Российская Академия Наук
Институт системного программирования

Реализация функций мобильности в протоколе IPv6 и анализ их безопасности

Обзор

Москва 2004 г.

Список исполнителей

Исполнитель	Контактная информация	Примечания
Шнитман Виктор Зиновьевич, зам. директора ИСП РАН	vzs@ispras.ru	Автор

История документа

№ версии	Дата	Примечания
1.0	27.12.2004	Обзор опубликован

Аннотация

В данном документе представлен обзор функций мобильности, предложенных в спецификации протокола RFC 3775 «Поддержка мобильности в IPv6». Мобильность узлов в глобальной сети приводит к возникновению новых угроз для безопасности всей сети и обмена информацией между узлами, как мобильными так и стационарными. В обзоре представлены принципы функционирования мобильного IPv6, анализ возможных атак и уязвимостей, которые возникают при появлении мобильных узлов в Интернете, а также принятых в указанном документе проектных решениях по обеспечению безопасности этого протокола.

Исследование выполнено в рамках проекта по гранту Российского фонда фундаментальных исследований № 04-07-90308 «Верификация функций безопасности и мобильности протоколов IP».

Содержание

1. Введение

Стандарты мобильного IPv6 разрабатываются рабочей группой IETF Mobile IP [1], начиная с 2000 года. За это время этой рабочей группой было выпущено 24 черновые спецификации. Наконец, в июне 2004 года была опубликована основная спецификация RFC 3775 «Mobility Support in IPv6» (Поддержка мобильности в IPv6) [2], которая предлагается в качестве стандарта Internet.

Заметим, что развертывание IPv6 позволило рабочей группе Mobile IP практически начать разработку заново и благодаря возможности ретроспективного взгляда создать протокол поддержки мобильности, который более тесно интегрирован в IP, чем протокол мобильного IPv4 (MIPv4). Как говорит само название протокола MIPv6, он сильно связан с протоколом MIPv4, но имеет несколько тонких отличий, которые привели к созданию более простого и упорядоченного протокола.

Следует отметить, что в то время как целью спецификации является фиксация результата разработки, ее разработчики стремились также представить и неявные предположения и проектные решения, принятые при разработке мобильного IPv6, выпустив черновой документ [3]. Понимание исходных предпосылок значительно упрощает понимание причин выбора тех или иных решений, связанных с вопросами обеспечения безопасности, а также ограничений, присущих принятым решениям. Поэтому данный обзор в значительной степени базируется на указанной работе.

Обзор состоит из 7 разделов. В разделе 2 рассматриваются основные принципы функционирования MIPv6. Раздел 3 посвящен принципам и целям разработки системы безопасности MIPv6. В разделе 4 проанализирована степень опасности введения протокола MIPv6. В разделе 5 рассмотрены основные виды угроз и способы их ограничения. Раздел 6 посвящен собственно решениям по безопасности, принятым в проекте стандарта MIPv6. В разделе 7 анализируются оставшиеся угрозы безопасности, взаимодействие с IPsec, а также ряд вопросов, связанных с использованием MIPv6.

2. Принципы работы мобильного IPv6

2.1. Предположения относительно существующей инфраструктуры IP

Одной из целей разработки протокола мобильного IP была возможность реализации мобильности без внесения больших изменений в существующее сетевое обеспечение. Это было особенно важно для протокола IPv4 с его огромной инсталлированной базой, но те же самые цели разработки были унаследованы мобильным IPv6.

Наиболее важные базовые предположения разработчиков MIPv6 относительно основного протокола и инфраструктуры IPv6 можно выразить следующим образом:

- Маршрутные префиксы, доступные узлу, определяются его текущим местоположением, и, поэтому, при перемещении узел должен менять свой IP-адрес.
- Предполагается, что инфраструктура маршрутизации является безопасной, правильно функционирующей, и обеспечивает доставку пакетов на их место назначения, которое указано в них полем адреса назначения.

Эти предположения объясняются следующим. Во-первых, в текущей рабочей практике IPv6 префиксы IP-адресов распределяются иерархическим способом. Это ограничивает количество элементов таблицы маршрутов, которую должен обрабатывать каждый отдельный маршрутизатор. Важное следствие заключается в том, что именно топология сети определяет, какие глобально маршрутизируемые адреса доступны в данном местоположении. А именно, сами узлы не могут свободно решать, какие глобально

маршрутизируемые адреса использовать, а должны полагаться на маршрутные префиксы, предоставляемые локальными маршрутизаторами с помощью сообщений Router Advertisement (объявление маршрутизатора) или сервером DHCP. Другими словами, IP-адреса представляют собой именно то, что говорит их название, адреса, т.е. локаторы или указатели местоположения.

Во-вторых, в текущей структуре Internet маршрутизаторы совместно поддерживают распределенную базу данных топологии сети и пересылают каждый пакет на то местоположение, которое определяется адресом назначения, передающимся в пакете. Для поддержки топологической информации маршрутизаторы должны доверять друг другу, по крайней мере, в известной степени. Маршрутизаторы узнают топологическую информацию от других маршрутизаторов, и они не имеют иной возможности, как только доверять своим соседним маршрутизаторам относительно топологии удаленной сети. На границе административных доменов для ограничения количества возможно неверной маршрутной информации, полученной от доменов-партнеров, используются правила политики маршрутизации. Хотя в основном этот подход используется для исправления административных ошибок, он помогает также с точки зрения безопасности. Задача заключается в поддержке разумно точного представления о топологии сети, даже если кто-то предоставил системе маршрутизации неверную информацию.

При разработке MIPv6 явно предполагалось, что маршрутизаторы и правила политики конфигурируются разумным способом и что результирующая инфраструктура маршрутизации достаточно надежна. А именно, предполагалось, что система маршрутизации поддерживает точную информацию относительно топологии сети, и что она способна, поэтому, маршрутизировать пакеты на их место назначения. Если это предположение нарушается, то нарушается работа самой сети Internet в том смысле, что пакеты направляются на неправильное местоположение. Такое фундаментальное нарушение работоспособности Internet делает безнадежными любые другие усилия по обеспечению правильной доставки пакетов (т.е. любые усилия, необходимые для анализа безопасности мобильного IP).

2.2. Проблема мобильности и проектные решения MIPv6

2.2.1. Принципы работы

Протокол мобильного IP призван одновременно решить две проблемы. Во-первых, он позволяет сеансам транспортного уровня (соединениям TCP, транзакциям, основанным на UDP) продолжаться, даже если мобильный узел перемещается и меняет свой IP-адрес. Во-вторых, он позволяет мобильному узлу оставаться достижимым по постоянному IP-адресу – «домашнему адресу» (HoA - home address).

Последнее проектное решение можно также выразить другими словами: целью MIPv6 является сохранение идентифицирующих свойств IP-адресов. А именно, разработчики MIPv6 придерживались мнения, что IP-адреса могут использоваться в качестве естественных идентификаторов узлов, как они использовались с самого начала создания сети Internet. Вообще говоря, это мнение расходится с существовавшими альтернативными проектами, в которых свойства идентификации и локации были разделены.

