МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

**(ФГБОУ ВО «КубГУ»)**

**Кафедра вычислительных технологий**

**КУРСОВАЯ РАБОТА**

**ИЗУЧЕНИЕ ПРИНЦИПОВ ОРГАНИЗАЦИИ АТАК НА AD-HOC СЕТИ И ИХ МОДЕЛИРОВАНИЕ**

Работу выполнила \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_Т.В. Карпова

Факультет компьютерных технологий и прикладной математики курс 3

Направление 02.03.02 - «Фундаментальная информатика и информационные технологии»

Научный руководитель

доц., канд. тех. наук, доц.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Т.А. Приходько

Нормоконтролер, преп., канд. тех. наук.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Е.Е. Полупанова

Краснодар 2017

СОДЕРЖАНИЕ

[ВВЕДЕНИЕ 3](#_Toc483031256)

[1 Виды атак на мобильные ad-hoc сети 4](#_Toc483031257)

[2 Архитектура Ad-hoc сети и сенсорного узла 7](#_Toc483031258)

[3 Построение модели сети 8](#_Toc483031259)

[4 Моделирование атак 11](#_Toc483031260)

[4.1 Моделирование DOS атаки 12](#_Toc483031261)

[4.2 Моделирование атаки Sybil 14](#_Toc483031262)

[4.3 Моделирование Sinkhole атаки 17](#_Toc483031263)

[ЗАКЛЮЧЕНИЕ 19](#_Toc483031264)

[СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 20](#_Toc483031265)

# ВВЕДЕНИЕ

Обеспечение безопасности в ad-hoc сетях является сложной задачей по следующим причинам:

* в такой сети более вероятна возможность прослушивания сообщений по сравнению с проводными сетями;
* также узлы могут свободно перемещаться и не находятся в физически защищенных местах, поэтому один из них может быть захвачен злоумышленником;
* в связи с отсутствием централизованного управления перехватить любую атаку сложно;
* в сетях широко распространены ошибки, связанные с изменениям конфигурации сети, внешней среды, следовательно, ошибки, обусловленные вредоносными действиями сложнее вычислить;
* батареи устройств, не должны быть слишком большими, поэтому решения в области безопасности должны быть энергоэффективными;
* ad-hoc сеть может состоять из тысячи устройств, механизмы, обеспечивающие безопасность должны быть масштабируемыми;
* в данной сети могут добавляться или удаляться устройства, в связи с этим требуется использование сложных алгоритмов маршрутизации, которые учитывали бы изменения топологии и вероятность появления некорректной информации.

Изучение принципов организации атак необходимо для выявления уязвимости сетей и разработки методов защиты информации с целью обеспечения безопасной работы.

# 1 Виды атак на мобильные ad-hoc сети

Атаки, направленные на ad-hoc сети можно разделить на три класса: целеориентированные (активные либо пассивные), ориентированные на направление (внутренние либо внешние), уровне-ориентированные (согласно модели OSI) рисунок 1.

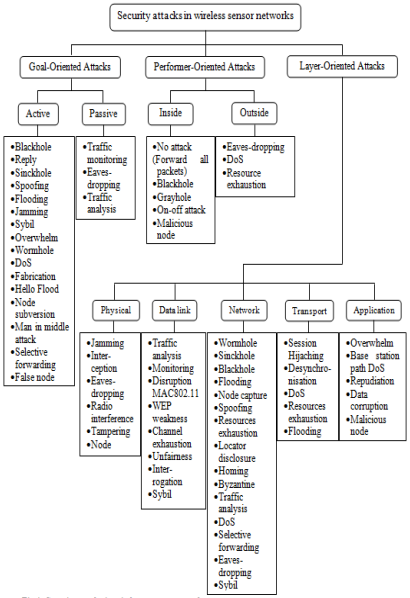


Рисунок 1 - Классификация видов атак на ad-hoc сети

В этой работе будем рассматривать только первый вид атак – целеориентированные.

