УДК 681.324

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ВЗАИМООБУЧЕНИЯ ДВУХ НЕЙРОННЫХ СЕТЕЙ ПРИ ОБМЕНЕ КЛЮЧЕВОЙ ИНФОРМАЦИЕЙ

П.П. Урбанович, К.В. Чуриков

В статье рассматриваются алгоритмы взаимного обучения нейронных сетей на основе архитектур TPM, TPCM, BPM, выполняющих генерацию секретных ключей для шифрования данных по открытым каналам связи. Разработана программа, реализующая алгоритмы, и на основе данных, полученных в результате работы программы, выполнен анализ эффективности перечисленных методов. Полученные результаты анализа позволили сделать вывод об эффективности применения рассмотренных методов в зависимости от требований, предъявляемых к уровню защиты информации.

Введение

Нейрокриптография – это раздел криптографии, изучающий применение стохастических алгоритмов на основе искусственных нейронных сетей, в частности, для шифрования данных. В криптоанализе используется способность нейронных сетей исследовать пространство решений.

Существует также возможность создавать новые типы атак на существующие алгоритмы шифрования, основанные на том, что любая функции может быть представлена нейронной сетью. Взломав алгоритм, можно найти решение, по крайней мере, теоретически.

При этом используются такие свойства нейронных сетей, как взаимное обучение, самообучение, и стохастическое поведение, а также низкая чувствительность к шуму, неточностям (искажения данных, весовых коэффициентов, ошибок в программе). Сети позволяют решать проблемы криптографии с открытым ключом, распределения ключей, хеширования и генерации псевдослучайных чисел.

Для обмена ключами между двумя абонентами наиболее часто используется алгоритм Диффи-Хеллмана [1]. Его более безопасная замена основана на синхронизации двух древовидных машин четности (TPM, tree parity machines). Синхронизация этих машин похожа на синхронизацию двух хаотических осцилляторов в теории хаотических связей (chaos communications).

В статье анализируются некоторые важные аспекты, относящиеся к установлению режима синхронизации между двумя нейронными сетями, на основе чего определяется взаимный секретный ключ.

Основная часть

В основе рассматриваемого метода лежит известная архитектура TPM, представляющая собой особый вид многоуровневой нейронной сети прямого распространения (рис. 1).

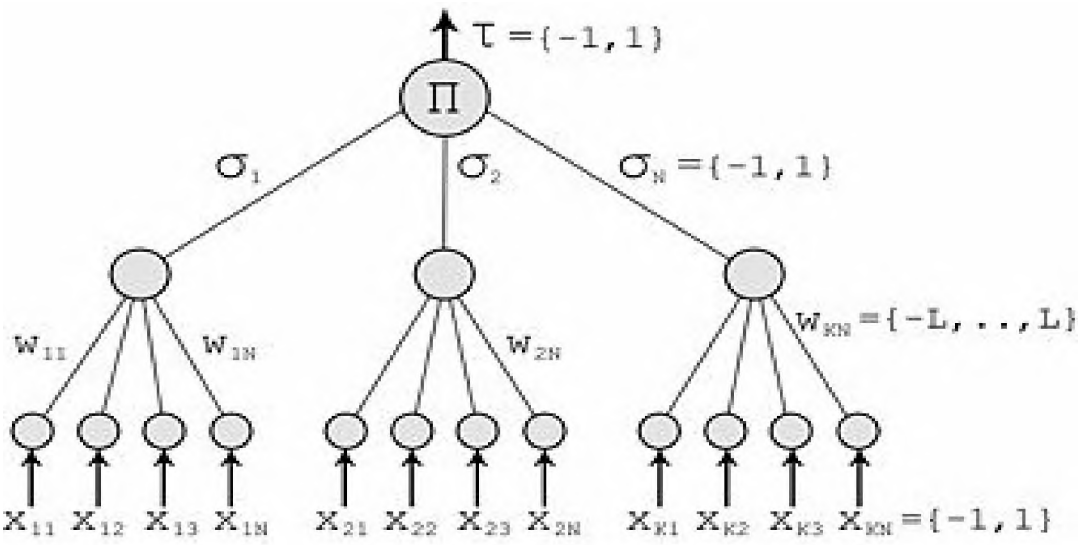

Рис. 1. Архитектура нейронной сети на основе TPM

На рис. 1 обозначены: x_{ij} – значения входных нейронов соответственно (1), получаемые из вектора входных значений X_{KN}, где $i \in [1;K]$, а $j \in [1,N]$, w_{ij} – значения весовых коэффициентов (2), задающихся случайным образом при первой инициализации нейронной сети.

