УДК 681.3.06:519.248.681

И. Е. АНТИПОВ, д-р техн. наук, Т. А. ЯЩЕНКО, НУХ ТАХА НАСИФ

ПРИМЕНЕНИЕ НЕЧЕТКОЙ ЛОГИКИ ДЛЯ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ СЕТЕЙ НА ОСНОВЕ ТЕХНОЛОГИИ WI-FI

Введение

В настоящее время беспроводные сети очень актуальны и играют важную роль в жизни людей. Многие фирмы с успехом применяют беспроводные локальные сети для управления процессом производства, больницы развертывают беспроводные сети с целью повышения эффективности эксплуатации и удобства. Базовым для беспроводных локальных сетей является стандарт IEEE 802.11, различные версии которого регламентируют передачу данных в диапазонах 2,4 и 5 *ГГц*, что рассмотрено более подробно в [1, 2]. Дальность связи, как правило, не превышает 200 *м*.

Поскольку устройства стандарта 802.11 связываются друг с другом через радиоэфир, то любая другая станция, использующая этот диапазон, тоже способна принять эти данные. Для обеспечения хотя бы минимального уровня безопасности беспроводной сети используют механизмы шифрования, основанные на алгоритмах WPA и WPA2 (Wi-Fi Protected Access) [1] и системы обнаружения вторжений IDS [3].

В статье рассмотрен алгоритм анализа состояния беспроводной Wi-Fi сети с использованием элементов нечеткой логики. Этот алгоритм позволяет принимать решение о наличии потенциальной угрозы безопасности с учетом различных или быстро меняющихся условий, которые системы обнаружения вторжений (Intrusion Detection System (IDS)) не учитывают.

Анализ существующих систем обнаружения вторжений и их недостатков

По способам определения вредоносного трафика IDS подразделяются на: signature-based (сигнатурного метода), policy-based (метода, основанного на политике) и anomaly-based (метода аномалий), который далее и будет рассматриваться более подробно.

Системы обнаружения вторжений, построенные по методу аномалий, позволяют обнаруживать как атаки известных типов, так и атаки, сигнатуры которых еще не разработаны. Принцип функционирования таких систем основан на определении ненормального (необычного) поведения на хосте или в сети. Речь идет о том, что на основании анализа работы сети принимается решение о блокировке работы всей сети, или отдельных пользователей. На основе нормального описания состояния сети устанавливаются четкие границы аномальности, при переходе которых определяется вторжение.

Однако данные системы имеют ряд недостатков, существенно ухудшающих качество работы беспроводной сети. Во-первых, установление четкой границы между нормальным и ненормальным поведением системы приводит к большому количеству ложных сигналов. Реагирование системы безопасности на ложный сигнал об аномальности путем ограничения доступа пользователя к ресурсам сети может ухудшить работу организации, эксплуатирующей сеть. Во-вторых, вышеуказанная система не является адаптивной к изменению условий функционирования сети (так, например, ночью условия функционирования сети существенно отличаются от дневного времени и т. д.). Поэтому актуальной задачей является усовершенствование систем обнаружения вторжений в направлении принятия решения относительно аномальности сети в изменяющихся условиях ее функционирования.

Нечеткая логика для анализа состояния сети

Нечеткая логика – раздел математики, являющийся обобщением классической логики и теории множеств. В основе нечеткой логики лежит теория нечетких множеств, где функция принадлежности элемента множеству не бинарная (да/нет), а может принимать любое значение в диапазоне 0...1. Четкая логика манипулирует результатами, которые могут быть или

истиной, или ложью. Нечеткая логика применяется в тех случаях, когда для описания состояния системы в дополнение к «да» и «нет» могут применяться описания «скорее да, чем нет», «может быть», «скорее нет, чем да» и т. д.

Идея состоит в том, чтобы на первом этапе количественные оценки параметров (скорость, количество абонентов и др.) преобразовать в величины нечеткой логики путем их сравнения с типовыми параметрами, а затем принимать решение о вмешательстве в работу сети путем комплексной оценки совокупности величин нечеткой логики.

