УДК 621.9.048.7

ВЫБОР ПАРАМЕТРОВ И ОБОСНОВАНИЕ СТРУКТУРЫ СИНХРОНИЗИРУЕМЫХ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ В ЗАДАЧЕ ФОРМИРОВАНИЯ ОБЩЕГО СЕКРЕТА

Голиков В.Ф., Радюкевич М.Л., Слепцов А.П.

Белорусский национальный технический университет, Минск, Республика Беларусь, vgolikov@bntu.by

В работах [1,2] предлагается использование двух синхронизируемых ИНС, соединенных открытым каналом связи для конфиденциального формирования криптографических ключей. В [1,2] рассматриваются возможности по формированию такого же ключа третьей стороной, прослушивающей канал связи и синхронизирующей свою сеть. Вместе с тем, представляет немалый интерес стойкость предлагаемого способа формирования общего ключа по отношению к простейшей атаке-полному перебору возможных значений формируемого ключа. Практически также отсутствуют исследования по выбору структуры и параметров, синхронизируемых ИНС. Несомненно, оба эти вопроса тесно связаны между собой, т.к. очевидно, что, чем больше размерность ИНС (количество слоев, количество персептронов, количество входов каждого персептрона, диапазон возможных значений весовых коэффициентов), тем выше устойчивость способа к силовой атаке. Однако нерациональное завышение этих параметров ведет к затягиванию достижения синхронизации санкционированных ИНС, что может привести к повышению эффективности других атак, упоминавшихся выше.

В связи с этим представляет интерес обоснование рациональных значений параметров ИНС с точки зрения криптографических требований и анализ устойчивости предлагаемого способа формирования криптографических ключей к силовой атаке.

Обоснование структуры ИНС и выбор ее параметров, на наш взгляд, целесообразно начать с выбора диапазона значений весовых коэффициентов (ВК) персептронов, от которого с одной стороны зависит количество персептронов и количество их входов, с другой - длительность процесса достижения полной синхронизации. Указанные закономерности носят противоречивый характер и нуждаются в анализе.

Исследуем ИНС, состоящую из одного слоя персептронов, предложенную в [1,2], рис.1. Каждый персептрон имеет *n* входов и прямоугольную функцию активации $\sigma(*)$ рис.2.

До начала синхронизации абоненты *A* и *B* независимо друг от друга формируют вектор весовых коэффициентов

$$\vec{w}\mathrm{a} = wa_{11},wa_{12} ,\dots,wa_{1n},wa_{21},wa_{22},\dots,wa_{2n} ,\dots,wa_{K1},wa_{K2},\dots,wa_{Kn}, \quad (1)$$

$$\vec{w}b = wb_{11},wb_{12} ,\dots,wb_{1n},wb_{21},wb_{22},\dots,wb_{2n} ,\dots,wb_{K1},wb_{K2},\dots,wb_{Kn}, \quad (2)$$

