ОПИСАНИЕ ПОЛЕЗНОЙ МОДЕЛИ К ПАТЕНТУ
(12)

РЕСПУБЛИКА БЕЛАРУСЬ

НАЦИОНАЛЬНЫЙ ЦЕНТР ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **BY** (11) **7114**
(13) **U**
(46) **2011.04.30**
(51) МПК (2009)
H 04L 9/00

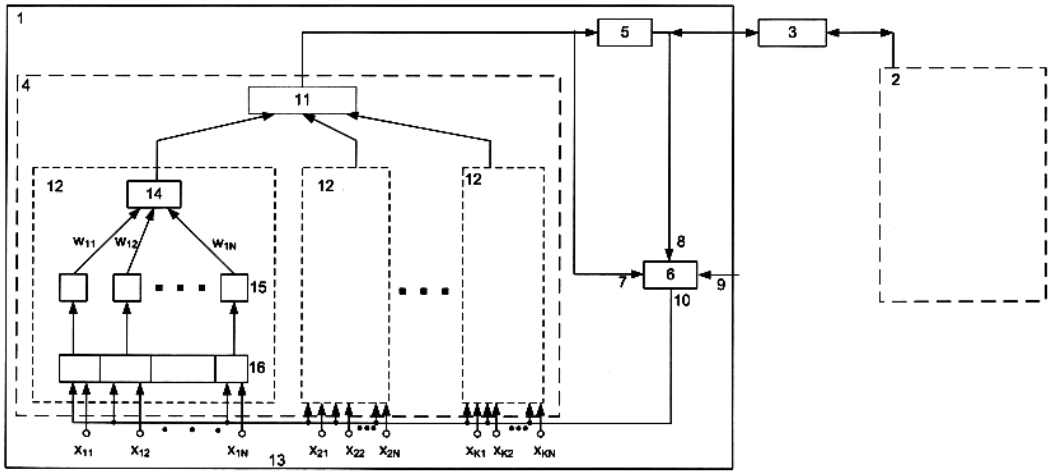
(54) **УСТРОЙСТВО ОБМЕНА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИЕЙ НА ОСНОВЕ НЕЙРОСЕТЕВЫХ ТЕХНОЛОГИЙ**

(21) Номер заявки: u 20100500
(22) 2010.05.27
(71) Заявитель: Учреждение образования "Белорусский государственный технологический университет" (BY)

(72) Авторы: Урбанович Павел Павлович (BY); Плонковски Мартин Даниел (PL); Чуриков Константин Валерьевич (BY)
(73) Патентообладатель: Учреждение образования "Белорусский государственный технологический университет" (BY)

(57)

Устройство, содержащее первую и вторую искусственные нейронные сети на основе первого искусственного нейрона каждая, выходами соединенные с первыми входами соответственно первого и второго блоков анализа и входами соответственно первого и второго коммутаторов, выходы которых соединены с каналом связи (передачи) информации, подсоединенным на соответствующей стороне ко второму входу соответствующего блока анализа, имеющего управляющий вход, и выход каждого из блоков анализа соединен с N-разрядным первым входом соответствующей искусственной нейронной сети, вторые N-разрядные входы каждой из которых являются входами начальной инициализации сети, причем каждая из искусственных нейронных сетей состоит из N-разрядного блока инициализации пороговых элементов, N пороговых элементов и суммирующего блока, выход которого является выходом искусственной нейронной сети, а N входов суммирующего блока соединены с выходами соответствующих пороговых элементов, входами соединенных с соответствующими выходами блока инициализации пороговых элементов, **отличающееся**



Фиг. 1

BY 7114 U 2011.04.30

тем, что в первую и вторую нейронные сети введены блоки перемножения, (k-1) искусственных нейронов, каждый из которых имеет ту же структуру и такие же внутренние связи, как и первый нейрон, выходы первого и (k-1) искусственных нейронов соединены со входами блока перемножения, выход которого образует новый выход нейронной сети и подключается к входу соответствующего коммутатора и первому входу соответствующего блока анализа, выход которого соединен также с первыми входами N-разрядного блока инициализации пороговых элементов каждого из (k-1) искусственных нейронов, другие входы каждого N-разрядного блока инициализации пороговых элементов каждого из (k-1) искусственных нейронов соединены с другими группами входов начальной инициализации сети.

