УДК 004.056.53 (004.733)

Т.А. Гришечкина

АНАЛИЗ АТАК НА СЕТЕВЫЕ ПРОТОКОЛЫ В МОБИЛЬНЫХ СЕНСОРНЫХ СЕТЯХ AD HOC*

Работа посвящена анализу атак на сетевые протоколы в мобильных сенсорных сетях ad hoc с использованием различных моделей и методов. Рассмотрены особенности строения и характеристики данных сетей как объектов информационной безопасности и объектов атак и на основании этого приводятся различные выявленные уязвимости и типы атак, применимые к сетевым протоколам. Рассматривается вероятное дальнейшее поведение атакующего и, следовательно, направление дальнейшего развития атаки. Показана роль требований к информационной безопасности, предъявляемых к беспроводным самоорганизующимся сетям. В конце статьи делаются выводы о целесообразности развития новых методов защиты информации в данных сетях.

Мобильные сенсорные сети ad hoc; беспроводные сети; сети MANET; информационная безопасность; типы атак.

T.A. Grishechkina

ANALYSIS OF ATTACKS IN MOBILE AD HOC NETWORKS USING VULNERABILTIES IN NETWORK PROTOCOLS

The paper is intended to analyze attacks in mobile ad hoc networks using vulnerabilities in network protocols with the use of different models and methods. Structure and characteristics of Ad-Hoc networks as information security objects and targets of attack are analyzed. Based on the results of that analysis, different discovered vulnerabilities and methods of attack on network protocols used in such networks are given. In sight of discovered vulnerabilities, further possible behavior of attacker and prospective objects of attacks are considered. Role of information security requirements for ensuring security of wireless Ad-Hoc networks are shown. In the end, conclusions about the need for development of new information security methods for these networks are provided.

Mobile ad hoc networks; wireless networks; MANET; information security; attack type.

При переводе с латинского языка словосочетание «Ad hoc»означает выражение «для данного случая, как сложилось». В технической литературе по сетям наиболее точным переводом, отражающим суть термина, можно считать перевод – «эпизодическая» сеть. Мобильные сенсорные сети Ad hoc (или MANET-сети) представляют собой беспроводные сети передачи данных, ограниченные пропускной способностью и зоной радиовидимости беспроводной связи, где каждый узел может выполнять функции маршрутизатора и принимать участие в ретрансляции пакетов. Узлом такой сети может быть ноутбук, КПК, мобильный телефон или любое другое мобильное устройство, которое может связываться с другими устройствами. Топология сети будет меняться в течение времени, поскольку узлы не только могут добавляться или отсоединяться, но и могут изменять свое местоположение. Сеть создается, управляется и организуется лишь самими узлами без помощи какой-либо централизованной системы или фиксированной инфраструктуры. Следовательно, платформой сети является само взаимодействие между узлами, на которых эта сеть построена. Узел не только использует сеть для обмена данными с другими узлами, но и поддерживает саму сеть путем выполнения функций маршрутизации. Узел, который хочет связаться с другим узлом, находящимся вне зоны его видимости, взаимодействует с промежуточными узлами для передачи

* Работа выполнена при поддержке гранта РФФИ №12-07-92693-ИНД_а.

своих пакетов. Если сравнивать централизованные сети с сетями MANET, то можно сказать, что у последних имеются явные преимущества, так как они легко могут устанавливаться и демонтироваться, поскольку не имеют фиксированной привязки. На рис. 1 предоставлен пример сети MANET, где каждый узел предоставлен мобильным устройством с обозначенным радиусом радиоохвата.

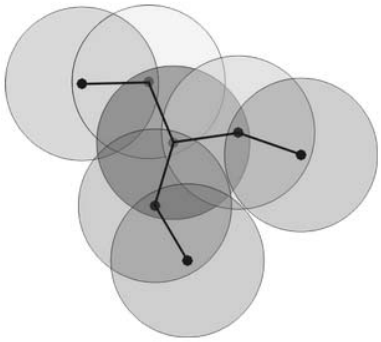

Рис. 1. Структура сети MANET

Сеть MANET является привлекательным и экономически эффективным решением для обеспечения связи в тех районах, где ненадежна или вовсе отсутствует фиксированная инфраструктура. Таким образом, подобные сети обладают большой привлекательностью для применения их во время военных действий, в силовых структурах, в структурах МЧС (особенно при поисково-спасательных операциях) и в системах транспорта. Так как у сети отсутствует централизованное управление, то они максимально подходят для военных и коммерческих сетей, требующих большой надежности [1]. Помимо работы в качестве автономных сетей, сети ad hoc могут быть также подключены к Интернету или другим сетям, тем самым расширяя свои возможности.