Сложность первого этапа состоит в том, что для различного времени суток, разных дней недели и разных сезонов типовые параметры могут существенно отличаться. Поэтому для корректного преобразования необходимо иметь базу данных, вариант структуры которой изображена на рис. 1

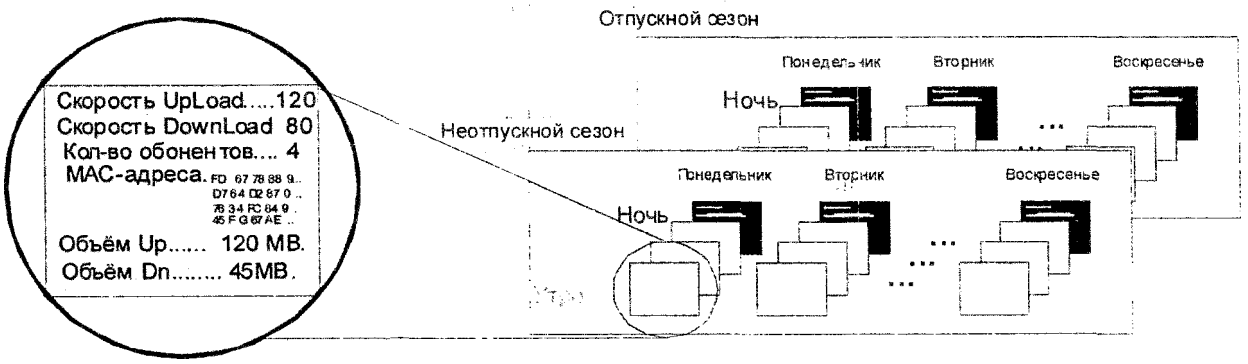

Рис. 1

Преобразование параметров в величины нечеткой логики происходит с помощью оценочных шкал и лингвистических переменных [4]. В зависимости от времени суток, типовых параметров, кривая, по которой оценивается степень аномальности сети, изменяет свой вид. На рис. 2 показаны оценочные кривые в разные периоды времени, характеризующие скорость передачи данных. Для примера покажем, что если для второй кривой типовая скорость передачи должна быть 100 *Мбит/с*, то если в сети скорость передачи 125 *Мбит/с*, то будет принято решение – «повышенная аномальность сети». Аналогичные кривые составляются для всех типовых параметров.

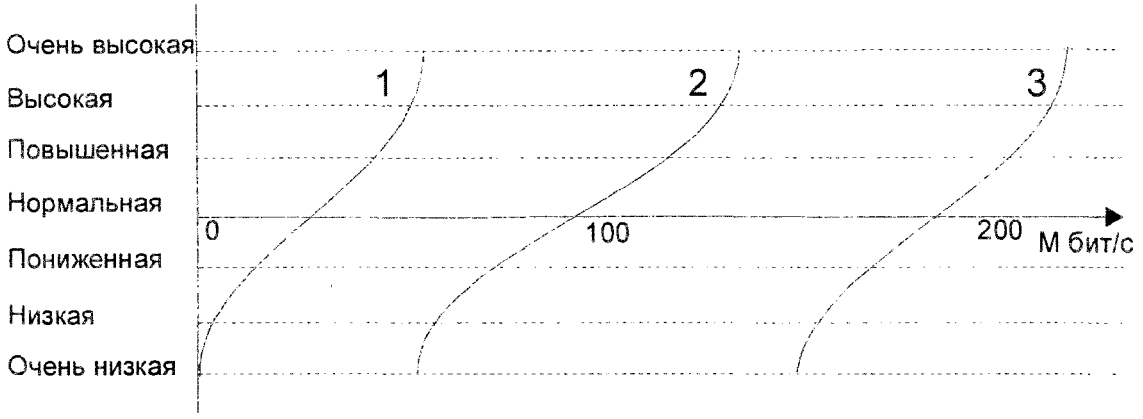

Рис. 2

После преобразования признаков в нечеткие лингвистические переменные проводится комплексная оценка всех параметров с учетом весовых коэффициентов, погодных условий, уровня помех и базы данных по предыдущим вторжениям, для принятия решения о состоянии аномальности всей сети. Сначала оценивается общая картинна для всех типовых параметров, полученных ранее. После этого полученная картина сравнивается с базой данных и производит поиск похожего результата.

Структура модели

В общем виде модель принятия решения (об аномальности сети), с использованием нечеткой логики, можно представить в виде алгоритма, рис. 3.

