УДК 004.056

П. П. Урбанович, проф., д-р техн. наук (БГТУ, г. Минск);
М. Плонковски, дир-р ин-та матем. и информат., канд. техн. наук,
Д. Карчмарски (Люблинский Католический ун-т, г. Люблин, Польша)

АНАЛИЗ СХОДИМОСТИ ВЕСОВЫХ КОЭФФИЦИЕНТОВ ДВУХ НЕЙРОННЫХ СЕТЕЙ ПРИ ИХ СИНХРОНИЗАЦИИ

Синхронизация – явление, которое можно наблюдать во многих физических, технических, а также биологических системах. В общем случае две одинаковые системы в режиме синхронизации характеризуются одинаковой динамикой процессов.

Одной из относительно новых идей является применение нейронных сетей (НС) в криптографии. Это касается проблемы обмена закрытыми (секретными) ключами по незащищенным каналам связи [1].

Протокол обмена ключами, использующий НС, базируется на синхронном обучении сетей, базовая архитектура которых обозначается как TPM (Tree Parity Machine, древовидная машина четности; рис.1). Обучение двух НС (A и B) с использованием их общих выходных величин ведет к возникновению идентичных векторов весов (входных значений). Сети обмениваются между собой выходными величинами (τA и τB), при этом секретными остаются внутренние состояния векторов весов.

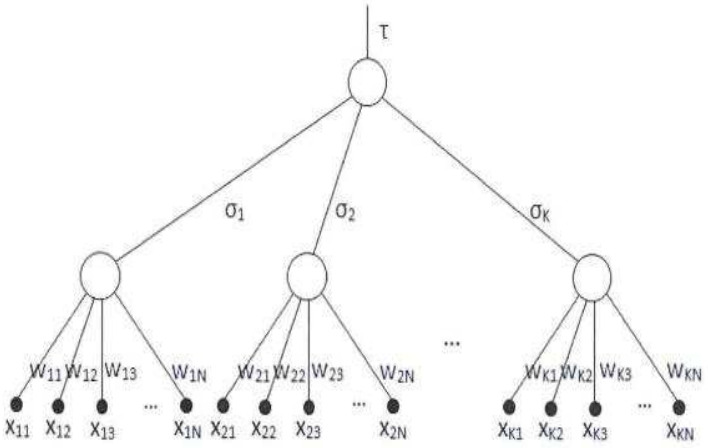

Рис.1. Архитектура TPM

Архитектура TPM состоит из двух уровней. Элементы первого уровня – это персептроны, имеющие N-элементные векторы весов, wk – ($\{w_{k,1}, w_{k,2}, ..., w_{k,N}\}$, где $1 \le k \le K$, K – число персептронов), величины которых – это действительные числа. Значения вышеуказанные весов могут принимать значения: $w_{k,j} \in \{-L, L + 1, \ldots, L\}$. Вход персеп-

тронов составляет K·N-элементных векторов $\{x_{k,1}, x_{k,2}, ..., x_{k,N}\}$, часто отождествляемых с одним N·K-элементным вектором $[x_1, x_2, ..., x_N]$ [1, 2]; $x_{k,j} \in \{-1, 1\}$. Выход σ_k k-го элемента в скрытом слое определяется формулой:

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

Общий выход НС – есть произведение

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

Определение 1. Две НС (A и B) на основе архитектуры TPM, характеризующиеся одинаковыми параметрами (K, N, L) и предназначенные для согласования криптографических ключей, будем называть *нейрокриптографическими сетями* (НКС) и обозначать $\langle \mathrm{TPM(K,N,L)_A} \rangle$ и $\langle \mathrm{TPM(K,N,L)_B} \rangle$. При этом соответствующие значения весовых коэффициентов сетей могут отличаться.

Особенности функционирования и взаимного обучения (синхронизации) двух сетей на основе действительных (TPM), а также комплексных чисел (TPCM), кватернионов (TPQM) и октонионов (TPOM) описаны, например, в [1, 2] (TPM) и в [3–6] – остальные.

