У даній статті запропонована структура моделі, яка імітує роботу бездротової Wi-Fi мережі і враховує можливість вторгнень, збоїв і перешкод з використання комп'ютерної програми Delphi. Дана модель призначена виключно для того, щоб перевірити запропоновані алгоритми її захисту, що базуються на нечіткій логіці

Ключові слова: бездротова мережа, модель роботи Wi-Fi мережі, безпека

В данной статье предложена структура модели, которая имитирует работу беспроводной Wi-Fi сети и учитывает возможность вторжений, сбоев и помех с использование компьютерной программы Delphi. Данная модель предназначена исключительно для того, чтобы проверить предложенные алгоритмы её защиты, основанные на нечеткой логике

Ключевые слова: беспроводная сеть, модель работы Wi-Fi сети, безопасность

УДК 681.3.06:519.248.681

РАЗРАБОТКА МОДЕЛИ WI-FI СЕТИ С ЦЕЛЬЮ ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ

И. Е. Антипов
Доктор технических наук, профессор*
E-mail: i_ant@mail.ru
Т. А. Василенко
Аспирант*
E-mail: Skorpy_h7@mail.ru
И. В. Михеев*
E-mail: medvedmiv@gmail.com
*Кафедра радиоэлектронных устройств
Харьковский национальный университет радиоэлектроники
пр. Ленина, 14, г. Харьков, Украина, 61166

1. Введение

Удобство беспроводных сетей неоспоримо: они обеспечивают связь и доступ в Internet за пределами нашего рабочего места или офиса. Поэтому они стали одними из наиболее популярных периферийных устройств. Кроме того, достаточно подключить эти устройства к электрической сети, чтобы Wi-Fi-совместимые ноутбуки смогли устанавливать сетевые соединения без проводов. С другой стороны, удобный сетевой доступ связан с огромным риском для сети и данных, так как в выбираемом по умолчанию режиме многих недорогих беспроводных точек доступа злоумышленники могут легко подключиться к сети и похитить данные. Поэтому актуальной задачей является усовершенствование защиты беспроводных сетей в направлении принятия решения относительно аномальности сети в изменяющихся условиях ее функционирования.

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].

2. Актуальность работы

Проверка работоспособности и эффективности предложенного алгоритма может быть осуществлена на реальной сети, либо на её модели, реализованной в виде компьютерной программы, имитирующей работу сети. Второй вариант предпочтительнее, поскольку предоставляет гораздо больше возможностей и реализуется значительно проще.

В настоящее время уже существует ряд систем моделирования беспроводных сетей. Например, TamoGraph [3], который анализирует модель, отражающую характеристики здания, помогает определить оптимальное количество, расположение и настройки точек доступа. Профессиональным инструментом для проектирования беспроводных сетей является Fluke Networks AirMagnet Planner [4], учитывающий типы и характеристики строительных материалов, препятствия для распространения радиосигналов, конфигурации точек доступа и т. д.

Программный пакет Network Simulator предназначен для имитационного моделирования систем связи различного назначения [5, 6].

Таким образом, разработанные ранее и представленные выше модели предназначены для развертывания сети, но, к сожалению, не учитывают возможность вторжений, сбоев, помех и т. д. Отсюда следует вывод, что актуальной является задача разработки специальной модели, которая имитирует работу Wi-Fi сети и предназначенной исключительно для того, чтобы проверить предложенные алгоритмы её защиты, основанные на нечеткой логике [1, 2].

3. Реализация функции централизованной координации PCF

В данной статье рассматривается модель в виде программы, которая имитирует работу беспроводной

Wi-Fi сети в режиме централизованной координации PCF.

Перед разработкой программы были рассмотрены алгоритмы работы базовой станции и абонентов по отдельности [7, 8]. Процедуры, предусмотренные в алгоритме, в действительности выполняются на разных устройствах, которые независимы и не имеют полной информации друг о друге, общаются только через радио эфир. Для того чтобы реализовать все эти алгоритмы на одном компьютере, было принято решение разделить их на несколько процедур, выполняемых не одновременно (хотя в действительности, многие из них происходят одновременно). Также в программе предусмотрены разнообразные виды атак.

Для сетей с точкой доступа используется механизм регламентирования коллективного доступа, известный как функция централизованной координации (PCF). На центр координации возлагается задача управления коллективным доступом всех остальных узлов сети к среде передачи данных на основе определенного алгоритма опроса или исходя из приоритетов узлов сети.