(56)

1. Конопелько В.К., Липницкий В.А., Дворников В.Д. и др.Теория прикладного кодирования: Учеб. пособие в 2 т. Т. 1 / Под ред. проф. В.К. Конопелько. - Мн.: БГУИР, 2004. - С. 216.

2. Mutual learning in a tree parity machine and its application to cryptography: Phys. Rev. E 66, 066135 (2002) [13 pages] / Ido Kanter, and Wolfgang Kinzel.

3. Volkmer M., Wallner S. Tree Parity Machine Rekeying Architectures, Computers // IEEE Transactions. - 2005. - Vol. 54, Iss.4. - P. 421-427.

Полезная модель относится к технике связи, а именно к устройствам обмена конфиденциальной информацией при помощи открытых каналов передачи данных на основе искусственных нейронных сетей, составляющих общую систему передачи информации в обоих направлениях.

Известно техническое решение устройства, реализующего криптосистему обмена конфиденциальной информацией с тайным ключом [1], содержащее блоки зашифрования и расшифрования информации, соединенные каналом связи, и осуществляющее преобразование информации на основе алгоритма DES. Достоинством такого решения является сравнительно небольшая длина используемого ключа, обеспечивающего приемлемый уровень криптографической стойкости. Недостатком такого решения является необходимость обмена ключами между двумя сторонами по открытым (публичным) каналам связи, что может привести к перехвату сообщения о ключе третьей стороной и тем самым к возможности несанкционированного использования третьей стороной чужой конфиденциальной информации.

Наиболее близкое по технической сущности техническое решение к заявляемой полезной модели имеет устройство, содержащее первую и вторую искусственные нейронные сети на основе первого искусственного нейрона каждая, выходами соединенные с первыми входами соответственно первого и второго блоков анализа и входами соответственно первого и второго коммутаторов, выходы которых соединены с каналом связи (передачи) информации, подсоединенным на соответствующей стороне ко второму входу соответствующего блока анализа, имеющего управляющий вход, и выход каждого из блоков анализа соединен с N-разрядным первым входом соответствующей искусственной нейронной сети, вторые N-разрядные входы каждой из которых являются входами начальной инициализации сети, причем каждая из искусственных нейронных сетей состоит из N-разрядного блока инициализации пороговых элементов, N пороговых элементов и суммирующего блока, выход которого является выходом искусственной нейронной сети, а N входов суммирующего блока соединены с выходами соответствующих пороговых элементов, входами соединенных с соответствующими выходами блока инициализации пороговых элементов [2].

Основу описываемого устройства составляет искусственная нейронная сеть, построенная на основе искусственного нейрона.

Математически работу нейрона (в общем случае нейронной сети) можно описать как:

$$S = \sum_{i=1}^{N} w_i x_i \ , \qquad (1)$$

где или x_i и w_i - соответственно i-е входной сигнал и весовой коэффициент нейрона. В устройстве [2] значение x_i, соответствует входному сигналу i-го порогового элемента, значение w_i - внутреннему состоянию i-го порогового элемента, значение S есть сигнал на выходе суммирующего блока. Входная величина для обеих сетей - это случайный вектор X, $x_i \in \{-1,1\}$. Таким образом, значение выхода нейронной сети равно скалярному произведению входных значений на векторы весовых коэффициентов (нейрон с линейной функцией активации).

Первая (А) и вторая (В) сети, построенные на основе абсолютно одинаковой архитектуры, обмениваются между собой по открытому каналу связи выходными значениями. Начальное выходное значение формируется на основе случайно выбранных на каждой из сторон значений, подаваемых на входы начальной инициализации сети А и В. Значения внутренних состояний пороговых элементов каждой из сетей также принимают случайные значения. Именно значения весовых коэффициентов и являются той информацией, которая в режиме синхронизации двух сетей принимается обеими сторонами в качестве конфиденциальной и используется этими сторонами как секретный ключ при дальнейшем обмене информацией с использованием стандартных алгоритмов зашифрования/расшифрования данных.