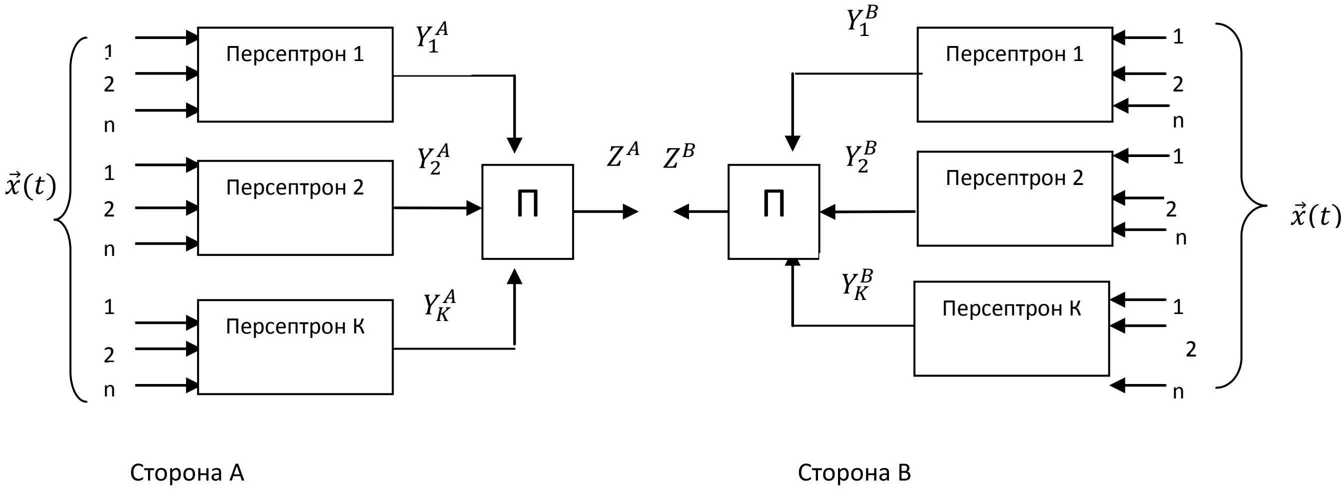

Рисунок 1- Синхронизируемые ИНС

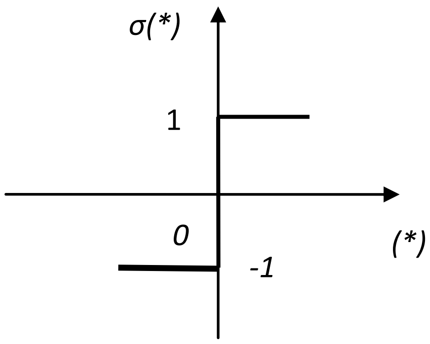

Рисунок 2 - Функция активации

где $wa_{ij}, wb_{ij} \in [-L, L]$, $i = 1, 2, \dots, K$; $j = 1, 2, \dots, n$; L - целое число. Каждый элемент этих векторов w_{ij} есть случайное целое число с дискретным равномерным законом распределения (рис.3)

$$P\left(w_{ij} = s_{ij}\right) = \frac{1}{2L+1}, \quad \text{где } s_{ij} = -L, -L+1, \dots, -1, 0, 1, \dots, L-1, L.$$

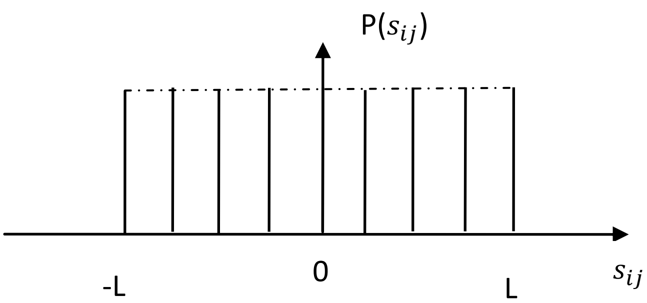

Рисунок 3 - Закон распределения начальных значений весовых коэффициентов

Каждый шаг синхронизации начинается с подачи на входы обеих сетей выбранного случайным образом вектора

$$\vec{x}(t) = x_{11}, x_{12}, \dots, x_{1n}, x_{21}, x_{22}, \dots, x_{2n}, \dots, x_{K1}, x_{K2}, \dots, x_{Kn}, \quad (3)$$

где $x_{ij} \in [-1,1]$ – дискретная случайная величина с равномерным распределением. Для каждого персептрона выходная величина равна

$$Y_i^{A/B} = \sigma(\sum_{j=1}^{n} w_{ij}^{A/B} x_{ij}) \quad (4)$$

Индекс A/B означает, что операция касается обеих сетей A и B, а единичный индекс – что операция касается одной сети соответственно. Функция активации $\sigma(*)$ имеет вид

$$\sigma(*) = \begin{cases} 1, & \sigma(*) \geq 0, \\ -1, & \sigma(*) < 0. \end{cases} \quad (5)$$

Затем вычисляется выходная величина Z для каждой из сетей

$$Z^{A/B} = \prod_{i=1}^{K} Y_i^{A/B} = \prod_{i=1}^{K} \sigma(\sum_{j=1}^{n} w_{ij}^{A/B} x_{ij}) \quad (6)$$