Таким образом, координации опрашивает все узлы сети, внесенные в его список, и на основании этого опроса организует передачу данных между всеми узлами сети. Важно отметить, что такой подход полностью исключает конкурирующий доступ к среде и делает невозможным возникновение коллизий, а для время зависимых приложений гарантирует приоритетный доступ к среде.

Во время режима PCF точка доступа опрашивает все узлы сети о кадрах, которые стоят в очереди на передачу, посылая им служебные кадры POLL. Опрашиваемые узлы в ответ на получение кадров POLL посылают подтверждение ACK. Если подтверждения не получено, то точка доступа переходит к опросу следующего узла.

Кроме того, чтобы иметь возможность организовать передачу данных между всеми узлами сети, точка доступа может передавать кадр данных (DATA) и совмещать кадр опроса с передачей данных (кадр DATA+POLL). Аналогично узлы сети могут совмещать кадры подтверждения с передачей данных DATA+ACK. На рис. 1 показана организация передачи данных между узлами сети в режиме PCF.

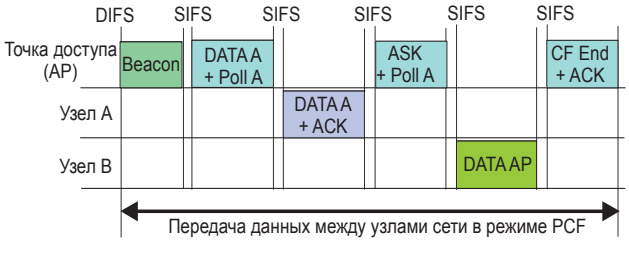

Рис. 1. Организация передачи данных между узлами сети комбинированный кадр данных, подтверждения

Допускаются следующие типы кадров во время режима PCF: DATA – кадр данных; CF_ACK – кадр подтверждения; CF_POLL – кадр опроса; DATA + + CF_ACK – комбинированный кадр данных и подтверждения; DATA + CF_POLL – комбинированный кадр данных и опроса; DATA+CF_ACK+CF_POLL – и опроса; CF_ACK+CF_POLL – комбинированный кадр подтверждения и опроса.

Все абоненты сети, перед тем как начать передачу данных, принимают маячок, который несет служебную информацию о продолжительности одного цикла и позволяет синхронизировать работу всех узлов сети. Для реализации приема данных от точки доступа в процедуре работы абонентов предусмотрены такие операции, как прием пакета, проверка контрольной суммы (в программе прописан генератор случайных чисел, работа которого приводит к совпадению контрольной суммы в 99 %), формирование подтверждения о получении данных и отправка подтверждения.

Также в этой процедуре 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 процедуре работы абонентов предусмотрен прием запросов от точки доступа (пакета Pool) и пакета, свидетельствующего об окончании цикла. На рис. 2 представлен алгоритм работы абонентов в режиме PCF.

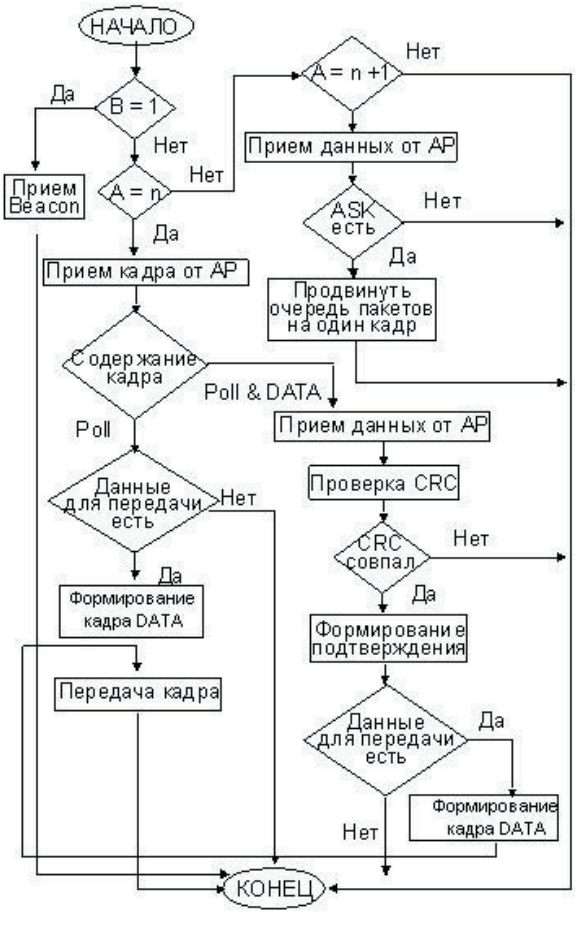

Рис. 2. Алгоритм работы абонентов в режиме PCF

В режиме PCF общение абонентов происходит исключительно через точку доступа, поэтому требуется многократное обращение к ней, причем на разных этапах это участие различно. Точка доступа инициирует начало цикла ожиданием времени difs и передачей маячка (beacon).

