УДК 004

Применение механизмов нечеткой логики при анализе и выявлении аномального поведения сетевого трафика

Симанович А.А.

(Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, г. Санкт-Петербург)

Научный руководитель —- к.т.н., доцент Исаев А.С.

(Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, г. Санкт-Петербург)

В настоящее время используются различные методы для обеспечения безопасности информации и сохранения необходимой работоспособности компьютерных систем. Для обнаружения аномального трафика используются технологии обнаружения сетевых атак. Их принято делить на категории: обнаружение аномалий и злоупотреблений. Преимущество метода обнаружения аномалий заключается в том, что используется шаблон нормального поведения трафика. Если поведение трафика при сравнении с паттерном сильно отличается, тогда система сообщает о выявлении атаки. Целью данной работы является рассмотрение механизмов нечеткой логики, преимущества и недостатки ее использования при анализе и выявлении аномального поведения сетевого трафика.

Для получения вывода в системе с использованием логики, необходимо определить входы и выходы системы, а также описать правила, которые связывают входные данные и выходное значение. По итогу классической логики возможно два варианта значения x: Истина и Ложь, в случае с трафиком набор возможных выводов выглядел бы следующим образом: T(трафик)={Нормальный\/Аномальный}.

Преимуществом нечеткой логики над классической является возможность описать случайные события, которые могут протекать по-разному при одних и тех же условиях. С помощью использования нечеткой логики можно относить элемент к нескольким категориям одновременно, но в разной степени принадлежности. В случае поведения трафика, можно относить шаблон поведения трафика одновременно к разным типам атаки с разной степенью схожести.

В случае применение нечеткой логики к сетевому трафику, составляя терм-множество по критерию типы атак для выявления аномалий сетевого трафика, терм-множество состоит из термов: Denial of Service Attack (DoS), User to Root Attack (U2R), Remote to Local Attack (R2L), Probe. Если принадлежность поведения трафика не будет выше определенного уровня, заданное поведение трафика будет расцениваться как нормальное.

В действующих системах обнаружения вторжений обнаружения вторжений метод выявление аномалий на основе нечеткой логики является одним из нескольких использующихся методов. При рассмотрении аномального поведения трафика участвуют множество характеристик и параметров. Использование нечеткости в представлении характеристик помогает сгладить разделение нормального и аномального поведения сетевого трафика, что уменьшает количество ошибок.

Нечеткая логика также используется в генетических алгоритмах. В большинстве случаев для выявления аномального поведения трафика, достаточно рассмотреть основные параметры трафика. В случае трафика генами являются параметры, а хромосома состоит из последовательности параметров. Начальная популяция генерируются случайным образом, где каждая хромосома представляет собой возможное решение проблемы аномалии поведения трафика (набор параметров). Через некоторое количество поколений значение хромосомы должно сходиться к значению, которое является лучшим решением заданной

проблемы. Цель состоит в том, чтобы увеличить сходство правил, извлеченных из данных без вторжений.

Использование нейронный сетей удобно для задач распознавания образов, но обучение их происходит достаточно медленно. Системы с нечеткой логикой наоборот хороши для получения выводов, но не могут автоматически приобретать знания. В гибридных сетях выводы делаются на основе нечеткой логики, а функции принадлежности формируются с использованием алгоритмов обучения нейронных сетей. Также для обучения нейронной сети могут быть применены механизмы нечеткой логики, использованные в генетическом алгоритме. Примером такой сети является сеть нечеткого вывода ANFIS, которая доступна в пакете Fuzzy Logic Toolbox, входящий в систему MATLAB.

В данной работе были рассмотрены механизмы нечеткой логики, преимущества и недостатки ее использования в области выявления аномального поведения сетевого трафика. Также нечеткая логика используется в генетических алгоритмах и нейронный сетях. Создание гибридных сетей является наиболее перспективным направлением из представленных, так как в нем присутствуют преимущества как нечеткой логики, так и нейронных сетей, и они способны обнаружить ранее неизвестные атаки и самостоятельно обучаться.