В данной статье проанализируем особенности сходимости векторов весовых коэффициентов двух НС в процессе их синхронизации (взаимного обучения), действующих на основе алгебры действительных чисел. Из (2) следует, что $\tau = 1$ при четном количестве выходов $\sigma_k = -1$ и наоборот.

Определение 2. Пусть даны две НКС: $\langle \mathrm{TPM(K,N,L)_A} \rangle$ и $\langle \mathrm{TPM(K,N,L)_B} \rangle$. Состояние обеих НКС называем синхронизированным, если для всех $k \in \{1; K\}$ справедливо равенство: $w_k^A = w_k^B$.

Начальное состояние синхронизируемых сетей A и B – это случайный выбор компонент w_j^A и w_j^B, $j = 1, ... N$ 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 t обучения общий случайный входной вектор $\mathbf{x}$ поступает на входы двух сетей, которые генерируют два выходных бита: σ^A и σ^B ($\sigma^{A/B}$) согласно (1).

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 выбранных алгоритмов: Хебба (Hebbian learning rule), анти-Хебба (anti-Hebbian learning rule), «случайного блуждания» (random walk learning rule) [2]. Там же анализируется причина того, почему однонаправленное обучение НС и двунаправленная синхронизация двух НС демонстрируют разные эффекты.

Мы ограничимся в докладе рассмотрением влияния числа K на процесс синхронизации $\langle \mathrm{TPM(K,N,L)_A} \rangle$ и $\langle \mathrm{TPM(K,N,L)_B} \rangle$ по Хеббу.

Вводится параметр *dist* $((\mathbf{w}^A)_i, (\mathbf{w}^B)_i) = d_i$ – расстояние между векторами весов при $t = i$; $i = 0, 1, \ldots$. Векторы $(\mathbf{w}^A)_i$, $(\mathbf{w}^B)_i$, а также вектор $\mathbf{x}_i$ рассматриваются в N-мерном евклидовом пространстве. Гиперплоскость, определяемая вектором $\mathbf{x}_i$, делит это пространство на две части. Точки, соответствующие векторам весом, могут находиться в одной части, либо в разных.

Анализ показывает, что при K=1 процесса синхронизации как такового нет. При K=2 *wA* и *wB* не сходятся. Дальнейшее увеличение K в рамках вариации набора параметров (K, N, L) сетей $\langle \mathrm{TPM(K,N,L)_A} \rangle$ и $\langle \mathrm{TPM(K,N,L)_B} \rangle$ подтверждает, в основном, соответствующие результаты из [2–6] и других источников.

ЛИТЕРАТУРА

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

2. Ruttor, A. Neural Synchronization and Cryptography/ A. Ruttor. Dissertation zur Erlangung des naturwissenschaftlichen Doktorgrades der Bayerischen Julius-Maximilians-Universitat Wurzburg. – Wurzburg, 2006. – 119 p.

3. 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.

4. Плонковски, М. Синхронизация криптографических ключей на основе нейронных сетей и в системах криптопреобразования на основе XML / М. Плонковски, П. П. Урбанович // Труды БГТУ. Сер. VI, Физико-математические науки и информатика. – 2006. – Вып. XIV. – С.152–155.

5. Урбанович, П. П. Анализ синхронизации нейронных сетей в прикладной криптографии / П. П. Урбанович, И. А. Бирюк, М. Д. Плонковски // Информационные технологии и системы 2019 (ИТС 2019): материалы международной научной конференции, Минск, 30 октября 2019 г. = Information Technologies and Systems 2019 (ITS 2019): Proc. of the Intern. Conf., Minsk, 30th October 2019. – Минск: БГУИР, 2019. – С. 278-279.

6. 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, June 25 - 28, 2019. – Lublin University of Techn., 2019. – P. 32.