На основании сравнения обоих полученных выходных величин реализован процесс синхронизации. Коррекция векторов весов обеих сетей происходит только тогда, когда обе выходные величины равны друг другу ($Z^A = Z^B$). Внутри данной сети корректируются веса только тех персептронов, выходная величина которых равна величине Z всей сети. Процесс коррекции идет по правилу Хэбба

$$w_{ij}^{A/B} = \begin{cases} w_{ij}^{A/B} + Z^{A/B} * x_{ij}, \text{если } Z^A = Z^B \ \text{ а } Z^{A/B} = Y_i^{A/B}) \geq 0, \\ w_{ij}^{A/B}, \quad \text{в противном случае.} \end{cases}$$

Кроме того, учитывается ограничение $w_{ij}^{A/B} \in [-L, L]$

$$w_{ij}^{A/B} = \begin{cases} \pm L, & \text{если } |w_{ij}^{A/B}| > L, \\ w_{ij}^{A/B}, & \text{в противном случае.} \end{cases}$$

Процесс синхронизации продолжается до полного совпадения векторов $\overrightarrow{wa}, \overrightarrow{wb}$, после чего абоненты A и B имеют общую секретную информацию, представляющую собой последовательность десятичных чисел вида

$$\vec{w}^{A/B} = w_{11}, w_{12}, \dots, w_{1n}, w_{21}, w_{22}, \dots, w_{2n}, \dots, w_{K1}, w_{K2}, \dots, w_{Kn}. \quad (8)$$

Выбор параметров и обоснование структуры ИНС

Решение этой задачи, на наш взгляд, следует начать с выбора диапазона значений ВК, который вместе с количеством входов n и числом персептронов K задает с одной стороны множество возможных значений $\vec{w}^{A/B}$, с другой сильно влияет на длительность процесса согласования ВК сетей A и B. Увеличение L приводит к увеличению множества возможных значений $\vec{w}^{A/B}$, т.е. к увеличению криптостойкости, но при этом увеличивается длительность процесса согласования ВК, т.е. снижается скорость работы алгоритма. С точки зрения обеспечения требуемой криптостойкости следует отдать предпочтение первому фактору. Поэтому величину L будем выбирать исходя из криптографических факторов.

Используя (8), сформируем общее секретное число как конкатенацию значений ВК

$$S = w_{11} \parallel w_{12} \parallel \dots \parallel w_{1n} \parallel w_{21} \parallel w_{22} \parallel \dots \parallel w_{2n} \parallel \dots \parallel w_{K1} \parallel w_{K2} \parallel \dots \parallel w_{Kn} \qquad (9)$$

Как видно из (9) длина сформированной секретной последовательности в битах равна

$d_{(2)} = nK\ |w_{ij(2)}|$, где $|w_{ij(2)}|$ - разрядность двоичного числа, обозначающего значение ВК. Возникает вопрос о выборе разрядности двоичного числа при переходе от десятичного формата ВК к двоичному. Как уже указывалось выше, диапазон изменения значений десятичных чисел w_{ij} задается величиной L и равен [$-L,L$]. Таким образом, количество возможных значений w_{ij} равно $2L+1$. Двоичным числом длиной l можно описать 2^lдесятичных чисел, а так как $2L+1$ нечетное число, то точное его описание для произвольно выбранных значениях L невозможно. Избыточная разрядность нежелательна, так как это приведет к избыточному количеству нулей в ключевой последовательности. Поэтому предлагается следующая методика. Уменьшим количество возможных значений w_{ij} на единицу и вычислим необходимую разрядность l:$2L = 2^l$, откуда

$$l = \ln\,(2L). \qquad (10)$$

В таблице 1 приведены значения L и соответствующие значения l .

