмов машинного обучения, *SDN* может адаптироваться к различным сценариям сетевого трафика, оптимизируя маршрутизацию и уменьшая вероятность перегрузки сети [5, 6].

Также стоит отметить, что совместное использование ИИ и *SDN* не ограничивается только вопросами надежности, но и открывает новые горизонты для безопасности, управления полосой пропускания и сокращения времени отклика в сетевых системах.

Актуальность применения ИИ в *SDN*

С ростом сложности сетевых систем и увеличением объемов данных, передаваемых через сети, становится все более важным иметь возможность эффективного управления сетью, а также обеспечивать ее надежность и безопасность. Традиционные методы управления сетью, основанные на статических правилах и политиках, становятся неадекватными в динамично меняющемся сетевом окружении. В этом контексте, применение ИИ в *SDN* предоставляет уникальные возможности для автоматизации, оптимизации и улучшения отказоустойчивости сетевых систем [7].

Основные понятия и проблемы

SDN представляет собой подход к созданию сетей, в котором управление сетью централизовано и отделено от аппаратных средств. Это позволяет сетевым администраторам легче управлять трафиком и ресурсами, но также вводит риск отказа центрального контроллера или проблем с коммуникацией между контроллером и сетевыми устройствами.

Основные вызовы в области отказоустойчивости *SDN* включают [8, 9]:

- Обнаружение и восстановление от сбоев сети.
- Обеспечение непрерывности работы сети при отказе одного или нескольких узлов.
- Защита от сетевых атак.
- Роль искусственного интеллекта.

ИИ может быть использован для повышения отказоустойчивости *SDN* сетей, обеспечивая:

- Прогнозирование сбоев: используя машинное обучение можно анализировать исторические данные о работе сети, чтобы предсказать возможные сбои и принять меры по их предотвращению.
- Адаптивное управление трафиком: алгоритмы ИИ могут адаптировать маршруты трафика в режиме реального времени для минимизации задержек и предотвращения перегрузок, что улучшает надежность сети.
- Обнаружение и смягчение атак: ИИ может быть использован для мониторинга сетевого трафика на предмет аномалий, которые могут

указывать на сетевую атаку, и автоматически применять меры по смягчению угроз.

Исследование алгоритмов

Глубокое обучение для прогнозирования сбоев

Один из подходов к повышению отказоустойчивости *SDN* – использование глубокого обучения для прогнозирования сбоев. Глубокие нейронные сети (ГНС) обучаются на больших наборах данных о производительности сети, чтобы предсказать вероятность сбоев в определенных узлах или компонентах сети. Это позволяет операторам сети принимать проактивные меры для предотвращения сбоев или минимизации их воздействия на сеть [10].

Обучение с подкреплением для адаптивного управления трафиком

Обучение с подкреплением (*RL*) представляет собой тип машинного обучения, в котором агент обучается, взаимодействуя с окружающей средой. В контексте *SDN*, алгоритмы *RL* могут быть использованы для адаптации маршрутов трафика в режиме реального времени. Агент, управляющий трафиком, может учиться оптимизировать маршруты, уменьшать задержки и предотвращать перегрузку сети, получая вознаграждение за улучшение производительности сети.

Анализ временных рядов для обнаружения аномалий

Анализ временных рядов с использованием ИИ может быть эффективным подходом к обнаружению аномалий в сетевом трафике, которые могут указывать на сбои или атаки. Методы, такие как *LSTM* (*Long Short-Term Memory*), могут использоваться для анализа паттернов сетевого трафика и выявления отклонений от нормы.

Интеграция ИИ и *SDN*

Динамическая оптимизация маршрутизации

ИИ может быть использован для анализа сетевого трафика в режиме реального времени и динамической оптимизации маршрутов передачи данных. Алгоритмы машинного обучения, такие как обучение с подкреплением, помогают в определении наиболее эффективных путей для передачи данных на основе текущих условий сети, минимизируя задержки и предотвращая перегрузку сетевых узлов [11].

Обнаружение и смягчение атак

Используя техники глубокого обучения и анализа временных рядов, ИИ может выявлять аномальные шаблоны в сетевом трафике, которые могут указывать на сетевые атаки или сбои. Это позволяет системам *SDN* быстро реагировать на потенциальные угрозы и применять стратегии смягчения для обеспечения непрерывности работы сети.