Пассивные атаки подразумевают несанкционированное прослушивание сообщений. Атакующая сторона не прерывает работу сети, а только пытается узнать информацию, прослушивая трафик. Обычно такие атаки сложно обнаружить. Для активной атаки недоброжелатель должен проникнуть в произвольное сообщение сети, с целью перенаправления пакета, к атакующей стороне, например, для нарушения работы сети. Основное отличие активных атак от пассивных в том, что активные атаки могут быть обнаружены.

Активные атаки, в свою очередь, разделяют на шесть групп:

* + атаки выбрасывания пакетов;
  + атаки с использованием фальсификации;
  + атаки «червоточины»;
  + атаки, использующие модификацию полей протоколов сообщений;
  + спуфинг-атаки;
  + атаки постановки помех.

Суть атаки выбрасывания пакетов состоит в том, что злоумышленник выборочно или полностью выбрасывает пакеты, нарушая нормальную работу сети. Данные атаки можно подразделить на два типа:

* черная дыра: вредоносный узел анализирует протокол маршрутизации, далее узел объявляет себя знающим короткий маршрут до узла назначения, когда все пакеты доходят до вредоносного узла, он делает их выброс;
* серая дыра: отличается от предыдущей тем, что атакующий выбрасывает не все пакеты, а предварительно осуществляет их отбор, основанный на намерениях атакующего.

Атака с использованием фальсификации реализуется при помощи фальсификации сообщений и делится на три вида:

* фальсификация сообщений об ошибках маршрута: вредоносный узел может отправлять фальшивые сообщения о недоступности некоторого узла;
* направление испорченного содержимого кэша в DSR: с помощью протокола DSR сети могут изучать информацию о маршрутизации, прослушивая передачи на направлениях, к которым не имеют отношения, чтобы добавить информацию в собственный кэш, вредоносный узел может этим воспользоваться и испортить содержимое кэш-паияти;
* переполнение таблицы маршрутизации: вредоносный узел может создавать маршруты к несуществующим узлам, тем самым переполняя таблицу маршрутизации, что не позволит создавать новые маршруты к существующим узлам.

При атаке «червоточины» (wormhole attack) злоумышленник перехватывает пакеты от одного узла, и передает на другой отдаленный узел. Данная атака мешает протоколам маршрутизации правильно выстраивать маршруты между узлами.

При атаке с использованием модификации протокола сообщений злоумышленник изменяет поля в протоколах маршрутизации, нарушая при этом процесс передачи информации.

Атаки с использованием подделки идентификации (спуфинг) строятся на том, что узел-злоумышленник выдает себя за другой узел, нарушая при этом конфиденциальность. Для этого необходимо подменить свой IP или MAC адрес на адрес другого узла. Примером такой атаки может служить создание маршрутных петель, что в конечном итоге приведет к недоступности узлов. Другим примером спуфинг атаки является атака Сибилы (Sybil attack). С ее помощью узлы злоумышленника могут не только подделать идентификацию, но и доказать свою подлинность путем предоставления ложных удостоверений.

Атаки постановки помех широко распространены в беспроводных сетях, и приводят к засорению канала передачи различными помехами.

В данной работе будут промоделированы следующие атаки:

* атака Sybil;
* DOS атака;
* атака Sinkhole.

DOS (отказ в обслуживание) перегружает систему огромным количеством запросов, из-за этой атаки эффективность и производительность сети может быть уменьшена.

Атака Sinkhole основана на подмене узла назначения, и перенаправлении всех пакетов, адресованных ему узлу-злоумышленнику.

При проектировании беспроводной сети необходимо учесть обеспечение безопасности. Для расчета уровней риска угроз необходимо разработать методику с использованием экспертных оценок, учитывающих вероятность угроз и ущерб при реализации этих угроз. Получить оценки можно проделав анализ угроз и проведя их моделирование.