Таблица 1- Необходимая разрядность

L	2	4	8	16	32
l	2	3	4	5	6

Тогда таблица для перевода десятичных чисел в двоичные, например, для $L = 4$ имеет вид

Таблица 2- Результаты перевода

$w_{ij(10)}$	0	1	2	3	4	-1	-2	-3	-4
$w_{ij(2)}$	000	001	010	011	100	101	110	111	-

С учетом (10) длина сформированной секретной последовательности в битах равна

$$d_{(2)} = nK \ln(2L). \quad (11)$$

Необходимую длину ключа, как следует, из (11) можно обеспечить соответствующим выбором n, K, L. Однако, эти параметры влияют и на длительность процесса синхронизации. Эксперименты показывают, что увеличение $d_{(2)}$ в два раза за счет увеличения L с 4 до 8 (при $nK = 3 * 100$) увеличивает среднее число необходимых тактов почти в 10 раз, в то время как увеличение $d_{(2)}$ в два раза за счет увеличения nK с 3*50 до 3*100 (при $L = 4$) увеличивает среднее число необходимых тактов только на 30%. В связи с этим нецелесообразно выбирать значение L более 8. В качестве примера расчета определим параметры сети, обеспечивающей формирование ключа длиной 256 бит. Зададимся $L = 4$, тогда $nK = \frac{256}{\ln(2L)} = 84$. Окончательно можно выбрать K=3, n =28.

Анализ устойчивости к силовой атаке

Анализ устойчивости к силовой атаке начнем с рассмотрения простейшего варианта сети - одиночного персептрона с n входами. После первого такта синхронизации становятся известными значения: $\vec{x}(1)$ и Z^A, Z^B, равные соответственно Y^A, Y^B. Исследуем, какие возможности появляются у криптоаналитика при наличии такой информации. Очевидно, что, например, при $Z^A = 1$ выполняется неравенство

$$\sum_{j=1}^{n} w_{ij}^A x_{ij}(1) \geq 0. \quad (12)$$

Перебрав все множество возможных значений w_{ij}^A, оставим для дальнейшего рассмотрения только те значения w_{ij}^A, для которых (12) справедливо. Аналогично после второго такта получим неравенство

$$\sum_{j=1}^{n} w_{ij}^A x_{ij}(2) \gtreqless 0 \quad (13)$$

и проверим его выполнение для отобранного множества значений w_{ij}^A. При этом коррекцией ВК можно пренебречь, так как несложно показать, что ее проведение можно свести только к изменению правой части (13). Таким образом, после m тактов удастся отобрать некое подмножество возможных значений w_{ij}^A, среди которого находится искомая совокупность.

Оценим трудоемкость предлагаемой процедуры. Количество возможных значений w_{ij}^A, которые следует перебрать после первого такта синхронизации равно

$$M_1 = (2L + 1)^n.$$

Количество значений $\vec{w}$a, «прошедших отбор» M_2, зависит от значений $\vec{x}(1)$ и истинных значений $\vec{w}a^*$ и является случайной величиной. Т.к. распределение вероятностей $\vec{w}$a и $\vec{x}(t)$ является равномерным и симметричным относительно 0, то в среднем следует ожидать, что $M_2 \approx \frac{M_1}{2}$. Аналогично $M_3 \approx \frac{M_2}{2}$. Однако, как бы велико не было значение m, «отфильтрованное» множество $\vec{w}$a, содержащее истинное значение

$\vec{w}a^*$ остается значительным и определить его точное значение не представляется возможным. При этом, примерный объем перебора значений по крайней мере составляет

$o(n, L) > 1{,}5(2L+1)^n$.

Кроме того, при этом требуется значительный объем памяти, не менее чем $0{,}5(2L+1)^n$ чисел разрядностью $2^{\ln(2L)}$. Оценим эти объемы для рассмотренного ранее примера $L = 4$, $n = 84$:

$$1{,}5(2L+1)^n = 1{,}5 * 9^{84} \approx 1{,}5 * 1{,}43 * 10^{80} \approx 2{,}145 * 2^{380},$$
$$0{,}5(2L+1)^n = 0{,}5 * 1{,}43 * 10^{80} \approx 0{,}715 * 10^{80}$$

Таким образом, даже для простейшей сети выбором n, L можно обеспечить требуемую вычислительную сложность перебора.

1. Kanter I. The Theory of Neural Networks and Cryptography / I. Kanter, W.Kinzel // Quantum Computers and Computing. —2005. — Vol. 5, №.1. — P. 130—140.
2. Ruttor A. Neural Synchronization and Cryptography. Dissertation zur Erlangung des naturwissenschaftlichen Doktorgrades Der Bayerischen Julius-Maximilians-Universitat Wurzburg, 2006.