Хотя у технологии построения сетей MANET широкий спектр областей применения, вопрос об обеспечении безопасности в ней все еще актуален. Так как мобильные устройства объединены в сеть при помощи беспроводных технологий, передача информации и личные данные абонентов более уязвимы по сравнению с фиксированными устройствами проводной сети. Кроме того, решения, найденные для проводных сетей не так просто адаптировать для беспроводных.

Основными характеристиками мобильных одноранговых ad hoc сетей являются [1]:

1. *Беспроводные соединения*: узлы в пределах своего радиодиапазона общаются друг с другом при помощи беспроводных линий связи. Соединения между узлами могут иметь различную пропускную способность так как не регламентировано количество радиоинтерфейсов, каждый из которых может иметь различную мощность приема/передачи и функционировать в различных частотных диапазонах.
2. *Динамическая сетевая топология*: в сети могут появляться новые и удаляться существующие узлы, кроме того все узлы мобильны, то есть могут свободно перемещаться, создавая новые соединения.
3. *Мобильность*: устройства могут свободно перемещаться из одного места в другое. По скорости перемещений их разделяют на «сверхмобильные» (когда узлом становится устройство, находящееся внутри движущегося транспорта) и «относительно статические» (когда узлом связи становится мобильное устройство, использующееся либо на малой скорости, либо вообще неперемещаемое).

4. *Ограниченность используемых ресурсов*: так как сеть состоит из мобильных устройств, то каждый узел на сети не обладает сложными вычислительными ресурсами, большими объемами оперативной памяти и ограничен в пропускной способности.
5. *Отсутствие центрального узла*: на сети нет центрального управляющего узла или сервера для координации узлов.
6. *Отсутствие фиксированной инфраструктуры*: вся инфраструктура не фиксирована и поддается более простой настройке.
7. *Отсутствие постоянного электропитания*: мобильные узлы используют в своей работе электропитание, предоставляемое аккумулятором, который истощается в течение долгого времени и должен быть перезаряжен.
8. *Разнородность*: каждый узел в сети может отличаться от другого узла по таким параметрам, как вычислительные ресурсы, батареи и мобильность благодаря тому, что сеть может включать в себя различное мобильное оборудование, как, например, сотовые телефоны, КПК, ноутбуки и т.д.
9. *Самоорганизация*: сеть создается и управляется лишь самими узлами, автономно проверяя работоспособность и определяя собственные параметры конфигурации, такие как, например, адресация, маршрутизация, положение идентификации и управления питанием.
10. *Сотрудничество*: все узлы сети из-за отсутствия вспомогательных узлов вынуждены сотрудничать друг с другом для управления сетью. Таким образом каждый узел сети не только использует сеть в качестве абонента, но и поддерживает маршрутизацию сообщений по сети до других узлов.

Обеспечение безопасности в ad hoc сетях является сложной задачей в силу следующих причин [2]:

1. *Уязвимость каналов*: в любой беспроводной сети в связи с общедоступной средой передачи намного больше вариантов прослушивания и подкладывания в каналы сообщений по сравнению с проводными сетями. Узлы, принадлежащие злоумышленникам, могут осознанно изменять, удалять, подделывать, добавлять и перехватывать как управление так и данные трафика, создавать наплывы ложных сообщений, и, вообще уклоняться от выполнения используемых протоколов.
2. *Уязвимость узлов*: узлы свободно перемещаются и не находятся при этом в физически защищенных местах, что может привести к захвату одного из них злоумышленником. Таким образом, необходимы меры для того, чтобы препятствовать подмене узлов.
3. *Отсутствие центральной инфраструктуры*: из-за того, что один узел может контролировать лишь небольшую группу соседних узлов, любую атаку становится сложно перехватить. Кроме того, классические системы безопасности, такие как центры сертификации и центральные серверы неприменимы для данных сетей.
4. *Самостоятельность узлов*: в данной сети сложно обнаружить самостоятельную деятельность. Любой узел может отказаться от совместной работы для того, чтобы сохранить мощность и избежать перегрузок.
5. *Системные ошибки*: такие ошибки, как постепенное замирание, потеря пакетов, блокировки и перегрузки широко распространены на сетях связи. Таким образом, ошибки, связанные с вредоносными действиями, будет сложнее вычислить.
6. *Ограниченная вычислительная способность*: сложные криптографические алгоритмы не могут быть применимы из-за ограниченных вычислительных возможностей сети. Их применение могло бы привести к незначительным задержкам на сети. Против узлов, обладающими с малыми вычислительными ресурсами может применяться DoS-атака.

