УДК 681.3:004.56.55

О. М. Весельская, ассистент
(Национальный авиационный университет, Украина)

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ В САМООРГАНИЗУЮЩИХСЯ БЕСПРОВОДНЫХ СЕТЯХ

В данной статье рассмотрены беспроводные самоорганизующиеся сети, основные типы атак, проводимые на них и методы повышения безопасности. Выявлены максимально возможные на сегодняшний день средства и методы защиты для обеспечения безопасности в данных сетях.

В последнее время невероятно быстро развиваются беспроводные сети (БС) передачи информации. По пропускной способности они не уступают выделенным медным линиям. Помехоустойчивость, надежность и защищенность современных протоколов передачи сделали БС передачи информации явлением повсеместным, а оборудование для них – массовым продуктом. Бесспорным лидером на рынке продуктов для БС является оборудование, отвечающее стандартам IEEE 802.11. В данной работе приведена классификация БС стандарта IEEE 802.11, основное внимание будет уделено беспроводным самоорганизующимся (Ad-Hoc) сетям.

В эпоху коммуникационных устройств, социальных сетей и прочих сервисов сообщение на расстоянии и мгновенный обмен информацией кажутся чем-то само собой разумеющимися. Однако возможность оставаться на связи именно в те моменты, когда коммуникационная инфраструктура оказывается нарушенной, приобретает особое значение. Парализовать инфраструктуру сотовой связи могут не только масштабные природные катаклизмы – даже банальное отключение электропитания способны превратить наши мобильные устройства в бесполезные игрушки. В подобных случаях все более привлекательным вариантом становится создание Ad-Hoc сети. Вместе с тем, само понятие БС, приводит к возникновению большого количества возможных уязвимостей для атак и проникновений, которые были бы гораздо затруднены в стандартной проводной сети. Из-за динамически меняющейся топологии сети и отсутствия централизованного управления, данный вид сетей уязвим для ряда атак. Поэтому аспект безопасности является очень важным в таких сетях.

В указанной научной литературе приведены криптографические методы для БС в целом [1], стандарты безопасности [2], а также угрозы, атаки и подходы к защите информации [3]. Приведены разные типы атак, проводимые на Ad-Hoc сети[4]. Для более глубокого изучения данной темы необходимо иметь общее представление об обеспечении максимальной безопасности, учитывая специфику Ad-Hoc сетей. Эффективность подобных работ в значительной мере определяется правильной оценкой эволюционных процессов, свойственных для отрасли информационных технологий. Целью данной статьи является на базе изученной научной литературы и статей [1-15] исследовать Ad-Hoc сети, выявить угрозы криптозащиты, источники их уязвимости, типы атак и, на основании данного исследования, составить перечень методов и средств защиты для обеспечения максимальной безопасности в Ad-Hoc сети.

Первый международный стандарт IEEE 802.11, разработка которого была завершена в 1997г., является базовым стандартом и определяет протоколы, необходимые для организации беспроводных локальных сетей Wireless Local Area Network (WLAN) [5]. Организация WECA – Wireless Ethernet Compatibility Alliance [6], стала выступать в качестве гаранта совместимости оборудования для БС от разных производителей. В настоящее время членами WECA являются более 80 компаний, в том числе Cisco, Lucent, 3Com, IBM, Intel и ряд других известных производителей сетевого оборудования. В терминологии WECA соответствие оборудования требованиям IEEE 802.11 обозначается как Wi-Fi (Wireless Fidelity – дословно переводится на русский язык как "беспроводная точность") [7].

Существуют различные подходы к классификации беспроводных технологий. По дальности действия: беспроводные персональные сети (WPAN — Wireless Personal Area Networks) [8]. Примеры технологий — Bluetooth. Зона действия – до 10 м; WLAN [9]. Примеры технологий — Wi-Fi. Зона действия – до 100 м.; беспроводные сети масштаба города (WMAN — Wireless Metropolitan Area Networks) [10]. Примеры технологий — WiMAX[11]. Зона действия – до 50 км. По технологии: локальные сети, Ad-Hoc сети. Основные различия между этими типами сетей – параметры передачи.

Ad-Hoc сети. Суть Ad-Hoc сетей – предоставление абоненту возможности доступа к различным сетевым услугам посредством передачи и приема «своего» трафика через соседних абонентов. На данный момент широким фронтом идут исследования и применения Ad-Hoc сетей в следующих сферах: военная связь, интеллектуальные транспортные системы, локальные сети, сенсорные сети. В настоящее время существует несколько «базовых» технологий для самоорганизующихся сетей: Bluetooth; ZigBee; WiFi 802.11