# 2 Архитектура Ad-hoc сети и сенсорного узла

На рисунке 2 приведена базовая архитектура Ad-hoc сети и отдельного узла (датчика) сети и топологию соединения узлов. Каждый датчик узла может передать информацию базовой станции по выбранному маршруту согласно протоколу маршрутизации AODV (для нашего эксперимента), по этому маршруту он может отправлять и получать данные. Сенсорный узел состоит из системы позиционирования, мобилайзера, собственно датчика (sensing unit), блока обработки информации и блок передачи (Transmission unit). Блок питания узла подает питание на блок датчиков. БС - базовая станция, с помощью которой выполняется сбор информации с датчиков сети.

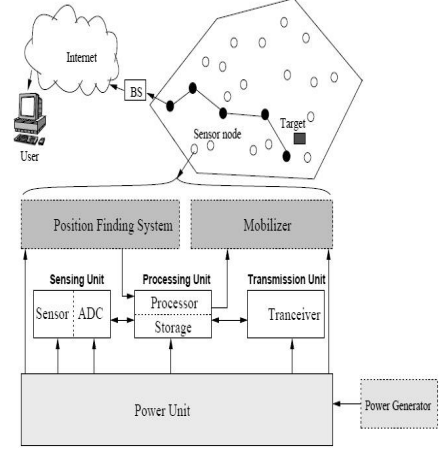


Рисунок 2 - Архитектура Ad-hoc сети и сенсорного узла

# 3 Построение модели сети

Используя средство моделирования NS2, можно промоделировать атаки в беспроводных ad-hoc сетях. NS2 создает копию сети в реальном времени. Этот симулятор стал одним из наиболее широко используемых средств моделирования с открытым кодом. Позволяет промоделировать сетевые атаки, протестировав сетевую безопасность. Конфигурацию эксперимента позволяет отобразить библиотека Nam, результаты эксперимента отображаются на графиках с помощью библиотеки Xgraph.

Постановка эксперимента отражена схемой на рисунке 3.

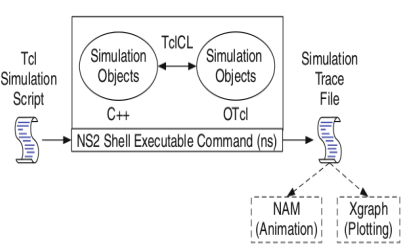


Рисунок 3 - Схема постановки эксперимента по моделированию атак.

Сначала необходимо сконфигурировать и настроить узлы, инициализировать объекты и файл трассировки (Simulation Trace File). Файл трассировки необходим для сбора информации о результатах моделирования для дальнейшего анализа результатов:

Для начала необходимо задать параметры узла, а также другие необходимые параметры: тип антенны, протокол маршрутизации, канал, очередь, MAC уровень и т.д:

set val(chan) Channel/WirelessChannel;

set val(prop) Propagation/TwoRayGround;

set val(netif) Phy/WirelessPhy;

set val(mac) Mac/802\_11;

set val(ifq) Queue/DropTail/PriQueue;

set val(ll) LL;

set val(ant) Antenna/OmniAntenna;

set val(ifqlen) 50;

set (nn) 10;

set (rp) AODV;

#set (rp) DSR;

set val(x);

set val(y);

set val(energymodel) EnergyModel;

set val(initialenergy) 100;

set src [lindex $argv 0]

set deat [lindex $argv 1]

set malicious [lindex $argv 2]

Далее нужно создать новый объект класса Simulator, в котором содержатся все методы необходимые для дальнейшего описания модели:

#Instialize Global Variables

set ns\_ [new Simulator]

set tracefd [open tracesh.tr w]

$ns\_ trace-all $tracefd

Затем откроем файл, который будет использоваться для записи выходных результатов моделирования для использования в nam:

set namtrace [open al.nam w]

$ns\_ namtrace-all-wireless $namtrace $val(x) $val(y)

Далее необходимо настроить топологию сети и установить значение сконфигурированных параметров:

set topo [new Topography]

$topo load\_flatgrid $val(x) $val(y)

create-god $val(nn)

set chan\_1 [new $val(chan)]