7. *Ограниченная мощность*: верхний предел, которым ограничивается мощность батареи мобильного устройства, не должен быть слишком большим, так как это может привести к ее неприменимости. Таким образом, решения в области безопасности должны быть энергоэффективными.
8. *Динамически изменяющаяся топология*: так как в данную сеть не только могут добавляться новые мобильные устройства и удаляться существующие, то требуется использование сложных алгоритмов маршрутизации, которые учитывали бы изменение топологии и вероятность появления некорректной информации, поступающей от скомпроментированных узлов.
9. *Большая сеть*: сеть ad hoc может состоять из сотен или даже тысяч узлов. Механизмы, обеспечивающие безопасность, должны быть масштабируемы для того, чтобы справиться с такой большой сетью.

Исходя из этих причин, можно предположить, что атаки, применимые против сетей ad hoc, как правило, делятся на два класса: пассивные и активные. Хотя они могут быть запущены на разных уровнях стека протоколов, мы рассмотрим в основном атаки, касающиеся сетевого уровня.

При совершении пассивной атаки, злоумышленник не вмешивается в процесс маршрутизации, а прослушивает пересылаемый трафик, извлекая ценную информацию о топологии сети, примерном расположении узлов, взаимодействии между узлами и т.д. Например, если узел злоумышленника заметит, что один узел сети запрашивается чаще остальных, то вероятно будет сделан вывод о ценности этого узла для функционирования сети. После данного анализа, злоумышленник может переключиться от пассивных действий к активным и совершить попытку атаковать сеть с целью вывести данный узел из строя, что приведет к частичному или полному разрушению сети. С другой стороны, он может передать информацию сообщнику, который и запустит атаку. От данного типа атаки сложно защититься и его практически невозможно обнаружить. При пассивных атаках злоумышленником не затрагиваются доступность и целостность сети, но зато нарушается конфиденциальность.

А вот при совершении активной атаки, узлы злоумышленника могут вмешаться в функциональность протоколов маршрутизации путем изменения полей сообщений управления, информации о направлении, перенаправления сетевого трафика или запустив атаку отказа в обслуживании (DoS-атаку).

В основном, активные атаки на протоколы маршрутизации ad hoc сетей можно разделить на различные группы [3]:

1. Атаки выбрасывания пакетов.
2. Атаки с использованием фальсификации.
3. Атаки «червоточины».
4. Атаки, использующие модификацию полей протоколов сообщений.
5. Спуфинг-атаки.
6. Атаки постановки помех.

Атаки выбрасывания пакетов. В данном типе атаки злоумышленник выборочно или полностью выбрасывает пакеты, нарушая нормальную работу сети. В зависимости от модели, данная атака может быть далее разделены на два типа:

I. *Черная дыра*: для проведения данной атаки, узел злоумышленника сперва анализирует протокол маршрутизации, используя пассивные атаки прослушивания сетевого трафика. Далее, на этапе открытия направления протокола маршрутизации, узел злоумышленника объявляет себя знающим точный и короткий путь к необходимому узлу для того, чтобы иметь возможность перехватывать пакеты. Наконец, когда все пакеты до необходимого узла передаются к узлу атакующего, он осуществляет их выброс.

Данная атака ухудшает доступность, так как после ее проведения на сети начинают использоваться неоптимальные маршруты. Конфиденциальность нарушается из-за того, что злоумышленник пожжет перед выбросом прослушать весь целевой трафик, идущий к целевому узлу.

II. *Серая дыра*: данная атака отличается от предыдущей тем, что атакующий выбрасывает не все пакеты, а предварительно осуществляет их отбор на те, которые он перешлет далее и на те, которые будут выброшены [4]. Решения принимаются основываясь на намерениях атакующего. Данную атаку довольно сложно обнаружить потому что выброс пакетов может быть связан не только с действиями атакующего, но и с обрывами, зависящими от перегруженности узлов.

Атаки с использованием фальсификации. Такой тип атак реализуется при помощи фальсификации сообщений и его можно разделить на следующие три вида:

I. *Фальсификация сообщений об ошибках маршрута*: у протоколов AODV и DSR есть меры технического обслуживания по сохранению неустойчивых маршрутов в то время, как образующие их узлы перемещаются или недостижимы. Если узел назначения или промежуточный узел движется вдоль активного пути или попытки соединения с ним неудачны, то узел, предшествующий обрыву соединения, рассылает сообщение об ошибке маршрута всем активным соседним узлам. После этого узлы в своих таблицах маршрутизации удаляют маршрут к неработающему узлу. Узел злоумышленника может запустить атаку отказа в обслуживании против легитимного узла, рассылая ложные сообщения о его недоступности.

