УДК 004.56

ФОРМИРОВАНИЕ ОБЩЕГО СЕКРЕТНОГО КЛЮЧА НА ОСНОВЕ СИНХРОНИЗИРУЕМЫХ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ С ИСПОЛЬЗОВАНИЕМ РАЗНОСКОРОСТНОЙ КОРРЕКЦИИ ВЕСОВЫХ КОЭФФИЦИЕНТОВ

В.Ф. ГОЛИКОВ, Н.В. БРИЧ

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск, 220013, Беларусь

Поступила в редакцию 18 мая 2015

Искусственные нейронные сети можно использовать для решения задачи формирования общего секретного ключа. В качестве секретного криптографического ключа будут выступать статистические веса межнейронных соединений синхронизированных искусственных нейронных сетей. Предложенный в статье алгоритм позволяет значительно сократить время достижения синхронизации. Предложенное правило коррекции эффективно решает задачу сближения соответствующих весовых коэффициентов, синхронизируемых искусственными нейронными сетями.

Ключевые слова: искусственные нейронные сети, криптография, секретный ключ.

Искусственные нейронные сети (ИНС) − математические модели, программные и аппаратные реализации, построенные по принципу организации и функционирования биологических нейронных сетей. Важными свойствами нейронных сетей являются возможность обучения и синхронизации. Синхронизированными считаются ИНС, весовые коэффициенты (ВК) которых одинаковы. Разместив ИНС на обоих концах тракта передачи информации и определив момент окончания синхронизации, можно использовать статистические веса межнейронных соединений в качестве секретного ключа [1]. Криптостойкость такой схемы обуславливается тем, что время, необходимое для синхронизации ИНС, намного меньше времени, затрачиваемого на обучение ИНС. Это означает, что время, за которое легитимные пользователи сформируют общий секрет, меньше, чем время, необходимое злоумышленнику для взлома (в случае, если злоумышленник также использует ИНС).

Архитектура на стороне отправителя (A) и получателя (B) представляет собой двуслойный персептрон (TPM-архитектура), состоящий из K внутренних персептронов, каждый из которых имеет N входов (рис. 1).

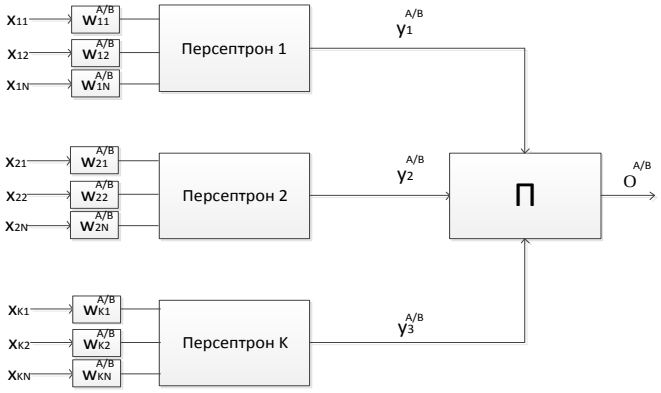

Рис. 1. Синхронизируемая ИНС

Значения дискретной входной величины с равномерным распределением обозначено как $x_{kj} = \pm 1$, где $k = 1,2,\ldots,K$, $j = 1,2,\ldots,N$. Значение на выходе k-го внутреннего персептрона отправителя (получателя) обозначено как $y_k^{A/B}$. Значения ВК обозначены как w_{kj}. Индекс A/B означает, что операция касается обеих сетей A и B, а единичный индекс − что операция касается одной сети соответственно. Схема одного цикла синхронизации для стандартного протокола представлена на рис. 2.

