ИССЛЕДОВАНИЕ НАДЕЖНОСТИ БЕСПРОВОДНЫХ СЕТЕЙ СВЯЗИ МЕТОДОМ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ В СРЕДЕ ANYLOGIC

В. И. Закиров, В. В. Золотухин (Красноярск)

Современные беспроводные сети связи составляют серьезную конкуренцию проводным способам доступа с использованием металлических и оптических кабелей связи. Это объясняется тем, что скорость передачи данных в беспроводных сетях, таких как Wi-Fi и WiMAX, уже составляет несколько мегабит в секунду, чего достаточно для удовлетворения запросов даже самых продвинутых пользователей сети Интернет, а по удобству работы такие сети вне конкуренции [1]. Особенно актуальным оказывается использование беспроводных сетей в тех случаях, когда прокладка кабеля невозможна или нецелесообразна по экономическим, эстетическим соображениям либо просто при нехватке времени на развертывание кабельной инфраструктуры.

Однако все беспроводные сети связи обладают одним существенным недостатком по сравнению с проводными – они не гарантируют такого уровня безопасности и конфиденциальности, каким отличаются все технологии с закрытой средой передачи сигналов. Для получения доступа к сети связи на основе металлического кабеля, например витой пары UTP-5e, требуется непосредственный доступ к среде передачи, а в случае использования оптического кабеля подключение очень сложно реализовать даже при наличии подобного доступа. С беспроводными сетями связи всё обстоит иначе: поскольку такие технологии изначально ориентированы на использование открытой среды передачи радиосигналов, доступной практически любому пользователю в зоне действия антенны, то вопросы безопасности и надежности функционирования таких сетей приобретают новый смысл.

Структура беспроводной сети связи приведена на рис. 1.

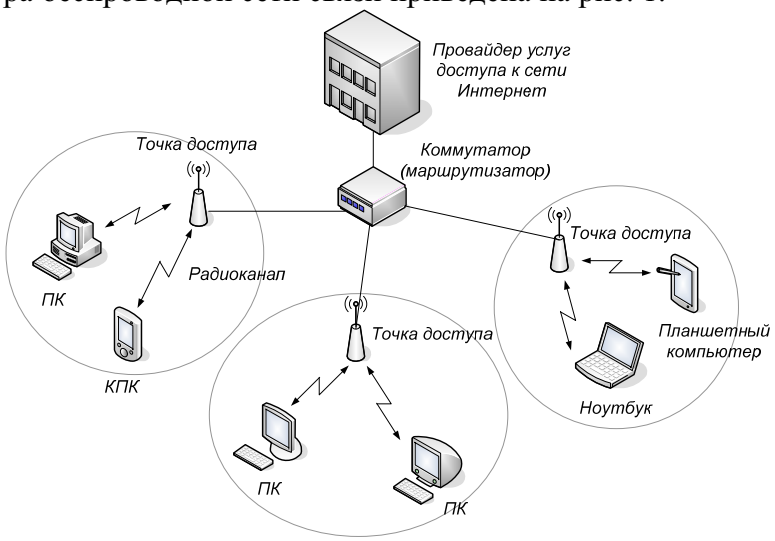

Рис. 1. Структура беспроводной сети связи

В состав сети входят следующие основные элементы:

– оборудование пользователей услугами связи, включающее в себя персональный компьютер (ноутбук, нетбук, планшетный компьютер или КПК) с оборудованием доступа к беспроводной сети связи (беспроводной адаптер или интерфейс);

– беспроводные точки доступа;

– беспроводная среда передачи информации (радиоканал);

– линии связи и оборудование провайдера услуг сети Интернет (в процессе моделирования не рассматриваются).