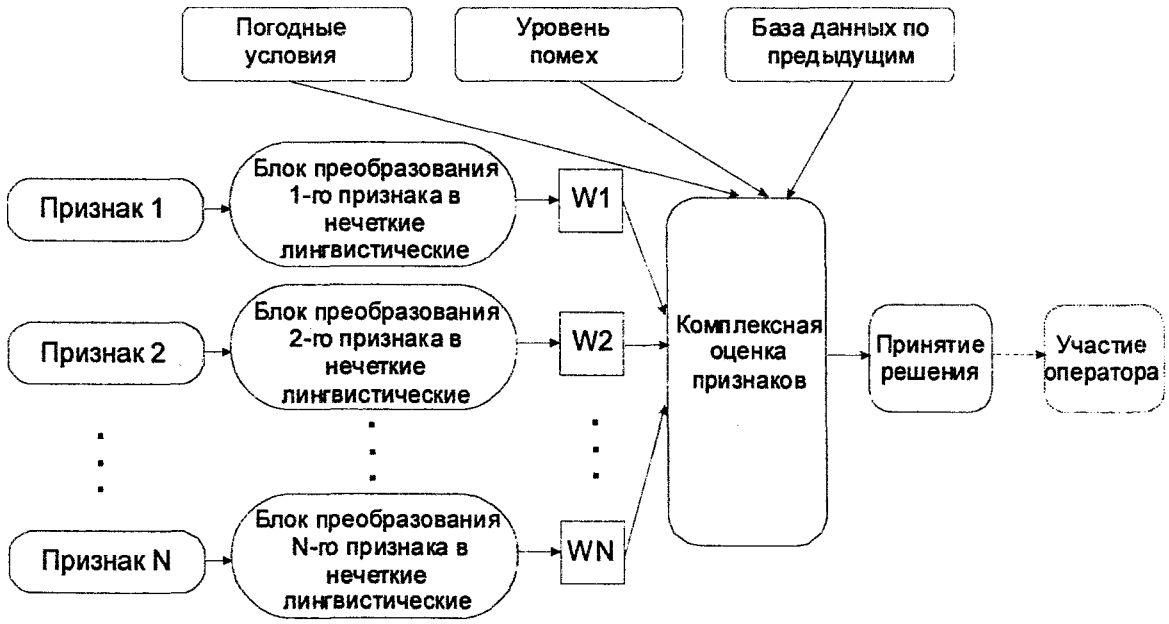

Рис. 3

Программы анализа сети позволяют получать многообразную информацию о ее состоянии. Можно выделить, например, четыре параметра.

1. Объем переданной и принятой информации (в виде пакетов в единицу времени или бит в единицу времени). Масштаб отображения можно менять от долей секунд до 10 минут. Пример графического представления показан на рис. 4.

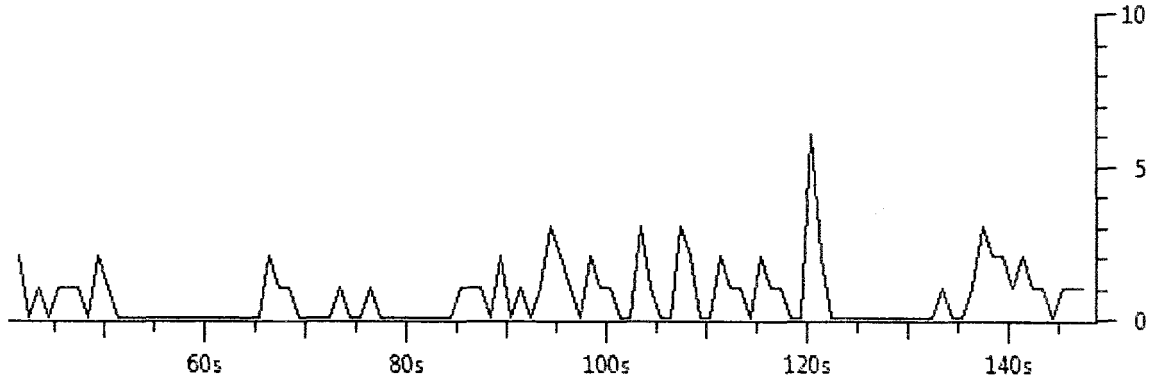

Рис. 4

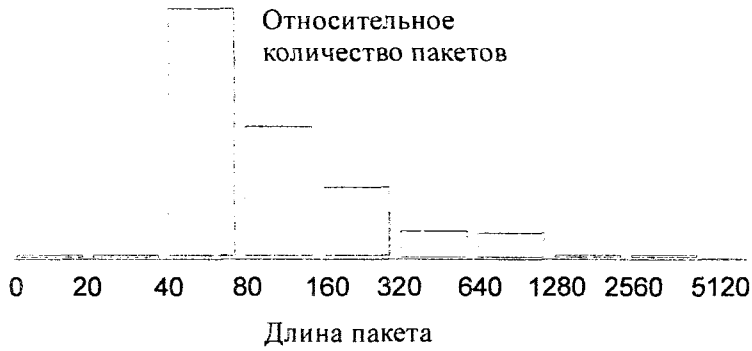

Рис. 5

2. Количество пакетов того или иного размера, которое может быть получено как в абсолютных цифрах, так и в относительных значениях. Данная информация может свидетельствовать о характере передаваемого трафика (http-пакеты, VoIP, служебные, UDP и др.) рис. 5. Степень опасности определяется с помощью сравнения