Таким образом, в проекте стандарта узазано, что каждый мобильный узел (MN - mobile node), участвующий в протоколе MIPv6, имеет постоянный «домашний адрес», который может использоваться для адресации мобильного узла независимо от его текущей точки подсоединения к сети IPv6. Сеть IPv6, которая соответствует префиксу домашнего адреса, называется «домашней сетью» (HN - home network) или просто «домом» мобильного узла. Мобильные узлы, перемещающиеся во «внешнюю сеть» (FN – foreign network), для

определения новой сети, а также для получения «временного адреса» (CoA - care-of-address) из диапазона адресов этой сети используют механизм автоматического конфигурирования. Для работы вне домашней сети мобильные узлы выбирают «домашнего агента» (HA - home agent) - IPv6-маршрутизатор, подсоединенный непосредственно к домашней сети. Этот процесс может осуществляться либо статически, либо динамически посредством механизма динамического определения адреса домашнего агента MIPv6. Точно так же, как и в MIPv4, когда мобильный узел находится за пределами своей домашней сети, домашний агент перехватывает пакеты, предназначенные мобильному узлу, и пересылает эти пакеты, туннелируя их на текущий адрес узла – «временный адрес». Транспортный уровень (например, TCP, UDP) использует домашний адрес в качестве постоянного (неизменяемого) идентификатора мобильного узла. Пакеты от мобильного узла к узлу-корреспонденту сначала туннелируются в обратном направлении домашнему агенту и затем обычным способом маршрутизируются из домашней сети узлу-корреспонденту. Этот основной режим работы двунаправленного туннелирования показан на рис. 1.

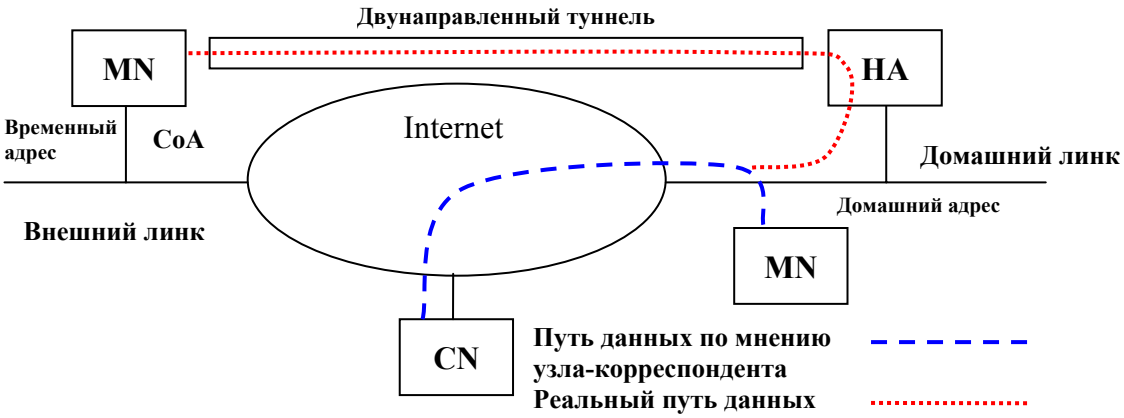

Рис. 1. Режим двунаправленного туннелирования.

Основной режим работы MIPv6 требует туннелирования пакетов через домашнего агента и приводит, тем самым, к более длинным путям их пересылки и понижению производительности. Такое туннелирование иногда называется треугольной маршрутизацией, поскольку первоначально планировалось, что пакеты от мобильного узла к его партнеру все еще могут проходить прямо в обход домашнего агента.

Чтобы смягчить потери производительности, в протокол MIPv6 включен режим работы, который позволяет мобильному узлу и его партнеру, узлу-корреспонденту (CN - correspondent node), после начальной установочной фазы осуществлять прямой обмен пакетами полностью в обход домашнего агента. Этот режим работы называется оптимизацией маршрутов (RO - route optimization) и предполагает подмену в каждом узле-корреспонденте маршрутной информации, связанной с домашним адресом, маршрутной информацией, указывающей временный адрес мобильного узла. Протокол MIPv6 обеспечивает такую функциональность путем введения так называемого кэша привязок и новых управляющих сообщений.

2.2.2. Кэш привязок

Ассоциация между домашним адресом мобильного узла и его текущим временным адресом называется «привязкой» (binding). Требуется, чтобы все узлы, участвующие в протоколе MIPv6, поддерживали специальную таблицу таких привязок, получившую название «кэша привязок». Для каждого мобильного узла, с которым в текущий момент времени осуществляется обмен информацией, в кэше привязок содержится один элемент. Как показано на рис. 2, каждый элемент кэша привязок для каждой привязки содержит

четыре основных поля (для обеспечения правильного упорядочивания управляющих сообщений имеются и другие поля, но для упрощения на рисунке они опущены). Домашний адрес является полем ключа для поиска в этом кэше.

Home Address	Care-of Address	Lifetime	Home Agent
3ffe:2101:0:b00::10	3ffe:2101:0:a00:260:97ff:fe8b:4c56	120	Yes
3ffe:2101:0:c00::15	3ffe:2101:0:b00:a00:6aff:fe2b:137c	43	No

Рис. 2. Кэш привязок.

Когда некоторый узел хочет передать IPv6-пакет удаленному мобильному узлу, в кэше привязок по полю home address осуществляется поиск IPv6-адреса мобильного узла. Если никакого совпадения не найдено, то пакет передается в соответствии с обычными таблицами маршрутизации IPv6. Однако если соответствие найдено, то исходный пакет до передачи инкапсулируется для того, чтобы его переадресовать на временный адрес, указанный в кэше привязок. Такая инкапсуляция гарантирует оптимальную маршрутизацию пакета на текущее местоположение мобильного узла. Форма, которую эта инкапсуляции принимает, зависит от состояния флага «home agent», который хранится в данном элементе кэша привязок.

2.2.2.1. Работа домашнего агента

Если в элементе кэша привязок установлен флаг «home agent», то узел, поддерживающий этот кэш, работает домашним агентом соответствующего мобильного узла. Если это имеет место, пакет был адресован на домашний адрес мобильного узла и перехвачен домашним агентом для последующей пересылки адресату, то, как показано на рис. 3, он инкапсулируется по принципам туннелирования «IPv6 в IPv6».

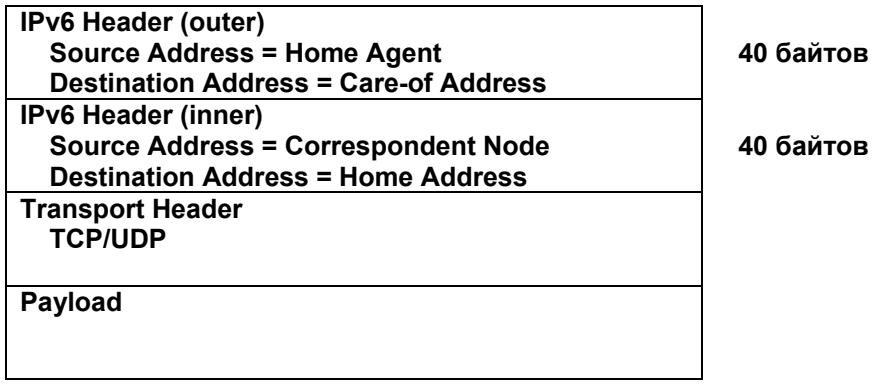

Рис. 3. Инкапсуляция IPv6 в IPv6

Как показано на рис. 1, IPv6-туннелирование используется домашними агентами для пересылки пакетов, маршрутизированных по неоптимальному маршруту в домашнюю сеть мобильного узла, когда последний находится вне дома. Такое туннелирование обеспечивает полное сохранение оригинального IPv6-пакета, что является важным преимуществом, поскольку любая модификация IPv6-заголовка может создать проблемы для протоколов более высоких уровней, например, для TCP. Перехваченные пакеты туннелируются непосредственно на текущий временный адрес мобильного узла, где они потом декапсулируются и далее обычным способом обрабатываются мобильным узлом.