Автоматическое восстановление после сбоев

С помощью ИИ *SDN* системы могут автоматически восстанавливать себя после сбоев, перенаправляя трафик через альтернативные маршруты и восстанавливая сетевые услуги без значительных прерываний.

Гибридные подходы: комбинирование искусственного интеллекта и традиционных методов для повышения отказоустойчивости в *SDN*

Помимо использования чистого ИИ для улучшения отказоустойчивости в *SDN*, гибридные подходы, которые комбинируют ИИ с традиционными методами

управления сетью, становятся все более популярными. Это связано с тем, что такие подходы позволяют совместить лучшие стороны обеих технологий [12].

Применение ИИ для предсказания сбоев

Одним из способов интеграции ИИ в *SDN* является использование алгоритмов машинного обучения для предсказания потенциальных сбоев в сети. Модели ИИ, обученные на исторических данных о сетевом трафике и производительности, могут предсказывать вероятность сбоев и предупреждать систему заблаговременно.

Традиционные механизмы устойчивости для реагирования на сбои

После того, как система была предупреждена о потенциальном сбое с помощью ИИ, традиционные механизмы отказоустойчивости, такие как протоколы маршрутизации с отказоустойчивостью, могут использоваться для обеспечения непрерывности работы сети. Это включает в себя перенаправление трафика через резервные маршруты, использование техник быстрого восстановления и другие методы.

Адаптивная оптимизация сетевых ресурсов

Гибридные системы также могут использовать ИИ для динамической оптимизации сетевых ресурсов, адаптируясь к изменяющимся условиям сети. В то же время, статические политики и правила, основанные на традиционных методах, являются основой для гарантирования стабильности и соблюдения стандартов безопасности.

Преимущества гибридного подхода

- Большая гибкость и способность адаптации к динамично меняющимся условиям.
- Комбинирование предсказательных возможностей ИИ с проверенными временем традиционными механизмами устойчивости для более надежного управления сетью.
- Снижение вероятности ложных срабатываний, поскольку традиционные методы могут служить проверкой достоверности предсказаний ИИ.
- Улучшение эффективности ресурсов путем оптимального распределения сетевого трафика и загрузки.

Недостатки и вызовы гибридного подхода

- Сложность интеграции: комбинирование ИИ с традиционными механизмами вероятно увеличит сложность системы, что затрудняет ее внедрение и обслуживание.
- Потребность в точных данных: для обеспечения эффективного прогнозирования сбоев, ИИ должен быть обучен на большом объеме качественных данных, что может быть ресурсоемким.
- Возможные конфликты между решениями, принятыми ИИ, и традиционными механизмами управления.

Гибридный подход, который комбинирует Искусственный Интеллект с традиционными методами управления сетью, предлагает перспективное решение для повышения отказоустойчивости в *SDN*. Тем не менее, это также влечет за собой ряд вызовов, которые должны быть преодолены для обеспечения эффективности и надежности данного подхода [13].

Для успешного применения гибридных подходов необходимо обеспечить тесное взаимодействие между компонентами ИИ и традиционными сетевыми протоколами, а также уделить внимание сбору и обработке данных высокого качества для обучения моделей ИИ.

По мере развития технологии, гибридные системы, которые могут адаптироваться и реагировать на изменения в сетевой среде, становятся все более важными для поддержания высокого уровня отказоустойчивости и обеспечения надежного функционирования сетей.

Будущие перспективы

Для дальнейшего улучшения отказоустойчивости *SDN* на базе ИИ следует рассмотреть несколько направлений исследований:

- Гибридные модели ИИ: интеграция различных методов машинного обучения, таких как глубокое обучение и обучение с подкреплением, возможно приведут к созданию более эффективных систем прогнозирования и адаптивного управления.
- Автономные сети: разработка сетей, способных автономно адаптироваться к изменяющимся условиям и восстанавливать себя после сбоев, с минимальным вмешательством человека.
- Интеграция с другими технологиями: совмещение ИИ с другими технологиями, такими как блокчейн, для создания безопасных и отказоустойчивых сетевых систем.
- Этические и правовые аспекты: изучение этических и правовых аспектов применения ИИ в управлении сетями, включая вопросы приватности, безопасности и ответственности.

