

APPLICATION OF FUZZY LOGIC TO IMPROVE SECURITY NETWORK BASED ON Wi-Fi TECHNOLOGIES

Antipov I.E., Vasilenko T.A.
Kharkov National University of Radio Electronics
14, Lenin Ave., Kharkov, 61166, Ukraine
Ph.: (050) 6691661, e-mail skorpy_h7@mail.ru

Abstract — The algorithm of work is based on intrusion detection systems in the Wi-Fi network using fuzzy logic. This algorithm permits making a decision about potential security risk, taking into account the different and rapidly changing conditions that intrusion detection systems can not take into account. Such parameters can be analyzed, the amount of transmitted and received data transfer rate, the dynamics of the packet, MAC-addresses of the users and the level of the signal. The proposed algorithm in the analysis of the Wi-Fi network based on fuzzy logic allows making decisions about anomalous network more adequately. The use of fuzzy logic makes possible adjusting the solutions depending on changes in network conditions.

ПРИМЕНЕНИЕ НЕЧЕТКОЙ ЛОГИКИ ДЛЯ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ СЕТЕЙ НА ОСНОВЕ ТЕХНОЛОГИИ Wi-Fi

Антипов И. Е., Василенко Т. А.
Харьковский национальный университет радиозлектроники
пр. Ленина, 14, Харьков, 61166, Украина
тел.: (050) 6691661, e-mail: skorpy_h7@mail.ru

Аннотация — Описан алгоритм работы на основе системы обнаружения вторжений в Wi-Fi сети с использованием нечеткой логики. Этот алгоритм позволяет принимать решение о наличии потенциальной угрозы безопасности с учетом различных или быстро меняющихся условий, которые системы обнаружения вторжений не учитывают. Могут анализироваться такие параметры, объем переданной и принятой информации, скорость передачи, дина пакета, MAC-адреса пользователей и уровень сигнала. 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.

I. 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 радиозфир, 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 работе 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.

II. Основная часть

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 — 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]. Чет-

кая 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.

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. 1 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.

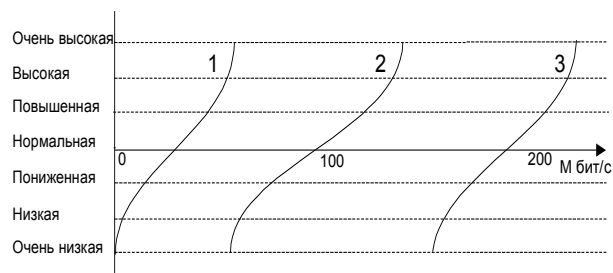


Рис. 1. Оценочная кривая.
Fig. 1. Evaluative curve

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 картина для всех типовых параметров, полученных ранее. После этого полученная картина сравнивается с базой данных и производится поиск похожего результата.

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

Программы анализа сети позволяют получать многообразную информацию о ее состоянии. Можно выделить, например, четыре параметра. Объем переданной и принятой информации (в виде пакетов в единицу времени или бит в единицу времени). Количество

пакетов того или иного размера, которое может быть получено как в абсолютных цифрах, так и в относительных значениях. MAC-адреса пользователей, находящиеся в радиусе действия сети Уровень сигнала для каждого пользователя, подключенного к сети.

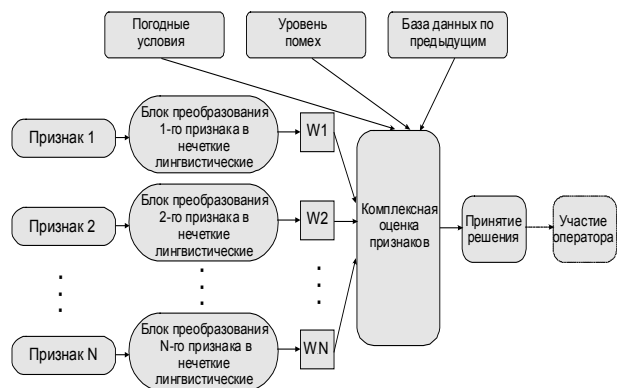


Рис. 2. Алгоритм принятия решений.
Fig. 2. Decision making algorithm

III. Заключение

1. 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.

2. 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. Так же 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).

IV. References

- [1] Proletarskii A.V., Baskakov I.V., Chirkov D.N. *Besprovodnye seti Wi-Fi* [Wi-fi wireless network]. BINOM. Laboratoriya znaniy, 2007. 178 p.
- [2] Shcherbakov V.B., Ermakov S.A. *Bezopasnost' besprovodnykh setei: standart IEEE 802.11* [Security of wireless networks: standard IEEE 802.11]. Moskva, 2010. 256 p.
- [3] *Sistemy obnaruzheniya vtorzhenii* [Intrusion definition systems]. Available at: <http://www.icmm.ru/~masich/win/lexion/ids/ids.html>. (accessed 30 July 2013).
- [4] Musiichenko V.A. *Modelirovanie i algoritimizatsiya intellektual'noi sistemy, stimuliruyushchei produktivnoe myshlenie (na primere meditsinskoj diagnostiki): diss. kand. tekhn. nauk.* [Modeling and algorithmization of intelligent system, which stimulates of productive thinking]. Khar'kov, 1999. 122 p.