УДК 519 П764

НЕЙРОСЕТЕВОЙ МЕТОД РАСПРЕДЕЛЕНИЯ СЕКРЕТНОГО КЛЮЧА В СИММЕТРИЧНОЙ КРИПТОСИСТЕМЕ

Р. Р. Бадретдинов, студент гр. 4167, I курс
Научный руководитель: Э. Г. Тахавова, к.э.н., доцент
Казанский национальный исследовательский технический
университет им. А. Н. Туполева-КАИ, г. Казань

Искусственные нейронные сети находят широкое применение в решении задач прогнозирования, классификации, а также при решении других задач различного вида [1]. Рассмотрим вариант применения нейронной сети в криптографии, а именно, сформируем нейронную сеть, способную генерировать секретный ключ в симметричной криптосистеме.

Для разработки искусственной нейронной сети может быть использован набор инструментов для синтеза и анализа нейронных сетей «Neural Network Toolbox» пакета прикладных программ Matlab. В качестве архитектуры нейронной сети выберем многослойную сеть прямого распространения, поскольку отсутствует необходимость в применении сети обратного распространения. Таким образом, формируемая нейронная сеть будет представлять собой многослойный персептрон. Обучение нейронной сети будем производить методом обратного распространения ошибки. По окончании выбора архитектуры сети происходит подбор характеристик формируемой нейронной сети. При выборе функции активации нейрона предпочтение отдаётся сигмоидной функции, представленной в виде гиперболического тангенса, поскольку применение данной функции является наиболее подходящим в нейронных сетях, где требуется высокая скорость вычислений. При формировании искусственной нейронной сети, предназначенной для решения рассматриваемой задачи, требование к высокой скорости вычислений обусловлено наличием большого числа нейронов во входном, скрытом и выходном слоях. Используемая функция тренировки модифицирует значения весовых коэффициентов связей нейронов в соответствии с методом оптимизации Левенберга-Маркара. Для решения рассматриваемой задачи достаточно взять число скрытых слоёв в нейронной сети равным 1. Количество нейронов в скрытом слое равно 64. Число входов и выходов нейронной сети может быть произвольным. В рассматриваемом случае число входов нейронной сети равно 64, и число выходов нейронной сети равно 256, что соответствует длине секретного ключа алгоритма шифрования AES (Advanced Encryption Standard)-256 [2]. Весовые коэффициенты связей нейронов сети инициализируются случайными значениями на интервале [-1.0, 1.0], поскольку произвольная инициализация значений весовых коэффициентов связей нейронов из указанного интервала не оказывает существенного влияния на скорость и качество обучения. По окон-

чании подбора характеристик формируемой искусственной нейронной сети происходит её обучение. В процессе обучения нейронной сети производится корректировка весовых коэффициентов связей нейронов, продолжающаяся до тех пор, пока значения выходных нейронов не будут полностью соответствовать целевым значениям выходных нейронов.

Схема искусственной нейронной сети, сформированной в соответствии с вышеизложенными условиями в системе Matlab, представлена на рис. 1.

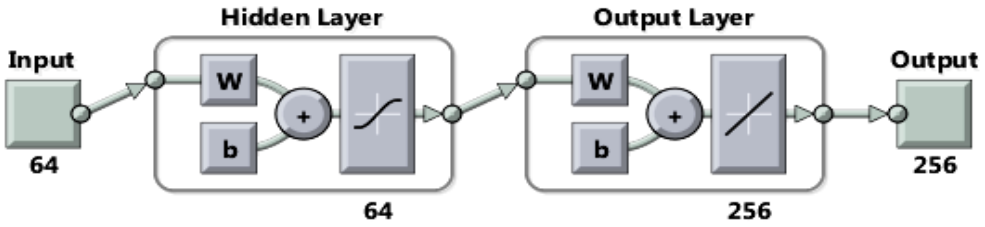

Рис. 1

В качестве входных данных для нейронной сети используется основной ключ, известный каждому участнику группы. Доставка основного ключа каждому из участников осуществляется однократно. В рассматриваемом случае длина основного ключа составляет 64 бита. Целевые значения выходного слоя нейронной сети представляют собой сгенерированный одним из участников секретный ключ. Длина секретного ключа в рассматриваемом примере составляет 256 бит, что позволяет применять данный ключ в алгоритме шифрования AES [2]. Формирование искусственной нейронной сети с последующим её обучением происходит на стороне участника сгенерировавшего секретный ключ. По завершении обучения полученная искусственная нейронная сеть может быть передана по незащищённому каналу связи группе лиц, участвующих в обмене информацией, разглашение которой третьему лицу недопустимо. Получив обученную нейронную сеть, каждый участник группы приобретает возможность генерации секретного ключа, путём подачи на вход нейронной сети основного ключа.

При возникновении необходимости смены секретного ключа, одна из сторон формирует и обучает новую искусственную нейронную сеть, на основе нового сгенерированного секретного ключа. Впоследствии, новая сформированная искусственная нейронная сеть рассылается участникам группы, что в свою очередь приводит к генерации на сторонах участников отличного от предыдущего секретного ключа. В случае перехвата нейронной сети, во время её передачи по каналу связи, третьей стороной, последняя лишена возможности получения секретного ключа, не обладая знанием об основном ключе. Таким образом, наиболее вероятным способом получения секретного ключа является компрометация основного ключа, вследствие чего предъявление высоких требований к условиям хранения основного ключа является необходимым.

Преимуществом рассмотренного подхода является отсутствие передачи секретного ключа по каналу связи, что снижает шансы получения третьей стороной секретного ключа. Таким образом, нейронная сеть может выступать в качестве оптимального решения задачи распределения секретного ключа в симметричной криптосистеме.

Список литературы:

1. Червяков Н.И., Галушкин А.И., Евдокимов А.А., Лавриненко А.В., Лавриненко И.В. Применение искусственных нейронных сетей и системы остаточных классов в криптографии. Изд-во: Физматлит, 2012. 280 С.

2. Баричев С.Г., Гончаров В.В., Серов Р.Е. 2.4.2. Стандарт AES. Алгоритм Rijdael // Основы современной криптографии. – М.: Горячая линия - Телеком, 2002. С. 30-35.