МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий

Кафедра информационных систем и технологий

Специальность Информационные системы и технологии

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №14 НА ТЕМУ:**

Согласование криптографических ключей на основе технологий искусственных нейронных сетей

Выполнил студент 3 курса 1 группы

Кашперко Василиса Сергеевна

2023 г.

Цель: изучение основ построения и функционирования искусственных нейронных сетей (ИНС), а также использования ИНС в криптографии; приобретение практических навыков программной реализации алгоритма согласования ключевой информации на основе технологии ИНС.

*Теоретические сведения*

Решением проблемы распространения ключа в симметричных системах шифрования занимались такие ученые, как А. Климов, А. Митягин, А. Шамир, Б.Р. Приянка, А. Мартин. Ими было предложено использование криптографического алгоритма, основанного на синхронизации нейронных сетей.

*Основные принципы построения и основы моделирования ИНС*

Человеческий мозг состоит главным образом, из большого числа соединенных друг с другом элементарных нервных клеток – нейронов.

Основная способность нейронов – возможность управления и выработки импульсов.

Нейрон:

– дендрит (тело клетки, имеющее древовидную структуру);

– аксон (длинный отросток нейрона (длинное волокно), который руководит импульсами от тела клетки к другим нейронам).

Синопсисы – биохимические стыки, соединяющие аксон с дендритами других нейронов.

У. МакКаллок и У.Питтсом представили модель искусственного нейрона, называемый также персептроном или перцептроном, симулирующий работу биологического нейрона.

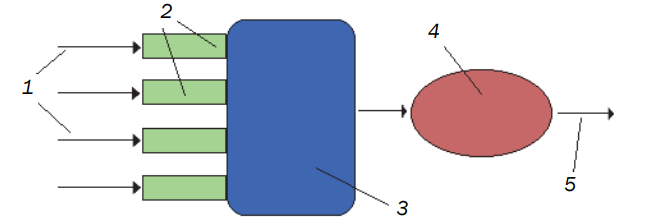


Рисунок 1 – Модель искусственного нейрона – персептрона:

1 – входы; 2 – веса; 3 – суммирующий блок; 4 – блок активации; 5 – выход

Главные элементы искусственного нейрона, являющиеся эквивалентами биологического нейрона:

– Входные значения – дендриты;

– Весовые коэффициенты – синапсы;

– Суммирующий блок – ядро;

– Функция активации – основание аксона;

– А выходное значение – аксон.

Значение выхода нейрона равно скалярному произведению входных значений на векторы весовых коэффициентов (нейрон с линейной функцией активации). Действие такой сети основывается на вычислении выходов каждого из нейронов на основе общего выходного вектора X.

*Архитектура TPM*

В основе нейросетевой криптографии лежат TPM.

Древовидная машина чётности (Tree Parity Machine, TPM) – многоуровневая нейронная сеть прямого распространения, состоящая из:

– K\*N входных нейронов,

– K скрытых нейронов,

– одного выходного нейрона.

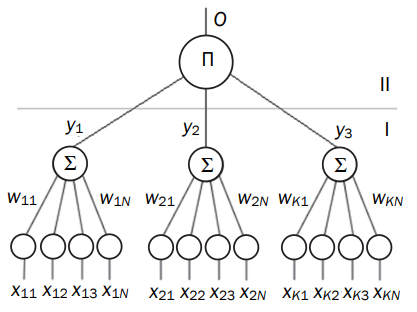


Рисунок 2 – Схема двух уровней модели TPM

Входные значения являются случ. и двоичными значениями ∈{–1, +1}.

Веса – дискретными числами между -L и +L, где L – заданный параметр.

На входные нейроны подаются сигналы, которые суммируются скрытыми нейронами. Сигналы с выходов скрытых нейронов суммируются выходным нейроном.

Как и в других НС, в TPM взвешенная сумма используется для определения выходных значений, а состояние скрытого нейрона определяется его суммарным входом.

Просто так такая модель бесполезна, так как не способна решать задачи.

Процесс обучения нейронной сети – обучение – основан на соответствующем подборе коэффициентов вектора весов в контексте решаемой задачи.

Основной концепцией синхронизации TPM является взаимное обучение. Процесс синхронизации начинается со случайно заданных входных векторов и случайно выбранных весовых коэффициентов. Обновление весов происходит только в том случае, если выходные значения двух TPM равны.

*Достижение равенства весов*

У двух абонентов есть многослойная сеть TPM.

Инициализация нейронной сети. В начале процесса синхронизации значения весовых коэффициентов задаются случайным образом.

