ISSN 2074-7128

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

2012
1кзи

Министерство образования и науки РФ
Национальный исследовательский ядерный университет «МИФИ»
ВНИИПВТИ

Журнал зарегистрирован в Государственном комитете Российской Федерации по печати. Свидетельство № 017789. Издается с февраля 1994 г.

Журнал БИТ включен в Перечень ведущих рецензируемых научных журналов и изданий, в которых должны быть опубликованы основные научные результаты диссертации на соискание ученой степени доктора и кандидата наук (редакция апреля 2008 г.).

Специальный выпуск «Комплексная защита информации-XVII»

Верстка: М. В. Данилова
Дизайн: М. А. Каганова
Редактор: С. В. Конявская
Технический редактор: Н. Ф. Зернова
Корректор: А. В. Духанина
Оригинал-макет: редакционно-издательский сектор ВНИИПВТИ

П. П. Урбанович, М. Долецкий,
Беларусь, Белорусский государственный технологический университет

МОДЕЛИРОВАНИЕ И АНАЛИЗ ПРОЦЕССА СИНХРОНИЗАЦИИ НЕЙРОННЫХ СЕТЕЙ ДЛЯ ОБМЕНА КРИТИЧЕСКОЙ ИНФОРМАЦИЕЙ

Идея использования нейросетевых технологий для криптографических приложений связана с проблемой обмена ключами через незащищенные каналы передачи. Протокол обмена ключами, который используется в нейросетевых криптографических технологиях, опирается на синхронном «обучении» сетей (*A* и *B* – со стороны отправителя и получателя сообщений соответственно) [1]. Процесс «обучения» двух нейронных сетей с использованием их общих параметров ведется до появления так называемых идентичных весовых коэффициентов (векторов весов). Такое состояние сетей называют состоянием синхронизации. Сети обмениваются между собой выходными и входными параметрами; при этом секретными должны оставаться внутренние значения весовых коэффициентов. Следовательно, значения весовых коэффициентов могут использоваться как секретные ключи в процессе передачи информации по незащищенным каналам.

Архитектуру сети (известную как TPM – Tree Parity Machine, рис.1) составляет трехслойный персептрон с одним скрытым слоем, который состоит с *K* нейронов. Каждый из них имеет *N* входов. Поэтому размер входного вектора равен *K*N*. Соответствующие входные числа обозначим как X_{kj} , где k =1, 2, ..., *K* и j = 1, 2, ..., *N*. Для упрощения полагаем, что каждый элемент вектора *X* (информация на входе сети) принимает только бинарные величины: X_{kj} = ±1. И, наконец, величины вектора весов (*W*) – это целые числа, находящиеся в некотором интервале: [*-L, L*] [2].

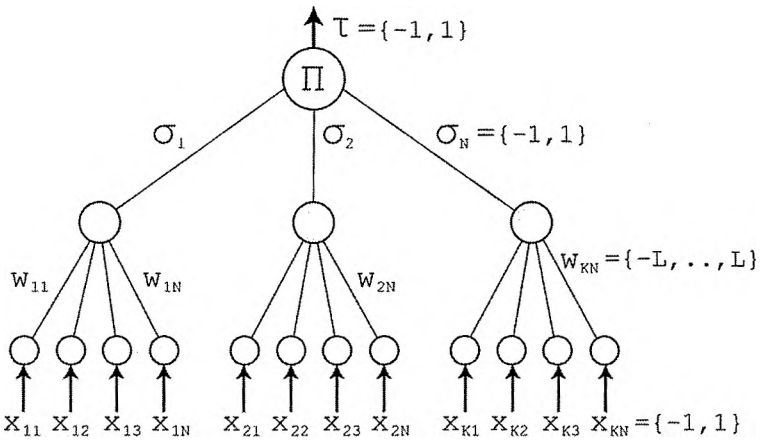

Рис.1. Архитектура нейронной сети

Сначала каждая из сетей генерирует свой собственный весовой коэффициент. Таким образом, начальные состояния сетей – разные, и начальный коэффициент является величиной секретной. После этого каждая из сетей «обучается» с использованием выходной информации (т) другой сети.