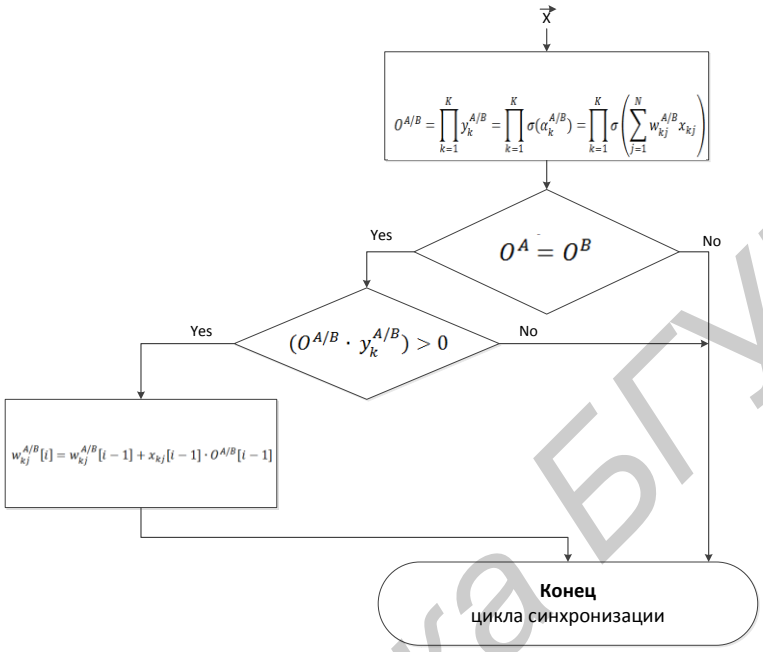

Рис. 2. Один цикл синхронизации двух ИНС

В процессе синхронизации по открытому каналу передаются только значения входного вектора и выходных значений $O^{A/B}$. Выходная величина $O^{A/B}$ каждой ИНС рассчитывается по формуле (1):

$$O^{A/B} = \prod_{k=1}^{K} y_k^{A/B} = \prod_{k=1}^{K} \sigma(\alpha_k^{A/B}) = \prod_{k=1}^{K} \sigma\left(\sum_{j=1}^{N} w_{kj}^{A/B} x_{kj}\right), \quad (1)$$

где $w_{kj}^{A/B}$ − вектор весовых коэффициентов сети, $\sigma(\alpha_k^{A/B})$ − модифицированная функция знака.

Модифицированная функция знака согласно формуле (2):

$$\sigma(\alpha_k^{A/B}) = \begin{cases} 1, \sigma(\alpha_k^{A/B}) \geq 0, \\ -1, \sigma(\alpha_k^{A/B}) < 0. \end{cases} \quad (2)$$

В работах [1, 2] предложено корректировать весовые коэффициенты по правилу Хэбба согласно формуле (3):

$$w_{kj}^{A/B}[i] = w_{kj}^{A/B}[i-1] + x_{kj}[i-1] \cdot O^{A/B}[i-1]. \quad (3)$$

Подробный анализ динамики изменения весовых коэффициентов синхронизируемых сетей, проведенный авторами в [3], показал, что сближение значений соответствующих весовых коэффициентов различных сетей обусловлено исключительно наличием границ $[-L, L]$. Причем сближение относительно часто сопровождается простоями или движением в противоположные стороны, что еще хуже.

Таким образом, стороны A и B по открытому каналу связи обмениваются значениями $O^{A/B}$. Если выходы обеих сетей идентичны $O^A = O^B$, то векторы весов тех персептронов, для которых $(O^{A/B} \cdot y_k^{A/B}) > 0$, подвергаются коррекции по формуле (3). Значения ВК принадлежат

конечному множеству дискретных значений $[-L,L]$. Если $|w_{kj}^{A/B}|>L$, тогда $w_{kj}^{A/B}=L$ с соответствующим знаком.

Таким образом, в процессе синхронизации по открытому каналу передаются только значения входного вектора и выходные значения $O^{A/B}$. Начальные значения ВК $w_{kj}^{A/B}$ выбираются независимо случайным образом и являются секретными. Общий секретный ключ формируется из значений весовых коэффициентов после вхождения ИНС в синхронизм.

Проведенные исследования [4] показали, что количество тактов, необходимых для достижения синхронизации, составляет единицы и десятки тысяч тактов в зависимости от архитектуры ИНС и ее параметров. Это существенно увеличивает время формирования общего ключа. Исходя из этого, важнейшей задачей при использовании ИНС для формирования общего секретного ключа является сокращение числа необходимых тактов.