$ns\_ node-cofig

-adhocRouting $val(rp)\

-llType $val(ll)\

-macType $val(mac)\

-ifqType $val(ifq)\

-ifqLen $val(ifqlen)\

-antType $val(ant)\

-propType $val(prop)\

-phyType $val(netif)\

-topoInstance $topo \

-agentTrace ON \

-routerTrace ON\

-macTrace ON \

-movementTrace OFF\

# 4 Моделирование атак

Любой узел, создаваемый в NS2 можно сделать вредоносным. Для этого необходимо при генерации узла добавить следующий код:

$ns at 50.0 "[$node\_ (30) set ragent\_] malicious"

Для настройки такого узла необходимо добавить некоторые строки в встроенный в NS2 файл с открытым кодом AODV.cc:

#Attack

if ( strcmp(argv[1], “malicious”) ==0) {

malicious=true;

return TCL\_OK;

}

//malicious code

if (malicious==true){

drop(p,DROP\_RTR\_ROUTE\_LOOP)

}

Данный код является общим для всех моделируемых атак.

## 4.1 Моделирование DOS атаки

DOS атаки имеют отличие от других атак, так как их целью не является получение доступа к информации. Их задача вывести из строя сеть, перегрузив ее огромным количеством запросов или сообщений. Они могут использоваться как вспомогательные атаки, чтобы сначала вывести из строя сеть, а затем проникнуть в нее для получения доступа к необходимой информации. DOS атаку трудно предотвратить, для борьбы с ней необходимо перекрывать или фильтровать ненужный трафик.

Скрипт для моделирования DOS атаки:

set udp\_(1) [new Agent/UDP]

$ns attach-agent $node(0) $udp\_(1)

Эти строки создают CBR агент и прикрепляют его к вредоносному узлу 0 (CBR - 'constant bit rate' - источник данных с постоянной скоростью). Интервал между отсылкой пакетов устанавливается равным 0.005 секунды (т.е. 200 пакетов в секунду):

set cbr\_(1) [new Application/Traffic/CBR]

$cbr\_(1) set interval\_ 0.005

$cbr\_(1) set random\_ 1

$cbr\_(1) set maxpkts\_ 10000

$cbr\_(1) attach-agent $udp\_(1)

Следующие строки создают Null агент, который работает как приемник трафика, и прикрепляют его к узлу назначения:

set null\_(1) [new Agent/Null]

$ns attach-agent $node(15) $null\_(1)

Далее необходимо соединить узлы между собой.

$ns connect $udp\_(1) $null\_(1)

$ns at 7.0 "$cbr\_(1) start"

$ns at 10.0 "$cbr\_(1) stop"

На рисунке 4 представлен результат работы выше приведенного скрипта.