Третья сторона (интруз – такая же нейронная сеть, пытающаяся синхронизироваться с сетями *A* и *B*), не может быстро восстановить эти секретные параметры. Однако, если третья сторона представляет собой объединение нескольких или большого числа таких же сетей, то вероятность доступа к секретной информации составляет критическую величину.

Описанная здесь технология породила несколько типов атак на сети A и B, наиболее эффективными из которых считаются геометрическая и генетическая [3, 4]. Первая относится к числу наиболее известных. В этом случае вероятность синхронизации интруза (только одна сеть) с сетями *A* и *B* уменьшается геометрически с ростом *L*. Статистические результаты, полученные в результате моделирования трехстороннего процесса (участвуют сети *A*, *B* и третья – сеть интруза), показали, что близкой к оптимальной является структура сетей *A* и *B* при *K*=3. Эффективность генетической атаки (популяция сетей третьей стороны может составлять несколько тысяч) значительно снижается при увеличении значений весовых коэффициентов.

При реализации любой атаки на сети *A* и *B* чрезвычайно важным является определение состояния синхронизации между *A* и *B*. Иначе говоря, установление того, после какого числа шагов (циклов) обмена данными между сетями при одинаковых и неизменяющихся выходных сигналах ситуацию следует трактовать как наступление состояния синхронизации.

Целью проведенных нами исследований было определение зависимости наступления состояния синхронизации между сетями *A* и *B* в зависимости от параметров сетей. Исследовались два случая: компьютерная программа симуляции работы сетей «имеет» доступ к весовым коэффициентам обеих сетей и может остановить (на основе анализа этих параметров) процесс синхронизации (обучения сетей); во втором случае решение о наступлении состояния синхронизации принимается после определенного числа шагов неизменных выходных значений. Кроме того, изучению и анализу подвергались длительности периодов (максимальное число циклов), в течение которых состояние синхронизации не нарушается.

При этом предполагалось, что один цикл состоит из следующих операций:

1) генерирование входного вектора *X* для сетей *A* и *B*,
2) вычисление выходных значений τ^A и τ^B,
3) обмен выходными значениями: τ^A – к сети *B* и τ^B – к *A*,
4) адаптация (обучение) сетей.

Для каждой пары сетей выполнено не менее 1000 опытов. При этом сети характеризовались следующими параметрами: *K*=3, *N*=4, *L* ∈ [5;50]. Для каждого сочетания *K-N-L* получены распределения количества опытов от числа циклов, после которых наступило состояние синхронизации. На рис.2 представлена одна из таких гистограмм, которая характеризует сети с параметрами 3-4-5.