Ключевой задачей является обеспечение требуемого уровня безопасности информации, циркулирующей в сети. Острота этой проблемы связана прежде всего с используемой средой передачи данных – радиоэфиром. Осуществить перехват информации в радиоэфире намного проще, чем в проводных и кабельных сетях, – достаточно обзавестись комплектом пользовательского оборудования. Поэтому в спецификации стандартов 802.11 определен протокол защиты БС WEP (Wired Equivalent Privacy). WEP – это криптографический механизм, созданный для обеспечения безопасности сетей стандарта 802.11. Этот механизм разработан с единственным статическим ключом, который применяется всеми пользователями. Исследование WEP-шифрования выявило уязвимые места, из-за которых атакующий может полностью восстановить ключ после захвата минимального сетевого трафика. Второй протокол защиты, появившийся позже – WPA (Wi-Fi Protected Access). Данный стандарт тоже подвержен взлому, однако в гораздо меньшей степени. Обычно для сведения на нет усилий по взлому WPA требуется регулярно менять ключи шифрования, этого часто оказывается достаточно.

Источники уязвимостей в Ad Hoc сетях:

Уязвимость каналов к прослушиванию и подкладыванию сообщений, в связи с общей доступностью среды передачи, как и в любых БС. Незащищённость узлов от злоумышленника, который легко может получить один в распоряжение, так как обычно они не находятся в безопасных местах, таких как сейфы. Отсутствие инфраструктуры делает классические системы безопасности, такие как центры сертификации и центральные серверы, неприменимыми. Динамически изменяющаяся топология требует использования сложных алгоритмов маршрутизации, учитывающих вероятность появления некорректной информации от скомпрометированных узлов или в результате изменения топологии.

Атаки на протоколы маршрутизации в Ad Hoc сетях. Как и в проводных сетях связи, в беспроводных Ad-Hoc сетях существует два вида атак против протоколов маршрутизации: пассивные атаки и активные атаки[14].

Пассивные атаки. Пассивные атаки, как правило, подразумевают несанкционированное «подслушивание» пакетов, которые посылают протоколы маршрутизации. В этом случае атакующая сторона не прерывает работу маршрутизирующего протокола, а только пытается узнать ценную информацию, прослушивая трафик маршрутизации. Главное преимущество атакующей стороны при пассивных атаках заключается в том, что в беспроводной среде связи атаку обычно невозможно обнаружить. И так же сложно защитить от таких атак. Более того, маршрутная информация может раскрыть информацию о взаимодействии между узлами или выявить их адреса. Если маршрут к конкретному узлу сети используется более часто, чем к другим узлам, этот узел может привести к остановке работы всей сети. Другая «интересная» информация, которую можно извлечь из маршрутных данных заключается в расположении узлов. Даже когда было бы невозможно установить точное местоположение узла, можно узнать информацию о сетевой топологии.

Активные атаки**.** Для осуществления активной атаки недоброжелатель должен уметь проникать в произвольный пакет сети. Цель может заключаться в том, чтобы привлечь (перенаправить) пакеты, предназначенные другим узлам, к атакующей стороне для анализа или просто для нарушения работы сети. Главное отличие по сравнению с пассивными атаками заключается в том, что активные атаки могут быть иногда обнаружены. Это делает их менее привлекательными для большинства взломщиков.

Типы активных атак, которые могут быть легко осуществлены в Ad Hoc сетях [15]:

1. Чёрная дыра. В этом случае «недружелюбный» узел использует протокол маршрутизации для объявления себя в качестве кратчайшего пути к узлам, чьи пакеты он хочет получить. В протоколе, основанном на широковещании, взломщик слушает запросы маршрутов. Когда взломщик получает запрос маршрута к требуемому узлу, он посылает ответ с чрезвычайно коротким маршрутом. Если злополучный ответ достигает узел до того как придет верный ответ, то фальшивый маршрут создан.

2. Переполнение таблицы маршрутизации. При таком способе атаки вредитель пытается создать маршруты к несуществующим узлам. Цель атаки заключается в создании маршрутов, которые бы предотвратили создание новых маршрутов путем переполнения таблицы маршрутизации протокола.

3. Спуфинг. Подделка идентификации. Цель атаки - заставить остальные узлы считать узел, проводящий атаку, не тем, кем он является на самом деле. Успешно проведя атаку, злоумышленник получает возможность проводить какие-либо действия от чужого имени, тем самым нарушается конфиденциальность.

4. Испытание бессонницей. Цель атаки – израсходовать энергию целевого узла, запасённую в его источнике питания. Побочным эффектом испытания бессонницей является нарушение доступности. Для осуществления этой атаки могут быть использованы другие, например чёрная дыра, для направления большого трафика на целевой узел.

6. Эгоистичность. Склонность узла не предоставлять услуги другим, например услугу маршрутизации. Цель атаки – сохранить собственные ресурсы, например заряд батареи. Проблема эгоистичности узлов нова и особенно актуальна для самоорганизующихся сетей, так как узлы принадлежат разным административным доменам. Данная атака отрицательно влияет на доступность.

