УДК 681.3.06:519.248.681

И. Е. АНТИПОВ, д-р техн. наук, Е.Ю. БОНДАРЬ, канд. техн. наук, Т. А. ВАСИЛЕНКО

СОВЕРШЕНСТВОВАНИЕ МОДЕЛИ WI-FI СЕТИ С ЦЕЛЬЮ ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ

Введение

Исходя из популярности беспроводных Wi-Fi сетей задача защиты от несанкционированного доступа информации, хранимой в компьютерных системах, является актуальной. Эта задача решается с помощью комплекса средств, включающего в себя технические, программно-аппаратные средства и административные меры защиты информации. Причины, по которым взломщики атакуют беспроводные Wi-Fi-сети, могут быть разными: анонимный доступ, низкая вероятность быть пойманным, бесплатный канал, легкость проникновения, кража информации, подслушивание и модификация данных.

Актуальность работы

Для повышения безопасности беспроводной сети Wi-Fi был создан алгоритм анализа состояния 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 не учитывают [1, 2]. Проверка работоспособности и эффективности предложенного алгоритма может быть осуществлена на реальной сети, либо на ее модели, реализованной в виде компьютерной программы, имитирующей работу сети. Второй вариант предпочтительнее, поскольку предоставляет гораздо больше возможностей и реализуется значительно проще. В работе [3] была создана модель Wi-Fi сети, реализованная в виде компьютерной программы, которая имитирует работу абонентов и точки доступа в режиме централизованной координации (PCF).

Но на MAC уровне протокола 802.11 кроме PCF определяется два еще один вид коллективного доступа к среде передачи данных – режим распределенной координации (DCF). Причем, именно этот режим работы сети является наиболее уязвимым с точки зрения несанкционированного доступа к ней, так как при этом абоненты общаются между собой, минуя точку доступа.

Поэтому актуальной задачей является усовершенствование защиты беспроводных сетей в направлении принятия решения относительно аномальности сети в изменяющихся условиях ее функционирования. В данной статье рассмотрена модель работы в режиме DCF.

Реализация функций распределенной координации DCF

Реализация сетей без точки доступа использует механизм регламентирования коллективного доступа, известный как функция распределенной координации DCF. Однако такой режим присутствует и в сетях с точкой доступа, дополняя функцию централизованной координации, накладываясь «поверх нее». Практически это означает, что в течение определенного промежутка сетевого цикла сеть работает в режиме PCF, а затем в режиме DCF.

Функция DCF основана на методе коллективного доступа с обнаружением несущей и механизмом избежания коллизий (Carrier Sense Multiple Access/Collision Avoidance, CSMA/CA). При такой организации каждый узел, прежде чем начать передачу, «прослушивает» эфир, и только при условии отсутствии сигнала других абонентов, может начать передачу своих данных. На рис. 1 представлен алгоритм работы функции распределенной координации DCF.

Все абоненты сети, перед тем как начать передачу данных, проверяют, свободна среда или нет. Если среда оказывается свободной, абоненты выжидают в течение определенного промежутка времени, что значительно снижает вероятность возникновения коллизий, поскольку вероятность того, что два узла сети будут выжидать в течение одного и того же промежутка времени, чрезвычайно мала. Этот промежуток является случайным и складывается из двух составляющих: обязательного промежутка DIFS (DCF Interframe Space) и выбираемого случайным образом промежутка обратного отсчета (Backoff time).

