УДК 681.322

А.В. Крыжановский

Применение искусственных нейронных сетей в системах обнаружения атак

Рассматриваются особенности применения искусственной нейронной сети для обнаружения атак. По сравнению с традиционными, рассматриваемая система имеет ряд существенных преимуществ.

Современные средства обнаружения атак на основе экспертных систем используют правила, идентифицирующие известные атаки. Эти правила предоставляются администратором, автоматически создаются системой или используются оба варианта [1]. Правила используются системой для вынесения заключений о состоянии защиты на основе данных, полученных от системы обнаружения атак. Экспертные системы требуют частого обновления, в противном случае ослабляются способности системы защиты, а пользователи вводятся в заблуждение относительно защищенности сети.

Подобные системы не способны обнаруживать сценарии атак в течение продолжительных периодов времени. Атаки, в которых множество взломщиков работают согласованно, плохо обнаруживаются экспертными системами. Эти системы не обладают достаточной гибкостью при реализации структуры типа «правило—проверка». Незначительные вариации деталей атаки могут привести к пропуску атаки.

В последние годы разработаны различные подходы к проблеме обнаружения атак, опирающиеся на системы, отличные от экспертных. В частности, к числу таких подходов относится использование искусственных нейронных сетей [2, 3].

В отличие от экспертных систем, которые могут дать пользователю определенный ответ о соответствии анализируемых и хранящихся в базе данных характеристик, нейронная сеть проводит анализ информации и предоставляет возможность оценки согласования данных с характеристиками, которые она обучена распознавать. Достоверность оценки полностью зависит от эффективности этапа обучения.

Первоначально нейронная сеть обучается путем правильной идентификации предварительно выбранных объектов предметной области. Реакция нейронной сети анализируется, и система настраивается таким образом, чтобы достичь удовлетворительных результатов. В дополнение к первоначальному периоду обучения нейронная сеть «набирается опыта» с течением времени по мере того, как она проводит анализ данных, связанных с предметной областью.

В связи с ограниченными возможностями экспертных систем представляется перспективной разработка адаптивных систем анализа сетевых данных и управления средствами защиты. Системы обнаружения атак на базе нейронных сетей в перспективе могли бы решить многие из проблем, не решаемых экспертными системами.

Основные преимущества систем обнаружения атак на основе нейронных сетей:

– гибкость и адаптивность алгоритмов, способность анализировать данные из сети, даже если эти данные являются неполными и/или искаженными, высокая скорость обработки данных, обеспечивающая работу системы в режиме реального времени;

– способность «изучения» характеристик атак и выделение элементов, отличающихся от наблюдаемых ранее.

Существующие в настоящее время недостатки систем обнаружения атак на основе нейронных сетей являются продолжением их достоинств и поэтому их следует рассматривать как резерв для дальнейшего совершенствования. К этим особенностям можно отнести:

– точное описание поведения системы в целом и отдельных ее элементов невозможно в силу стохастического характера функционирования системы, можно лишь с определенной степенью вероятности рассчитывать на некоторый положительный результат;

– существуют проблемы, связанные с обучением системы, поскольку на этом этапе необходимо сформировать большое количество атак, особенно на первоначальном этапе.

Существуют два основных варианта реализации систем обнаружения атак. Первый основан на объединении нейронной сети с уже существующей экспертной системой. При этом можно уменьшить число «ложных срабатываний» экспертной системы и, следовательно, увеличить ее чувствительность. Этот вариант предпочтителен и в экономическом аспекте, так как не требует демонтажа установленной системы.

Второй вариант предполагает установку автономной системы обнаружения атак на основе нейронной сети на отдельном компьютере. Все сообщения о подозрительных событиях направляются администратору безопасности и/или в систему автоматического реагирования. По сравнению с первым подходом существует всего один уровень анализа, и поэтому скорость работы системы выше.

В статье рассматриваются результаты эксперимента, поставленного с целью изучения возможностей выделения нейронной сетью атак из типичного сетевого трафика.

Построение и тестирование нейронной сети осуществлялось с помощью программы Statistica Neural Networks v4.0e (www.statsoft.ru/home/).

В ряде приложений нейронные сети предназначены для идентификации сетевых событий, а в данном случае рассматриваемая модель предназначена для тестирования способности нейронной сети

идентифицировать атаки. В основу модели положена MLP-архитектура (Multi Layer Perceptron – многослойный персептрон), которая состоит из четырех полностью связанных слоев с девятью входными узлами и одним выходным (рис. 1).