Генерация случайного входного вектора, который подается на вход НС.

Вычисление значения скрытых и выходного нейронов.

Проверка равенства выходных значений обоих НС.

В случае несовпадения выходных значений необходимо вернуться ко второму шагу. Если выходные значения равны, тогда для каждой НС используем одно из трех правил обучений, представленных ниже.

После достижения полной синхронизации НС на основе полученных весовых коэффициентов генерируется ключ шифрования.

Для достижения полной синхронизации древовидных машин четности можно использовать три правила обучения:

Правило обучения Хебба – если сигнал перцептрона неверен и равен нулю, то необходимо увеличить веса тех входов, на которые была подана единица.

Правило анти-Хеба – если сигнал перцептрона неверен и равен единице, то необходимо уменьшить веса тех входов, на которые была подана единица.

Случайное блуждание – это математическая модель, описывающая случайное движение частицы или объекта в пространстве. В случайном блуждании, на каждом шаге, объект перемещается в случайном направлении или случайно изменяет свою позицию в зависимости от вероятностей.

Представленные правила обучения должны гарантировать, нахождение весовых коэффициентов в допустимом диапазоне между –L и +L.

С учетом вышесказанного можно сделать вывод о том, что конечным результатом процесса синхронизации является получение одинаковых значений весовых коэффициентов двух НС.

Синхронизация двух TPM-машин может использоваться для обмена ключевой информацией, аналогично обмену ключами в алгоритме Диффи-Хеллмана.

*Алгоритм синхронизации двух TPM-машин*

Сгенерировать для каждой машины вектор случайных весовых коэффициентов;

Сгенерировать случайных вектор из K\*N входных значений;

Вычислить значения на выходах скрытых нейронов;

Вычислить значения на выходах выходных нейронов;

Применить подходящее правило обучения;

Сравнить полученные выходные значения обоих машин: если значения равны, значит синхронизация достигнута; если значения отличаются, перейти к шагу.

*Ход работы*

В процессе выполнения лабораторной работы было создано программное приложение, которое осуществляет свыше 900 синхронизаций между двумя TPM-машинами.

Для достижения этой синхронизации были использованы заданные параметры и применен метод обучения Хебба.

На рисунке 3 изображен результат работы программы и выведен график зависимости среднего числа шагов для достижения синхронизации от числа синхронизаций.



Рисунок 3 – Результат работы программы

По данному рисунку можно получить такие данные:

– Было использовано правило обновления random\_walk;

– Синхронизация машин составила 958 обновлений;

– На синхронизацию машин было затрачено время в количестве 18 секунд;

– Обновления машины Евы составили 181 штуку, однако синхронизация машины Евы не была получена.

Импортируются необходимые модули: Machine из модуля machine, numpy, time и sys.

Задаются параметры машин: k = 100, n = 10, l = 10.

Выбирается правило обновления из трех доступных вариантов: hebbian, anti\_hebbian или random\_walk.

Создаются три машины: Alice, Bob и Eve.

Определяется функция random() для генерации случайных чисел.

Определяется функция sync\_score() для оценки синхронизации между двумя машинами.

Устанавливаются флаги и переменные для отслеживания процесса синхронизации.

Запускается цикл while, который продолжается до достижения синхронизации.

Внутри цикла генерируется случайный вектор X.

Получаются выходы машин Alice, Bob и Eve на основе входного вектора X.

Машины Alice и Bob обновляются в соответствии с выходами друг друга, используя выбранное правило обновления.

Если выходы машин Alice, Bob и Eve равны, то машина Eve также обновляется.

Рассчитывается показатель синхронизации между машинами Alice и Bob.

Записывается значение показателя синхронизации в список sync\_history.

Выводится текущий прогресс синхронизации.

Если показатель синхронизации равен 100%, устанавливается флаг синхронизации в True.

Вычисляется время, затраченное на синхронизацию.

Выводятся результаты синхронизации и информация о машине Eve.

Строится график изменения показателя синхронизации во времени с использованием библиотеки matplotlib.

Данный код реализует модель TPM и проводит эксперименты по синхронизации и обновлению матрицы весов двух экземпляров класса TPM. Третья машина пытается синхронизироваться, однако из-за ограничений в random\_walk ей это не удается.

График зависимости среднего количества обновлений от номера итерации позволяет оценить эффективность синхронизации между двумя TPM.