Рассматриваемая архитектура состоит из одного выходного нейрона, K скрытых нейронов и $K*N$ входных нейронов. Входные нейроны принимают двоичные значения:

$$x_{ij} \in \{-1;+1\} \ . \tag{1}$$

Веса (весовые коэффициенты), влияющие на входные значения нейрона (между входными и скрытыми нейронами), соответствуют:

$$w_{ij} \in \{-L,...,0,...,+L\} . \tag{2}$$

Значение сигнала на выходе каждого скрытого нейрона есть сумма произведений входного значения и весового коэффициента:

$$\begin{aligned} \sigma_i &= \operatorname{sgn}\Big(\sum_{j=1}^{N} w_{ij} x_{ij}\Big), \\ \operatorname{sgn}(x) &= \begin{cases} -1 \ if \ \ x \le 0, \\ 1 \ \ if \ \ x > 0. \end{cases} \end{aligned} \tag{3}$$

Значение сигнала выходного нейрона есть произведение выходных сигналов всех скрытых нейронов:

$$\tau = \prod_{i=1}^{K} \sigma_i . \tag{4}$$

Выходное значение также является величиной двоичной.

Алгоритм обмена информацией на основе TPM.

Рассматриваем две сети (A и B), каждая из которых построена на основе архитектуры TPM (см. рис.1). Сети обмениваются выходными величинами по открытым каналам. Синхронизация сетей происходит в соответствии со следующим алгоритмом.

1. Задаем случайные значения весовых коэффициентов $w_{11},w_{12},\ldots,w_{KN}$.
2. Выполняем следующие шаги, пока не наступит состояние синхронизация:
   2.1. Генерируем случайный входной вектор $X(x_{11},\ldots,x_{1N},\ldots,x_{KN})$.
   2.2. Вычисляем значения по формуле (3).
   2.3. Вычисляем значение по формуле (4).
3. Сравниваем выходы двух TPM:
   Если выходы разные, то осуществляется переход к п.2.1
   Если выходы одинаковые, то применяем выбранное правило к весовым коэффициентам

После наступления состояния синхронизации (веса w_{ij} обоих TPM одинаковы) абоненты (сети) A и B могут использовать веса в качестве ключевой информации для дальнейшего обмена шифрованой информацией.

Этот метод известен как двунаправленное обучение.

Алгоритм обучения двух сетей на основе алгебры комплексных чисел (сети TPCM, tree parity complex machines) схож с алгоритмом, рассмотренным для TPM [1]. Отличие состоит, понятно, в применении алгебры комплексных чисел.

Метод обратного распространения ошибки (BPM, BackPropagation mistake) – метод обучения многослойного персептрона. Впервые метод был описан в [2, 3]. Далее существенно развит в [4, 5]. Этот метод основан на итеративном градиентном алгоритме, который используется с целью минимизации ошибки работы многослойного персептрона.

Основная идея метода состоит в распространении сигналов ошибки от выходов сети к ее входам в направлении, обратном прямому распространению сигналов в обычном режиме работы. В [5] предложен общий метод («принцип двойственности»), применимый к более широкому классу систем, включая системы с запаздыванием, распределенные системы, и т.п.

Сущность алгоритма BackPropagation (анализ проводится применительно к рис. 1).

1. Инициализировать w_{ij} малыми случайными значениями (w_{ij} близки к 0).
2. Повторить шаг 2 d раз (для всех d от 1 до m, где m=K*N – количество входных нейронов):
   2.1. Подать сигналы, обозначаемые вектором $\{x_i^d\}$ на вход сети и подсчитать выходы o_i каждого узла ($\{x_i^d\}$ – сигналы на входах i-го нейрона на шаге d).