2.2.2.2. Работа узла-корреспондента

Если в элементе кэша привязок флаг «home agent» обнулен, или узел является первоисточником пакета, то, как показано на рис. 4, для переадресации IPv6-пакета на

соответствующий временный адрес используется специальный заголовок маршрутизации IPv6 (заголовок маршрутизации типа 2).

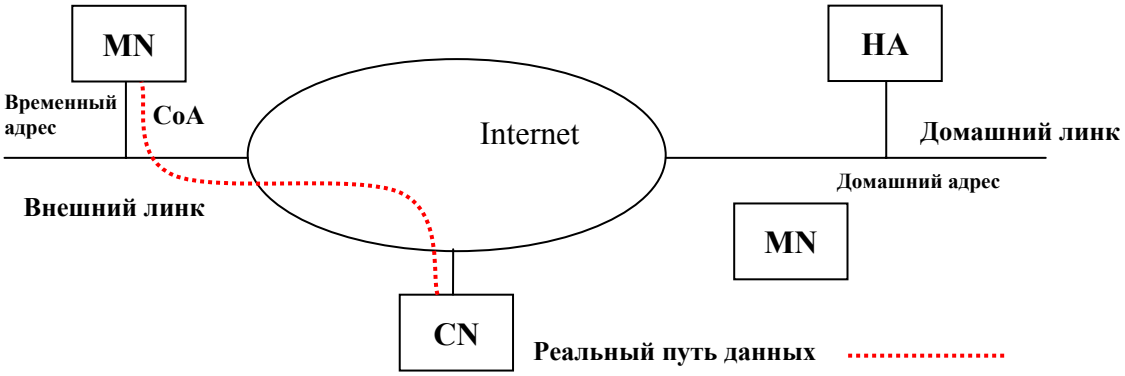

Рис. 4. Маршрутизация с использованием оптимизации маршрутов

Как видно из рис. 5, использование заголовка маршрутизации IPv6 существенно сокращает эффективную полосу пропускания, необходимую для инкапсуляции пакета по сравнению с туннелированием IPv6 в IPv6. Это решение позволило сократить размер пакета на 16 байт (если бы использовалось туннелирование IPv6 в IPv6, то поле IPv6-адреса источника как внутреннего, так и внешнего IPv6-заголовков было бы одним и тем же, что приводило бы к потере полосы пропускания).

IPv6 Header (outer) **Source Address = Correspondent Node** **Destination Address = Care-of Address**	**40 байтов**
IPv6 Routing Header (тип 2) **Next Hop = Home Address**	**24 байта**
Transport Header **TCP/UDP**	
Payload	

Рис. 5. Использование заголовка маршрутизации типа 2.

Таким образом, каждый раз, когда используется оптимизация маршрутов, узел-корреспондент в действительности исполняет две роли. Во-первых, как обычно, он является источником пакетов, которые посылает. Во-вторых, для пакетов он действует как первый маршрутизатор, в действительности выполняя маршрутизацию от источника. А именно, когда узел-корреспондент отсылает пакеты, он просматривает свои структуры данных MIPv6, предназначенные для оптимизации маршрутов (кэш привязок), и, если необходимо, переадресует пакеты. Как уже отмечалось элемент кэша привязок (BCE - Binding Cache Entry) содержит домашний адрес и временный адрес мобильного узла, и регистрирует тот факт, что пакеты, местом назначения которых является домашний адрес, должны теперь посылаться на временный адрес. Таким образом, режим оптимизации маршрутов задает собой локальную, не соответствующую обычным правилам маршрутизацию.

Пакеты, покидающие узел корреспондента, маршрутизируются от источника на временный адрес мобильного узла. Каждый пакет включает заголовок маршрутизации, который содержит домашний адрес мобильного узла. Таким образом, логически пакет сначала маршрутизируется на временный адрес, а затем фактически с временного адреса

на домашний адрес. На практике, конечно, пакет принимается мобильным узлом на временный адрес, а заголовок позволяет мобильному узлу только выбрать сокет, ассоциированный с домашним адресом, вместо сокета, ассоциированного с временным адресом. Однако этот механизм имеет сходство с маршрутизацией от источника, поскольку в узле-корреспонденте имеется связанное с ним состояние маршрутизации и используется заголовок маршрутизации. Тем не менее, чтобы избежать рисков, связанных с использованием более универсального варианта (тип 0), этот заголовок маршрутизации имеет специальный тип (тип 2).

2.2.3. Управление привязками

Использование кэша привязок и IPv6-инкапсуляции предоставляет мобильным узлам механизм оптимальной маршрутизации. Однако этот механизм полагается на то, что хранящиеся в этом кэше привязки являются правильными и обновленными. Конечно, для защиты от полного отказа машины (который является достаточно распространенным в мобильной среде из-за ограниченного времени жизни батареи питания и т. п.), а также от длительных периодов отключения мобильных узлов от сети, элементы кэша привязок мобильного узла должны восстанавливаться даже после периода полного отключения или потери состояния мобильными узлами или узлами-корреспондентами.

Протокол MIPv6 поддерживает согласованное состояние кэшей привязок путем использования специальных управляющих сообщений. Основными сообщениями, связанными с управлением привязками являются сообщения Binding Update (обновление привязки), Binding Acknowledgement (подтверждение привязки), Binding Refresh Request (запрос обновления привязки) и Binding Error (ошибка привязки). В оставшейся части этого раздела описываются эти четыре управляющих сообщения, а также то, как они взаимодействуют для обеспечения правильного и своевременного обновления состояния кэшей привязок. Заметим, что протокол MIPv6 определяет еще четыре управляющих сообщения, которые используются для выполнения процедуры обратной маршрутизируемости (см. раздел 6.1) и обеспечивают авторизацию обновлений привязки.

Во всех обменах сообщениями, связанными с созданием привязок и управлением ими, мобильными узлами, узлами-корреспондентами и домашними агентами используется новый заголовок расширения IPv6 - заголовок мобильности (Mobility Header). Тип сообщения определяется полем типа заголовка мобильности.

2.2.3.1. Сообщения Binding Update

Сообщения Binding Update (обновление привязки) передаются мобильными узлами домашним агентам и узлам-корреспондентам для создания или обновления элемента в их кэшах привязок, связанного с соответствующим домашним адресом мобильного узла. В частности, они используются мобильным узлом для уведомления других узлов о его временном адресе.