Среди всех известных показателей надежности сетей связи для оценки качества функционирования беспроводных сетей наиболее подходящими являются коэффициент готовности, вероятность безотказной работы и вероятность связности. Последний показатель применим только к сети связи определенной топологии [2], а задача данной работы заключается в исследовании одного простого сегмента сети – между пользователем и точкой доступа. Поэтому основное внимание уделяется такому показателю надежности, как коэффициент готовности. Следует заметить, что документом [3] регламентируется минимальное значение коэффициента готовности для сетей передачи данных, равное 0,99.

К основным причинам отказа беспроводных сетей связи можно отнести:

а) отказ радиоканала (беспроводной среды передачи информации):

– замирания в канале;

– помехи и интерференция;

б) отказ аппаратного обеспечения;

в) отказ программного обеспечения (сбои и «зависание»);

г) отказ вследствие целенаправленной атаки на систему.

В результате исследования возможных причин и последствий подобных видов отказов, а также их влияния на работу беспроводной сети связи, была разработана имитационная модель функционирования беспроводной сети в условиях воздействия всех перечисленных дестабилизирующих факторов (рис. 2). Для моделирования функционирования беспроводной сети связи использовалась среда имитационного моделирования AnyLogic [4].

В качестве основных блоков имитационной модели были выбраны объекты класса state chart (диаграммы состояний), позволяющего задать весь процесс функционирования беспроводной сети связи в виде множества состояний системы с разными коэффициентами готовности и переходов между состояниями, которые осуществляются с определенными вероятностями, задаваемыми статически или вычисляемыми динамически в процессе моделирования.

В качестве основных состояний системы использовались:

– обычное работоспособное состояние системы «work»;

– атака на систему «attack»;

– отказ системы «fail»;

– замирания в канале «fading».

К преимуществам AnyLogic можно отнести возможность создания сложных, комплексных состояний, включающих в себя множество более простых состояний и переходов между ними. В качестве примера подобного сложного состояния можно привести состояние «attack», включающее в себя такие простые состояния, как aggression, substitution device, intercept, overflow, virus, modification и denial of service.

Состояние «work» является простым и соответствует наиболее вероятному работоспособному состоянию системы беспроводной связи, в котором коэффициент готовности $K_г$ равен единице, а пропускная способность B максимальна. В результате воздействия внешних и внутренних дестабилизирующих факторов возможны переходы в другие состояния с определенными вероятностями (интенсивностями). Каждое из таких состояний характеризуется определенным коэффициентом готовности и пропускной способностью сети.

Из рабочего состояния возможны переходы в нерабочие состояния в случае появления замираний (fading), в случае атаки на систему (attack), а также в случае отказа беспроводной сети (fail).

