УДК 681.3.06:519.248.681

И. Е. АНТИПОВ, д-р техн. наук, Т. А. ВАСИЛЕНКО, В.С. ВОВЧЕНКО

ПРИМЕНЕНИЕ ТЕОРИИ ИГР ДЛЯ ЗАЩИТЫ БЕСПРОВОДНЫХ WI-FI СЕТЕЙ

Введение

Беспроводные технологии прочно вошли в нашу жизнь. С их помощью организуются точки доступа в Интернет и строятся полноценные локальные сети, в том числе в местах, где проводная сеть в принципе невозможна. Преимущества использования беспроводной сети Wi-Fi неоспоримы. С ее помощью можно избавиться от многочисленных кабелей, также плюсом является свобода передвижения и перемещения техники в пределах радиуса действия сети, а также возможность подключения к сети двух и более компьютеров. Эти и другие достоинства привлекают многих пользователей.

Однако не следует забывать о безопасности. Устройства стандарта 802.11 связываются друг с другом через радиоэфир, что делает их уязвимыми к попыткам несанкционированного доступа. Плохо защищенная беспроводная сеть может обернуться потерей средств за интернет трафик (в лучшем случае) и потерей личной информации, хранящейся на компьютере, что для компаний, хранящих конфиденциальную информацию, недопустимо.

Причины, по которым взломщики атакуют беспроводные сети, достаточно ясны: анонимный доступ, низкая вероятность быть пойманным, бесплатный канал и легкость проникновения. Поэтому ведущие страны мира уделяют большое внимание усовершенствованию систем защиты беспроводных сетей. Злоумышленник, используя средства нападения, способен в короткое время вывести из строя беспроводную сеть, построенную на традиционных принципах и остаться не пойманным. Даже если взломщик будет пойман, то доказать его вину практически невозможно, если до или после атаки он изменил MAC-адрес на своей плате для беспроводного доступа и удалил со своего компьютера все данные, связанные с атакой. Поэтому достаточно сложно обеспечить стойкую защиту без приложения специальных технических средств противодействия.

Анализ существующих систем защиты и их недостатков

Для обеспечения хотя бы минимального уровня безопасности беспроводной сети используют механизмы шифрования, сетевые экраны и системы обнаружения вторжений. Последние, 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, и на основании такого анализа принимается решение о блокировке работы всей сети, или отдельных пользователей. На основе нормального описания состояния сети устанавливаются границы аномальности, переход которых идентфицируется как вторжение.

Тем не менее, такие средства не останавливают злоумышленников, так как эти средства имеют ряд недостатков, существенно ухудшающих качество работы беспроводной сети. С одной стороны, они недостаточно интеллектуальны, вследствие чего не способны обнаруживать новые виды атак, а с другой, вызывая ложные тревоги в штатных ситуациях, могут препятствовать нормальной работе сети.

Цель работы – анализ возможности повышение уровня безопасности информационной системы с беспроводной Wi-Fi сетью на базе теории игр.

Теория игр в защите беспроводных сетей

Разработанная ранее модель, основанная на нечеткой логике, адекватно принимает решения об аномальности сети и в зависимости от изменения условий ее функционирования дает возможность его корректировать [1]. Но при каждом нападении она отключает отдельного абонента или сеть. Однако в современных условиях злоумышленник способен быстро

разобраться в принципах защиты беспроводной сети и в короткое время осуществить вмешательство в ее работу с использованием новейших технологий. Учитывая это, необходимо постоянно совершенствовать методы защиты беспроводных сетей, в том числе применять нестандартные средства, иначе злоумышленник рано или поздно достигнет своей цели. Для минимизации потерь информации, хранимой или передаваемой в беспроводной сети, необходимо дополнение модели аппаратом, который будет управлять средствами защиты информационной системы.

Задача защиты беспроводных сетей является многофакторной, в ней участвуют несколько сторон, каждый со своими целями, интересами и техническими возможностями. Они действуют независимо друг от друга «на общем поле».

Подобные задачи встречаются в других сферах, например, таких как экономика, торговля ценными бумагами, спортивные соревнования и др. Для их решения и выработки различных стратегий поведения в указанных сферах часто применяется теория игр, которая представляет собой раздел математики, изучающий формальные модели принятия оптимальных решений в условиях конфликта [4]. При этом под конфликтом понимается явление, в котором участвуют различные стороны, наделенные различными интересами и возможностями выбирать доступные для них действия в соответствии с этими интересами.

Первоначально теория игр начала развиваться в рамках экономической науки, позволив понять и объяснить поведение экономических агентов в различных ситуациях. Позднее область применения теории игр была расширена на другие социальные науки; а в настоящее время значение теории игр существенно возросло во многих областях наук.

Теория игр предполагает наличие сторон с противоположными интересами. Взаимосвязь между ними определяется так называемой платежной матрицей. Матричная игра, в которой игрок взаимодействует с окружающей средой и решает задачу определения наиболее выгодного варианта поведения, называется статистической игрой. Игрок в таком случае – лицо, принимающее решение.