Чтобы гарантировать, что «устаревшие» привязки не будут поддерживаться кэшами привязок бесконечно долго, мобильный IPv6 применяет механизмы мягкого состояния и сборки мусора для удаления устаревших привязок. Это означает, что каждое обновление привязки содержит поле времени жизни, которое определяет, в течение какого периода времени эта привязка остается годной. После того, как это время жизни истечет, привязка удаляется из кэша привязок. Значение времени жизни устанавливается и обновляется с помощью соответствующего поля времени жизни, содержащегося в сообщениях Binding Update. Нулевое значение времени жизни в обновлении привязки указывает на удаление соответствующей привязки.

После принятия решения о смене своего временного адреса мобильный узел должен, прежде всего, зарегистрировать этот временный адрес в своем домашнем агенте (путем

посылки ему сообщения Binding Update). Кроме того, если мобильный узел хочет, чтобы домашний агент продолжал его обслуживать по истечении текущего периода регистрации, мобильный узел задолго до истечения этого периода времени должен послать ему новое сообщение Binding Update, даже если он не менял своего временного адреса.

В общем случае, после того, как мобильный узел послал сообщение Binding Update домашнему агенту для регистрации своего нового временного адреса, он должен инициировать регистрацию этого временного адреса во всех узлах–корреспондентах, в кэшах привязок которых для его домашнего адреса ранее были созданы соответствующие элементы. Это осуществляется путем просмотра так называемого списка обновлений привязки (см. раздел 2.2.5). Запускаемые процедуры могут использоваться либо для обновления, либо для удаления информации о привязке в узле-корреспонденте.

Для тех узлов, которые отсутствуют в списке обновлений привязки мобильного узла, мобильный узел может инициировать регистрацию в узле-корреспонденте в любой момент времени после посылки сообщения Binding Update своему домашнему агенту. Соображения относительно того, когда (и при каких условиях) инициировать эту процедуру, зависят от конкретного перемещения и характера трафика мобильного узла и, к сожалению, в спецификации [2] точно не определены. В ней говорится только, что мобильный узел «может» инициировать регистрацию в узле-корреспонденте в ответ на получение пакета, который прошел через туннель IPv6 в IPv6 от домашнего агента этого мобильного узла. Прием такого пакета неявно указывает на то, что узел-корреспондент, который сформировал этот пакет, не имеет привязки для данного мобильного узла (иначе пакет доставлялся бы с помощью заголовка маршрутизации).

Важно отметить, что в любом случае до выполнения собственно регистрации в узле-корреспонденте (посылки сообщения Binding Update) спецификация требует выполнения процедуры обратной маршрутизируемости, т.е. авторизации соответствующей привязки (см. раздел 6).

2.2.3.2. Сообщения Binding Acknowledgement

В отличие от обновлений привязки, сообщения Binding Acknowledgement (подтверждение привязки) посылаются мобильным узлам узлами-корреспондентами и домашними агентами. Они обеспечивают мобильным узлам обратную связь в ответ на обновления привязки и используются для обеспечения надежной доставки обновлений привязки, а также для указания ошибок, которые возникли во время их удаленной обработки. Мобильные узлы сопоставляют подтверждения привязки с соответствующими им обновлениями привязки путем сравнения порядковых номеров сообщений.

2.2.3.3. Сообщения Binding Refresh Request

Узлы-корреспонденты и домашние агенты, обнаружив в своем кэше привязок элемент, срок годности которого почти истек, могут принять решение послать соответствующему мобильному узлу сообщение Binding Refresh Request (запрос обновления привязки). Получение мобильным узлом этого сообщения приводит к передаче нового обновления привязки источнику запроса. Этот механизм позволяет узлам-корреспондентам избежать коротких периодов неоптимальной маршрутизации, возникающих в результате истечения срока годности правильной привязки.

2.2.3.4. Сообщения Binding Error

Сообщение Binding Error используется узлом-корреспондентом для сигнализации ошибки, связанной с мобильностью, такой, например, как неуместная попытка использования опции места назначения Home Address (см. раздел 2.2.6) без существующей привязки.

2.2.4. Агент-посредник протокола Neighbor Discovery

Поскольку при неоптимальной маршрутизации пакеты маршрутизируются в домашнюю сеть мобильного узла, размещение домашних агентов в пограничных IPv6-маршрутизаторах позволяет им эффективно перехватывать такие пакеты, т.к., вероятно, они должны пройти через этот маршрутизатор. Однако нельзя всегда полагаться на предположение о том, что пакеты будут автоматически проходить через этот маршрутизатор. Например, рассмотрим случай, когда узел-корреспондент находится в домашней сети мобильного узла. Если узел-корреспондент должен послать этому мобильному узлу пакет, то его таблица маршрутов будет указывать на то, что мобильный узел доступен непосредственно и не требует пересылки маршрутизатором. В этом случае домашний агент не будет способным перехватить пакет.

Мобильный IPv6 решает эту проблему с помощью метода, который называется proxy neighbor discovery – агент-посредник протокола Neighbor Discovery (proxy ND). Протокол Neighbor Discovery идейно подобен протоколу ARP для IPv4 и является стандартным протоколом IPv6 для определения MAC-адресов по IPv6-адресам. Proxy ND заставляет IPv6-узел выдавать себя за другой узел на уровне MAC путем «неправильных» ответов на запросы соседей своим собственным MAC-адресом. Домашние агенты используют механизм proxy ND, чтобы обеспечить перехват любых IPv6-пакетов для мобильного узла, передаваемых в его домашней сети. Чтобы это выполнить, домашние агенты поддерживают также специальную таблицу - proxy neighbor discovery table, которая содержит IPv6-адреса, для которых домашний агент действует как посредник. Добавление и удаление элементов этой таблицы происходит по мере добавления и удаления элементов кэша привязок с установленным флагом «home agent».

2.2.5. Список обновлений привязки

В процессе перемещения мобильного узла из одной сети в другую важно, чтобы сообщения обновления привязки как можно скорее передавались домашнему агенту этого узла и узлам-корреспондентам, чтобы содействовать быстрой передаче обслуживания. Поэтому мобильные узлы для обновления устаревших привязок не могут просто полагаться на механизм тайм-аута мягкого состояния, используемого в кэшах привязок, поддерживаемых узлами-корреспондентами (обычное время жизни привязки составляет порядка нескольких минут). С этой целью в мобильных узлах хранится дополнительная структура данных, список обновлений привязки, которая отслеживает состояние привязок в каждом узле-корреспонденте и каждом домашнем агенте.

Список обновлений привязки содержит по одному элементу для каждого узла-корреспондента или домашнего агента, которому было послано обновление привязки. Элементы этого списка содержат такую информацию, как адрес и момент времени, когда было послано обновление привязки, состояние любого неподтвержденного обновления, время жизни привязки, флаг домашнего агента и порядковый номер последней передачи. В списке обновлений привязки по мере истечения времени жизни соответствующих привязок осуществляется сборка мусора. Кроме того, список обновлений привязки содержит данные, связанные с выполнением процедуры обратной маршрутизируемости.

Поддержка списка обновлений привязки позволяет реализовать значительно более быструю передачу обслуживания. После того, как была обнаружена передача обслуживания и завершено автоконфигурирование нового временного адреса мобильного узла, осуществляется проход по списку обновлений привязки, и каждому узлу, находящемуся в списке, посылается сообщение обновления привязки, и, следовательно, осуществляется обновление информации в кэшах привязок всех активных узлов-корреспондентов.