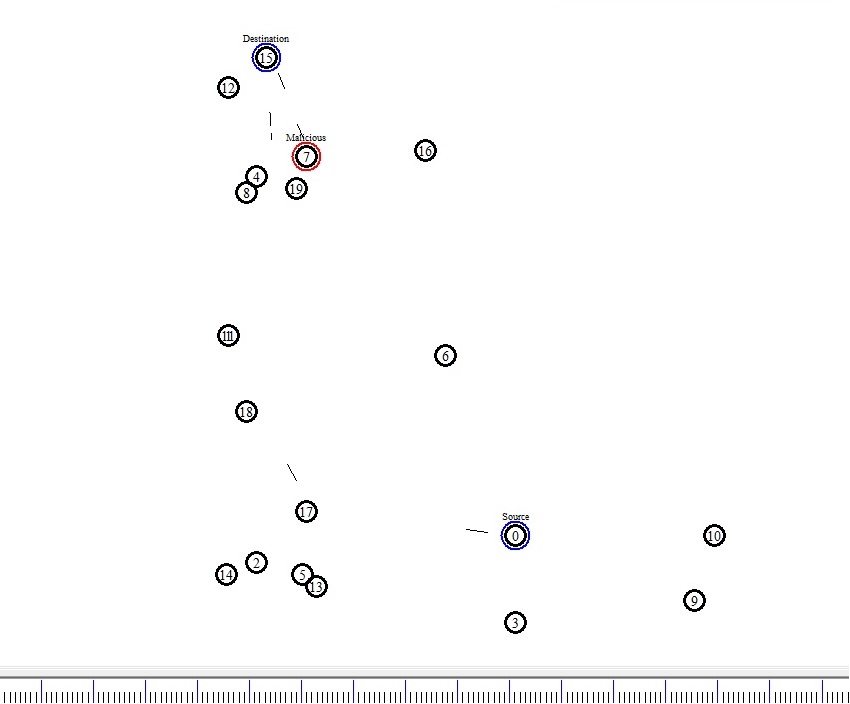


Рисунок 4 – Анимация атаки DOS в симуляторе

Здесь узел 15 является узлом назначения, узел 0 исходный узел. Вредоносный узел 7 посылает огромное количество пакетов в узел назначения, так как буфер узла ограничен через некоторое время узел начнет отбрасывать пакеты из вредоносного узла, а также из исходного узла 0, что приведет к потере информации и ухудшит обслуживание сети.

Для анализа, проведенного моделирования атаки изобразим результаты графически, с помощью визуализатора TraceGraph.

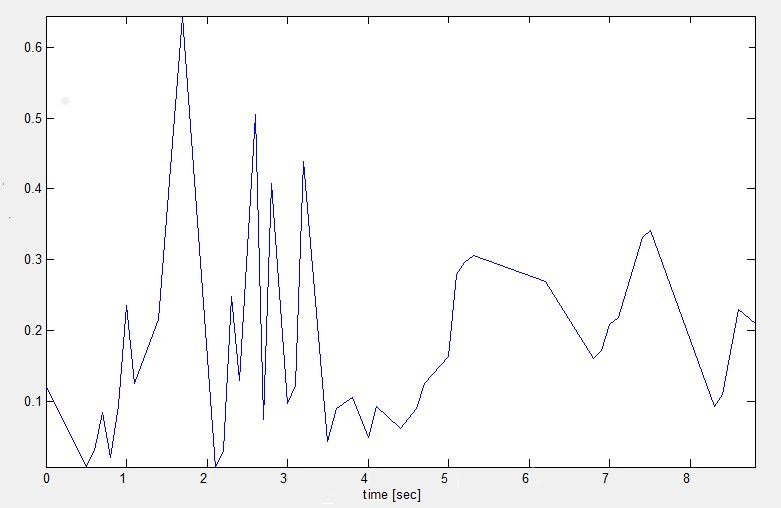
На рисунке 5 показано поведение трафика на узле 15. После того, как вредоносный узел 7 начинает отправлять на узел назначения огромное количество пакетов, трафик резко поднимается, далее узел 15 начинает отбрасывать приходящие пакеты, и трафик падает.

Рисунок 5 – Потери трафика

На рисунке 5 x – ось времени, время моделирования задано в секундах, а ось у – количество приходящего в узел назначение трафика в Мбит/с.

## 4.2 Моделирование атаки Sybil

Атака Sybil – одна из самых вредоносных и опасных атак в беспроводных сетях. Атакующий узел может получить IP-адрес или Mac-адрес некоторого узла сети или нескольких узлов, для того чтобы присвоить его себе и выдать себя за этот узел. Таким образом, он может украсть какие-либо данные, либо отбрасывать приходящие ему сообщение, что приведет к нарушению работы сети. Также данная атака может подорвать децентрализованность сети.

