УДК 004.056

ВЕРОЯТНОСТНАЯ ОЦЕНКА ПРОСТРАНСТВА РЕШЕНИЙ ДЛЯ ДВУХ НЕЙРОННЫХ СЕТЕЙ TPM ПРИ ИХ СИНХРОНИЗАЦИИ

П. П. Урбанович[1,2], М. Плонковски[2], Д. Карчмарски[2]
[1]Белорусский государственный технологический университет, Минск
e-mail: pav.urb@yandex.by
[2]Люблинский католический университет им. Яна Павла II, Польша
e-mail: marcin.plonkowski@kul.pl

Одним из относительно новых направлений применения нейронных сетей (НС) является криптография [1]. Протокол обмена криптографическими ключами, использующий НС, базируется на синхронном взаимном обучении сетей, называемых TPM (Tree Parity Machine, древовидная машина четности). Обучение двух НС (A и B) по определенным правилам (Хебба, анти-Хебба или случайного блуждания) с использованием их общих выходных величин ведет к возникновению идентичных векторов весов ($\mathbf{w}^A = \mathbf{w}^B$). Сети обмениваются между собой выходными величинами (τ^A и τ^B), при этом секретными остаются внутренние состояния векторов весов.

Архитектура TPM состоит из двух слоев. Элементы скрытого слоя – это персептроны, характеризующиеся N-элементными векторами весов: $w_k = \{w_{k,1}, w_{k,2}, ..., w_{k,N}\}$, где $1 \le k \le K$, K – число персептронов; величины $w_{k,j}$ – действительные числа. Вышеуказанные веса могут принимать значения $w_{k,j} \in \{-L, L+1, ..., L\}$. Вход персептронов составляет K N-элементных векторов $x_k = \{x_{k,1}, x_{k,2}, ..., x_{k,N}\}$, часто отождествляемых с одним N K-элементным вектором $\mathbf{x} = \{x_1, x_2, ..., x_N\}$ [1, 2]; $x_{k,j} \in \{-1, 1\}$. Выход σ_k k-го элемента в скрытом слое определяется формулой

$$\sigma_k = sgn\,(w_k \cdot x_k) = sgn\,\{\sum_{j=1}^{N}(w_{k,j} \cdot x_{k,j})\}. \qquad (1)$$

Общий выход НС есть произведение

$$\tau = \prod_{k=1}^{K}\sigma_k. \qquad (2)$$

Будем использовать формальные определения понятий «нейрокриптографическая сеть, НКС» (обозначается как $\langle \mathrm{TPM}(K,N,L)\rangle$) и «синхронизированные НКС (A и B)» (обозначаются как

$\langle \mathrm{TPM}(K, N, L)_A \rangle$ и $\langle \mathrm{TPM}(K, N, L)_B \rangle$). Состояние обеих НКС называем синхронизированным, если для всех $k \in \{1; K\}$ справедливо равенство $w_k^A = w_k^B$. Процесс синхронизации сетей $\langle \mathrm{TPM}(K, N, L)_A \rangle$ и $\langle \mathrm{TPM}(K, N, L)_B \rangle$ является случайным. Он состоит из дискретных шагов, в которых векторы весов нейронных сетей корректируются (подстраиваются друг к другу) в соответствии с одним из указанных выше алгоритмов [2, 3].

Начальное состояние синхронизируемых сетей A и B – это случайный выбор компонент w_j^A и w_j^B, $j = 1, \ldots N$ для двух векторов весов $\mathbf{w}^A$ и $\mathbf{w}^B$. Вероятность $P(\mathbf{w}^A = \mathbf{w}^B) = 1/(2L + 1)^{KN}$. На каждом шаге обучения случайный входной вектор x поступает на входы двух сетей, которые генерируют два выходных бита σ^A и σ^B ($\sigma^{A/B}$) согласно (1). На начальном и каждом последующем шаге синхронизации НКС весовые коэффициенты являются элементами множества, определяемого декартовым произведением множеств $(\{-L, L\})^N$, число которых равно K. Интерес представляет анализ размерности такого пространства для $\langle \mathrm{TPM}(K, N, L)_{A,B} \rangle$, удовлетворяющего критерию безопасного размера (KN) генерируемого криптографического ключа при достижении состояния синхронизации. В литературе (например, [4]) безопасной принято считать систему TPM, в которой $N \geq 100$. При таком большом значении N путем вычислений невозможно точно определить размерность пространства (в разумные сроки). Поэтому следует ввести другой способ определения размера пространства.