2.3.6. Опция Home Address

Находясь вне дома, мобильные узлы имеют возможность выбора IPv6-адресов с глобальной областью действия для использования в качестве адреса источника исходящих IPv6-пакетов. При этом может использоваться либо домашний адрес узла, либо текущий временный адрес. Однако ни одна из этих возможностей не является особенно желательной. Если используется текущий временный адрес, то адрес источника для последующих пакетов будет меняться по мере осуществления передач обслуживания. Это часто создает непоправимые проблемы для протоколов более высоких уровней, таких как TCP, которые поддерживают транспортные идентификаторы и контрольные суммы, базируясь на адресах сетевого уровня. С другой стороны, если используется домашний адрес, то исходящие IPv6-пакеты становятся чувствительными к входной фильтрации.

Входная фильтрация осуществляется многими пограничными маршрутизаторами для увеличения безопасности сайта, который они обслуживают. Она включает контроль адреса источника всех входящих IP-пакетов и проверку того, что маршрут к этому адресу проходит через тот интерфейс, по которому получен пакет. Все пакеты, которые не прошли благополучно такую проверку, отбрасываются в качестве меры предосторожности системы безопасности. Это позволяет избежать многих атак на систему безопасности, которые пользуются подделкой адресов (см. ниже раздел 5). Таким образом, мобильные узлы, которые при работе во внешней сети указывают в IPv6-пакетах в качестве адреса источника свой домашний адрес, могут ошибочно интерпретироваться маршрутизаторами, выполняющими входную фильтрацию, как представляющие угрозу системе безопасности.

Протокол MIPv6 определяет новую опцию места назначения IPv6, которая называется Home Address и может предоставить протоколу транспортного уровня надежное решение, которое не чувствительно к входной фильтрации. На рис. 6 показана опция Home Address.

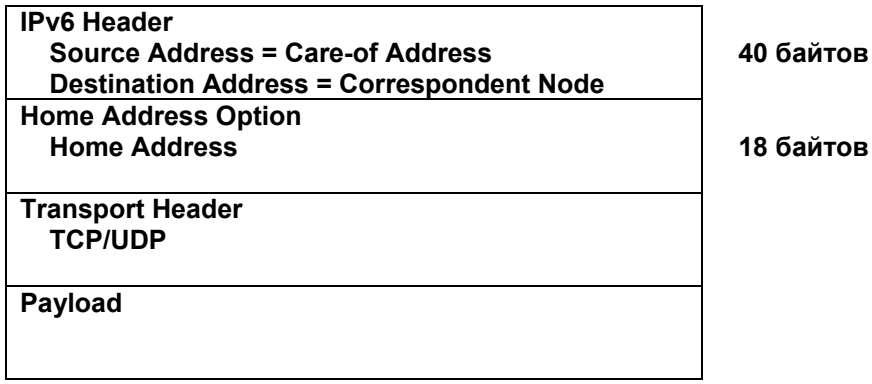

Рис. 6. Опция Home Address.

Спецификация MIPv6 устанавливает, что мобильные узлы в качестве адреса источника своих IPv6-пакетов должны использовать временный адрес, избегая, тем самым, входной фильтрации. Однако любые протоколы более высоких уровней должны предполагать, что адресом источника исходящих пакетов является домашний адрес. Все исходящие из мобильного узла пакеты включают опцию Home Address. При получении узлом-корреспондентом адрес, находящийся в опции Home Address, заменяет адрес источника пакета до того, как начнется любая обработка более высокого уровня.

2.2.7. Механизм определения домашнего агента

Протокол MIPv6 обеспечивает также поддержку нескольких домашних агентов, и, кроме того, ограниченную поддержку реконфигурации домашней сети. В этих случаях мобильный узел может не знать IP-адреса своего собственного домашнего агента, и

префиксы домашней подсети могут даже меняться со временем. Механизм, известный под названием «dynamic home agent address discovery» (динамическое определение адреса домашнего агента) позволяет мобильному узлу динамически определить IP-адрес домашнего агента в его домашней сети, даже когда мобильный узел находится вне дома. Мобильные узлы могут также узнать новую информацию относительно префиксов домашней подсети с помощью механизма «mobile prefix discovery» (мобильного определения префиксов).

Первый механизм включает в себя процедуру присоединения всех домашних агентов в домашней сети к адресу типа «Mobile IPv6 Home-Agents anycast address» [4]. Каждым домашним агентом поддерживается список домашних агентов, в котором хранится информация относительно каждого маршрутизатора, который действует как домашний агент в одной и той же подсети. Информацию для этого списка домашние агенты получают из периодических не запрошенных сообщений Router Advertisement, в которых установлен признак Home Agent (H). IP-адреса в этом списке хранятся в порядке приоритета домашних агентов в домашней сети. Мобильный узел посылает на адрес «Mobile IPv6 Home-Agents anycast address» сообщение ICMP Home Agent Address Discovery Request (запрос для определения адреса домашнего агента) для префикса своей собственной домашней подсети. Это сообщение будет получено «ближайшим» маршрутизатором, который выполняет в домашней сети функции домашнего агента. В ответном сообщении ICMP Home Agent Address Discovery Reply мобильный узел получит список домашних агентов. Это позволяет ему начать процесс регистрации временного адреса в домашнем агенте.

Второй механизм также основан на сообщениях ICMP. Сообщение ICMP Mobile Prefix Solicitation посылается мобильным узлом своему домашнему агенту, когда первый находится вне дома. Целью сообщения является запрос от домашнего агента сообщения ICMP Mobile Prefix Advertisement, которое позволит мобильному узлу получить префиксную информацию относительно его домашней сети. Эта информация может использоваться для конфигурирования и обновления домашнего адреса в соответствии с изменениями в префиксной информации, представленной домашним агентом.

2.3. Сравнение MIPv6 и MIPv4

Архитектура MIPv6 по сравнению с архитектурой MIPv4 имеет целый ряд преимуществ. Как пояснено выше, главные преимущества заключаются в возможности автоконфигурирования мобильных клиентов в удаленных сетях, которая позволяет подсоединиться к сети без использования внешних агентов, а также в возможности оптимизации маршрутов благодаря использованию обновлений привязки, посылаемых узлу-корреспонденту. Кроме того, существенно увеличенное пространство адресов позволяет разворачивать крупномасштабные мобильные IPv6-сети, используя глобально достижимые адреса (заметим, что мобильному клиенту в любой момент времени при перемещении из одной сети в другую требуется по крайней мере два IPv6-адреса), а предложенный метод определения домашних агентов позволяет разворачивать масштабируемые фермы домашних агентов.

Под более абстрактным углом зрения мобильность IPv6 можно определить как механизм управления локальными, не соответствующими обычной работе, изменениями маршрутной информации, позволяющими направить на другой адрес (временный адрес) пакеты, которые реально посылаются на домашний адрес. Этот механизм управляется в том смысле, что локальные, не соответствующие обычной маршрутизации маршруты (маршруты от источника) создаются и уничтожаются динамически, базируясь на командах, которые посылаются мобильным узлом. Он является локальным в том смысле, что не соответствующие обычной маршрутизации маршруты являются действительными только на домашнем агенте, а также на узлах-корреспондентах, если используется

оптимизация маршрутов. Созданные части состояния являются исключениями в том смысле, что они имеют приоритет по отношению к обычной топологической маршрутной информации, доставляемой совместно маршрутизаторами.