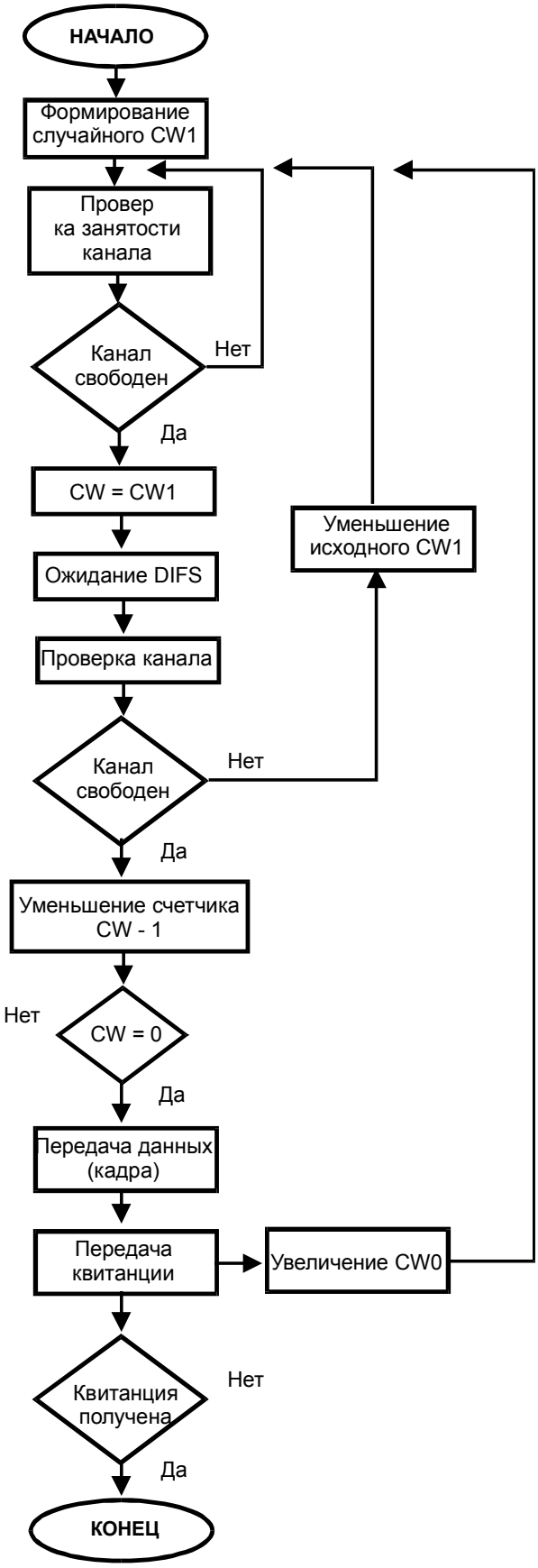

Рис. 1

Для того чтобы гарантировать всем абонентам сети равноправный доступ к среде передачи данных, необходимо определить алгоритм выбора длительности промежутка обратного отсчета (Backoff time). Промежуток обратного отсчета хотя и является случайным, но в то же время определяется на основании множества некоторых дискретных промежутков времени, то есть равен целому числу элементарных временных промежутков, называемых тайм-слотами (SlotTime).

Для выбора промежутка обратного отсчета каждый узел сети формирует так называемое окно конкурентного доступа (Contention Window, CW), использующееся для определения количества тайм-слотов, в течение которых станция выжидала перед передачей. Фактически окно CW – это диапазон для выбора количества тайм-слотов, причем минимальной размер окна определяется в 31 тайм-слот, а максимальный размер – в 1023 тайм-слота. Промежуток обратного отсчета определяется как количество тайм-слотов, определяемое исходя из размера окна CW.

Когда узел сети пытается получить доступ к среде передачи данных, то после обязательного промежутка ожидания DIFS запускается процедура обратного отсчета, то есть включается обратный отсчет счетчика тайм-слотов начиная от выбранного значения окна CW. Если в течение всего промежутка ожидания среда оставалась свободной (счетчик обратного отсчета равен нулю), то узел начинает передачу.

После успешной передачи окно CW формируется вновь. Если же за время ожидания передачу начал другой узел сети, то значение счетчика обратного отсчет останавливается и передача данных откладывается.

При этом очевидно, что чем большее число раз узел откладывает передачу по причине занятости среды, тем выше вероятность того, что в следующий раз он получит доступ к среде передачи данных. На рис. 2 показана реализация равноправного доступа к среде передачи данных в режиме DCF.