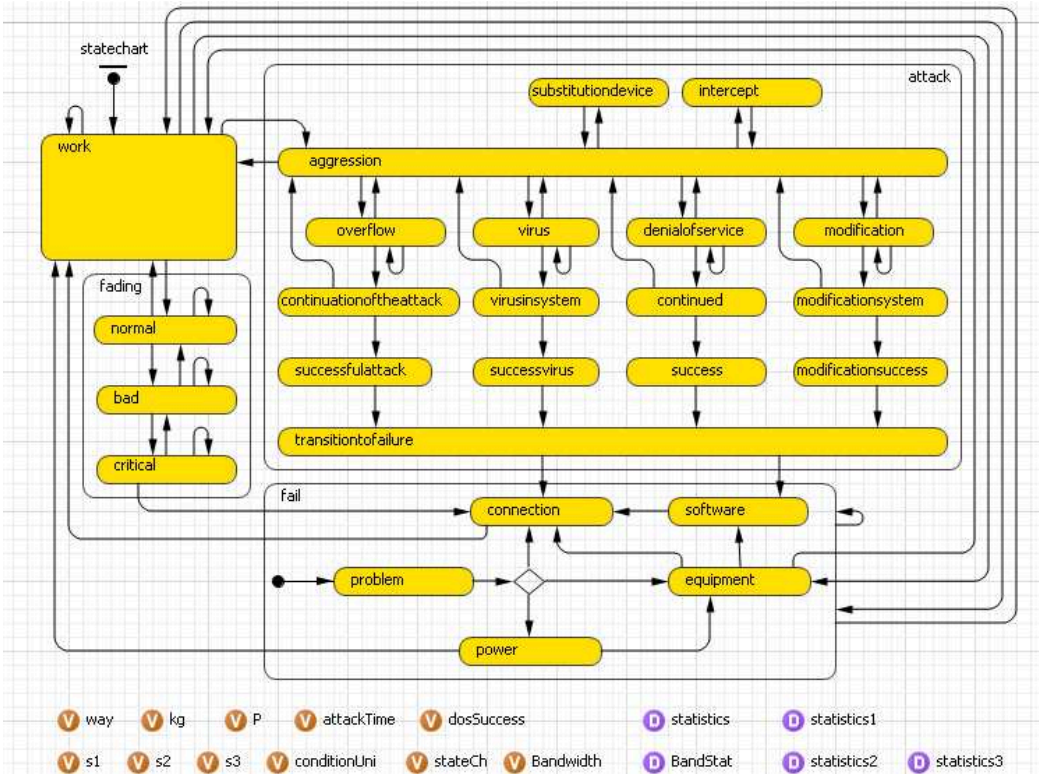

Рис. 2. Имитационная модель функционирования беспроводной сети связи в AnyLogic

«Отказ сети» представляет собой сложное состояние, состоящее из нескольких состояний – проблема с сетью (problem), отключение электропитания системы (power), отказ в соединении (connection), отказ оборудования (equipment) и сбои в работе программного обеспечения (software).

«Отказ в соединении» может произойти и в случае перехода из состояний fading и attack, а из рабочего состояния возможен переход непосредственно к отказу оборудования или к отказу сети. Отказ сети логически представлен в виде появления блока «проблема с сетью», из которого уже с помощью ветвления возможны переходы к «отказу оборудования», «отказу в соединении», «отказу питания».

Сложное состояние «отказ сети» позволяет смоделировать ситуацию с отказом питания. В этом случае возможен отказ оборудования и, как следствие, отказ в соединении. При потере питания возможно и его быстрое восстановление с последующим переходом обратно в рабочее состояние. При отказе оборудования соответственно отказывает и программное обеспечение. Состояние attack также является сложным, состоящим из следующих состояний:

– переходное состояние («aggression») представляет собой состояние перед непосредственным началом атаки, когда злоумышленник уже находится в сети, характеризуется незначительным снижением коэффициента готовности сети;

– состояние «подмена устройства» («substitution device») – в случае неавторизированного доступа, не влечет за собой отказ сети;

– состояние «перехват» («intercept») – в случае перехвата пакетов сети часть информации может теряться, состояние также не влечет за собой отказ сети;

– состояние начала модификации сети («modification») – в случае попытки изменить структуру сети или модифицировать ее с какой-то целью (например, грабежа), из этого состояния система может перейти к более опасным для нее состояниям, вплоть до полного отказа;

– состояние дальнейшей модификации сети («modification system») – произошло частичное перестроение сети;

– состояние полной модификации сети («modification success») – сеть полностью изменена в соответствии с желаниями злоумышленника; из этого состояния сеть переходит в неисправное состояние (либо connection, либо software);

– состояние начала отказа в обслуживании («denial of service») – возникает в случае попытки лишить обслуживания абонентов сети, при переходе в менее безопасные состояния может привести к отказу в соединении либо к отказу программного обеспечения;

– состояние частичного отказа в обслуживании («continued»), когда полностью связь ещё не потеряна, но наблюдается существенное снижение пропускной способности;

– состояние успешной атаки, направленной на отказ в обслуживании («success») – злоумышленник уже нарушил соединение, из него система переходит в состояние отказа (либо connection, либо software);

– состояние заражения системы («virus») – в случае появления вредоносных программ; при переходе в состояния с большей степенью заражения может привести к отказу;