II. *Направление испорченного кэша в DSR*: при помощи протокола DSR узлы сети могут изучать информацию о маршрутизации, прослушивая передачи на направлениях, к которым не имеют отношения. Узел добавляет эту маршрутную информацию в свой собственный кэш. Злоумышленник может воспользоваться этим методом изучения маршрутов и испортить данный кэш. Например, если узел злоумышленника M узел хочет начать DoS атаку против узла X, он должен просто передавать поддельные пакеты с исходными маршрутами к узлу X через себя. Любые другие соседние узлы, прослушивающие передачу пакета, могут добавить данный путь в свой кэш.

III. *Переполнение таблицы маршрутизации*: узел злоумышленника может создавать маршруты к несуществующим узлам. Смысл этой атаки заключается в создании такого множества маршрутов, которое не позволит создавать новые маршруты из-за переполнения таблиц маршрутизации узлов. Данная атака наносит урон критерию доступности из-за того, что существующие на сети таблицы маршрутов начинают хранить неактуальную информацию.

Атаки «червоточины» (wormhole attack). При таком типе атаки, атакующий перехватывает пакеты от одного узла сети и посредством туннеля передает их в другой отдаленный узел сети [5]. Данная атака препятствует протоколам маршрутизации, использующимся в сети (таким как DSR и AODV), правильно выстраивать маршруты между узлами, находящимися на расстоянии в один или нескольких узлов.

Атаки с использованием модификации протокола сообщений. Текущие протоколы маршрутизации предполагают совместное использование беспроводной среды, так что узлы не изменяют поля протокола сообщений, передаваемых между ними. Пакеты протокола маршрутизации несут важную информацию управления, определяющую режим передачи данных в ad hoc сетях. Узлы зло-

умышленников или узлы, подверженные риску быть захваченными злоумышленниками, могут принимать непосредственное участие в открытии нового маршрута, а также в перехвате и фильтрации пакетов протокола маршрутизации, нарушая при этом процесс передачи информации. Благодаря видоизменению полей в протоколах маршрутизации, узды злоумышленников могут стать причиной перенаправления сетевого трафика и DoS атак. Например, на рис. 2 узел злоумышленника X, изменяя пакеты управления может объявлять более короткий маршрут к узлу D, чем существующий маршрут у данному узлу, который объявляется узлом B. Таким образом, узел X может добиться успеха в прослушивании трафика, проходящего через него или препятствовать его прохождению к узлу D.

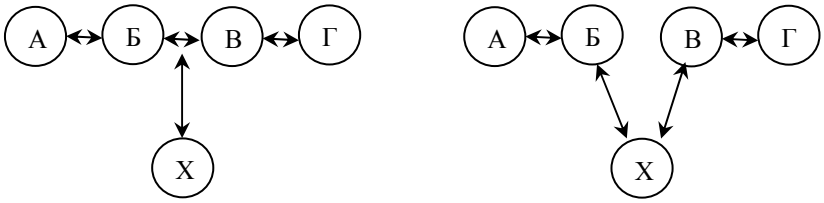

Рис. 2. Атака с использованием модификации протокола сообщений

Атаки могут быть классифицированы как атаки удаленной переадресации и атаки отказа в обслуживании.

I. *Удаленная переадресация с измененным порядковым номером маршрута dest_sequence_#*: данная атака возможно благодаря таким протоколам, как протокол вектора расстояния по запросу AODV [6], который конкретизирует и утверждает маршруты, задавая определенные последовательные номера для маршрутов и записей в таблице маршрутизации на пути к определенной цели. В протоколе AODV любой узел может переключить трафик через себя, объявив маршрут к узлу с большим последовательным номером пункта назначения dest_sequence_#, чем есть на самом деле. Таким образом, узел злоумышленника может перехватывать все сообщения к интересующему его узлу сети.

II. *Переадресация с модификацией параметра hop_cnt*: в таких протоколах, как AODV, длина маршрута представлена параметром hop_cnt в пакете запроса маршрута RREQ. Объявляя кратчайший маршрут (самое минимальное значение параметра hop_cnt) к определенному месту назначения, узел злоумышленника может добиться успеха в переключении через себя всего трафика до целевого узла. Как только он расположится между двумя взаимодействующими узлами, то сможет производить атаки выбрасывания пакетов, DoS-атаки или же использовать свое положение в качестве первого шага атаки man-in-the-middle.