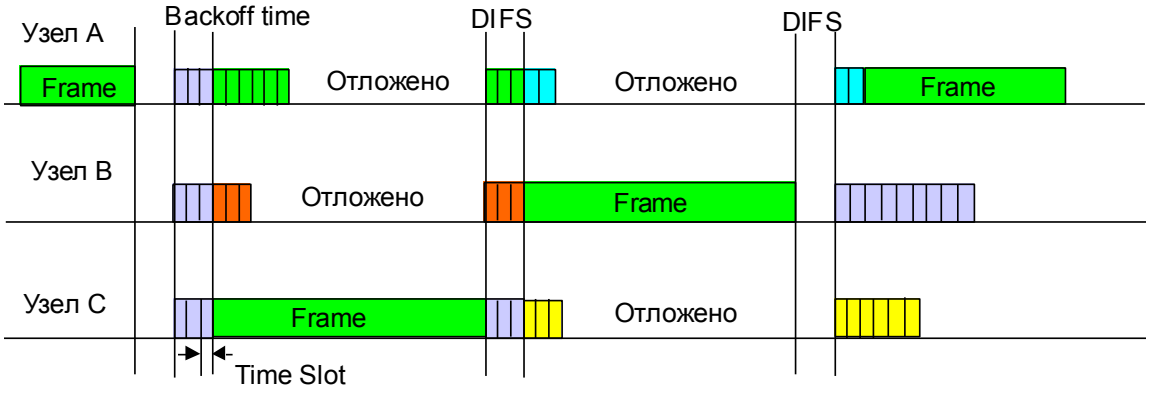

Рис. 2

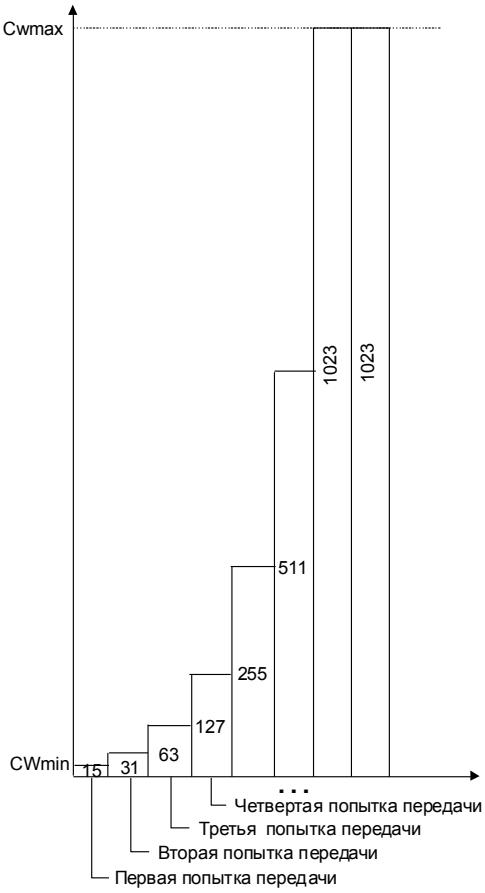

Рис. 3

После каждого успешного приема кадра принимающая сторона через короткий промежуток SIFS (Short Interframe Space) подтверждает успешный прием, посылая ответную квитанцию – кадр ACK (ACKnowledgement) (рис. 2). Если в процессе передачи данных возникла коллизия, то передающая сторона не получает кадр ACK, свидетельствующий об успешном приеме. В этом случае размер CW-окна для передающего узла увеличивается почти вдвое. Так, если для первой передачи размер окна равен 31 слоту, то для второй попытки передачи он уже составляет 63, для третьей – 127, для четвертой – 255, для пятой – 511, а для всех последующих – 1023 слота, что показано на рис. 3.

Таким образом, для каждой i-й передачи (если все предыдущие оказались безуспешными) размер CW-окна увеличивается по следующему правилу: CWi=CWi-1+1. И увеличение размера окна происходит динамически, по мере роста числа коллизий, что позволяет, с одной стороны, уменьшить временные задержки, а с другой – снизить вероятность возникновения коллизий.

Рассмотренный механизм регламентирования коллективного доступа к среде передачи данных имеет одно узкое место – так называемую проблему скрытых узлов. Из-за естественных препятствий возможна ситуация, когда два узла сети не могут «слышать» друг друга напрямую. Такие узлы называют скрытыми. Для того чтобы разрешить проблему скрытых узлов, функция DCF опционально предусматривает возможность использования алгоритма RTS/CTS.

Программно функция распределенной координации DCF выполняется как отдельная процедура. Сначала идет проверка на занятость канала, если канал свободен, ожидается время difs. Затем каждая станция сети, желающая передать данные, формирует свое случайное окно конкурентного доступа. Та станция, у которой оно оказалось наименьшим, начинает передачу кадра, определяется признак занятости канала и ожидается подтверждение. Если подтверждение не принято, время окна увеличивается вдвое и происходит переход на начало процедуры. Когда абонент получает подтверждение, он формирует новое случайное число для передачи очередных данных. Те станции, у которых окно конкурентного доступа оказалось больше, уменьшают окно конкурентного доступа вдвое, и происходит переход на начало процедуры.

В данной процедуре также предусмотрена передача данных, которая состоит из таких операций, как формирование пакета данных (данные появляются с вероятностью 10 %), отправка данных и ожидание подтверждения о получении пакета.

В программной реализации работы беспроводной сети поочередность прохождения процедур осуществляется с помощью вызывающей программы, которая в нужной очередности обращается к каждой из них.

Результаты моделирования

Результаты моделирования функции распределенной координации DCF, выполненные в среде Delphi, представлены на рис. 4.