Режим синхронизации двух сетей основывается на их взаимном "обучении" в процессе обмена выходными значениями и складывается из соответствующего числа шагов синхронизации, в каждом из которых блок анализа на каждой стороне сравнивает выходное значение "собственной" сети, поступившее на последнем шаге на первый вход соответствующего блока анализа, с выходным сигналом другой сети, поступившим с выхода этой другой сети через канал связи на второй вход блока анализа. Выходной сигнал блока анализа на каждой стороне корректирует через соответствующий блок инициализации пороговых элементов внутренние состояния связанных с ними пороговых элементов сети. Процесс "обучения" продолжается до тех пор, пока каждая из сторон не "убедится" в наступлении состояния синхронизации.

Третья сторона (третья нейронная сеть, интруз), пытающаяся синхронизировать свое состояние с состоянием сетей А и В, основывается только на доступных значениях выходных параметров сетей. Поскольку число N изначально является секретным, то третья сторона имеет малые возможности получить информацию о значениях весовых коэффициентов сетей А и В, принятых в качестве ключа шифрования. В этом заключаются положительные свойства данного устройства перед аналогом: в повышении уровня конфиденциальности обмена информацией по открытым каналам связи.

Однако недостатком технического решения [2], ограничивающим достижимый уровень конфиденциальности, является использование алгебры целых чисел.

Проблема касается особенностей практического применения всей системы. Обмен информацией в компьютерных системах базируется на пространстве битов или на дискретных величинах. Поэтому обоснованным является вопрос: будет ли правильным (или сходящимся к общему вектору) процесс обмена ключами для векторов весов с дискретными (битовыми) величинами. Рассмотренный выше процесс синхронизации сходится только тогда, когда векторы весов нормализованы на каждом шаге обучения. Этап нормализации накладывает некоторые ограничения на величины векторов весов. Этого типа ограничение используется в системе, основанной на дискретных величинах векторов весов. Каждая величина вектора весов сетей А и В останется в границах следующего множества:

$$w_i^{A/B} \in \{-L, -L+1, ..., 0, ..., L-1, L\},$$

где L - это установленное целое число. Следовательно, каждая величина вектора весов (внутренние состояния пороговых элементов) может принять одно из 2L + 1 возможных значений; из того факта, что величины входного вектора x являются дискретными числами ({-1, 1}), вытекает, что величины их активизированных весов могут принимать три значения: 1, 0 или -1. Случай получения нулевой величины означает либо несоответствие выходных величин обоих персептронов, либо выход за пороговую величину данного ограничения. Второй случай, когда не происходит активизация величины вектора весов вследствие нарушения границы $|L|$, представляет собой единственную возможность для величин вектора весов приблизиться друг к другу на единицу. Говоря точнее, величины последующих элементов векторов весов движутся по прямой линии в пространстве [-L, L]. Если весы подчиняются процессу обучения, то соответствующие им величины движутся в одном направлении. Если одна из величин нарушит границу (-L либо L), то ей будет возвращено значение нарушенной границы и она в действительности не выполнит никакого движения (останется неизмененной). Это означает, что если соответствующая величина второго вектора весов производит движение по направлению к упомянутой границе, то расстояние между теми двумя величинами сократится на 1. Следовательно, этот случай является сущностью процесса синхронизации, так как обеспечивает сокращение дистанции между соответствующими величинами векторов весов. Для двух персептронов с N-мерными векторами весов существует N двухэлементных групп (пар величин), которые движутся в промежутке [-L, L].

Опыты показывают, что для набора параметров N = 100 и L = 3 две сети (A и B) синхронизируют свои внутренние векторы весов приблизительно за 100 шагов обучения. Вдобавок время синхронизации логарифмически увеличивается с ростом величины N. Нужно также добавить, что интруз, "наблюдающий" за процессом обмена данными двух сетей (A и B), способен синхронизироваться с их векторами весов. Поэтому единичный персептрон, реализованный в известном решении в виде N-разрядного блока инициализации пороговых элементов, N пороговых элементов и суммирующего блока, не может быть использован как практически безопасный источник обмена секретным ключом (какой-нибудь криптографической системы, построенной на основе известного решения [2]).

