УДК 003.26.09

Формирование общего секрета с помощью синхронизируемых искусственных нейронных сетей и его уязвимости

Ксеневич А.Ю., Голиков В.Ф.
Белорусский национальный технический университет

Безопасная пересылка данных является одним из самых важных вопросов в современном информационном мире. Ключевую роль в этой сфере играет криптография, позволяющая шифровать важную информацию, защищая тем самим ее от несанкционированного доступа.

Безопасность криптографических систем зависит от трудности решения проблем теории чисел (например, проблема факторизации, проблема дискретного логарифмирования). Однако рост вычислительной мощности современных компьютеров требует применения всё более длинных целых чисел, составляющих параметры криптографических систем. С другой стороны, использование всё более длинных целых чисел вызывает рост вычислительной сложности криптографических алгоритмов. Поэтому так интересны любые новаторские криптографические системы, не использующие теорию чисел.

Одной из таких новых идей является применение нейронных сетей для формирования общего криптографического ключа при обмене информацией по незащищенным каналам связи. Эта задача решается в настоящее время в основном с использованием алгоритма Диффи-Хеллмана. Протокол формирования общего ключа, использующий нейронные сети, базируется на их синхронном обучении. Обучение двух нейронных сетей с использованием их общих выходных величин ведёт к возникновению идентичных векторов весов. Сети обмениваются между собой выходными и входными величинами, при этом секретными остаются внутренние состояния векторов весов. Следовательно, вектор весов может составлять секретный ключ, использующийся для дальнейшей передачи информации по незащищенным каналам. Третья сторона, следящая за обменом информации между обеими сетями, пытается восстановить внутренние значения векторов весов сетей. В докладе анализируется безопасность метода по отношению к различным атакам третьей стороны. Методом имитационного моделирования определены вероятность достижения полной синхронизации между санкционированными пользователями за отведенное число тактов синхронизации и вероятность достижения полной синхронизации третьей стороны с одним из санкционированных пользователей. Показано, что последняя вероятность может достигать величины, при которой использовать данный метод не безопасно.