Скрипт для моделирования атаки:

Эти строки создают Null агент, работающий как приемник трафика и прикрепляют его к узлу назначения 6:

set null\_ [new Agent/Null]

$ns attach-agent $n(6) null\_

Далее создается UDP агент и прикрепляется к исходному узлу:

set udp\_ [new Agent/UDP]

$ns attach-agent $n(3) $udp\_

Затем создаем CBR агент. Устанавливается интервал между отсылкой пакетов, равный 0.2 секунды, и их максимальное количество:

set cbr\_ [new Application/Traffic/CBR]

$cbr\_ set interval\_ 0.2

$cbr\_ set random\_ 1

$cbr\_ set maxpkts\_ 100

Эти строки соединяют узлы между собой и определяют, что пакеты будет передаваться в узел назначения с 0.5 по 10.0 секунды симуляции:

$ns connect $udp\_ $null\_

$ns at 0.5 "$cbr\_ start"

$ns at 10.0 "$cbr\_ stop"

Далее для наглядности добавим к узлу назначения и исходному узлу информацию о них:

$ns at 0.0 "n(3) label Source"

$ns at 0.0 "n(6) label Destination"

Рисунок 6 показывает моделирование атаки Sybil. Узел 3 действует как источник, а узел 6 является узлом назначения. Исходный узел начинает отправлять пакеты в узел назначения через самый короткий путь, который найден протоколом маршрутизации. Промежуточный узел 17 действует как вредоносный узел и на 0.8 секунде симуляции, начинает отбрасывать пакеты, прибывающие из узла 3, и информация не доходит до узла назначения.

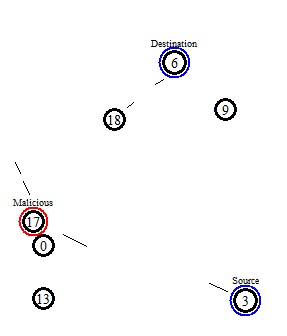


Рисунок 6 – Анимация Sibil атаки в симуляторе

Более наглядно это можно увидеть на графике изображенном на рисунке 7. Данный график показывает трафик в Мбит/с приходящий на узел назначения 6(ось у), на они х указано время симуляции в секундах. Видно, что на 0.8 секунде происходит резкое сокращение приходящего трафика, в связи с тем, что вредоносный узел начинает отбрасывать пакеты, предназначенные для узла назначения 6.

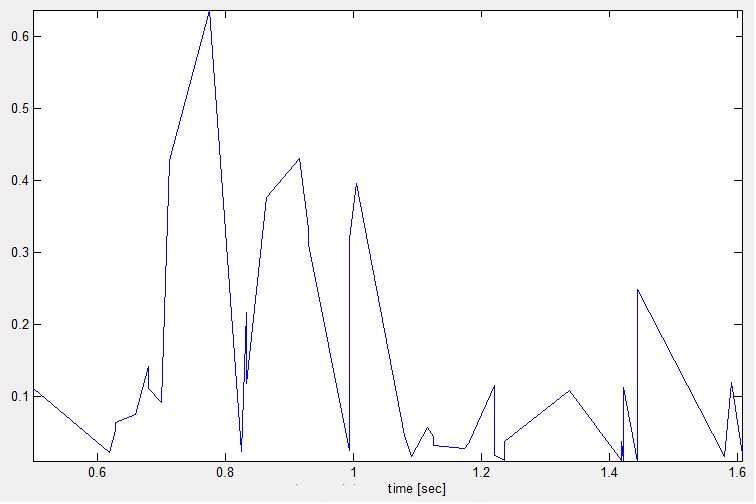


Рисунок 7 – Динамика трафика на узле назначения

## 4.3 Моделирование Sinkhole атаки

Беспроводные сети состоят из множества узлов. Работа сети может быть организована следующим образом: один узел отправляет собранные по всей сети данные в некоторую станцию для обработки. Атака Sinkhole чаще всего бывает замечена именно в таких случаях. Это серьезная угроза узлу, объединяющему сеть. Вредоносный узел помещается как можно ближе к узлу назначения, чтобы притянуть весь возможный максимальный трафик сети. Он заменяет узел назначения и другие, близкие к нему узлы. Для этого, в начале атакующий узел собирает информацию о соседних узлах.