Функция распределенной координации не отрицает функцию централизованной координации, а скорее дополняет ее. В течение определенного промежутка времени реализуется механизм PCF, а затем – DCF, а потом все повторяется заново. Длительность промежутка DCF должна быть достаточной для того, чтобы обеспечить возможность передать хотя бы один кадр.

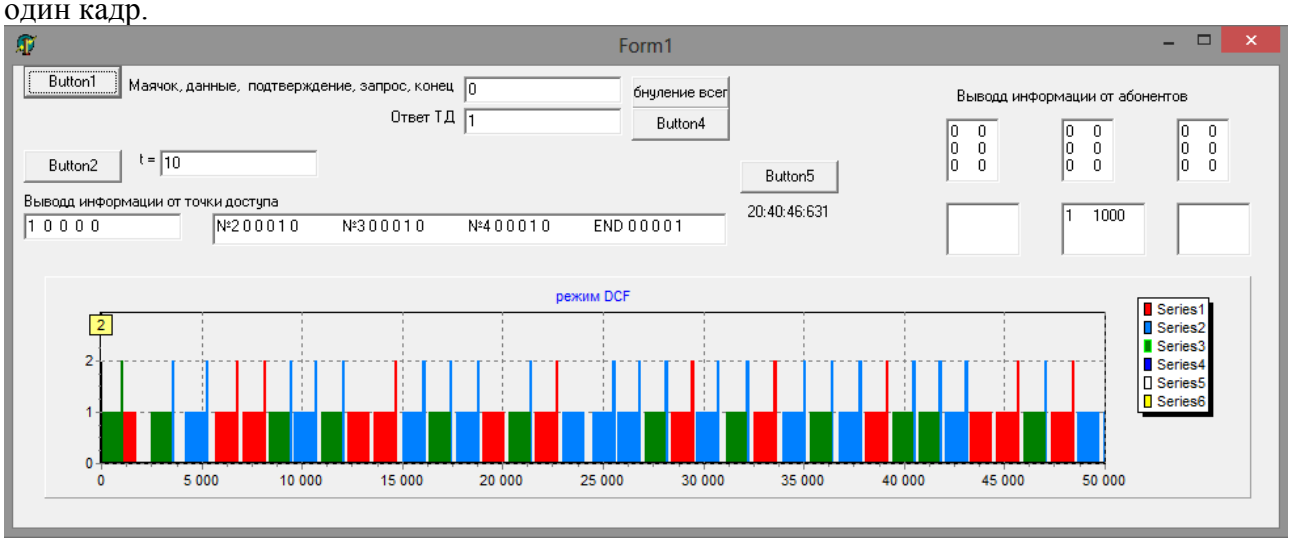

Рис. 4

Выводы

В среде Delphi была усовершенствована модель Wi-Fi сети, реализованная в виде компьютерной программы, имитирующая работу Wi-Fi сети, которая позволяет учесть возможность вторжений, сбоев и помех. Ранее разработанная модель, работающая в режиме централизованной координации, была дополнена режимом распределенной координации, без которого проверка защищенности беспроводной сети была бы неполной.

В дальнейших исследованиях с помощью данной программы планируется проанализировать работу сети и действия злоумышленника, направленные на беспроводную сеть. Данная программа дает возможность сделать выводы об уровне защищенности беспроводной сети и проверить идеи защищенности беспроводной сети, основанные на нечеткой логике.

Список литературы: 1. *Антипов, И. Е.* Применение нечеткой логики для повышения безопасности беспроводных сетей на базе технологии Wi-Fi / И. Е. Антипов, Т. А. Ященко, Нух Таха Насиф // Радиотехника. – 2011. – Вып. 165. – С. 103 – 106. 2. *Антипов, И. Е.* Применение теории игр для защиты беспроводных wi-fi сетей / И. Е. Антипов, Т. А. Ященко, В. С. Вовченко // Радиотехника. – 2013 – Вып. 173. – С. 104-107. 3 *Антипов, И. Е.* Разработка модели Wi-Fi сети с целью предотвращения вторжений / И. Е. Антипов, Т. А. Василенко, Е.Ю. Бондарь // Восточно-Европейский журнал передовых технологий сб. – 2014. – Вып. 1/9 (67). – С. 4 – 8 4. *Пролетарский, А. В.* Беспроводные сети Wi-Fi / А.В. Пролетарский, И. В. Баскаков, Д. Н. Чирков. – БИНОМ. Лаборатория знаний, 2007. – 178 с.

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 11.03.2014