Также с помощью теории игр решаются подобные задачи для защиты когнитивного радио [2]. В [3] рассматривается теория игр для анализа состояния сети на физическом уровне: «Стратегиями защиты являются параметры и режимы работы радиосвязи (рабочая частота, вид сигнально-кодовой конструкции, мощность сигнала), а стратегиями нападения – разные виды преднамеренных помех» [3]. Но так как попытка вмешательства в работу сети – это не только постанова помех, но и подбор паролей, смена MAC-адресов, доступ к внешней сети от имени абонентов этой сети и т. д. Поэтому защита должна быть реализована не только на физическом уровне.

Можно ожидать, что дополнение рассмотренной в [1] модели защиты, основанной на нечеткой логике, игровым подходом, который учитывает многообразие и эффективность стратегий в условиях неопределенности, будет целесообразным (рис. 1).

Дело в том, что в существующих системах защиты беспроводных сетей существует только два исхода – либо злоумышленник реализует свои замыслы, либо нет. Но во втором случае попытка несанкционированного взлома, скорее всего, повторится, но уже другим способом.

Если использовать теорию игр и, вместо того чтобы закрыть доступ злоумышленнику к сети, вступить с ним в игру, можно предположить, что в результате такого игрового подхода можно обмануть взломщика и убедить его в реализации задуманного (например, с помощью подмены трафика). Задача, которая ставится в этом случае, состоит не в поиске оптимального решения, а в поиске выигрышной стратегии.

В классической постановке матрица игры может быть задана табличным способом, что показано на рис. 2

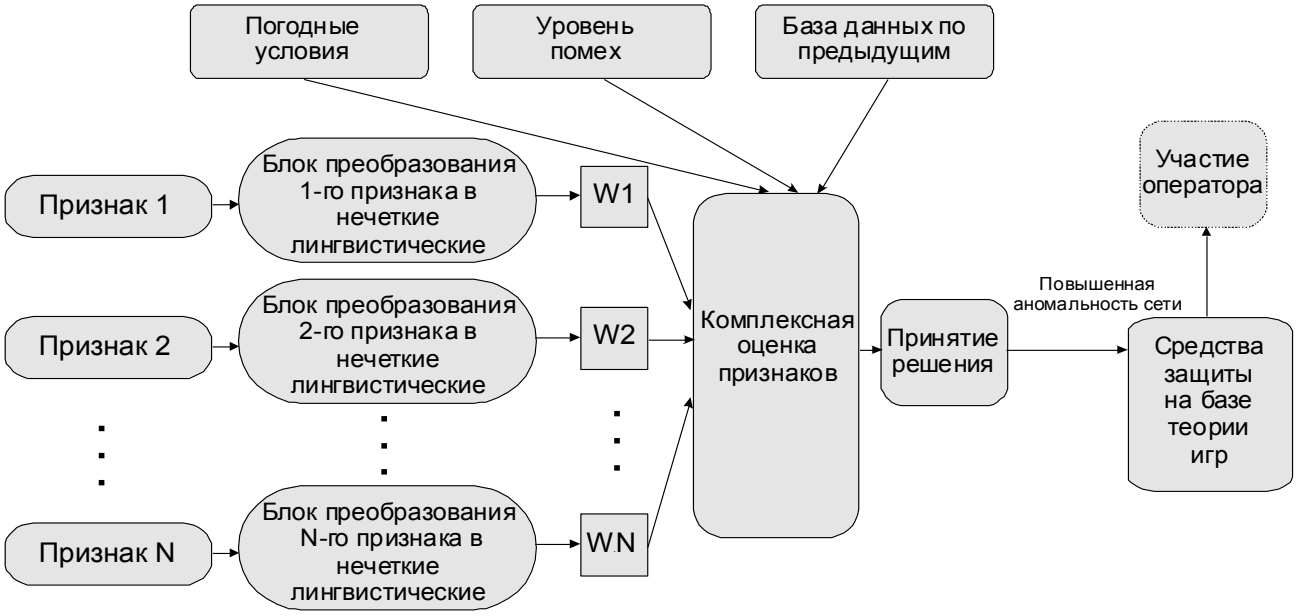

Рис.1

Стратегии защиты	Стратегии нападения					
	b_1	b_2	b_3	b_4	…	b_j
a_1	W_{11}	W_{12}	W_{13}	W_{14}	…	W_{1j}
a_2	W_{i2}	W_{22}	W_{23}	W_{24}	…	W_{2j}
a_3	W_{31}	W_{32}	W_{33}	W_{34}	…	W_{3j}
a_4	W_{41}	W_{42}	W_{43}	W_{43}	…	W_{4j}
…	…	…	…	…	…	…
a_i	W_{i1}	W_{i2}	W_{i3}	W_{i4}	…	W_{ij}

Рис.2

В данной игре строки матрицы a_1, a_2,...., a_i – стратегии защиты беспроводной сети, а столбцы матрицы b_1, b_2,..., b_j – средства нападения на беспроводную сеть, W_{ij}, $i = 1…m$, $j = 1…n$ – ожидаемый выигрыш при использовании стратегии ai в случае, если среда находится в состоянии b_j. Особенностью является принцип формирования элементов матрицы.

