

УДК 004.89

ТЕСТИРОВАНИЕ УСТОЙЧИВОСТИ МОДЕЛЕЙ НА ОСНОВЕ ИМИТАЦИИ РАСПРЕДЕЛЁННОГО ШУМА

Шейхов Г.В., Старший оператор научной роты, III курс
Военная академия связи имени Маршала Советского Союза С. М. Буденного,
г. Санкт-Петербург

В последние годы распределённое обучение и использование больших нейросетей стали неотъемлемой частью современных систем искусственного интеллекта, обеспечивая масштабируемость и эффективность обработки огромных массивов данных. Вместе с этим возросла и потребность в глубоком понимании устойчивости обученных моделей, особенно в условиях, когда входные данные подвержены различным видам искажений, включая шум, возникающий в распределённых системах передачи, обработки и сбора информации.

Одним из ключевых вызовов становится оценка поведения моделей при воздействии так называемого распределённого шума – случайных или структурированных возмущений, которые не локализованы в одном источнике, а формируются из множества разнородных и зачастую независимых факторов, проявляющихся в распределённой среде. Методика тестирования устойчивости моделей с использованием имитации распределённого шума представляет собой систематический подход, направленный на выявление и количественную оценку влияния таких возмущений на качество и стабильность работы искусственных нейронных сетей [1].

Распределённый шум может иметь разную природу и возникать на разных уровнях архитектуры систем машинного обучения. Это может быть влияние неточного измерения сенсоров, потеря пакетов данных в сетевых протоколах, временные задержки и вариации в потоках данных, ошибки при передаче между распределёнными узлами, а также системные сбои, вызванные параллельной обработкой и конкуренцией за ресурсы.

В совокупности эти факторы создают сложную, многомерную картину возмущений, которая существенно влияет на качество входной информации и, следовательно, на предсказания модели. При этом традиционные методы тестирования, ориентированные на локальные и изолированные искажения, не способны адекватно смоделировать и оценить подобные многофакторные и распределённые воздействия.

Для адекватного тестирования устойчивости в таких условиях необходима разработка и внедрение специальных методов имитации распределённого шума, которые позволяют воспроизводить реальные сценарии работы систем в контролируемой среде. Это достигается за счёт создания комплексных моделей шума, объединяющих статистические характеристики, временные корреляции, пространственное распределение и вариативность параметров. Имитация может включать генерацию шумов с заданной спектральной плотностью, моделирование временных выбросов, коррелированных помех, а также пространственно распределённых искажений, отражающих реальные особенности каналов связи и среды сбора данных [2].

Важным элементом методики является интеграция этих моделей шума непосредственно в процесс тестирования обученных моделей, что позволяет не только наблюдать влияние искажений на конечный результат, но и проводить анализ изменений внутренних представлений и поведения нейросети. При этом применяются разнообразные метрики устойчивости: помимо традиционных показателей качества классификации или регрессии, учитываются показатели стабильности выходных распределений, изменчивости активаций слоёв, а также динамические характеристики реакции модели на серии шумовых импульсов или временных паттернов. Такой комплексный анализ обеспечивает более глубокое понимание устойчивости модели к сложным и реалистичным воздействиям [3].

Особое внимание уделяется построению автоматизированных тестовых сред и фреймворков, которые способны воспроизводить сценарии распределённого шума в реальном времени и масштабировать проверки на большие объёмы данных и различные архитектуры моделей. Эти среды включают в себя инструменты для генерации шума с гибким управлением параметрами, мониторинга состояния модели и агрегации результатов тестирования в удобные для анализа отчёты. Такой инструментарий позволяет эффективно интегрировать тестирование устойчивости в процессы MLOps, обеспечивая регулярный контроль качества и своевременное выявление деградаций в работе моделей [4].

Методика имитационного тестирования с распределённым шумом играет ключевую роль в критически важных приложениях, где высокая степень надёжности и безопасность данных являются приоритетом. Это касается областей автономного вождения, медицинской диагностики, промышленного мониторинга, финансовых технологий и других. В этих сферах сбои, вызванные непредсказуемыми шумовыми воздействиями, могут привести к серьёзным последствиям, поэтому способность систем выдерживать и корректно работать в условиях распределённых помех становится обязательным требованием.

Кроме того, разработанная методика способствует исследованию и оптимизации архитектур моделей с целью повышения их робастности. Анализ результатов тестирования позволяет выявлять уязвимые места в сети, которые особенно чувствительны к шуму, и разрабатывать методы регуляризации, адаптивной нормализации, избыточного кодирования и иных техник, направленных на усиление устойчивости. Это создаёт замкнутый цикл улучшения качества, в котором имитационное тестирование служит не только инструментом верификации, но и источником ценных данных для оптимизации [5].

В итоге, методика оценки устойчивости обученных моделей посредством имитации распределённого шума представляет собой современный и комплексный подход, способный повысить надёжность и безопасность искусственного интеллекта в условиях реальных и сложных сценариев эксплуатации. Она объединяет теоретические модели шума, инженерные решения по их генерации и масштабированию, а также практические инструменты анализа поведения моделей.

Реализация и распространение таких методик являются важным шагом на пути к созданию доверенных, прозрачных и устойчивых систем машинного обучения, способных эффективно функционировать в динамично меняющейся и потенциально враждебной среде.

Список литературы:

1. Fawzi, A. Robustness of Classifiers : From Adversarial to Random Noise / A. Fawzi, S.-M. Moosavi-Dezfooli, P. Frossard // Advances in Neural Information Processing Systems. – 2016. – Vol. 29.
2. Hosseini, H. Google Cloud Vision API Is Not Robust to Noise / H. Hosseini, B. Xiao, R. Poovendran // 2017 16th IEEE International Conference on Machine Learning and Applications. – Cancun : IEEE, 2017. – P. 101-105. – DOI 10.1109/ICMLA.2017.0-172.
3. Rusak, E. A Simple Way to Make Neural Networks Robust against Diverse Image Corruptions / E. Rusak, L. Schott, R. S. Zimmermann [et al.] // Computer Vision - ECCV 2020. – Cham : Springer, 2020. – P. 53-69. – DOI 10.1007/978-3-030-58580-8_4.
4. Michaelis, C. Benchmarking Robustness in Object Detection : Autonomous Driving when Winter Is Coming / C. Michaelis, M. Mitzkus, R. Geirhos [et al.] // arXiv. – 2019. – arXiv:1907.07484.
5. Basu, S. Influence Functions and Robustness of Minimum Risk Training / S. Basu, X. You, L. Feizi, S. Feizi // Advances in Neural Information Processing Systems. – 2020. – Vol. 33. – P. 13850-13861.