III. *Отказ в обслуживании с модификацией исходного маршрута*: благодаря таким протоколам динамической маршрутизации источника как DSR [7], маршрутизация от луча к лучу определяется с использованием маршрутизации источника пакетов данных. Если проверка целостности маршрутизации источника отсутствует, узел злоумышленника может создавать на сети петли или запускать атаку отказа в обслуживании.

Атаки с использованием подделки идентификации (спуфинг). Данный тип атаки строится на том, что узел злоумышленника выдает себя за другой узел, нарушая при этом конфиденциальность [8]. Для этого необходимо исказить свою идентичность путем замены своего IP или MAC адреса на адрес другого узла. После того, как подмена идентификации произошла, узел злоумышленника может,

например, объявить о неправильной маршрутизации с другими узлами сети. Очевидным примером такой атаки сможет служить создание маршрутных петель, что в конечном итоге приведет к недоступности узлов или разделению сети.

Другим примером спуфинг атаки является атака Сибилы (Sybil attack). С помощью нее узлы злоумышленника могут не только подделывать идентификацию, но и доказывать свою подлинность путем предоставления ложных удостоверений. При осуществлении такой атаки могут создаваться ложные удостоверения о надежности определенного узла для привлечения к нему больших объемов трафика.

Атаки постановки помех. Данная атака широко распространена в сетях связи с беспроводной средой передачи данных и приводит к засорению канала передачи разного рода помехами, производимыми злоумышленниками. При удачном проведении атаки не нарушается конфиденциальность и целостность передачи сообщений, но понижается доступность узлов сети.

Очевидно, что в мобильных сенсорных сетях ad hoc решение задач информационной безопасности имеет существенные различия от традиционных решений, связанных с фиксированной инфраструктурой. После проведенного анализа видно, что на защищенность влияет несколько особенностей: отсутствие инфраструктуры, незащищенность беспроводных каналов и наличие маломощных и слабозащищенных устройств. Рассмотренные атаки выявляют уязвимости в протоколах AODV и DSR, поэтому требуются новые методы защиты информации для обеспечения безопасной работы.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Миночкин А.И., Романюк В.А.* Методология оперативного управления мобильными радиосетями // Зв'язок. – 2005. – № 2. – С. 53-58.
2. *Аманжолова С.Т., Медведев С.А.* Протоколы маршрутизации в беспроводных mesh-сетях // Журнал студенческих научных работ КазНТУ. – 2011. Электронный ресурс. URL: http://portal.kazntu.kz/files/publicate/2012-04-27-1899_0.pdf (дата обращения 23.10.2012).
3. *Gupte S., Singhal M.* Secure routing in mobile wireless ad-hoc networks, Ad Hoc Netw. – 2003. – № 1. – P. 151-174.
4. *Priyanka Goyal, Vinti Parmar, Rahul Rishi.* MANET: Vulnerabilities, Challenges, Attacks, Application, IJCEM International Journal of Computational Engineering & Management. – 2011. – Vol. 11. – P. 32-37.
5. *Иващук И.Ю.* Предотвращение wormhole атак в беспроводных сетях с помощью пакетных меток // Научно-технический вестник СПбГУ ИТМО. – 2008. – № 52. – С. 188-194.
6. *Perkins C.E., Royer E.M.* Ad-hoc on-demand vector routing, in: Proceedings of Second IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, February 1999, – P. 90-100.
7. *Johnson D.B., Maltz D.A.* Dynamic source routing in ad hoc wireless networks, in: Mobile Computing, Kluwer Academic Publishers, 1996. – P. 153-181.
8. *Весельская О.М.* Обеспечение безопасности в самоорганизующихся беспроводных сетях // Материалы X Международной научно-технической конференции «Авиа-2011». – Киев, 2011. – С. 80-83.

Статью рекомендовал к опубликованию к.ф.-м.н. Л.И. Кренов.

Гришечкина Татьяна Андреевна – Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Южный федеральный университет»; e-mail: taonix@mail.ru; 347928, г. Таганрог, ул. Чехова, 2; тел.: 88634371905; кафедра безопасности информационных технологий; инженер.

Grishechkina Tatiana Андреевна – Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education "Southern Federal University"; e-mail: taonix@mail.ru; 2, Chekhova street, Taganrog, 347928, Russia; phone: +78634371905; the department of security in data processing technologies; postgraduate student.