Одним из подходов, позволяющих ускорить процесс синхронизации, является оптимизация правила коррекции весовых коэффициентов. Значения *i*-го ВК одной ИНС «догоняет» значение *i*-го ВК другой сети за счет наличия границ возможных значений ВК $[-L,L]$, когда *i*-й ВК сети А упирается в границу и останавливается, а *i*-й ВК сети В продолжает движение к этой границе. Поскольку направление движения значения ВК обеих сетей меняется случайным образом, то они могут «дрейфовать» между $-L$ и L большее количество тактов, пока не сравняются около одной из границ, а затем начнут дрейфовать синхронно. Этим и объясняется ограниченное количество тактов синхронизации, необходимое для полного выравнивания всех ВК сетей. Например, для $N=3$, $n=100$ и $L=8$ число необходимых тактов составляет несколько тысяч.

Очевидно, что для сокращения числа тактов, необходимых для полной синхронизации, нужно увеличить скорость изменения ВК при коррекции. Однако при этом существует опасность, что значения весовых коэффициентов могут сконцентрироваться около границы $-L$ и L, что резко уменьшит неопределенность сформированного ключа. Такой исход следует учитывать при выборе правила коррекции.

Сформулируем основные принципы, которые нужно соблюдать при выборе правила коррекции.

1. Корректируемый ВК должен увеличиваться (при $x_i>0$) или уменьшаться (при $x_i<0$). Скорость изменения его величины должна зависеть от его удаленности от границы L ($-L$).

2. При коррекции ВК на стороне А не должны обгонять ВК на стороне В, двигающиеся в том же направлении. Он может только догонять их в точках L ($-L$).

3. Закон распределения вероятностей значений ВК после окончания синхронизации должен быть равномерным.

Известно [5], что для соблюдения третьего принципа на каждом такте коррекции функция преобразования текущих значений ВК, равномерно распределенных, должна быть линейной. В качестве таковой выберем линейное преобразование

$$w_{kj}^{A/B}(i)=w_{kj}^{A/B}(i-1)+\Delta(i)\cdot x_{kj}(i). \qquad (4)$$

Или упрощенно по формуле (5):

$$w(i)=w(i-1)+\Delta(i)x(i), \qquad (5)$$

где $\Delta(i)=f(w(i),L)$.

Для обеспечения линейности выберем согласно (6)

$$f\left(w(i),L\right)=k\left[L-w(i-1)\cdot x(i)\right], \qquad (6)$$

где k – коэффициент (константа), задающий скорость коррекции для линейной модели.

Проанализируем (5) для случая положительного коэффициента скорости коррекции $k>0$. Получаем:

$$w(i)=w(i-1)+k\left[L-w(i-1)x(i)\right]x(i)\,. \qquad (7)$$

Если $w(i-1)>0$ и $x(i)=1$, то приращение ВК положительно и его величина зависит от удаления значения ВК от границы L, к которой он движется. Если $x(i)=-1$, то приращение отрицательно и равно $-(L+w(i-1))$. В этом случае ВК перемещается к отрицательной границе $-L$. Результаты представлены на рис. 3.

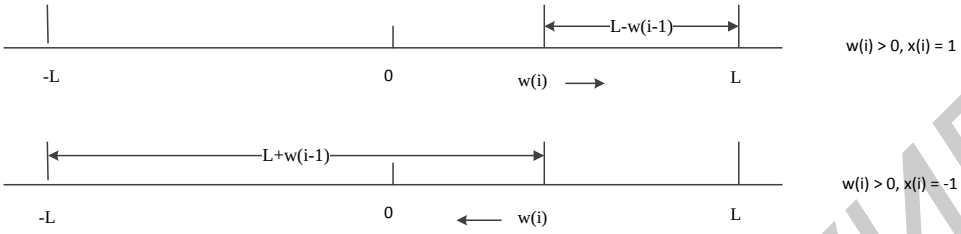

Рис. 3. Движение значений ВК ИНС при коррекции ВК

Аналогично для случая, когда $w(i-1)<0$. Выбор значения коэффициента скорости коррекции k происходит следующим образом. Очевидно, что значение k будет существенно влиять на линейность используемого преобразования. Действительно, модель (7) коррекции остается линейной в пределах изменения $-L\le w(i)\le L$, при больших значениях k закон распределения будет отличаться от равномерного. При этом значения ВК будут собираться у границ интервала $[-L,L]$, что недопустимо с точки зрения качества криптографического ключа. С другой стороны, величина k должна обеспечивать достаточно большую скорость коррекции ВК.