Заключение

SDN представляет собой переломный момент в сфере сетевых технологий, обеспечивающих гибкость, масштабируемость и централизованное управление сетевыми ресурсами. Однако, с новыми возможностями возникают и новые вызовы, особенно в области обеспечения отказоустойчивости и надежности сетей. ИИ возникает как мощный инструмент, способный внести значительный вклад в решение этих проблем, благодаря своей способности обрабатывать большие объемы данных и принимать решения в режиме реального времени.

В статье были рассмотрены различные аспекты применения ИИ для повышения отказоустойчивости в *SDN*, включая использование машинного обучения для предсказания сетевых сбоев, оптимизации маршрутизации и управления сетевым трафиком. Особое внимание было уделено гибридным подходам, которые комбинируют ИИ с традиционными сетевыми протоколами и механизмами управления.

Несмотря на значительные преимущества, которые ИИ может принести в *SDN*, существует ряд вызовов, включая сложность интеграции, потребность в высококачественных данных для обучения, а также вопросы безопасности и приватности.

Литература

1. Гетьман А.И., Маркин Ю.В., Евстропов Е.Ф., Обыденков Д.О. Обзор задач и методов их решения в области классификации сетевого трафика // Труды ИСП РАН, 2017. – Т. 29. – № 3. – С. 117-150. DOI: 10.15514/ISPRAS-2017-29(3)-8.

2. Boutaba R., Salahuddin M. A., Limam N., Ayoubi S., Shahriar N., Solano F. E., Rendon O. M. A comprehensive survey on machine learning for networking: evolution,

applications and research opportunities // Journal of Internet Services and Applications, 2018. – № 9. – P. 1-99. https://doi.org/10.1186/s13174-018-0087-2.
3. Harkut Dr Dinesh. An Overview of Network Traffic Classification Methods. 2015.
4. Шелухин О.И., Ерохин С.Д., Ванюшина А.В. Классификация IP-трафика методами машинного обучения. Под ред. О.И. Шелухина. М.: Горячая линия – Телеком, 2018. – 282 с.
5. Xie J. et al. A Survey of Machine Learning Techniques Applied to Software Defined Networking (SDN): Research Issues and Challenges // IEEE Communications Surveys & Tutorials. 2018. P. 393-430. https://doi.org/10.1109/comst.2018.2866942.
6. Zhao Y., Li Y., Zhang X., Geng G., Zhang W. and Sun Y. A Survey of Networking Applications Applying the Software Defined Networking Concept Based on Machine Learning // IEEE Access, 2019. – V. 7. – P. 95397-95417. https://doi.org/10.1109/ACCESS.2019.2928564.
7. Mohammed A.R., Mohammed S.A. and Shirmohammadi S. Machine Learning and Deep Learning Based Traffic Classification and Prediction in Software Defined Networking // Proc. 2019 IEEE International Symposium on Measurements & Networking (M&N). – P. 1-6. https://doi.org/10.1109/IWMN.2019.8805044.
8. Singhal P., Mathur R., Vyas H. State of the Art Review of Network Traffic Classification based on Machine Learning Approach // Proc. International Conference on Recent Trends in Engineering & Technology, 2013. – P. 12-15.
9. Nguyen T., Grenville A. A survey of techniques for internet traffic classification using machine learning // IEEE Communications Surveys and Tutorials, 2008. – V. 10. – P. 56-76.
10. Patcha A. and Park J.-M. An overview of anomaly detection techniques: Existing solutions and latest technological trends // Computer Networks, 2007. – V. 51. – № 12. – P. 3448-3470.
11. Latah M., Toker L. Artificial Intelligence Enabled Software Defined Networking: A Comprehensive Overview // IET Networks, 2018. – V. 8. https://doi.org/10.1049/ietnet. 2018.5082.
12. Buczak A. L. and Guven E. A survey of data mining and machine learning methods for cyber security intrusion detection // IEEE Communications Surveys & Tutorials, 2016. – V. 18. – № 2. – P. 1153-1176.
13. Hodo E., Bellekens X. J., Hamilton A. W., Tachtatzis C., and Atkinson R. C. Shallow and Deep Networks Intrusion Detection System: A Taxonomy and Survey // ArXiv, 2017. abs/1701.02145.