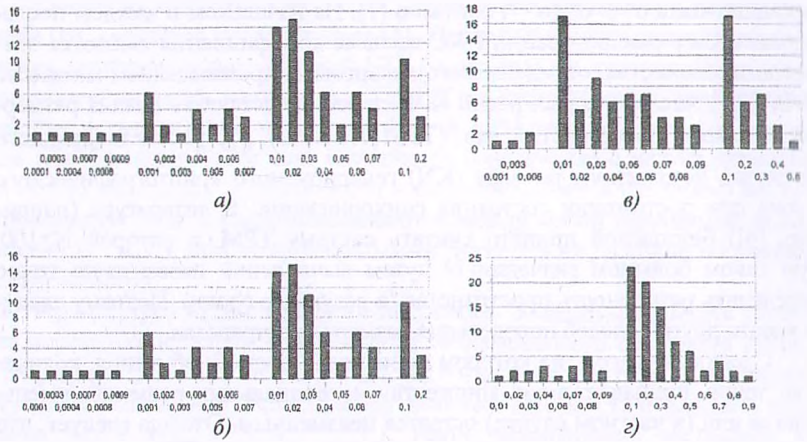
С каждым шагом, на котором происходит процесс обучения, количество точек, принадлежащих множеству потенциальных решений, уменьшается или (в частном случае) остается неизменным. Отсюда следует, что чем больше сделано шагов, тем меньше пространство. Поскольку размер пространства изменяется в процессе синхронизации, полезно определить его меру.

Вводится вероятностная оценка пространства решений по поиску состояний $w_k^A = w_k^B$ на основе вероятности $|\langle \mathrm{TPM}(K,N,L) \rangle|_P$, которая означает, что случайно взятые (на определенном шаге синхронизации) значения векторов весовых коэффициентов будут одинаковыми [5]. Величину ($|\langle \mathrm{TPM}(K,N,L) \rangle|_P$) будем использовать как меру размерности пространства. В соответствии с этим параметром можно осуществлять выбор параметров (K, N, L) сетей A и B по определенному критерию. Кроме того, такой анализ может дать, например, ответ на вопрос, какая сеть лучше – $\langle \mathrm{TPM}(K = N = 20, L = 5) \rangle$ или $\langle \mathrm{TPM}(K = 3, N = 15, L = 10) \rangle$.

Выполнено 100 тестовых операций синхронизации сетей A и B. В ходе каждого теста случайным образом выбирались и анализирова-

лись пары весовых коэффициентов. Такая выборка продолжалась до тех пор, пока не будет найдено 10 правильных решений, т. е. точек, соответствующих состоянию синхронизации сетей. Результаты эксперимента представлены ниже в виде гистограмм (по оси Y – количество тестов, по оси X – вероятность наступления состояния синхронизации).

Вероятность $|\cdot|_P$ для параметров сетей, соответствующих *а) – г)* на гистограммах, составляет соответственно 0,000015625; 0,000003231; 0,000016463; 0,000558611. Отсюда следует вывод: размерность пространства разная даже при одинаковых параметрах TPM. В следующей серии тестов для НКС с параметрами *а)* подсчитано $|\cdot|_P$ для 300, 400 и 500 шагов синхронизации: 0,005939510651; 0,008368333333; 0,025484444444.



Графическое отображение результатов эксперимента:
а) K=3, N=40, L=5; *б)* K=4, N=40, L=5; *в)* K=5, N=40, L=5; *г)* K=6, N=40, L=5

Другие результаты эксперимента подтверждают, что размерность пространства значительно возрастает с увеличением N.

Список литературы

1. Kanter, I. Secure exchange ofinformation by synchronization of neural networks / I. Kanter, W. Kinzel, E. Kanter // Europhys. Lett. – 2002. – No. 57. – P. 141–147.

2. Плонковски, М. Криптографическое преобразование информации на основе нейросетевых технологий / М. Плонковски, П. П. Урбанович // Тр. БГТУ. Сер. VI. Физ.-мат. науки и информ. – 2005. – Вып. XIII. – С. 161–164.

3. Плонковски, М. Синхронизация криптографических ключей на основе нейронных сетей и в системах криптопреобразования на основе XML / М. Плонковски, П. П. Урбанович // Тр. БГТУ. Сер. VI. Физ.-мат. науки и информ. – 2006. – Вып. XIV. – С. 152–155.

4. Ruttor, A. Neural Synchronization and Cryptography / A. Ruttor. – Wurzburg, 2006.

5. Urbanovich, P. Probabilistic measure of space for neurocryptographic system solutions / P. Urbanovich, D. Karczmarski, M. Plonkowski // Proc. of 11th Intern. Conf. NEET'2019, Zakopane, Poland, 25–28 June 2019. – Lublin University of Techn., 2019. – P. 32.