Технической задачей заявляемой полезной модели является создание надежной высокоэффективной аппаратуры передачи информации по открытым каналам связи, обеспечивающей более высокий по сравнению с известными решениями уровень конфиденциальности (секретности).

Поставленная задача решена при создании заявляемой полезной модели с техническими результатами:

выход искусственной нейронной сети имеет 4 либо 8, либо 16 значений (в сравнении с 2 в известном решении);

множество, ограничивающее увеличение величины вектора весов, может принять любую форму,

что в совокупности обеспечивает более высокое относительное время, требуемое интрузу для синхронизации вектора весов своей сети с векторами весов сетей A и B.

Для достижения указанных технических результатов в устройство, содержащее первую и вторую искусственные нейронные сети на основе первого искусственного нейрона каждая, выходами соединенные с первыми входами соответственно первого и второго блоков анализа и входами соответственно первого и второго коммутаторов, выходы которых соединены с каналом связи (передачи) информации, подсоединенным на соответствующей стороне ко второму входу соответствующего блока анализа, имеющего управляющий вход, и выход каждого из блоков анализа соединен с N-разрядным первым входом соответствующей искусственной нейронной сети, вторые N-разрядные входы

каждой из которых являются входами начальной инициализации сети, причем каждая из искусственных нейронных сетей состоит из N-разрядного блока инициализации пороговых элементов, N пороговых элементов и суммирующего блока, выход которого является выходом искусственной нейронной сети, а N входов суммирующего блока соединены с выходами соответствующих пороговых элементов, входами соединенных с соответствующими выходами блока инициализации пороговых элементов, введены в первую и вторую нейронные сети блоки перемножения, (k-1) искусственных нейронов, каждый из которых имеет ту же структуру и такие же внутренние связи, как и первый нейрон, выходы первого и (k-1) искусственных нейронов соединены со входами блока перемножения, выход которого образует новый выход нейронной сети и подключается к входу соответствующего коммутатора и первому входу соответствующего блока анализа, выход которого соединен также с первыми входами N-разрядного блока инициализации пороговых элементов каждого из (k-1) искусственных нейронов, другие входы каждого N-разрядного блока инициализации пороговых элементов каждого из (k-1) искусственных нейронов соединены с другими группами входов начальной инициализации сети.

Таким образом, каждый из введенных искусственных персептронов имеет N входов. Следовательно, вектор входных значений всей сети равен $k \cdot N$. В этой структуре приняты следующие обозначения: x_{ij} - j-тый вход i-того персептрона, y_i - выход i-того персептрона, где $i = 1, 2, ..., k$ и $j = 1, 2, ...N$. Для упрощения принято, что величины входного вектора бинарны - $x_{ij} = \pm 1$. Каждый из персептронов имеет веса, которые получают j-тую величину входа в i-том персептроне. Следовательно, величины векторов весов обозначены как w_{ij}. Выход всей сети, O - это произведение всех выходных величин внутренних k искусственных персептронов.

Формально структура предлагаемого устройства состоит из двух уровней. Элементы первого уровня - это искусственные нейроны (персептроны), имеющие N-элементные векторы весов ($[w_{i1}, w_{i2}, ..., w_{iN}]$, где $1 \le i \le k$), величины которых зависят от используемой алгебры. Второй уровень составляет блок перемножения (который может быть реализован также в виде персептрона), выходное значение которого - это произведение выходов всех искусственных нейронов, составляющих первый уровень.

Полезная модель поясняется фигурами чертежей:

фиг. 1 - структурная схема устройства обмена конфиденциальной информацией;

фиг. 2 - точки, составляющие входные величины вектора X;

фиг. 3 - точки, которые могут составлять элементы вектора весов;

фиг. 4 - точки, являющиеся выходными величинами персептронов;

фиг. 5 - упрощенная схема представления функции знака.

Заявляемое устройство представлено на фиг. 1 в виде структурной схемы.