шаблона с реальной картиной передаваемых пакетов, их разность определяет опасность вторжения и может определяться по формуле

$$\varepsilon = \sqrt{\sum_{i=1}^{10} (\Delta N_i)^2}, \qquad (1)$$

где ε – величина пропорциональная ошибке; ΔN_i – разность шаблона и измеряемого значения.

3. MAC-адреса пользователей, находящиеся в радиусе действия сети, рис. 6.

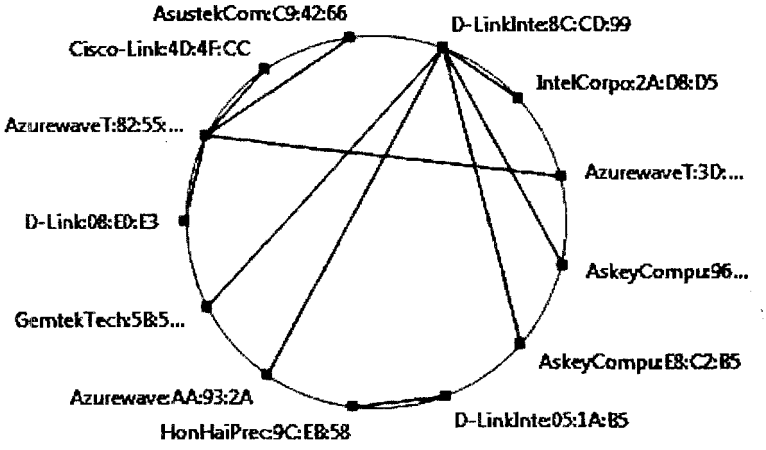

Рис. 6

4. Уровень сигнала для каждого пользователя, подключенного к сети (в процентах от максимального или в децибелах).Задача повышения безопасности Wi-Fi сетей является актуальной и ее актуальность будет возрастать по мере увеличения количества Wi-Fi оборудования у пользователей и существующих точек доступа. Одно только шифрование не решает задачу безопасности, поскольку, во-первых, методы дешифрования развиваются не менее успешно, чем методы шифрования, а во-вторых, безопасность сетей не сводится только к защите передаваемых данных. Работоспособность сети можно нарушить и не зная алгоритмов шифрования и ключей.

Выводы

Существующие методы анализа работы сетей не полностью удовлетворяют существующим требования. Четкие границы определения аномальности приводят к большому количеству ложных сигналов, что значительно ухудшает работу сети. Также существующие системы защиты не учитывают условия функционирования сети (день недели, время суток и т. д.)

Предложенный в работе алгоритм анализа состояния Wi-Fi сети на основе нечеткой логики позволяет более адекватно принимать решения об аномальности сети. Применение нечеткой логики дает возможность корректировать решения в зависимости от изменения условий функционирования сети. Система может работать как в автоматическом режиме (сама принимает решение), так и с помощью оператора (эксперт, проанализировав полученные результаты, в зависимости от ситуации сам принимает решение).

Список литературы: 1. *Пролетарский А. В., Баскаков И. В., Чирков Д. Н.* Беспроводные сети Wi-Fi. БИНОМ // Лаборатория знаний. – 2007. – 178 с. 2. *Щербаков В.Б., Ермаков С.А.* Безопасность беспроводных сетей: стандарт IEEE 802.11. – М., 2010. – 256 с. 3. *Системы* обнаружения вторжений. [электронный ресурс] http://www.icmm.ru/~masich/win/lexion/ids/ids.html. 4. *Мусийченко В.А.* Моделирование и алгоритмизация интеллектуальной системы, стимулирующей продуктивное мышление (на примере медицинской диагностики) : Дис... канд. техн. наук. – Харьков, 1999.- 122 с

Харьковский национальный университет радиоэлектроники

Поступила в редколлегию 17.02.2011