выполняет проверку электронной цифровой подписи в два шага. На первом этапе вычисляет значение открытого ключа на основе открытой ключевой информации доверителя Боба и доверенной стороны Алисы:

$$y_p = (y_A \cdot y_B)^{h(m_W||K)} \cdot K \bmod p,$$

где y_A – открытый ключ доверенной стороны, y_B – открытый ключ доверителя.

На втором этапе происходит проверка цифровой подписи по алгоритму Эль-Гамаль с использованием открытого ключа y_p. В результате проверки доверенной цифровой подписи проверяющая сторона может убедиться в целостности переданного документа, однозначно идентифицировать доверителя и доверенную сторону.

На основе приведенных выше вычислений можно сделать следующие выводы: доверенная сторона не может сгенерировать подпись идентичную оригинальной подписи доверителя, доверитель не может сгенерировать защищенную доверенную подпись от лица доверенной стороны, доверительно может наложить ограничения на сферу возможного применения цифровой подписи с использованием полномочий, результирующая электронная цифровая подпись однозначно идентифицирует доверителя и доверенную сторону.

Для реализации математической модели использовался язык программирования Java и криптографическая библиотека с открытым исходным кодом Bouncy Castle. Корректное функционирование было проверено с использованием модульных тестов.

Таким образом, была разработана и реализована математическая модель защищенной доверенной цифровой подписи с полномочиями. Рассматриваемая модель за счет использования генерируемого секретного значения позволяет избежать передачи ключевой информации доверителя, однозначно идентифицировать доверителя и доверенную сторону, исключает возможность доверителю выдать себя за доверенную сторону, а также дает возможность ограничить применение доверенной подписи за счет использования полномочий. Эти свойства выделяют данную схему по сравнению с другими алгоритмами доверенной цифровой подписи.

Список использованных источников:

1. Mambo, M. Proxy Signatures: Delegation of the power to sign Foundation / M. Mambo, K. Usuda, and E. Okamoto // IEICE Trans. Fundamentals Volume E79-A, Number 9, Sep 9, - 1996. – P. 1338-1354.
2. Sattar, A. A practical proxy signature scheme / A. Sattar, Y. Sufian // IJDIWC – 2012. – P. 27 – 35.
3. ElGamal, T. A public key cryptosystem and a signature scheme based on discrete logarithms / T. ElGamal // IEEE Trans. On Information Theory, Vol. IT-31, No. 4 – 1985 - P 86-91
4. Толюпа, Е.А. Некоторые протоколы доверенной цифровой подписи / Е.А. Толюпа – Математические методы криптографии №1(11) - 2011 – с 70-78.
5. Kim, S. Proxy signatures, revisited // Information and Communications / S. Kim, S. Park, D. Won // Security (ICICS'97). 1997. LNCS. V. 1334, P. 223–232
6. Lee, B. Strong proxy signature and its applications / B. Lee, H. Kim, K. Kim // Proc. of the 2001 Symposium on Cryptography and Information Security (SCIS'01), Oiso, Japan, Jan. 23–26, 2001. V. 2/2. P. 603–608

МЕТОДЫ ПОСТРОЕНИЯ И СИНХРОНИЗАЦИИ КРИПТОГРАФИЧЕСКИХ СИСТЕМ НА ОСНОВЕ НЕЙРОННЫХ СЕТЕЙ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Плехова Т. В.

Ярмолик В. Н. – д.т.н., профессор

Из-за процесса постоянного роста вычислительных мощностей современных компьютеров, а также технологий сетевых и нейронных вычислений сделало возможным дискредитацию криптографических систем еще недавно считавшихся практически нераскрываемыми. Таким образом возникает актуальность в поиске новых подходов к построению криптографических систем. Примером такого подхода является построение криптографических систем на основе нейронных сетей.

Нейронные сети не программируются в привычном смысле этого слова, они обучаются. Возможность обучения — одно из главных преимуществ нейронных сетей перед традиционными алгоритмами. Технически обучение заключается в нахождении коэффициентов связей между нейронами. В процессе обучения нейронная сеть способна выявлять сложные зависимости между входными данными и выходными, а также выполнять обобщение. Это значит, что, в случае успешного обучения, сеть сможет вернуть верный результат на основании данных, которые отсутствовали в обучающей выборке, а также неполных и/или «зашумленных», частично искаженных данных.