Для реализации передачи маячка в процедуре работы с точкой доступа предусмотрены следующие операции: этап обращения к точке доступа; задержка времени difs; формирование маячка; передача маячка; ожидание задержки sifs и передача управления в вызывающую программу.

После передачи маячка точка доступа по очереди совершает опрос каждого абонента сети о наличии у них, данных на передачу, отправляя кадр pool. И если имеются данные для абонента, вместе с опросом отправляются и данные.

Для реализации отправки данных в процедуре работы с точкой доступа предусмотрены следующие операции:

– анализ этапа обращения к точке доступа;

– формирование запроса pool;

– формирование кадра данных (данные для абонентов появляются с вероятностью 10 %);

– проверка контрольной суммы (если были получены данные);

– формирование подтверждения (если были получены данные);

– отправка пакета запрос + данные + подтверждение (если они имеются);

– ожидание минимальной задержки sifs;

– передача управления в вызывающую программу.

После того, как последний абонент сети будет опрошен, точка доступа отправляет всем абонентам сообщение об окончании цикла.

В программной реализации работы беспроводной сети, общение точки доступа с абонентами, осуществляется с помощью вызывающей программы, которая в нужной очередности обращается к каждой из процедур.

4. Реализация функций сети

Формирование данных для передачи имеет случайный характер. В модели вероятность появления данных для передачи осуществляется путём моделирования случайного числа в диапазон 0 до 1000. Если случайно сгенерированное число с равномерны законом распределения в диапазоне от 0 до 1000 оказывается меньше 990, то считается, что данные для передачи есть.

Прием пакета тем или иным узлом сети – явление в общем случае случайное. Его вероятность обусловлена наличием помех, коллизий, а также возможным вмешательством нарушителей. Если не рассматривать вмешательство нарушителей, то вероятность приёма пакета можно оценить как вероятность искажения пакета:

$$P_f=1-(1-P_0)^{m+n}, \quad (1)$$

где P_0 – вероятность битовой ошибки;

$(1-P_0)$ – вероятность не искажения 1 бита;

$(1-P_0)^{m+n}$ – вероятность искажения (n+m) бит.

В модели вероятность искажения пакета оценивается согласно (1) путём моделирования случайного числа в диапазон 0 до 1000.

Если случайно сгенерированное число с равномерны законом распределения в диапазоне от 0 до 1000 оказывается меньше 990, то считается, что пакет не искажён.

Счет времени в модели происходит не только в реальном времени. Созданы два счетчика, один считает реальное время длительности эксперимента.

Второй счетчик считает длительность всех этапов приема передачи в сети. В зависимости от оборудования, частоты, мощности длительности этапов передачи могут изменяться. В рамках работы были использованы такие временные интервалы: ASK (подтверждение) = 304 мкс; DATA (данные) = 937 мкс; DIFS (временной интервал) = 100 мкс; SIFS (временной интервал) = 10 мкс; CRS (контрольная сумма) = 304 мкс; POLL (запрос) = 352 мкс.

5. Реализация действий злоумышленника

При использовании беспроводных сетей возникает множество угроз безопасности. Наиболее опасные угрозы информационной безопасности по данным лаборатории Касперского представлены на рис. 3 [9].

Анализ данного графика показывает, что на угрозы, реализуемые через сеть, приходится более половины всех инцидентов в сфере информационной безопасности.

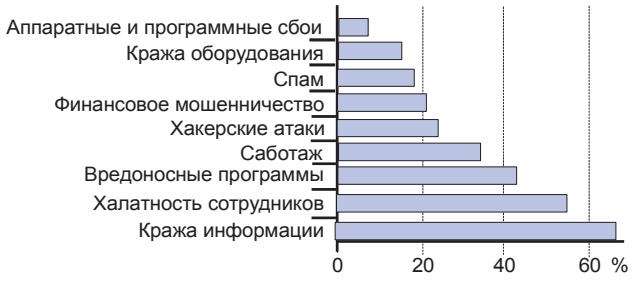

Рис. 3. Угрозы информационной безопасности

В беспроводных сетях выделяют следующие угрозы безопасности [10]: подслушивание, DoS атака, глушение, вторжение и модификация данных, атака «man in the middle». абонент-мошенник, ложная точка доступа, что более подробно рассмотрено в табл. 1.