2.2. Для всех K скрытых нейронов подсчитать

$$\delta_k = o_k(1 - o_k)(t_k - o_k).$$

2.3. Для каждого скрытого нейрона, начиная с предпоследнего, вычислить

$$\delta_j = o_j(1-o_j)\sum_k \delta_k w_{k,j,}\ .$$

2.4. Для каждого ребра $\{i, j\}$ сети вычислить

$$\Delta w_{i,j} = \alpha\Delta w_{i,j} + (1 - \alpha)\eta\delta_j o_{i\cdot},$$
$$w_{i,j} = w_{i,j} + \Delta w_{i,j},$$

где α - коэффициент инерциальнности для сглаживания резких скачков при перемещении по поверхности целевой функции

3. Обменяться (между сетями) значениями w_{ij}.

Для реализации анализируемых алгоритмов были разработаны компьютерные программы с использованием архитектуры клиент/серверного приложения.

Целью написания программ являлось исследование поведения нейронной сети после ее обучения (синхронизации). Нейронная сеть, синхронизирующаяся с помощью алгоритма BPM, для получения нового ключа должна заново синхронизироваться. В процессе имитации взаимного обучения сетей было замечено, что сети на основе архитектур TPM и TPCM после наступления состояния синхронизации на каждом новом шаге генерируют новый ключ.

Обобщенные результаты работы программы приведены на таблице.

Таблица. Результаты синхронизации нейронных сетей

№ шага после синхронизации	Ключевая информация на выходах двух сетей длинной N								
1 шаг	0	-2	1	1	3	1	1	-3	2
	0	-2	1	1	3	1	1	-3	2
2 шаг	2	-1	-3	0	2	3	2	0	-2
	2	-1	-3	0	2	3	2	0	-2
3 шаг	1	0	-2	-1	1	2	1	1	-1
	1	0	-2	-1	1	2	1	1	-1
4 шаг	2	-1	-1	0	2	3	2	0	-2
	2	-1	-1	0	2	3	2	0	-2
5 шаг	3	-2	-2	1	3	2	3	1	-3
	3	-2	-2	1	3	2	3	1	-3

Как видно из результатов, приведенных в таблице, сети, использующие архитектуру TPM или TPCM, генерируют идентичные ключи после их полной синхронизации, отличные от ключей на

предыдущем шаге. Данная особенность может применяться в системах с периодической сменой ключа, т.к. для генерации нового ключа нужен лишь один шаг, не требующий новой синхронизации, в отличие от сетей на основе BPM. Время установления синхронизации сетей на основе архитектуры TPM равнялось 22,179 секунд, на основе TPCM – 1800,27 секунды, на основе BPM – 35770,2 секунды (эксперимент проводился с использованием ПК с параметрами: core 2 duo T6400, 3 Gb ddr3). Отсюда можно сделать вывод о предпочтительной целесообразности использования архитектуры TPM, обусловленное сравнительно коротким времени синхронизации.

Литература

1. Плонковски, М. Криптографическое преобразование информации на основе нейросетевых технологий / М. Плонковски, П. П. Урбанович // Труды БГТУ. Сер. VI, Физ-мат. науки и информ. – 2005. – Вып. XIII – С. 161–164.
2. Галушкин, А. И. Синтез многослой-ных систем распознавания образов / А. И. Глушкин – М.: «Энергия», 1974.
3. Werbos, P. J. Beyond regression: New tools for prediction and analysis in the behavioral sciences / P. J. Werbos // Ph.D. thesis, Harvard University, Cambridge, MA. – 1974.
4. Rumelhart, D.E. Learning Internal Representations by Error Propagation. In: Parallel Distributed Processing / D.E. Rumelhart, Hinton G.E., Williams R.J. – vol. 1. – pp. 318–362. Cambridge, MA, MIT Press. 1986.
5. Барцев, С. И. Адаптивные сети обра-ботки информации/ С. И. Барцев, В. А.Охо-нин. – Красноярск : Ин-т физики СО АН СССР, 1986.

Павел Павлович Урбанович, профессор кафедры информационные системы и технологии Белорусского государственного технологического университета, докт. техн. наук, профессор, upp@rambler.ru

Константин Валерьевич Чуриков, магистрант кафедры информационные системы и технологии Белорусского государственного технологического университета, chkv85@gmail.com