Можно сказать, что домашний адрес играет двойную роль: идентификатора оконечной точки (EID - end-point identifier) и постоянного локатора мобильного узла. Временный адрес представляет собой чисто временный локатор, который указывает текущее местоположение мобильного узла. Узлы-корреспонденты эффективно выполняют маршрутизацию от источника, переадресуя трафик, предназначенный для домашнего адреса на временный адрес. Это отражается даже в структуре пакетов: пакеты передают явный заголовок маршрутизации.

Одной из известных проблем, которую пришлось решать разработчикам MIPv6, является проблема безопасности, или аутентификации обновлений привязки. В следующем разделе будут рассмотрены основные принципы создания системы безопасности MIPv6.

3. Принципы и цели разработки системы безопасности MIPv6

Разработчики MIPv6 и системы безопасности стремились следовать сквозному (end-to-end) принципу, чтобы должным образом отметить разницу в отношениях доверия между узлами, и чтобы установить явную цель в обеспечиваемом уровне защиты.

3.1. Сквозной принцип

Возможно, главным принципом разработки протоколов Internet является так называемый сквозной принцип [5]. В соответствии с этим принципом считается полезным исключить загрязнение сети состоянием соединений, и ограничить создание нового состояния только оконечными узлами, вовлеченными в обмен информацией.

В случае мобильного IPv6 сквозной принцип применяется посредством ограничения состояния, связанного с мобильностью, главным образом домашним агентом. Дополнительно, если используется оптимизация маршрутов, узлы-корреспонденты также поддерживают мягкое состояние о текущем временном адресе мобильного узла – кэш привязок (Binding Cache). Этот подход отличается от подхода, который использовал бы индивидуальные маршруты хостов в рамках основной системы маршрутизации. Такой подход создавал бы состояние на огромном числе маршрутизаторов сети. В мобильном IPv6 состояние должны создавать только домашний агент и обменивающиеся информацией узлы.

3.2. Предположения о доверии

В проекте безопасности мобильного IPv6 были приняты различные подходы для защиты обменов информацией между мобильным узлом и его домашним агентом и мобильным узлом и узлом-корреспондентом. В случае домашнего агента предполагалось, что мобильный узел и домашний агент знают друг друга благодаря предыдущим соглашениям, т.е. благодаря существующим деловым отношениям. В отличие от этого, строго предполагалось, что мобильному узлу и узлу-корреспонденту не нужны никакие предварительные соглашения, позволяя тем самым мобильному IPv6 функционировать в масштабируемой манере, и не требуя какого-либо конфигурирования в узлах корреспондентах.

3.3. Уровень защиты

Целью разработки системы безопасности считалось, что проект мобильного IPv6 должен быть «настолько же безопасен, насколько безопасен (не мобильный) IPv4 Internet» на

момент разработки MIPv6 в период 2001-2002 гг. В частности, это означает, что против злоумышленников, которые способны подключиться к пути между узлом-корреспондентом и домашним агентом, степень защиты мала. Целесообразность этого проста: в Internet 2001 года, если некоторый узел был способен подключиться к пути обмена информацией между двумя произвольными узлами, то он оказывался способным разрушать, модифицировать и подслушивать весь трафик между этими двумя узлами, если только не использовались средства защиты IPsec. Даже если использовались средства IPsec, злоумышленник все еще оставался способным выборочно блокировать обмен информацией, просто сбрасывая пакеты. Злоумышленник, контролирующий маршрутизатор, находящийся между двумя узлами, может также организовать атаку «затопления» путем переадресации на адрес третьей стороны потоков данных, передаваемях между двумя узлами (или, более практично, эквивалентный поток поддельных данных).

4. Анализ степени опасности MIPv6

Из вышеизложенного должно быть ясно, что опасности в мобильном IPv6 связаны с созданием (или удалением) локальных, не соответствующих обычной маршрутизации, маршрутов. В терминах мобильного IPv6 опасность заключается в возможности неавторизованного создания элементов кэша привязок. В зависимости от цели атаки, временных соотношений при ее реализации и местоположения злоумышленника, последствия атаки могут быть разными.

4.1. Возможные цели атак

По существу целью атаки могут стать любые стационарные или мобильные узлы или сети в Internet. Основные отличия связаны с целями атаки: намеревается ли злоумышленник направить в другую сторону (похитить) трафик, предназначенный для целевого узла и/или исходящий из целевого узла, или он намеревается стать причиной отказа в обслуживании для целевого узла или сети. Обычно в активной атаке цель не играет большой роли. Например, злоумышленник может организовать атаку «отказа в обслуживании» на заданном узле A путем обращения к большому количеству узлов с заявлением, что он является A, и последующем направлении трафика этих других узлов так, что A будет нанесен ущерб, поскольку он больше не будет способен получать пакеты от этих узлов. Сам A не должен вовлекаться вообще до того, как его обмены информацией начнут нарушаться. Более того, A не обязательно должен быть мобильным узлом; он вполне может быть стационарным узлом.

Мобильный IPv6 использует тот же самый класс IP-адресов как для мобильных узлов (т.е. домашних и временных адресов), так и для стационарных узлов. То есть, мобильные и стационарные адреса не различимы друг от друга. Злоумышленники могут воспользоваться этим, беря любой IP-адрес и используя его в некотором контексте, в котором обычно появляется только мобильный узел (домашние или временные адреса). Это означает, что атаки, которые были бы только заботой мобильных узлов, в действительности представляют собой угрозу для всех узлов IPv6.

В действительности роль мобильного узла представляется наиболее защищенной, поскольку в этой роли узел не должен поддерживать состояние относительно местоположения некоторых удаленных узлов. Наоборот, роль узла-корреспондента представляется наиболее слабой точкой, поскольку имеется не много предположений, на которых она может базировать создание своего состояния. А именно, злоумышленник имеет значительно более простую задачу ввода в заблуждение узла-корреспондента, чтобы тот поверил, что вероятно мобильный узел находится где-то, где его нет, чем ввести в заблуждение сам мобильный узел, чтобы он поверил в нечто подобное. С другой стороны, поскольку возможно атаковать узел косвенно, сначала нацелившись на его

партнеров, все узлы в некотором смысле одинаково уязвимы. Более того, (обычный) мобильный узел часто играет также роль узла-корреспондента, поскольку он может обмениваться пакетами с другими мобильными узлами (см. также раздел 7.4).