7. Жадность. Склонность узла использовать разделяемые ресурсы больше остальных, например среду передачи данных. Цель атаки – удовлетворить собственные потребности без учёта, вытекающего из этого ущербного положения остальных узлов. По сути, жадность и эгоистичность — две стороны одной монеты. Данная атака отрицательно влияет на доступность.

8. Обнаружение местоположения. Цель атаки – восстановление топологии прилегающей сети или восстановление цепочки узлов, расположенных на маршруте к целевому узлу, путём анализа полученной информации.

9. Постановка помех. «Засорение» канала передачи данных посторонними шумами. Цель атаки – сделать невозможным передачу данных через этот канал. Данная атака нарушает доступность.

Методы повышения безопасности в Ad-Hoc сетях: доступность серверов через некоторое количество узлов, схема разделения секрета, обновление долей секрета, поддержание различных путей, обнаружение маршрутов путём передачи сообщений, схема вероятностной безопасной маршрутизации.

Выводы. Количество атак для БС растет и видоизменяется каждый день. Для обеспечения максимальной безопасности необходимо использовать максимально возможное количество средств защиты и постоянно обновлять их:

1. Всегда отключать Wi-Fi-адаптер

2. Избегать передачи приватной и личной информации при работе в общедоступных Wi-Fi сетях.

3. Постоянно обновлять защитные программы, операционную систему, брандмауэр**.**

4. Проверять подлинность идентификатора сети (SSID) – это поможет предотвратить такую атаку как спуфинг.

5. Отключать функцию «Общий доступ к файлам и принтерам».

6. Для обеспечения дополнительной безопасности Wi-Fi-соединения можно использовать зашифрованные соединения.

Перечисленные методы защиты позволяют реализовать современное оборудование совместимое со стандартом 802.11. Этот комплекс мер обеспечивает начальный уровень защиты, ниже которого при проектировании Ad-Hoc сети опускаться нельзя.

Список литературы

1. Лукин М.А. Стандарты беспроводной связи/ М.А. Лукин //Современная электроника. — 2005. — №1. — С.10—12.

2. Галатенко В. А. Стандарты информационной безопасности / В. А. Галатенко. — Москва: Интернет-университет информационных технологий. — 2006. — 264 с.

3. An Initial Security Analysis of the IEEE 802.1x Standart [Electronic sourse] Arunesh Mishra, William A. Arbaugh.// Department of Computer Science University of Maryland College Park. — Maryland. — 2002 .— P. 56. — Mode of access: http://www.cs.umd.edu/~waa/1x.pdf

4. Анализ прорблем защиты от внешнего нарушителя. [Электронный ресурс] Статьи, аналитика. — 2010. — № 9. — С.12 -18. — Режим доступа: www.securitylab.ru

5. Томас Мауфер, WLAN: Практическое руководство для администраторов и профессиональных пользователей. — КУДИЦ–Образ. —2005. –354 с.

6. Wireless Ethernet Internet Security. [Electronic source] Internet Security. — Mode of access: www.wirelessethernet.org

7. Особенности настройки Wi-Fi сетей. [Электронный ресурс] Статьи 2009. — № 2. — С.24–26. — Режим доступа к журналу: www.telecom-master.ru

8. Telecommunications and information exchange between systems — Local and metropolitan area networks — Specific requirements. Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs (tm)) IEEE 802.15.1–2005. IEEE Standard for Information technology — 112 p.

9. Telecommunications and information exchange between systems– Local and metropolitan area networks– Specific requirements– Part II: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY). Specifications IEEE 802.11-1999. Information technology — 68 p.

10.В.А. Григорьев. Сети и системы беспроводного доступа. Григорьев В.А., Лагутенко О.И., Распопов Ю.А. — Экотрендз – М.:, — 2005. — С.381.

11.Ю.Г. Писарев В ожидании WiMAX// Вестник связи — 2005. —№4 — С. 126 –130.

12.НАУКА – это ЖИЗНЬ!// [Электронный ресурс] Самоорганизующиеся беспроводные сети Сборник научно-познавательных статей, заметок и публикаций — 2010. — № 9. —12 с. — Режим доступа к журналу : http://nauka.relis.ru/index.htm.

13.Лукин М.А. Стандарты беспроводной связи/ М.А. Лукин //Современная электроника, — 2005. — №1. — С.10—12.

14.Запечников С .В. Информационная безопасность открытых систем. в 2-х т / С.В.Запечников, Г.Милославская, А. И.Толстой, Д. В Ушаков. Угрозы, уязвимости, атаки и подходы к защите. М.: Горячая Линия — Телеком, Т.1. —2006. — 536 с.

15.Андреа Голдсмит, Самоорганизующиеся беспроводные сети/ Андреа Голдсми, Мюриел Медар и Мишель Эффрос. Самоорганизующиеся беспроводные сети пер. с англ. В.П.Николаева — Днепропетровск: Эра. — 2007. — 384 с.