В криптоанализе используется способность нейронных сетей исследовать пространство решений. Также имеется возможность создавать новые типы атак на существующие алгоритмы шифрования, основанные на том, что любая функции может быть представлена нейронной сетью. Взломав алгоритм, можно найти решение, по крайней мере, теоретически. При этом используются такие свойства нейронных сетей,

как взаимное обучение, самообучение, и стохастическое поведение, а также низкая чувствительность к шуму, неточностям (искажения данных, весовых коэффициентов, ошибки в программе). Они позволяют решать проблемы криптографии с открытым ключом, распределения ключей, хеширования и генерации псевдослучайных чисел.

Для обмена ключами между двумя абонентами наиболее часто используется алгоритм Диффи-Хеллмана. Его более безопасная замена основана на синхронизации двух древовидных машин четности (TPM, tree parity machines). Синхронизация этих машин похожа на синхронизацию двух хаотических осцилляторов в теории хаотических связей (chaos communications).

Динамика двух сетей и их весовых коэффициентов нашла применение в явлении, где сети синхронизируют состояния с идентичными весовыми коэффициентами, зависящими от времени. Эта концепция быстрой синхронизации по взаимному обучению может быть применена к протоколу обмена секретным ключом через публичный канал. А сгенерированный ключ может быть использован для шифрования и дешифрования передаваемого сообщения. Алгоритм не оперирует большими числами и методами из теории чисел, следовательно, приводит к быстрой синхронизации открытого ключа. Безопасность нейрокриптографии все еще обсуждается, но, так как метод основан на стохастическом процессе, есть небольшой шанс, что злоумышленник синхронизируется с ключом.

Также, было установлено, что защищенность обычных криптографических систем можно улучшить, увеличив длину ключа. В нейрокриптографии вместо ключа увеличивается синаптическая длина L. Это увеличивает сложность атаки экспоненциально, в то время как затраты абонентов на дешифрацию растут полиномиально. Таким образом, взлом подобной системы является NP-сложной задачей.

Криптографическая система на базе взаимодействующих нейронных сетей, представленная Кантером, Кинзело и Кантером (ККК), использует множество циклов, в которых каждая сторона выявляет один бит информации о текущем состоянии, а затем модифицирует его в соответствии с информацией, полученной от другой стороны. Если обозначить последовательность двух сторон, как A_i и B_i, то расстояние (A_{i+1},B_{i+1}) меньше расстояния (A_i,B_i) и $A_i = B_i$ для всех $i > i_0$. С точки зрения криптоанализа, состояния сторон становятся быстродвижущимися целями, а его общая задача состоит в том, как объединить биты информации о двух сходящихся последовательностях неизвестных состояний [3].

В проблеме совместного обучения каждая сеть используется и как обучающая сторона, и как сторона обучающаяся, и не существует фиксированной цели, к которой необходимо стремится. Наоборот, они преследуют друг друга по хаотичной траектории, которая первоначально управляется общей последовательностью случайных входов.

Каждая сторона в предложенной ККК-конструкции использует двухслойную нейронную сеть. Первый слой содержит K независимых персептронов, в то время как второй слой вычисляет равенство K скрытых слоев. Каждый из K персептронов имеет N весов $w_{k,n}$ (где $1 \le k \le K$ и $1 \le n \le N$). Эти веса целые числа в области {L, …, -L}, которые могут изменяться во времени. Дано N битовых входных значений $(x_{k,1}, \ldots, x_{k,N})$ (где $x_{k,n} \in \{-1, +1\}$), персептрон возвращает знак (который также принадлежит {*-l*, *+l*}) произведения $w_k x_k = \sum_{n=1}^{N} w_{k,n} x_{k,n}$. Выход o_k персептрона имеет простое геометрическое толкование: геперплоскость, которая перпендикулярна вектору весовых коэффициентов w, делит пространство пополам, а выход персептрона для входа x показывает, находятся x и w по одну сторону гиперплоскости или нет (т.е. меньше или больше 90° угол между w и x). Выход нейронной сети определяется как равенство $O = \prod_{k=1}^{K} o_k$ выходов K персептронов.

