Проект демонстрирует, как через игровые механизмы можно формировать системное понимание сложных социально-экономических процессов. Это особенно важно для подготовки молодого поколения к решению задач, связанных с реализацией Повестки дня в области устойчивого развития до 2030 года. Интеграция образовательных инноваций в процесс продвижения целей устойчивого развития способствует созданию инклюзивной и эффективной модели просвещения студентов.

Список использованных источников

1. Цели устойчивого развития [Электронный ресурс]. – Режим доступа: https://sdgs.by/ – Дата доступа: 14.10.2025.

УДК 004.85.056.5

А.В. Кизино
Белорусский государственный технологический университет
Минск, Беларусь

СРАВНЕНИЯ ХЭШЕЙ ДЛЯ ОЦЕНКИ СТЕПЕНИ СИНХРОНИЗАЦИИ НЕЙРОННЫХ СЕТЕЙ НА ОСНОВЕ АЛГЕБРЫ ДЕЙСТВИТЕЛЬНЫХ ЧИСЕЛ

Аннотация. *В статье представлен метод оценки синхронизации древовидных машин четности (TPM) на основе сравнения криптографических хэшей весовых векторов. В ходе анализа установлено, что подход значительно снижает объем передаваемых данных и повышает безопасность за счет однонаправленности хэш-функций и эффективен в системах с ограниченной пропускной способностью.*

A.V. Kizino
Belarusian State Technological University
Minsk, Belarus

HASH COMPARISONS FOR EVALUATING THE DEGREE OF SYNCHRONISATION OF NEURAL NETWORKS BASED ON REAL NUMBER ALGEBRA

Abstract. *The article presents a method for evaluating the synchronisation of tree-like parity machines (TPMs) based on comparing cryptographic hashes of weight vectors. The analysis shows that this approach significantly reduces the amount of data transmitted and increases security due to the unidirectionality of hash functions, and is effective in systems with limited bandwidth.*

Введение. Древовидные машины четности (Tree Parity Machines, TPM) представляют собой класс нелинейных дискретных нейронных сетей, впервые предложенные для криптографических приложений в конце XX века. Архитектура TPM состоит из трёх слоёв: входного слоя с бинарными входами (±1), скрытого слоя с K нейронов четности, каждый из которых выполняет операцию произведения, и выходного слоя, выдающего единственный бит четности [1].

Процесс синхронизации двух TPM-машин основан на принципе взаимного обучения, при котором обе машины получают одинаковые случайные входные последовательности и обмениваются только выходными битами tau. На основе совпадения или несовпадения выходных значений каждая машина адаптирует свои веса согласно специальному обучающему правилу. Изначально веса обеих машин инициализируются случайно и независимо, однако в результате итеративного процесса они приходят в состояние синхронизации, при котором обе машины выдают идентичные выходные последовательности и могут использовать полученные веса в качестве общего криптографического ключа.

Выделяются несколько основных подходов к оценке степени синхронизации TPM: выделение косинуса угла между весовыми векторами, вычисление евклидова расстояния в весовом пространстве и метод совпадения выходных сигналов. Классические методы оценки синхронизации сталкиваются с рядом ограничений. Прямое сравнение весовых векторов требует их передачи или хранения в доступном виде, что создает потенциальную уязвимость в криптографических приложениях. Атакующий, получивший доступ к весовым данным, может непосредственно восстановить криптографический ключ, минуя процесс синхронизации. Так же проблемой является то, что система предъявляет высокие требования к полосе пропускания. Каждый вес занимает несколько бит памяти, поэтому общий объем информации для передачи составляет $K \times N \times \log_2(2L+1)$ бит на одну проверку синхронизации. Для больших сетей (K=5-10, N=40-100) это может составлять сотни байт информации. В качестве недостатка так же выделяют чувствительность к коллизиям и шуму. В реальных системах с шумом или ошибками передачи методы прямого сравнения становятся менее надежными, требуя избыточного кодирования и повторной передачи. Так же, по мере увеличения параметров TPM (K, N, L) вычисление метрик синхронизации становится более затратным по времени и памяти [2].

Основная часть. Предлагаемый метод сравнения хэшей для оценки синхронизации TPM представляет качественный сдвиг в подходе к мониторингу и верификации синхронизации нейросетей. В отличие от классических методов, этот подход применяет криптографические хэш-функции к векторам весов или выходным данным сетей, получая компактное, фиксированное представление состояния системы.