4.2. Временные соотношения

Временные соотношения являются важным аспектом для понимания опасностей, связанных с мобильным IPv6. В стационарной сети IPv4 злоумышленник должен находиться между взаимодействующими узлами в то же самое время, когда эти узлы осуществляют обмен информацией. С возможностью в мобильным IPv6 создавать элементы кэша привязок ситуация меняется. Появляются новые опасности. Без надлежащей защиты злоумышленник может на время подключиться между домашним агентом и узлом-корреспондентом, создать элемент кэша привязок в узле-корреспонденте, покинуть свое местоположение и непрерывно обновлять в узле-корреспонденте информацию, касающуюся местоположения мобильного узла. Это приведет к тому, что узел-корреспондент будет посылать предназначенные мобильному узлу пакеты на неправильный адрес до тех пор, пока остается действительным элемент кэша привязок, т.е. обычно до тех пор, пока узел-корреспондент не перезагрузится. Обратное положение также возможно: злоумышленник может также организовать атаку, сначала создав элемент кэша привязок, а затем дав истечь сроку его годности в тщательно подобранный момент времени. Если срок годности значительного количества элементов кэша привязок, участвующих в передаче большого объема трафика, истечет в один и тот же момент времени, следствием может стать перегрузка домашнего агента или домашней сети.

4.3. Местоположение злоумышленника

В статической сети IPv4 Internet злоумышленник может получать пакеты, предназначенные для заданного адреса, только если он способен подключиться или контролировать узел на топологическом пути между отправителем и получателем. С другой стороны, злоумышленник может просто посылать поддельные пакеты почти отовсюду. Если мобильный IPv6 позволял бы посылать незащищенные обновления привязки, то злоумышленник мог бы создать элемент кэша привязок в любом узле-корреспонденте из любого места в Internet, просто послав узлу-корреспонденту подложное сообщение Binding Update. Вместо того чтобы выполнялось требование нахождения между двумя целевыми узлами, злоумышленник мог бы действовать из любого места в Internet.

Подытоживая можно сказать, что путем введения в узле-корреспонденте нового исключения в стандартную систему маршрутизации (кэша привязок), мобильный IPv6 вносит опасности изменения времени и места проведения атак. Без надлежащей защиты мобильный IPv6 позволит злоумышленнику действовать из любого места Internet и задолго до момента реальной атаки. В отличие от этого, в статической сети IPv4 Internet атакующие узлы должны существовать во время атаки и они должны располагаться на подходящем пути, иначе атака не будет возможной.

5. Угрозы и их ограничение

В данном разделе описаны атаки, направленные на механизм оптимизации маршрутов мобильного IPv6, а также связанные с ними механизмы защиты. Целью злоумышленника может быть порча кэша привязок узла-корреспондента, которая приведет к доставке пакетов на неправильный адрес. Это может подорвать секретность и целостность обменов информацией и вызвать отказ в обслуживании (DoS – denial of service) как на сторонах, участвующих в обменах информацией, так и на адресе, который получает нежелательные

пакеты. Злоумышленник может также использовать свойства механизма обновлений привязи для исчерпания ресурсов мобильного узла, домашнего агента или узла-корреспондента. Целью данного раздела является описание главных атак, а также обзор различных протокольных механизмов и их ограничений. Более подробно эти механизмы рассматриваются в разделе 6.

Важно понимать, что некоторые угрозы являются более серьезными, чем другие, некоторые можно смягчить, но не устранить полностью, некоторые угрозы могут представлять приемлемый риск, а некоторые угрозы могут оказаться слишком дорогими для предотвращения.

Разработчики MIPv6 рассматривали только активных злоумышленников. Основная причина такого подхода заключается в том, что для порчи кэша привязок злоумышленник должен рано или поздно послать одно или несколько сообщений. Таким образом, не имеет смысла рассматривать злоумышленников, которые только наблюдают сообщения, но не посылают никаких сообщений. В действительности, для среднего злоумышленника некоторые активные атаки запускать проще по сравнению с пассивными атаками. А именно, в большинстве активных атак злоумышленник может инициировать обработку обновлений привязки в любой момент времени, в то время как большинство пассивных атак потребуют от него подождать подходящих сообщений, которые должны быть посланы целевыми узлами.

5.1. Атаки на «владельцев» адресов

Наиболее очевидной опасностью в мобильном IPv6 является «хищение» адреса, т.е. злоумышленник незаконно утверждает, что он является данным узлом на данном адресе, а затем пытается «похитить» трафик, отправляемый на этот адрес. Имеются несколько вариантов этой атаки. Сначала будет описан основной вариант этой атаки, за чем последует описание того, как изменится ситуация, если целью является стационарный узел, и далее будет продолжено описание более сложных проблем, связанных с аспектами временных соотношений (так называемые «будущие» атаки), конфиденциальности и целостности, а также отказа в обслуживании.

5.1.1. Основной вариант атаки «хищения адреса»

Если бы обновления привязки вообще не аутентифицировались, то злоумышленник смог бы фабриковать и посылать поддельные обновления привязки из любого места Internet. Все узлы, которые поддерживают функциональность узла-корреспондента, превратились бы в невольных свидетелей этой атаки. Как пояснялось в разделе 4.1, отсутствует способ сообщения о том, какие адреса принадлежат мобильным узлам, которые действительно могут посылать обновления привязки, а какие адреса принадлежат стационарным узлам (см. ниже), поэтому потенциально любой узел (включая «статические» узлы) являются уязвимыми.

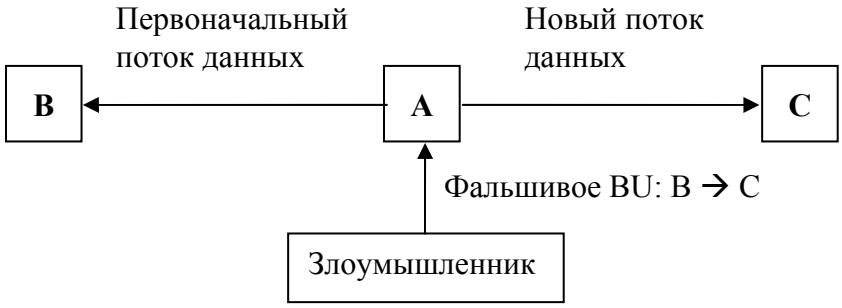

Рис. 7. Атака «хищения» адреса

Рассмотрим IP-узел A, посылающий IP-пакеты другому IP-узлу B. Злоумышленник может переадресовать пакеты на произвольный адрес C путем посылки A сообщения Binding Update. Домашним адресом (HoA - home address) в обновлении привязки будет B, а временным адресом (CoA - care-of address) будет C. После получения этого обновления привязки A будет посылать все пакеты, предназначенные узлу B, на адрес C (см. рис. 7).

Злоумышленник может выбрать, будет ли временный адрес его собственным текущим адресом, другим адресом в его локальной сети, или любым другим IP-адресом. Если злоумышленник выберет локальный временный адрес, на котором он сможет получать пакеты, то он окажется способным посылать узлу-корреспонденту последующие пакеты. Входная фильтрация в локальной сети злоумышленника не предотвращает подделку сообщений Binding Update, но заставляет злоумышленника либо выбирать временный адрес из диапазона адресов своей собственной сети, либо использовать под-опцию Alternate care-of address.

Механизм авторизации обновлений привязки, используемый в проекте безопасности MIPv6, предназначен в основном для смягчения этой угрозы, а также для ограничения возможного местоположения злоумышленника путем между узлом-корреспондентом и домашним агентом.

5.1.2. Хищение адресов стационарных узлов

Злоумышленник должен знать или пытаться отгадать IP-адреса как источника пакетов, которые должны быть направлены в другую сторону (A в примере выше), так и место назначения пакетов (B). Это означает, что трудно переадресовать все пакеты, поступающие на некоторый узел или от него, поскольку злоумышленнику необходимо знать IP-адреса всех узлов, с которыми тот осуществляет обмен информацией.