Найдем значение k. Закон распределения начальных значений ВК − равномерный со следующими характеристиками [3] согласно (8):

$$M\left[w(0)\right]=\sum_{j=-L}^{L} j\cdot P\left(w_j(0)=j\right)=\sum_{j=-L}^{L} j\cdot\frac{1}{2L+1}=0; \qquad (8)$$

$$D\left[w(0)\right]=\sum_{j=-L}^{L}(j-M[w(0)])^2\cdot P\left(w_j(0)=j\right)=\sum_{j=-L}^{L} j^2\cdot\frac{1}{2L+1}=\frac{L(L+1)}{3}.$$

Найдем эти характеристики после коррекции:

$$M\left[w(1)\right]=M\left[w(0)+k\left[L-w(0)x(1)\right]x(1)\right]=M\left[w(0)\right]+kM\left[Lx(1)\right]-kM\left[w(0)x^2(1)\right]=$$
$$=0+k\cdot L\cdot 0-k\cdot 0\cdot 1=0.$$

Для удобства вычисления преобразуем (7):

$$w(1)=w(0)+kLx(1)-kw(0)x^2(1)=w(0)[1-k]+kLx(1).$$

Найдем дисперсию $w(1)$, так как $w(0)$ и $x(1)$ − независимые случайные величины:

$$D\left[w(1)\right]=(1-k)^2\,D\left[w(0)\right]+k^2L^2D[x(1)]\,.$$

Дисперсия дискретной случайной величины $x(1)$ равна:

$$D\left[x(1)\right]=(x_1(1)-M[x(1)])^2\cdot P\left(x_1(1)=-1\right)+(x_2(1)-M[x(1)])^2\cdot P\left(x_2(1)=1\right).$$

Так как $M\left[x(1)\right]=0$, $x_1(1)=-1$, $x_2(1)=1$, $P\left(x_1(1)=-1\right)=P\left(x_2(1)=-1\right)=0,5$, то получаем $D\left[x(1)\right]=1$. В результате: $D\left[w(1)\right]=(1-k)^2\cdot D\left[w(0)\right]+k^2L^2$.

Потребуем, чтобы $D\left[w(1)\right]=D\left[w(0)\right]$:

$$(1-k)^2\,D\left[w(0)\right]+k^2L^2=D\left[w(0)\right]. \qquad (9)$$

Решая (9) относительно k, получим $k_1=0$, $k_2=\dfrac{2D[w(0)]}{D\left[w(0)\right]+L^2}=\dfrac{2L+2}{4L+1}$.

Решение $k_1 = 0$ является тривиальным, так как при нем коррекция не осуществляется. Следовательно, закон распределения ВК считается равномерным. Для $L \geq 5$ значение $k \approx 0,5$. С учетом найденного значения k: $w(1)=w(0)+\frac{1}{2}\left[L-w(0)x(1)\right]\cdot x(1)=\frac{1}{2}[w(0)+L\cdot x(1)]$.

Поскольку значения ВК могут принимать только целые значения, то

$$w(1)=\left\lceil \frac{1}{2}[w(0)+L\cdot x(1)] \right\rceil, \qquad (10)$$

где $\lceil * \rceil$ − округление до целого числа в меньшую сторону.

Последующая коррекция ВК по формуле (10) позволяет сохранить равномерный закон распределения значений ВК. Таким образом, окончательное выражение для ВК при предлагаемом правиле коррекции примет вид (11):

$$w_{k_j}^{A/B}(i)=\left\lceil \frac{1}{2}[w(i-1)+L\cdot x(i)] \right\rceil. \qquad (11)$$

Имитационное моделирование для 100000 экспериментов ($K=3, N=100, L=8$) показало, что использование предложенного алгоритма позволяет значительно ускорить время вхождения в синхронизм (рис. 4).