Существуют также другие угрозы безопасности сети (атаки на сетевое оборудование, тайные беспроводные каналы, возникающие вследствие ошибок конфигурирования, угрозы, связанные с криптозащитой и её стойкостью), но в рамках работы, посвящённой определению вторжений, они рассматриваться не будут.

По данным статистики «Лаборатории Касперского» наиболее распространенной угрозой является DoS атака.

Анализ статистики – это, безусловно, важно и полезно, но необходимо помнить, что в статистику попадают только обнаруженные атаки, не обнаруженные остаются не учтенными и об их статистических и прочих характеристиках никто не знает. Поэтому при защите беспроводных сетей необходимо учитывать не только самые распространенные угрозы, но и все потенциальные угрозы, которые могут быть использованы злоумышленником.

Таблица 1

Угрозы безопасности беспроводных сетей

Вид атаки	Что необходимо для реализации атаки	Характерные признаки идентификации атаки	Описание действий злоумышленника	Программная реализация (изменения в модели)
Подслушивание	Приёмник расположенный вблизи передатчика	Идентифицировать практически невозможно	Перехват радиосигнала и (при необходимости) дешифрование передаваемых данные	Добавляется ещё один абонент, который получает доступ ко всей (или к части) информации, передаваемой в сети, но сам ничего не передаёт
DoS атака (Denial of Service – отказ в обслуживании)	Создается устройство, которое заполняет весь спектр на частоте 2.4 ГГц помехами и нелегальным трафиком	Происходят регулярные ошибки при получении пакетов данных, иногда – невозможность подключиться к сети	Точка доступа перегружается многочисленными бессмысленными пакетами, вследствие чего обслуживание сети, практически, прекращается	Программное увеличение вероятности наличия пакетов для передачи от одного или нескольких абонентов (злоумышленников) с типичных 3...10% до аномальных 100
Глушение	Устройство для постановки помех во всём спектре частот, данной беспроводной сети		Генерируется радиошум на частоте работы беспроводной сети. Различают глушение клиентов и глушение базовой станции	Увеличение вероятности ошибочного приёма пактов с учётом расстояния от источника помех до абонента
Вторжение и модификация данных	Знание протокола и параметров сети, обладание приёмником, расположенным в радиусе действия сети	Пользователям отказано в доступе к сети.	Добавляется информация к существующему потоку данных. Возможно вмешательство на уровне пакетов (модификация данных пользователей), или на уровне управляющих команд, (вплоть до отсоединения пользователей от сети)	Новый абонент перехватывает интересующие данные, изменяет их и отсылает получателю
Атака «man in the middle»	Злоумышленнику требуется подробная информация о сети	Например, обнаружение точки доступа с SSID корпоративной сети, но отсутствующей в списке легальных устройств, может быть признаком такой атаки	Может использовать все вышеуказанные атаки	В модели реализуются все вышеуказанные угрозы
Абонент-мошенник	Знание протокола и параметров сети		Имитация клиентского профиля абонента для получения доступа к сети от его имени. (Может осуществляться путём похищения абонентского устройства)	Добавляется новый абонент, который имеет доступ ко всей информации, передаваемой в сети, и принимает участие в процессе передачи данных
Ложная точка доступа	Знание протокола и параметров сети, собственна точка доступа с имитацией сетевых ресурсов	В радиусе действия данной сети, появляется сигнал, от еще одной точки доступа	Организация ложной точки доступа с имитацией сетевых ресурсов для перехвата, например аутентификационной информации абонентов	В модель добавляется ещё ода точка доступа, которая имитирует существующую точку доступа

6. Выводы

В среде Delphi была создана новая модель, реализованная в виде компьютерной программы, имитирующая работу Wi-Fi сети, которая позволяет учесть возможность вторжений, сбоев и помех. Эта программа имитирует работу абонентов и точки доступа в режиме PCF (в дальнейшем будет рассмотрен и режим DCF).

Предложенный в работе алгоритм работы Wi-Fi сети дает возможность проанализировать работу сети и действий злоумышленника, направленные на эту сеть.

Это позволит сделать выводы об уровне защищенности беспроводной сети, а также дает возможность проверить идеи защищенности беспроводной сети, основанные на нечеткой логике.