Предусматривается, что сторонам известна матрица игры и конечное множественное число стратегий соперника, но неизвестно, какая стратегия реализуется в конкретной ситуации. В этом случае в матричной игре формализируется ситуация выбора стратегий защиты в условиях неопределенности, то есть каждая из сторон не имеет информации о действии, которое осуществляется другой стороной.

Когда система защиты обнаруживает вмешательство в сеть, на которое у нее нет готовой ответной стратегии, есть смысл применить стратегию, основанную на формировании аномального трафика для этого пользователя, т. е. создать для злоумышленника имитацию успеха его атаки путем изменения данных, которые он просматривает или копирует, но его действия, приводящие к нежелательным для сети последствиям, запрещены для выполнения удаленно под любыми привилегиями. Если цель злоумышленника заключается в изменении настроек, форматировании жесткого диска и т. п., можно предположить, что злоумышленник не станет повторять попытки атак (в связи с недостатком информации о подобных системах).

На рис. 3 показан пример реализации игрового подхода.

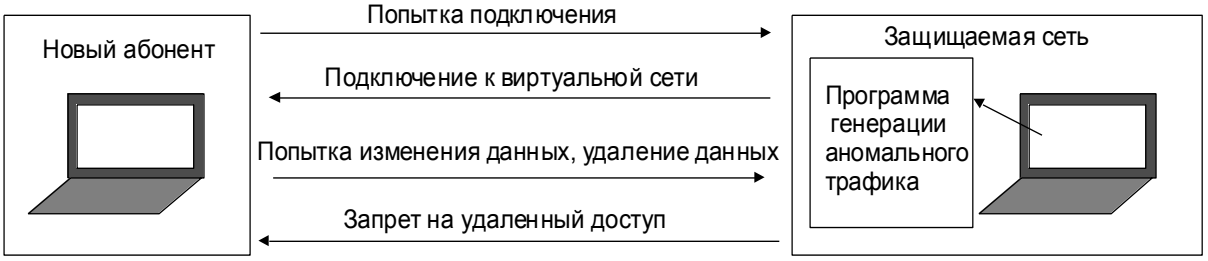

Рис. 3

Суть такого алгоритма управления заключается в сравнении большого количества возможных в данных условиях качественно разных решений, определении оптимального или наилучшего с учетом всех ограничений.

Таким образом, можно считать, что данный метод позволит защитить сеть от ранее неизвестных атак путем предотвращения необходимости их применения.

Система на основе такой методики должна будет останавливать злонамеренный трафик, в реальном времени обнаруживать атаки и делать это до поступления вредоносного трафика в информационную систему. Трафик должен предварительно обрабатываться программной моделью, имитирующей защищаемую сеть.

Теория игр не только позволит сформировать оптимальную стратегию, которая обеспечивает гарантии определенного выигрыша, но и позволит выдать рекомендации относительно ее изменения с целью увеличения выигрыша.

Выводы

Задача повышения безопасности Wi-Fi сетей является актуальной и ее актуальность будет возрастать по мере увеличения точек доступа и количества Wi-Fi оборудования у пользователей. 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.

Системы обнаружения вторжений также неполностью удовлетворяют существующим требования. Они недостаточно интеллектуальны, вследствие чего не способны обнаруживать новые виды атак, и вызывая ложные тревоги в штатных ситуациях, могут препятствовать нормальной работе сети.

Предложенный метод с применением теории игр позволит защитить сеть от ранее неизвестных атак путем предотвращения необходимости их применения.

Список литературы: 1. *Антипов И.Е., Ященко Т.А., Нух Таха Насиф.* Применение нечеткой логики для повышения безопасности беспроводных сетей на базе технологии Wi-Fi // Радиотехника. – 2011. – №165. – С. 103-106. 2. *Ошмарин Д.В.* Распределение канальных ресурсов в сетях когнетивного радио на основе теории игр // БИЗНЕС-ИНФОРМАТИКА. – 2010. – №4(14). – С. 38-45. 3. *Петров А.С., Вельченко С.А.* Методика управления защитой информационной системы в беспроводной сети на базе теории игр / Восточноукраинский национальный университет имени Владимира Даля. – 2012. – №8 (179).Ч.1. – С. 70-80. 4. *Оуэн Г.* Теория игр. – М. : Мир, 1971. – 230 с.

Харьковский национальный университет радиоэлектроники

Поступила в редколлегию 04.03.2013