– состояние дальнейшего заражения («virus in system») – антивирусная система не смогла сразу обнаружить угрозу, характеризуется снижением быстродействия системы;

– состояние успешного внедрения вредоносных программ («success virus») характеризуется нарушением работы системы, вследствие чего возможна потеря соединения или отказ программного обеспечения;

– состояние в случае начала атаки, направленной на переполнение системы, («overflow») – начинает внедряться большое количество пакетов в сеть, при переходах в дальнейшие состояния пропускная способность может снижаться вплоть до полного отказа;

– состояние дальнейшего переполнения («continuation of the attack») – число пакетов в системе уже значительно, но пока не является критичным;

– состояние успешного переполнения системы («successful attack») – когда число пакетов уже критично и далее следует переход в состояние отказа (либо connection, либо software);

– переход к отказу («transition to failure») – используется для упрощения схемы, являясь промежуточным состоянием между успешными атаками и отказом.

Вероятности переходов между состояниями могут задаваться исследователем либо в виде фиксированных чисел на основе собранной на практике статистики, либо в виде более сложных аналитических моделей. Например, авторами данной работы была использована математическая модель расчета вероятности успешной SYN-flood атаки на основе сетей Петри–Маркова, предложенная в [5]:

$$P(t) = 1 - e^{-\frac{t}{\tau}}, \qquad (1)$$

где $P(t)$ – вероятность успешной реализации атаки от времени t;

τ – среднее время перехода по всей сети Петри, равное в данном случае 11,15 с.

Разработанная имитационная модель может быть использована для исследования влияния различных способов структурного резервирования и методов защиты от атак на комплексные показатели надежности функционирования беспроводной сети связи, например на коэффициенты готовности $K_г$ и простоя $K_п$.

В таблице для примера приведены результаты моделирования функционирования системы.

Результаты моделирования функционирования беспроводной сети связи при различных методах резервирования и защиты

Вид воздействия	$K_г$ сети	Пропускн. способн.
Сканирование сети	1,000	1,000
Подмена устройства	0,999	0,990
Перехват пакетов	0,999	0,980
Отказ в обслуживании	0,998	0,950
Модификация сети	0,997	0,950
Вредоносные программы	0,997	0,950
Переполнение	0,997	0,950
Комплексная атака	0,995	0,900
Замирания	0,996	0,985
Атаки с учетом состояния радиоканала	0,994	0,884
Отказ элементов сети	0,997	0,994
Отказ сети с учетом всех воздействий	0,991	0,881

В заключение следует заметить, что наиболее острым вопросом данной имитационной модели остается выбор исходных данных для моделирования, в частности математических моделей для расчета вероятностей перехода из одного состояния в другое. По сути, от точности исходных данных будет во многом зависеть достоверность полученных результатов. В качестве исходных данных могут быть использованы результаты обработки накопленной статистики об отказах за определенный период времени, а также современные аналитические модели, подобные [5]. Причем в данной имитационной модели предусмотрена возможность отключения отдельных ветвей диаграммы состояний, что дает возможность исследовать последствия отдельных видов отказов и атак раздельно.

Литература

1. **Вишневский В. М. Портной С. Л., Шахнович И. В.** Энциклопедия WiMAX. Путь к 4G. М.: Техносфера, 2009. 472 с.
2. **Филин Б. П.** Методы анализа структурной надежности сетей связи. М.: Радио и связь, 1988. 208 с.
3. ГОСТ Р 53111-2008. Устойчивость функционирования сети связи общего пользования. Требования и методы проверки. М.: Стандартинформ, 2008. 16 с.
4. **Карпов Ю.** Имитационное моделирование систем. Введение в моделирование с AnyLogic 5. СПб.: БХВ-Петербург, 2005. 400 с.
5. **Радько Н. М., Скобелев И. О.** Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа. М.: РадиоСофт, 2010. 232 с.