Скрипт для моделирования данной атаки:

set tcp [new Agent/TCP]

set sink[new Agent/TCPSink]

$ns attach-agent $n(13) $tcp

$ns attach-agent $n(15) $sink

$ns connect $tcp $sink

set ftp [new Application/FTP]

$ftp attach-agent $tcp

$ns at 0.8 "$ftp start"

$ns at 10.0 "$ftp stop"

Узел 9 - исходный узел, узел 13 становится узлом назначения, и узел 15 назначен вредоносным узлом. Вредоносный узел притягивает весь максимальный возможный трафик в сети. Все пакеты, отправляемые от источника, отправлены во вредоносный узел вместо узла назначения, это можно увидеть на рисунке 8.

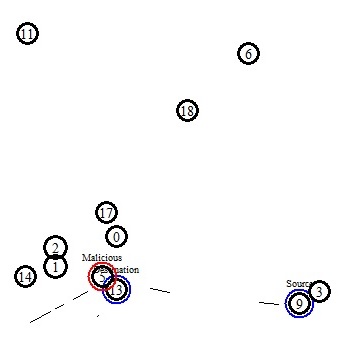


Рисунок 8 – Анимация атаки Sinkhole в симуляторе

# ЗАКЛЮЧЕНИЕ

Беспроводная сеть является источником повышенного риска несанкционированного доступа. Проникнуть в беспроводную сеть значительно проще, чем в обычную. Достаточно просто оказаться в зоне приема сигнала. Разница в безопасности проводных и беспроводных сетей в безопасности физического и MAC уровней.

На сегодняшний день используется сложные модели аутентификации, шифрование данные, контроль целостности их передачи, но тем не менее, вероятность доступа к информации злоумышленников весьма существенна.

В работе были рассмотрены одни из наиболее распространённых атак: DOS, Sybil, Sinkhole.

Была построена модель беспроводной сети, и смоделированы атаки. По результатам моделирование были построены графики, отображающие поведение трафика во время атак. Проведенный анализ может быть использован в качестве одного из показателей при проектировании сети. Следует учесть, что данные показатели не являются единственными критериями при обеспечении информационной безопасности беспроводных сетей.

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Датьев И.О., Павлов А.А. Моделирование беспроводных многошаговых самоорганизующихся мобильных сетей // Вестник Кольского научного центра РАН – 2016 - №1 (24) - С.116-126.
2. Датьев И.О., Павлов А.А. Протоколы маршрутизации в беспроводных сетях // Труды Кольского научного центра РАН - 2014 - №5 (24) - С.64-75.
3. Хоров Е.М. Знакомство с современными беспроводными технологиями. Многошаговые беспроводные сети: принципы построения и открытые задачи// Статья подготовлена в рамках работ по гранту Министерства образования и науки – 2012. – С. 6.
4. Network Simulator (Сетевой симулятор ns2) [Электронный ресурс]// URL: [telematika1.stu.neva.ru/FILES/KAFEDRA/STUDENTS/POSOBIE/ns-old-html/ns-old.htm#\_Toc464631228](http://telematika1.stu.neva.ru/FILES/KAFEDRA/STUDENTS/POSOBIE/ns-old-html/ns-old.htm#_Toc464631228) (дата обращения: 25 апреля 2017).
5. Климов И. А., Червинская Н. В. Сравнение протоколов маршрутизации для беспроводных мобильных ad-hoc сетей// ГВУЗ «Донецкий национальный технический университет» - Статья – С. 5.
6. Астраханцев А.А., Горбань С.М. сравнительный анализ эффективности протоколов маршрутизации в ad-hoc сетях// Статья - Харьковский национальный университет радиоэлектроники – 2013. – С. 4.
7. Cordeiro Carlos De Morais Ad Hoc & Sensor Networks: Theory and Applications // AgrawalWorld Scientific - 2006. – 641 С.
8. Chelli K. Security Issues in Wireless Sensor Networks:Attacks and Countermeasures // Proceedings of the World Congress on Engineering. – 2015. – С.234.
9. Singh T., Gandotra A. Replication of attacks in a wireless sensor network using ns2 // International Journal of Research in Engineering and Technology. – 2012. – С. 47.