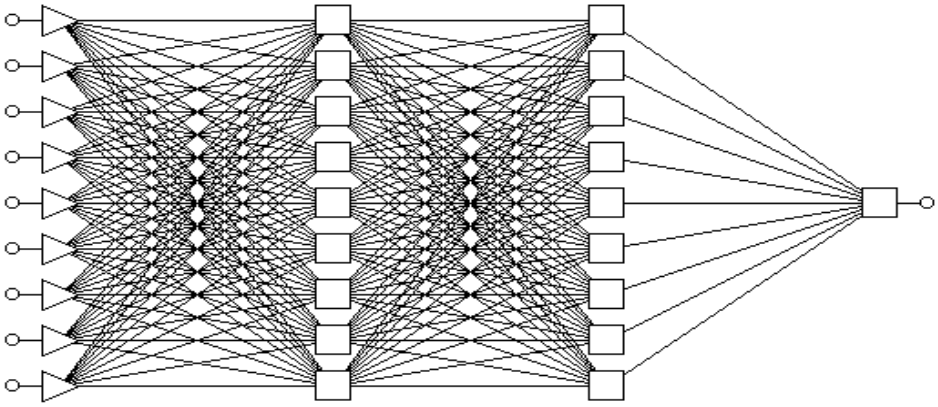

Рис.1. Модель нейронной сети

В настоящее время существуют различные архитектуры нейронных сетей. Основными преимуществами рассматриваемой архитектуры по сравнению с другими существующими являются гибкость и достаточно широкие функциональные возможности. К каждому из скрытых узлов и выходному узлу для различных по значимости соединений применялось преобразование на основе сигмоидной функции. В рассматриваемой модели выходное значение 0,0 указывает на отсутствие, а 1,0 – на наличие атаки.

Данные для обучения и тестирования модели собирались с помощью программы сниффера Ethereal-0.9 (www.ethereal.com), которая имеет достаточно простой графический интерфейс и позволяет наглядно рассматривать структуру и данные всех сетевых пакетов. Тестируемый хост был специально атакован с помощью системы анализа уязвимостей Nessus v1.1 (www.nessus.org). Данные хранились в базе данных на основе программы MySQL v. 3.23 (www.mysql.org). В эксперименте смоделирована одна из самых распространённых атак – атака на CGI-скрипты.

Приблизительно 312 отдельных событий, из которых около 100 – смоделированные атаки, собраны программой Ethereal-0.9 и помещены в специальную базу данных. Обучение нейронной сети проводилось с использованием алгоритма обучения с обратным распространением для 1000 итераций (эпох) выбранных для обучения данных. Аналогично архитектуре упреждающей нейронной сети использование данного алгоритма на этапе обучения основано на доказанных записях этого подхода при разработке нейронных сетей для широкого ряда приложений. Из 1000 записей, которые были предварительно обработаны перед использованием в модели, около 10 были произвольно выбраны для тестирования (так называемое контрольное множество), а оставшиеся использованы для обучения системы. В итоге обучения получены следующие результаты: среднеквадратическая ошибка данных обучения – 0,006826; тестирования – 0,007936. Полученные значения близки к ожидаемым среднеквадратическим значениям ошибки. После выполнения обучения и тестирования MLP нейронной сети состояния всех узлов сети были зафиксированы.

Результаты моделирования свидетельствуют о перспективности рассматриваемого подхода, но для функционирования сети в качестве эффективной системы обнаружения атак необходимо решить ряд важных задач. В частности, реальная система должна извлекать исходные данные из сетевого потока.

Литература

1. Sebring M., Shellhouse E. Expert Systems in Intrusion Detection: A Case Study. In Proceedings of the 11th National Computer Security Conference.

2. Круглов В.В., Борисов В.В. Искусственные нейронные сети. Теория и практика. – 2-е изд., стереотип. – М.: Горячая линия – Телеком, 2002. – 382 с.

3. James Cannady. Artificial neural networks for misuse detection // School of Computer and Information Science, Nova Southern University FortLauderdale, FL 33314.

Крыжановский Анатолий Владиславович
ГОУ ВПО Поволжская государственная академия телекоммуникаций и информатики
К.т.н., доцент кафедры ПДС
Эл. почта: kryzan@psati.ru

A.V. Krjzijzanovsky

Application of artificial neural networks in systems of attacks detection

In the report application features of an artificial neural network for attacks detection f are considered. In comparison with traditional, the considered system has a number of essential advantages which are discussed in the report.