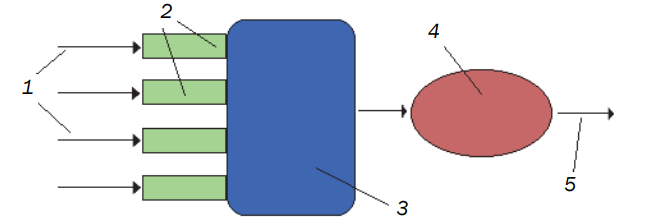
В контексте данного кода, синхронизация означает достижение одинаковых состояний у двух экземпляров класса TPM. Когда два экземпляра TPM становятся синхронизированными, это означает, что их матрицы весов W становятся одинаковыми.

В криптографии синхронизация нейронных сетей может использоваться для обеспечения безопасной коммуникации и шифрования данных. Например, можно использовать синхронизацию нейронных сетей для создания общего секретного ключа между двумя сторонами, который затем может быть использован для шифрования и дешифрования сообщений. При этом секретный ключ является результатом согласованности весов нейронных сетей и неизвестен злоумышленникам. Таким образом, синхронизация нейронных сетей может обеспечить надежность и безопасность в области криптографии.

Вывод: В процессе выполнения лабораторной работы мы изучили основы создания и функционирования искусственных нейронных сетей (ИНС) и их применение в криптографии. Мы рассмотрели криптографический алгоритм, который основывается на синхронизации двух нейронных сетей, и он позволяет решить проблему передачи секретного ключа в симметричных системах шифрования. Однако у этого алгоритма есть две уязвимости: его можно взломать с помощью простой или генетической атаки. В качестве основного метода защиты от простой атаки обычно предлагается использовать квантовые нейронные сети.

Контрольные вопросы

*1. Изобразить схематично структуру персептрона и пояснить аналогии между его компонентами и частями биологического нейрона?*



Модель искусственного нейрона – персептрона:

1 – входы; 2 – веса; 3 – суммирующий блок; 4 – блок активации; 5 – выход

Главные элементы искусственного нейрона, являющиеся эквивалентами биологического нейрона:

Входные значения – дендриты;

Весовые коэффициенты – синапсы;

Суммирующий блок – ядро;

Функция активации – основание аксона;

А выходное значение – аксон.

*2. Охарактеризовать (и показать на примерах) области использования ИНС.*

Искусственные нейронные сети (ИНС) являются мощным инструментом, который находит применение во многих областях. В области компьютерного зрения, ИНС используются для распознавания лиц, объектов и образов на изображениях.

Например, системы безопасности могут использовать ИНС для автоматического распознавания лиц и контроля доступа. В области обработки естественного языка, ИНС применяются для машинного перевода, анализа тональности текста, генерации текста и создания вопросно-ответных систем.

Медицина и биология также находят применение для ИНС, например, в диагностике заболеваний, прогнозировании и лечении.

Другие области применения ИНС включают финансовый анализ, автоматизацию производства, рекомендательные системы и управление энергосистемами.

С помощью ИНС можно решать сложные задачи, которые традиционными методами решить сложно или невозможно, и создавать инновационные решения для различных отраслей.

*3. Как в простейшем виде записывается формальное представление персептрона?*

,

где S – выходной сигнал,

– вес входного сигнала,

– значение входного сигнала.

*4. Охарактеризовать (и показать на примерах) области использования ИНС в криптографии.*

Искусственные нейронные сети (ИНС) также находят применение в криптографии. Они используются для решения задач, связанных с шифрованием и безопасностью данных.

Один из примеров таких методов может быть связан с использованием синхронизации TPM-машин.

*5. Дать пояснение к структуре и функционалу информационной системы на основе ИНС, предназначенной для согласования ключевой информации.*

На входные нейроны подаются сигналы, которые суммируются скрытыми нейронами. Сигналы с выходов скрытых нейронов суммируются выходным нейроном.

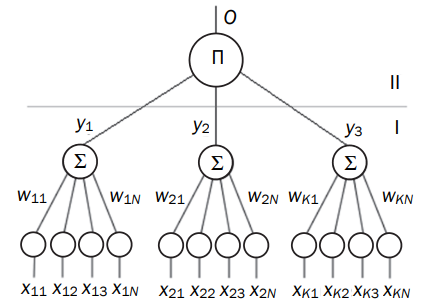


Схема двух уровней модели TPM

Синхронизацию нейронных сетей (далее НС) можно представить следующим образом: первоначально на вход НС поступают общие входные данные, являющиеся случайным набором.

Спустя короткое время достигается полная синхронизация, в результате которой весовые коэффициенты нейронных сетей оказываются равными.

Полученные значения весовых коэффициентов в дальнейшем используются в качестве ключа шифрования.

*6. Дать характеристику известным алгоритмам обучения ИНС.*

Известны различные алгоритмы обучения искусственных нейронных сетей (ИНС), каждый из которых имеет свои особенности.