Математически метод может быть представлен следующим образом: для вектора весов $w = (w_1, w_2, \ldots, w_{KN})$ вычисляется хэш-значение $H(w) = \text{SHA-256}(\text{serialize}(w))$, где serialize – функция, преобразующая вектор весов в последовательность байт. Синхронизация двух машин проверяется сравнением $H(w_1)$ и $H(w_2)$. Данный подход отличается от раннее описанных тем, независимо от размера весового вектора, хэш имеет фиксированный размер (например, 32 байта для SHA-256), тогда как полный вектор может занимать сотни байт, тем самым обеспечивая компактность представления данных. Функция вычисления хэша представлена на листинге 1.

```
        def update(self, x, tau_self, tau_other
            tau_self == tau_other:
            for k in range(self.K):
              if self.sigma[k] == tau_other:
                for j in range(self.N):
                   self.weights[k][j]   +=   self.sigma[k]   *
x[k][j]
                   self.weights[k][j] =
np.clip(self.weights[k][j], -self.L, self.L)

         def weights_hash(self):
             data = self.weights.astype(int).flatten()
             return
hashlib.sha256(data.tobytes()).hexdigest()
```

Листинг 1 – Функция обработки вывода весов векторов

Также, преимуществом является невозможность обратного восстановления. Криптографические хэш-функции обладают свойством однонаправленности – невозможно восстановить исходный вектор весов из его хэша, что существенно повышает безопасность. Передача 32 байт вместо нескольких сотен байт ускоряет коммуникацию и снижает энергозатраты в беспроводных системах.

Таблица 1. Сравнительная таблица методов оценки синхронизации

Критерий	Косинус угла	Евклидово расстояние	Сравнение хэшей	Метод совпадения выходов
Точность оценки	Высокая	Высокая	Бинарная	Низкая
Объем передаваемых данных	$K \times N \times \log_2(L)$	$K \times N \times \log_2(L)$	256-512 бит	1 бит на итерацию
Безопасность (раскрытие весов)	Низкая	Низкая	Высокая	Высокая
Вычислительная сложность	O(K×N)	O(K×N)	O(K×N) + O(hash)	O(1)

Предложенный метод обеспечивает существенное снижение объема трафика. Рассмотрим примерные параметры TPM: K=5, N=40, L=5. Размер полного весового вектора составляет примерно 200 байт (при 8-битовом представлении каждого веса). Размер SHA-256 хэша – 32 байта. Таким образом, экономия трафика и времени передачи данных составляет примерно 84%, что особенно значимо при необходимости множественных проверок синхронизации (рис.1).

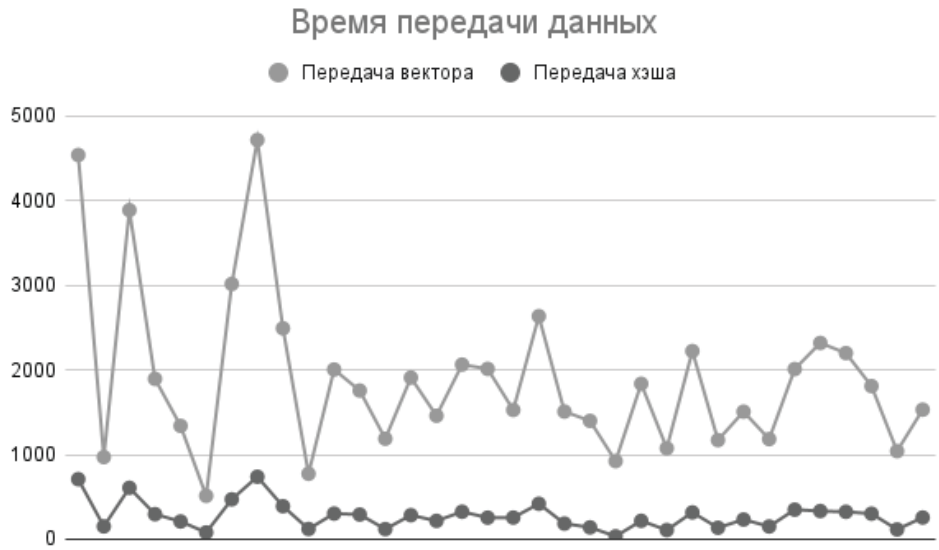

Рис. 1 – Сравнение скорости передачи данных (мс/ кол-во итераций)

Также, использование хэшей способствует повышению криптографической безопасности. Хэш-функции обладают свойством лавинного эффекта: даже минимальное изменение входных данных приводит к полному изменению выходного хэша. Это затрудняет попытки атакующего извлечь частичную информацию о весах и делает невозможным восстановление ключа из перехваченных хэшей.