Рис. 4. Скорость синхронизации ИНС при использовании улучшенного протокола

На рис. 4 на оси абсцисс отложен номер такта, на котором обе сети полностью синхронизировались; на оси ординат – частота наступления синхронизации на конкретном такте. Наилучший результат из 100000 экспериментов (имеется в виду результат, потребовавший наименьшее количество тактов для полной синхронизации двух ИНС) – 14 тактов. Наихудший результат (имеется в виду потребовавший наибольшее количество тактов для полной синхронизации двух ИНС) – 138 тактов.

Для сравнения, при использовании стандартного алгоритма коррекции для ИНС такой же конфигурации синхронизация в среднем проходит за 1922 такта (результат получен для 1000 экспериментов). Наименьшее количество тактов, необходимое для синхронизации в этом случае, − 1010 тактов; наибольшее (самая долгая синхронизация) − 3261 такт.

Таким образом, полученный выигрыш в скорости синхронизации при использовании нового алгоритма коррекции составляет более 20 раз. Возможность использования алгоритма для формирования общего секретного ключа опеределяется не только криптостойкостью самого протокола, но и качеством сформированного ключа. В результате анализа качества ключа, сформированного в результате синхронизации двух ИНС по улучшенному правилу коррекции, получены следующие результаты (рис. 5).

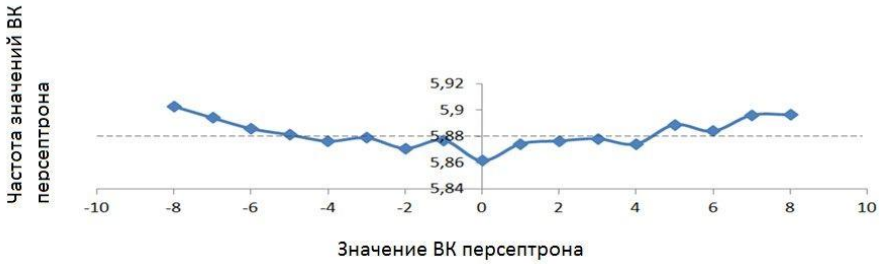

Рис. 5. Качество сформированного ключа

На рис. 5 по оси абсцисс отложено значение весового коэффициента персептрона; по оси ординат – частота значений весового коэффициента. В результате проведения 100 000 экспериментов установлено, что значения весовых коэффициентов после вхождения двух ИНС в синхронизм можно считать равновероятными.

Теоретически вероятность значений ВК при $L=[-8,8]$ равна $1/17=5,88$. Это значение совпадает с полученными в результате эксперимента данными.

Таким образом, предложенный в статье алгоритм позволяет значительно сократить время достижения синхронизации. Предложенное правило коррекции эффективно решает задачу сближения соответствующих ВК синхронизируемых ИНС.

COMMON SECRET KEY DERIVATION BASED ON SYNCHRONIZED ARTIFICIAL NEURONAL NETWORKS USING MULTISPEED WEIGHTED COEFFICIENTS CORRECTION

V.F. GOLIKOV, N.V. BRYCH

Abstract

It's possible to use artificial neuronal networks for secret key derivation. Transneuronal statistical weights of synchronized artificial neuronal networks will be used as a secret key. Proposed algorithm allows to decrease synchronization time meaningfully. Proposed correction rule helps to solve the problem of statistical weights binding while synchronizing artificial neuronal networks.

Список литературы

1. *Kanter I., Kinzel W.* // Quantum Computers and Computing. 2005. Vol. 5, №.1. P. 130−140.
2. *Kinzel W., Kanter I.* // 9th Int. Conf. on Neural Information Processing. Singapore, 2002.
3. *Голиков В.Ф., Брич Н.В.* // Системный анализ и прикладная информатика. 2013. № 1–2. С. 33–37.
4. *Брич Н.В.* // Матер. секционных заседаний студенческой научной молодежи Междун. форума студенческой и учащейся молодежи «Первый шаг в науку». Минск, 23–25 апреля 2014 г. С. 199–203.
5. *Голиков В.Ф., Брич Н.В., Пивоваров В.Л.* // Междунар. научн.-техн. интернет-конференция «Информационные технологии в образовании, науке и производстве». Минск, 16–17 ноября 2013.