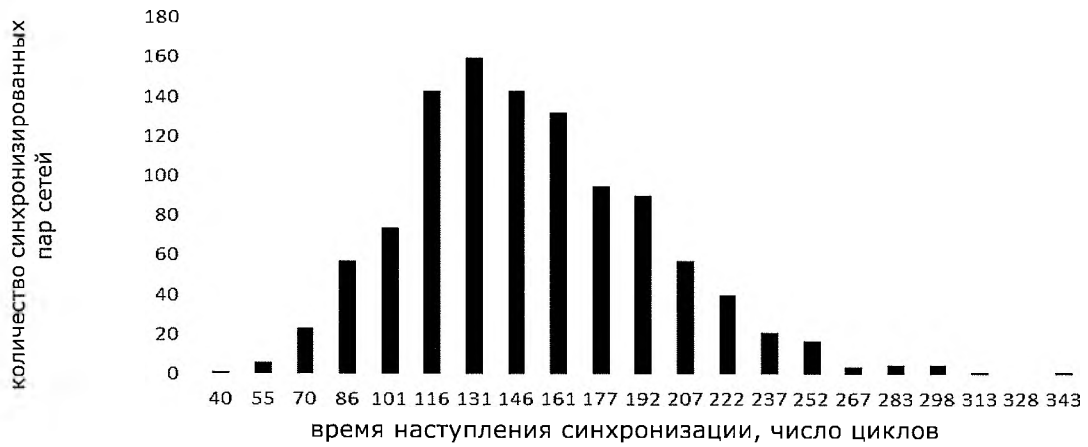

Рис.2. Распределение сетей по минимальному числу циклов обучения для наступления состояния синхронизации при K=3, N=4, L=5

Вторая из проанализированных ситуаций касается исследования наибольшего времени, в течение которого сети *A* и *B* обмениваются постоянной и неизменной информацией до наступления состояния полной синхронизации (сети находятся в состоянии обучения). Эта часть эксперимента выполнена для сетей с параметрами *K*=3, *N*=4, *L* ∈ [4;100]. Изучение результатов должно помочь в определении оптимального числа циклов обучения сетей, т. е. принятия решения об остановке процесса синхронизации.

Обобщенные статистические характеристики выполненных исследований в этой части приведены в таблице. Подтверждена почти очевидная закономерность: длительность максимального периода обмена неизменной информацией (колонка НИ в таблице) возрастает с увеличением значений весовых коэффициентов.

Таблица. Статистические результаты моделирования процессов синхронизации двух нейронных сетей

Сеть, *K-N-L*	Среднее время синхронизации, кол-во циклов	3 квартиль	4 квартиль	НИ, кол-во циклов	НИ, кол-во циклов для 3 квартиля, %	НИ, кол-во циклов для 4 квартиля, %
3-4-4	91,17	109,00	222	52	47,7	23,4

3-4-10	539,55	633,00	1194	154	24,0	13,0
3-4-20	2112,65	2459,00	5520	355	14,0	6,0
3-4-30	4557,41	5346,50	10286	683	13,0	7,0
3-4-40	8330,13	9801,00	17772	1022	10,0	6,0
3-4-50	12906,70	15003,75	26935	1549	10,0	6,0
3-4-60	18277,36	21230,25	40005	2014	9,0	5,0
3-4-70	24564,41	28231,00	62152	2035	7,0	3,0
3-4-80	32589,64	37747,00	71199	2859	8,0	4,0
3-4-90	40335,44	46884,00	93895	3287	7,0	4,0
3-4-100	49642,65	58387,00	97859	4653	8,0	5,0

Для примера, при небольших значениях весовых коэффициентов (возьмем первую строку таблицы) обмен одинаковыми и неизменными значениями весовых коэффициентов продолжался в среднем 52 цикла (пятая колонка), а максимальное время процесса синхронизации при этом составило 222 цикла (четвертая колонка). Это означает, что период взаимного обучения сетей до наступления состояния синхронизации, в течение которого пересылаемая между сетями информация не меняется (что можно оценить, как наступление состояния синхронизации) может составить 23,4% от наибольшей длительности процесса синхронизации (третий квартиль составляет половину четвертого).

СПИСОК ЛИТЕРАТУРЫ:

1. *Kanter W., Kinzel E.* Secure exchange of information by synchronization of neural networks// Europhys. Lett. 57. 2002, P. 141–147.
2. *Плонковски М., Урбанович П.П.* Криптографическое преобразование информации на основе нейросетевых технологии// Труды БГТУ. Сер. VI. Физико-математические науки и информатика. Мн.:БГТУ, 2005. С. 161–164.
3. *Klimov A., Mityagin A., Shamir A.* Analysis of Neural Cryptography // Advances in Cryptology—ASIACRYPT, 2002. – Springer, Heidelberg, 2003. P. 288–289.
4. *Ruttor A., Kinzel W., Naeh R., Kanter I.* Genetic attack on neural cryptography // Phys. Rev. E, 73(3):036121, 2006.