Одним из основных недостатков является потеря детализированной информации о синхронизации. Метод сравнения хэшей дает бинарный результат – синхронизировано или нет, – но не предоставляет информации о том, насколько близко сети находятся друг к другу. В отличие от косинуса угла, который колеблется от 0 до 1, хэш либо совпадает, либо нет. Это затрудняет отладку процесса обучения и анализ промежуточных стадий синхронизации. В качестве недостатка также стоит выделить дополнительные вычислительные затраты на хэширование. Каждая проверка синхронизации требует вычисления хэш-функции, что добавляет O(K×N) операций. Для систем реального времени с жесткими ограничениями на задержку это может быть критично.

Исходя из анализа данный метод может быть применим в системах с ограниченной полосой пропускания (беспроводные сети, IoT, спутниковые системы), где сокращение объема трафика имеет критическое значение, так же в облачных и распределённые системы, где минимизация передачи чувствительных данных снижает риск утечек и в системах реального времени с отложенной верификацией, где достаточно периодической проверки синхронизации без постоянного мониторинга.

Вывод. Метод сравнения хэшей для оценки синхронизации TPM представляет собой перспективное расширение арсенала инструментов для работы с нейрокриптографическими системами. Как самостоятельный подход, он обеспечивает качественное улучшение баланса между точностью оценки синхронизации и требованиями безопасности, особенно в условиях открытых или ненадежных каналов связи.

В качестве самостоятельного метода метод хэширования целесообразен при необходимости сокращения объема передаваемых данных и критичности защиты состояния сети и данных от раскрытия.

Основным ограничением самостоятельного использования данного метода является потеря детализированной информации о степени синхронизации, что затрудняет отладку и оптимизацию процесса обучения на стадии разработки и исследования.

Предложенных подход может выступать в качестве сопутствующей меры на ранних стадиях разработки для быстрой верификации состояния без отладки, а также как дополнение к классическим методам (косинус угла, расстояние) для обеспечения многоуровневой проверки в составе многостадийного протокола верификации, где хэш используется как первичный тест, а детализированная метрика – как вторичная проверка при обнаружении расхождений.

Список использованных источников

1. Урбанович, П. П. Нейросетевые технологии в криптографических приложениях : монография / П. П. Урбанович, М. Д. Плонковски, М. Долецки. – Минск : БГТУ, 2024. – 223 с. ISBN 978-985-897-160-1.

2. Обухова, Е.В. Влияние внутренних параметров на эффективность синхронизации машин четности в условиях сетевых задержек и потерь / Обухова, Е.В. // Информационно-коммуникационные технологии как драйвер технологического развития различных секторов экономики: сборник статей VIII Международной научно-технической конференции "Минские научные чтения - 2025", Минск, 2-5 декабря 2024 г.: в 3 томах. Минск : БГТУ, 2025 (в печати).

37.091.33-027.22:005.334

А.В. Козляковская, Д.В Шимкевич.
Белорусский государственный технологический университет
Минск, Беларусь

ИНТЕЛЛЕКТУАЛЬНО-РАЗВЛЕКАТЕЛЬНАЯ ВИКТОРИНА ПО ДИСЦИПЛИНЕ «МЕНЕДЖМЕНТ РИСКОВ И СТРАХОВАНИЕ»

Аннотация. *Интерактивная викторина по дисциплине «менеджмент рисков и страхования» стала эффективным инструментом для закрепления сложных понятий и терминов. Использование платформы Wayground обеспечило динамичность и удобное подключение студентов. Четыре формата заданий позволили развивать как скорость мышления, так и глубокое понимание терминологии. Наиболее результативными оказались задания на множественный выбор и заполнение пробелов, что способствовало лучшему запоминанию ключевых понятий страхового менеджмента.*

A.V. Kozlyakovskaya, D.V. Shimkevich
Belarusian State Technological University
Minsk, Belarus

INTELLECTUAL AND ENTERTAINING QUIZ ON THE DISCIPLINE “RISK MANAGEMENT AND INSURANCE”