В схеме ККК две стороны A и B начинают с проихвольных некоррелированных матриц весовых коэффициентов $\{w_{k,n}\}$. В каждом цикле новая произвольная матрица входов $\{x_{k,n}\}$ открыто выбирается (например, используя генератор псевдослучайной последовательности бит), а каждая сторона объявляет выход своей своей нейронной сети на заданном общем входном сигнале. Если два выходных бита совпадают, стороны остаются без действия и проходят в следующий цикл; иначе каждая сторона обучает собственную нейронную сеть в соответствии с выходом другой стороны. При обучении используется классическое правило обучения Хебба для обновления весовых коэффициентов персептрона. Тем не менее, каждой стороне известно только равенство выходов персептронов других сторон и таким образом правило модифицируется: в методе ККК каждая сторона модифицирует только те персептроны в своей сети, чьи скрытые входы отличаются от обозначенного выхода. С этой поправкой ККК показывает, что для некоторых вариантов K, N, L матрицы весовых коэффициентов двух сторон становятся непараллельными (то есть $w_{k,n}^{A} = -w_{k,n}^{B}$), для всех k и n) после достаточного небольшого числа циклов, и с этого момента они всегда формируют негативные выходы и обновляют свои весовые коэфициенты, переходя в новые непараллельные состояния. Две стороны могут быть осведомленными о полученной синхронизации, отмечая, что их выходные значения совпадают в течении 20-30 последовательных шагов. Раз в их сети стали синхронизированными, две стороны могли остановить и вычислить общий криптографический ключ путем хеширования своей текущей матрицы весовых коэффициентов (или ее отрицания).

Для того, чтобы показать возможность применения криптографических систем на основе нейронных сетей был проведен ряд экспериментов. Задачей экспериментов было показать, возможность использования подхода реализации криптографических систем на основе нейронных сетей, достигнуть сравнительно быстрого времени синхронизации нейронных сетей. Эксперименты производились над разными типами нейронных сетей: Tree Parity Machines, нейронные сети с хаотичным отображением, нейронные сети с обратной связью.

N	Среднее количество сообщений, шт	Среднее затраченное время CPU, с
3	798,53	0,134
4	370,63	0,072
5	362, 23	0,083
8	339,67	0,111
16	365,74	0,212
32	430,96	0,476
64	483,31	1,05
128	557,04	2,67
256	589,64	6,036
512	659,72	11,165
1024	720,32	24,436

Таблица 1 - Среднее количество сообщений при синхронизации TPM и среднее затраченное время CPU в зависимости от коэффициента N, определяющего количество входных нейронов

Для каждого вида нейронной сети было найдено оптимальное соотношение между сложностью полученной системы и времени, потраченном на ее синхронизацию. Для приведенного примера TPM при конфигурации K=4, L=3 наиболее оптимальное соотношение достигалось при N от 256 до 512.

Список использованных источников:

1. Dourlens, S., The first definition of the Neuro-Cryptography (AI Neural-Cryptography) applied to DES cryptanalysis by Sebastien Dourlens – 1995, France.
2. Kinzel, W., Neural Cryptography — Description of one kind of neural cryptography at the University of Würzburg – 2005, Germany.
3. Червяков, Н.И., Применение искусственных нейронных сетей и системы остаточных классов в криптографии / Червяков Н.И., Евдокимов А.А., Галушкин А.И., Лавриненко И.Н. / М.: ФИЗМАТЛИТ, 2012.- 280 с.

АВТОМАТИЗАЦИЯ СОЗДАНИЯ OLAP-КУБОВ НА БАЗЕ MSSQL ДЛЯ ОПТИМИЗАЦИИ ИНФРАСТРУКТУРЫ ИС ПРЕДПРИЯТИЯ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Коржовник Д. А.

Лапицкая Н. В. – к-т. техн. наук, доцент

При осуществлении проектов по созданию региональных информационно-аналитических систем (ИС), актуальные на тот момент технологии позволяли экономически выгодно внедрять в масштабах отдельно взятого субъекта системы с архитектурой на основе интегрированного хранилища данных (ИХД). Для решения задач отчетности, анализа бизнес-процессов и поддержки принятия решений, в качестве ИХД выступали реляционные базы данных (БД) на сервере системы управления базами данных (СУБД). После долгого периода эксплуатации основной проблемой оказался неизбежный рост сырых данных в системе, который стал приводить к задержкам в выполнении запросов от программного обеспечения (ПО) к ИХД на получение информации. Устранение проблемы зачастую осложнялось невозможностью получить исходные коды ПО или его поддержку, что способствовало поиску других способов работы с данными.

Один из обусловленных экономически подходов к решению подобной проблемы стало добавление нового модуля, с функционалом недостающим для приведения текущей инфраструктуры информационного взаимодействия системы (рисунок 1) к актуальным стандартам и технологиям построения аналитических систем, которые принято связывать с понятием «аналитическая пирамида»: на основе транзакционной системы формируются хранилища данных, необходимые для представления витрины данных, позволяющей создавать посредством OLAP-технологий аналитические приложения. Согласно представленной на рисунке 1 схемы информационная система собирает отчетную информацию, по разным, периодически изменяющимся статистическим показателям, от разных филиалов организации по региону. Перечень элементов на рисунке 1:

1. DW — хранилище данных с СУБД Oracle.
2. СИ — статистическая информация, показатели бухгалтерской, финансовой и т.п. отчетности