Устройство обмена конфиденциальной информацией состоит из абонента A1 и абонента B2, построенных одинаково и соединенных между собой каналом связи 3. Структура каждого из абонентов содержит искусственную нейронную сеть 4, первый коммутатор 5, первый блок анализа 6 с первым 7, вторым 8 и управляющим 9 входами и выходом 10. Структура искусственной нейронной сети 4 содержит блок перемножения 11, искусственные нейроны 12 с первого по k-ый, первыми входами соединенные с выходами 10 блока 6, а вторыми входами - с соответствующими группами входов 13 начальной инициализации сети. Структура каждого искусственного нейрона 12 содержит суммирующий блок 14, N пороговых элементов 15, N-разрядный блок начальной инициализации 16.

Устройство работает по принципу, описанному в применении к известному устройству [2] с точки зрения обмена информацией между абонентами A и B по каналу 3, анализа информации в блоке 6 и изменения значений весовых коэффициентов в процессе синхронизации сетей (взаимного обучения). Процесс взаимного обучения или синхронизации начинается с инициализации векторов весов обеих сетей. Их начальное состояние, выбираемое случайным образом на входах 13, остается секретным на протяжении всего

времени процесса обучения. Каждый последующий шаг начинается с подачи на входы обеих сетей выбранного случайным образом вектора X. Затем вычисляется выходная величина O на выходе блока 11 для каждой из архитектур следующим способом:

$$O^{A/B} = \prod_{i=1}^{k} y_i^{A/B} = \prod_{i=1}^{k} \sigma\left(\alpha_i^{A/B}\right) = \prod_{i=1}^{k} \sigma\left(\sum_{j=1}^{N} w_{ij}^{A/B} x_{ij}\right). \quad (2)$$

Индекс A/B обозначает, что данная операция касается обеих сетей A и B, а единичный индекс A или B обозначает, что операция касается соответственно только одной из сетей: A или B.

Кроме того, в формуле присутствует функция знака σ, которая для известного устройства может определяться следующим образом (приняв i = 1):

$$\sigma = \left(\alpha_i^{A/B}\right) = \begin{cases} 1, \alpha_i^{A/B} \geq 0 \\ -1, \alpha_i^{A/B} < 0 \end{cases}. \quad (3)$$

Выходная величина O на выходе 11 обеих сетей, вычисляемая на основании рассмотренных формул и общего входного вектора X, передается взаимно каждому из абонентов 1 через блоки 5 и двунаправленный канал 3. Следовательно, обе сети "знают" полученные выходные величины друг друга. Естественно, передача этой информации вызывает ее раскрытие, что приводит к тому, что третьи лица будут иметь доступ к ней. Из формулы (1) следует, что, в отличие от известного устройства, выходное значение целой архитектуры вычисляется как произведение выходных величин k искусственных нейронов 12.

На основании обеих полученных выходных величин реализован процесс обучения. Поскольку активизация векторов весов обеих сетей происходит только тогда, когда обе выходные величины равны друг другу, то есть $O^A = O^B$. Другое важное функциональное отличие предлагаемого решения состоит в том, что внутри данной сети модифицируются веса только тех персептронов 12, выходная величина которых y_k равна выходной величине O всей сети. Процесс обучения происходит в соответствии с правилом Хэбба, представленным в виде следующей формулы [3]:

$$w_{kj}^{A/B} = \begin{cases} w_{kj}^{A/B} + O^{A/B} x_{kj}, \ O^A = O^B \wedge O^{A/B} = y_k^{A/B} \\ w_{kj}^{A/B}, \text{ в противном случае} \end{cases}.$$

Также векторы весов на каждом шаге обучения должны быть подвержены процессу нормализации. Для персептронов 12, у которых величины весов являются целыми числами, процесс нормализации связан с необходимостью наложения ограничений на них.

На основе предложенной структурной схемы устройство может функционировать, в отличие от известного, на основе комплексных чисел, октонионов и кватернионов.

Рассмотрим для примера особенности использования комплексных чисел как базовой алгебры функционирования устройства.

