Математические структуры и моделирование
2011, вып. 23, с. 105–107

УДК 004.056.5

ОСОБЕННОСТИ РЕАЛИЗАЦИИ ПРОТОКОЛА ВЫРАБОТКИ ОБЩЕГО КЛЮЧА С ИСПОЛЬЗОВАНИЕМ ИСКУССТВЕННОЙ НЕЙРОННОЙ СЕТИ

А.И. Журавлёв, Д.Н. Лавров

В статье описываются особенности реализации алгоритма выработки общего ключа на основе синхронизации обучения искусственных нейронных сетей.

Одним из способов получения двумя абонентами Алисой и Бобом общего ключа является согласованное вычисление ключа в процессе взаимодействия абонентов. Обычно неотъемлемым элементом такого взаимодействия является использование криптографии. Относительно недавно появился новый алгоритм выработки общего ключа, основанный на использовании искусственных нейронных сетей. Искусственным нейронным сетям (ИНС) присущи многие свойства, которые используются в различных прикладных задачах. Например, возможно достижение состояния так называемой синхронизации ИНС, под которой следует понимать равенство значений весовых коэффициентов ИНС. Это явление и может служить основой для протокола выработки общего ключа [1].

Пусть у Алисы и Боба имеется по так называемой древовидной машине чётности (ДМЧ). ДМЧ — это ИНС, которую можно описать следующим образом. В ДМЧ содержится K нейронов скрытого слоя и 1 выходной нейрон. С каждым нейроном скрытого слоя связано N входов, причём с каждым входом связан весовой коэффициент $w[i,j]$ (i – индекс скрытого нейрона, j – индекс входа у скрытого нейрона). Все весовые коэффициенты являются целыми числами, лежащими в диапазоне от $-L$ до L. Внутреннее состояние скрытого нейрона определяется как взвешенная сумма его входов, а выход скрытого нейрона — это функция sgn (x) от внутреннего состояния, причём sgn $(x) = -1$ при $x = 0$. Выход выходного нейрона равен произведению выходов нейронов скрытого слоя.

Первоначально значения весов у ДМЧ Алисы и Боба заданы случайно. Значения весовых коэффициентов, внутренние состояния скрытых нейронов и их выходы держатся в секрете в течение всего алгоритма выработки общего ключа. Алгоритм описывается следующим образом.

Алиса и Боб, используя одинаковые входные векторы, вычисляют выходы своих ДМЧ и сообщают их друг другу. При неравных выходных значениях

Омский государственный университет им. Ф.М. Достоевского
E-mail: alizhur@yandex.ru, lavrov@omsu.ru

ДМЧ веса обоих ДМЧ не изменяются, а противном случае применяется некоторое обучающее правило, например обучающее правило Хеббиана:

$$w[i,j] = g(w[i,j] + x[i,j] * out * F(out(i), out) * F(outA, outB)),$$

где out — выход ДМЧ, у которой изменяются веса; $outA$ и $outB$ — это выходы ДМЧ Алисы и Боба соответственно; $x[i,j]$ — вход j скрытого нейрона i; $F(x,y) = 1$ при $x = y$, иначе $F(x,y) = 0$;

$$g(x) = \begin{cases} \text{sgn } (x) * L, |x| > L \\ x, |x| \leq L \end{cases}.$$

После некоторого числа итераций обе ДМЧ достигнут состояния синхронизации, причём при проведении итераций и далее весовые коэффициенты, очевидно, будут меняться, но их равенство не нарушится.

При реализации алгоритма возникает вопрос о том, когда следует прекращать его выполнение. Иными словами, требуется найти критерий синхронизации, удовлетворив который, можно будет остановить алгоритм. Возможны следующие подходы:

1. Полный перебор — обеим ДМЧ подаются на входы все возможные входные векторы, а вычисленные выходы ДМЧ сравниваются. При достижении синхронизации при всех входных векторах все соответствующие выходы ДМЧ будут совпадать.

2. Итеративный подход — заключается в эмпирическом оценивании необходимого числа итераций.

3. Использование дайджестов — сравнение Алисой и Бобом дайджестов, вычисленных от набора весов своих ДМЧ. Разумеется, могут быть предложены и другие надёжные криптографические методы для обмена информацией о весах, хотя их применение делает протокол схожим с традиционными аналогами.

В программной реализации у Алисы и Боба использованы по две дополнительные вспомогательные ДМЧ. Так, например, Алиса имеет не только ДМЧ, которая непосредственно участвовала во взаимодействии с Бобом при выработке общего ключа, но и её копия (то есть начальные веса копии и оригинала одинаковы), а также ДМЧ, значения весовых коэффициентов которой инициализированы случайно. Алиса наблюдает за своими вспомогательными ДМЧ и определяет, когда наступит их синхронизация. Далее, при взаимодействии с Бобом Алиса посылает дайджест набора весов Бобу после числа итераций, которое потребовалось для достижения синхронизации вспомогательных ДМЧ Алисы. Аналогично, Боб наблюдает за процессом синхронизации своих ДМЧ и использует полученное при этом число итераций при взаимодействии с Алисой. Участники протокола также могут согласовать перед началом взаимодействия

число итераций, после которых начнётся обмен дайджестами. Описанное применение дополнительных вспомогательных ДМЧ призвано снизить затраты на использование дайджестов.

В качестве источников входных векторов для ДМЧ Алисы и Боба можно использовать одинаковые ГПСП, инициализированные секретным зерном, которое известно лишь Алисе и Бобу. В таком случае может быть исключена передача входных векторов через открытый канал связи, причем возможному злоумышленнику становятся известны только выходы ДМЧ и дайджесты, что увеличивает надежность протокола, так как в описанных атаках на протокол роль Евы заключается в прослушивании взаимодействия Алисы и Боба (предполагается, что Ева не может изменять передаваемую Алисой и Бобом информацию). В ходе такого прослушивания Ева пытается добиться синхронизации одной или нескольких своих ДМЧ с ДМЧ Алисы или Боба, для чего Еве требуется знать и выходы, и входные векторы. В основе стойкости протокола лежит обоснованный факт того, что Алиса и Боб достигают синхронизации быстрее, чем Ева. Кроме того, при использовании ГПСП Алиса и Боб могут аутентифицировать друг друга, так как достижение синхронизации станет признаком знания секретного зерна обеими сторонами.

Достигнув синхронизации ДМЧ, Алиса и Боб могут провести определённые манипуляции над весами и получить из них общий ключ требуемой длины. Например, при $L = 7$ из двух весовых коэффициентов, склеив их, можно легко получить один байт ключа.

Важным моментом является качество получаемых ключей, о котором можно судить, например, по статистическим характеристикам генерируемой последовательности. Проведённые тесты говорят о равномерном распределении ключей.

Надёжность существующих протоколов выработки общего ключа основана, главным образом, на вычислительной сложности задач дискретного логарифмирования и факторизации. Улучшенные версии описанного протокола (не использующие, например, дайджесты весов) могут стать альтернативой применяемым сегодня протоколам.

Литература

1. Ruttor A. Neural Synchronization and Cryptography. Dissertation zur Erlangung des naturwissenschaftlichen Doktorgrades der Bayerischen Julius-Maximilians-Universit ät Würzburg. Würzburg, 2006. 122 p.