*Обратное распространение ошибки (Backpropagation):* Это один из наиболее распространенных алгоритмов обучения ИНС. Он основан на минимизации ошибки между предсказанными значениями ИНС и желаемыми значениями с использованием метода градиентного спуска.

*Генетические алгоритмы (Genetic Algorithms):* Этот алгоритм вдохновлен эволюцией в природе и использует понятия генетической мутации и селекции для оптимизации весов ИНС.

*Метод опорных векторов (Support Vector Machines, SVM):* SVM является алгоритмом классификации, но также может быть использован для обучения ИНС. Он стремится найти оптимальное разделение между классами данных.

*7. Какие алгоритмы используются для обучения ИНС, предназначенных для согласования ключевой информации между двумя сторонами?*

Для обучения ИНС, предназначенных для согласования ключевой информации между двумя сторонами, используются алгоритмы, например:

*Backpropagation* (Обратное распространение ошибки): Это наиболее распространенный алгоритм обучения ИНС, который может использоваться для обучения ИНС, осуществляющих согласование ключевой информации.

*Hopfield Network* (Сеть Хопфилда): Этот алгоритм основан на модели Хопфилда и позволяет обучать ИНС для решения задачи ассоциативной памяти и восстановления информации.

*Kohonen Self-Organizing Maps* (Карты самоорганизующихся Кохонена): Этот алгоритм может использоваться для обучения ИНС, чтобы они могли автоматически согласовывать ключевую информацию на основе данных входных паттернов.

*Recurrent Neural Networks* (Рекуррентные нейронные сети): RNN могут быть использованы для обучения ИНС, которые учитывают контекст и последовательность данных в процессе согласования ключевой информации.

*8. Могут ли легитимно участвовать в процессе синхронизации более трех сетей? Мотивируйте ответ?*

Да, легитимно можно использовать более трех сетей в процессе синхронизации. Это может быть обусловлено сложностью задачи, требующей более высокого уровня координации и обмена информацией между сетями.

Например, в сложных системах управления или анализа данных может потребоваться совместная работа нескольких нейронных сетей для достижения желаемых результатов.

Расширение сети с использованием дополнительных компонентов может улучшить ее способность решать более сложные задачи и повысить ее производительность. Следует учитывать, что при увеличении количества сетей возрастает сложность управления и синхронизации между ними, поэтому требуется аккуратное планирование и настройка системы для достижения эффективных результатов.

*9. Дать характеристику криптостойкости системы на основе двух взаимодействующих ИНС.*

Система на основе двух взаимодействующих искусственных нейронных сетей (ИНС) может обладать высокой криптостойкостью. Взаимодействие между ИНС может создать сложную структуру, которая усложняет взлом системы.

Криптостойкость определяется силой алгоритма и сложностью взлома, и использование двух ИНС может повысить эту сложность.

Одна ИНС может выполнять функцию шифрования, а другая - дешифрования. Каждая ИНС может использовать различные наборы весов, архитектуру или ключи, что делает систему более надежной и защищенной от криптоанализа.

Для достижения высокой криптостойкости, необходимо обеспечить надежность и безопасность каждой ИНС, включая защиту от взлома и атак на саму ИНС.

*10. Какие виды атак на нейрокриптографические системы вам известны? В чем заключается их сущность?*

Целью этих атак является нарушение безопасности системы, получение конфиденциальной информации или незаконный доступ к защищенным данным. Для защиты от таких атак необходимо принимать меры, такие как использование криптографических протоколов, контроль целостности данных, мониторинг и обнаружение аномалий, а также усиление безопасности нейронных сетей.

*Простая атака (Simple Attack)*: Это тип атаки, при котором злоумышленник пытается обойти или взломать систему, используя стандартные криптоаналитические методы, такие как перебор возможных ключей или атаку посредника.

*Генетическая атака (Genetic Attack)*: В этой атаке злоумышленник применяет методы генетического программирования или эволюционных алгоритмов для взлома системы путем подбора оптимальных параметров или нахождения уязвимостей.

*Атаки на саму нейронную сеть (Attacks on the Neural Network)*: Эти атаки направлены на саму нейронную сеть и могут включать в себя ввод искаженных данных, изменение весов или структуры сети, или внедрение шума для искажения вывода сети.

*Атаки на передачу данных (Attacks on Data Transmission)*: Эти атаки нацелены на перехват и изменение передаваемых данных между сторонами, включая атаки типа "человек посередине" (man-in-the-middle) или вмешательство в канал связи.