Литература

1. Антипов, И. Е. Применение нечеткой логики для повышения безопасности беспроводных сетей на базе технологии Wi-Fi [Текст] / И. Е. Антипов, Т. А. Ященко, Нух Таха Насиф. // Радиотехника: Всеукр. межвед. научн.-техн. сб. 2011 Вып. 165. С. 103-106.

2. Антипов, И. Е. Применение теории игр для защиты беспроводных wi-fi сетей [Текст] / И. Е. Антипов, Т. А. Ященко, В. С. Вовченко. // Радиотехника: Всеукр. межвед. научн.-техн. сб. 2013 Вып. 173. С. 104-107.
3. TamoGraph® Site Survey [Электронный ресурс]. Режим доступа: http:// http://www.tamos.com.
4. AirMagnet Planner [Электронный ресурс]. Режим доступа: http:// http://www.keenansystems.com.
5. Network simulation [Электронный ресурс]. Режим доступа: http:// http:// http://en.academic.ru.
6. SimulationTools.bib [Электронный ресурс]. Режим доступа: http:// http:// http:// http://www.idsia.ch.
7. Пролетарский, А. В. Беспроводные сети Wi-Fi [Текст] / А.В. Пролетарский, И. В. Баскаков, Д. Н. Чирков. – БИНОМ. Лаборатория знаний, 2007. – 178 с.
8. Джим Гейер. Беспроводные сети. Fi [Текст] / Джим Гейер. – М.: Издательский дом «Вильямс», 2005. – 192 с.
9. Kaspersky Security Bulletin. Развитие угроз в 2008 году [электронный ресурс] Режим доступа: http:// www.securelist.com
10. Шаньгин, В. Ф. Информационная безопасность компьютерных сетей и систем [Текст] / В. Ф. Шаньгин. – М.: ИД «ФЩРУМ» - ИНФРА-М, 2008. – 416 с.

УДК 004.056

АНАЛІЗ МОЖЛИВОСТЕЙ КВАНТОВИХ КОМП'ЮТЕРІВ ТА КВАНТОВИХ ОБЧИСЛЕНЬ ДЛЯ КРИПТОАНАЛІЗУ СУЧАСНИХ КРИПТОСИСТЕМ

Ю. І. Горбенко
Кандидат технічних наук, старший науковий співробітник*
Лауреат державної премії в галузі науки та техніки 2012 р.
E-mail: GorbenkoU@iit.com.ua
Р. С. Ганзя
Інженер*
E-mail: roman.ganzya@gmail.com
*Кафедра безпеки інформаційних технологій
Харківський національний університет радіоелектроніки
пр. Леніна, 16, м. Харків, Україна, 61166

На основі використання доступних джерел наводиться огляд та аналіз сучасних світових досягнень в області квантових обчислень та побудови квантового комп'ютера. Проводиться аналіз загроз безпеки відносно симетричних та асиметричних криптосистем у разі застосування методів квантового криптоаналізу. Наводяться оцінки просторових та часових складностей, яких потрібно досягати для успішного здійснення квантового криптоаналізу

Ключові слова: алгоритм Гровера, алгоритм Шора, квантовий комп'ютер, квантовий криптоаналіз

На основе использования доступных источников приводится обзор и анализ современных мировых достижений в области квантовых вычислений и построения квантового компьютера. Проводится анализ угроз безопасности относительно симметричных и асимметричных криптосистем в случае применения методов квантового криптоанализа. Приводятся оценки пространственных и временных сложностей, которые нужно достигать для успешного осуществления квантового криптоанализа

Ключевые слова: алгоритм Гровера, алгоритм Шора, квантовый компьютер, квантовый криптоанализ

1. Вступ

Ще в 60 – роках Гордон Мур [1] сформулював експериментально доведене ним твердження, згідно якого в напівпровідникових мікросхемах здійснюється практично щорічне подвоєння щільності транзисторів, тобто по суті зменшення розмірів елементів в два рази. Наведене твердження отримало назву закону Мура і справджується вже майже протягом 50 років. На сьогодні розмір елементів транзистора (і, відповідно, розмір області, в якій зберігається одиниця інформації – біт) становить нанометри. У зв'язку з цим виникає питання про принципові обмеження на розміри, швидкодію та теплообмін між елементами комп'ютерних схем при їх зменшенні. На думку фізика Р. Фейнмана "закони фізики не заперечують зменшення розмірів комп'ютера до тих пір, доки біти не досягнуть розмірів окремих атомів і закони квантової механіки не стануть