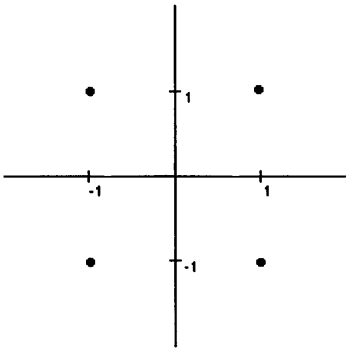
Вход блоков 12 составляет k N-элементных векторов $[x_{i1}, x_{i2}, ..., x_{iN}]$, где $1 \leq i \leq k$, часто отождествляемых с одним N·k-элементным вектором $[x_1, x_2, ..., x_{kN}]$ четырехвалентных комплексных чисел, выбранных из множества {(1,1), (-1,1), (-1,-1), (1,-1)}. Выходы суммирующих блоков 14 нейронов 12 - это четырехвалентные комплексные числа, принадлежащие множеству {(1,0), (0,1), (-1,0), (0,-1)} и обозначенные через $y_1, y_2, ..., y_k$. Для рассматриваемого примера функция знака выбирается из четырех возможных вариантов: (1,0), (0,1), (-1,0), (0,-1) - и будет вычисляться в блоке 11 следующим образом:

$$\sigma(\alpha_i) = \begin{cases} (1,\,0),\ \dfrac{7\pi}{4} < \arg(\alpha_i) \le \dfrac{\pi}{4} \\ (0,1),\ \dfrac{\pi}{4} < \arg(\alpha_i) \le \dfrac{3\pi}{4} \\ (-1,\,0),\ \dfrac{3\pi}{4} < \arg(\alpha_i) \le \dfrac{5\pi}{4} \\ (0,\,-1),\ \dfrac{5\pi}{4} < \arg(\alpha_i) \le \dfrac{7\pi}{4} \end{cases}.$$

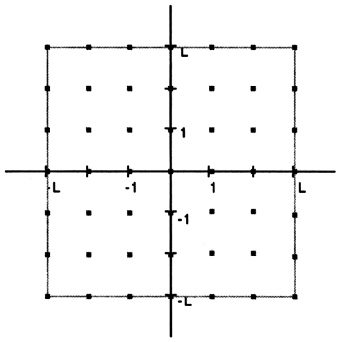
Входные величины (вектор X) принадлежат следующим множествам {(1,1), (-1,1), (-1,-1), (1,-1)}. В графическом виде эти числа представлены на графике четырьмя точками, размещенными по углам квадрата (фиг. 2); отметим, что подобное отображение для известного устройства представляется прямой линией. Величины векторов весов на выходах элементов 15 - это комплексные числа, заключенные в квадрате [-L, L] × [-L, L]. Их графическое представление будет иметь вид, показанный на фиг. 3. Выходные величины каждого из блоков 1 и 2, как произведение выходных величин блоков 14, также принадлежат множеству, представленному на фиг. 4. Функция знака σ представлена на упрощенной схеме на фиг. 5, где выходные величины обозначены точками, находящимися в соответствующих четвертях.

Далее оценим преимущества предлагаемого технического решения перед известным.

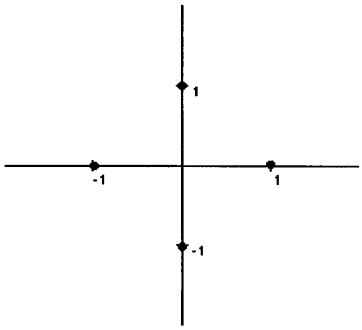
Данное устройство можно использовать для повышения надежности функционирования сети и эффективности организации передачи информации между сервером и клиентской частью.



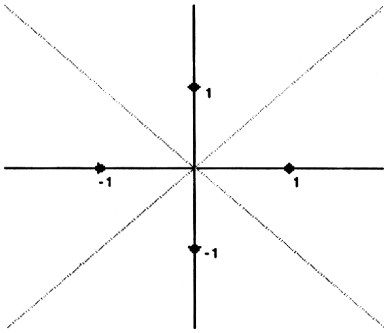
Фиг. 2



Фиг. 3



Фиг. 4



Фиг. 5

Национальный центр интеллектуальной собственности.
220034, г. Минск, ул. Козлова, 20.