Узлы с общеизвестными адресами, например, серверы и узлы, использующие бесконтекстное автоконфигурирование (автоконфигурирование без сохранения состояния), являются наиболее уязвимыми. Узлы, которые являются частью сетевой инфраструктуры, например, DNS-серверы, являются особенно интересными целями для злоумышленников и наиболее простыми для идентификации.

Узлы, часто меняющие свои адреса и использующие случайные адреса, являются относительно защищенными. Однако если они регистрируют свои адреса в динамической системе DNS, то они становятся более уязвимыми. Подобным образом, узлы, которые посещают общедоступные сети, например, беспроводные ЛВС аэропортов, рискуют раскрыть свои адреса. Свойства конфиденциальности IPv6-адресации [6] в некоторой степени смягчают эти риски, но следует заметить, что адреса не должны использоваться повторно до тех пор, пока еще имеются открытые сеансы, которые эти адреса используют.

Таким образом, наиболее уязвимыми для атак хищения адресов являются не мобильные узлы, а общеизвестные статические серверы. Более того, серверы часто работают под управлением старых и сильно оптимизированных операционных систем, и могут вообще не иметь связанного с мобильностью кода. Таким образом, разработка системы безопасности не может базироваться на идее о том, что мобильный узел может оказаться способным как-то определить, что кто-то похитил его адрес, и сбросить состояние в узле-корреспонденте. Вместо этого система безопасности в первую очередь должна предпринимать разумные меры для предотвращения создания ложных элементов кэша привязок.

5.1.3. Хищение «будущего» адреса

Если злоумышленник знает адрес, который узел, вероятно, выберет в будущем, он может организовать атаку хищения «будущего» адреса. Злоумышленник создает элемент кэша привязок, используя домашний адрес, который по его предположению целевой узел будет использовать. Если домашний агент допускает динамическое распределение домашних адресов, злоумышленник может оказаться способным это сделать законно. А именно, если злоумышленник является клиентом домашнего агента и способен получить домашний адрес на некоторое время, он может получить домашний адрес, а затем вернуть его назад домашнему агенту, когда элемент кэша привязок уже сформирован.

Теперь, если состояние элемента кэша привязок имеет продолжительный срок годности, целевой узел получит тот же самый домашний адрес, в то время как подложный элемент кэша привязок все еще действует, и злоумышленник становится способным запустить успешную атаку типа «человек посередине» или «отказ в обслуживании». Примененный в проекте безопасности MIPv6 механизм состоит в том, чтобы ограничить время жизни элемента кэша привязок несколькими минутами.

Заметим, что эта атака применяется только в довольно специфических условиях. Имеются также некоторые вариации этой атаки, которые теоретически возможны при наличии некоторых других условий. Однако все эти атаки ограничены временем жизни элемента кэша привязок и поэтому не имеют реального отношения к существующей в настоящее время спецификации MIPv6.

5.1.4. Атаки на секретность и целостность

При подделке обновлений привязки злоумышленник может переадресовать самому себе все пакеты, посылаемые между двумя IP-хостами. При посылке подложного обновления привязки узлу A, он может захватить (записать) данные, предназначенные для узла B. А именно, он может сделать вид, что является узлом B и похитить соединения узла A с узлом B, или установить новые подложные соединения. Злоумышленник может также послать подложные обновления привязки как A, так и B, и поставить самого себя посередине всех соединений между ними (атака типа «человек посередине»). В результате злоумышленник может оказаться способным видеть и модифицировать пакеты, посылаемые между A и B (см. рис. 8).

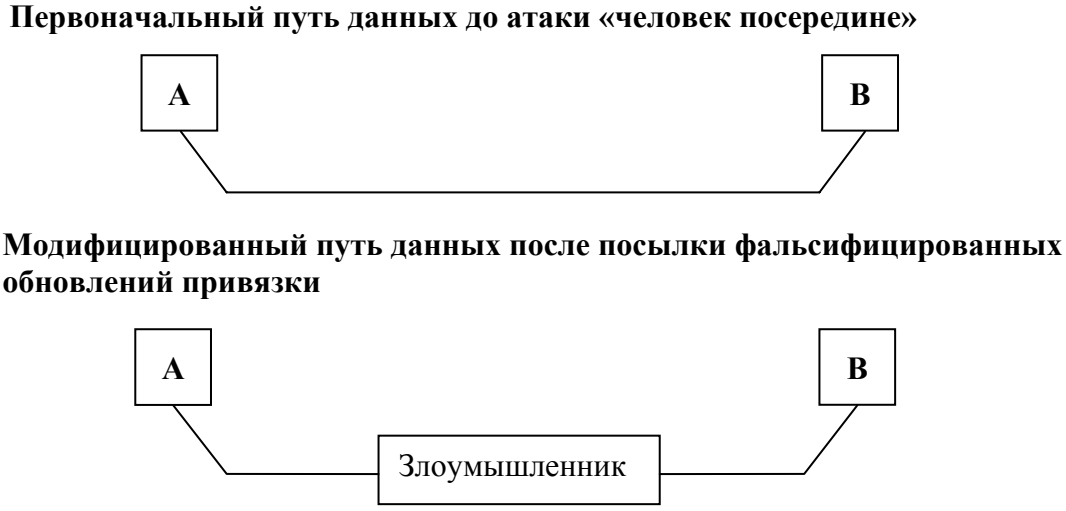

Рис. 8. Атака типа «человек посередине».

Строгие сквозные методы шифрования и защиты целостности, например, использование аутентифицированной защиты IPsec, могут предотвратить все атаки на секретность и целостность данных. Если данные защищены криптографически, подложные обновления

привязки могут привести к отказу в обслуживании (см. ниже), но не к раскрытию или порче чувствительных данных (возможно только обнаружение существования потоков трафика). Два фиксированных узла могут также защитить обмен информацией между собой путем отказа принимать друг от друга обновления привязки. С другой стороны, в данном случае входная фильтрация не помогает, поскольку злоумышленник в качестве временного адреса использует свой собственный адрес и не подделывает IP-адрес источника.

Применяемый в спецификации MIPv6 метод защиты заключается в аутентификации (хотя и слабой) адресов с помощью процедуры обратной маршрутизируемости (RR - return routability), которая ограничивает топологическое местоположение злоумышленника, из которого такая атака возможна (см. раздел 6.1).

5.1.5. Основной вариант атаки «отказа в обслуживании»

При посылке подложных обновлений привязки злоумышленник может переадресовать все пакеты, посылаемые между двумя IP-узлами, на случайный или несуществующий адрес (адреса). Таким способом он может оказаться способным остановить или нарушить обмен информацией между узлами. Атака является серьезной, поскольку любой узел Internet может оказаться ее целью, даже фиксированные узлы, принадлежащие к инфраструктуре (например, серверы DNS), являются уязвимыми. В этом случае также применяемым механизмом защиты является процедура обратной маршрутизируемости.

5.1.6. Повторное воспроизведение и блокирование обновлений привязки

Любой протокол аутентификации обновления привязки должен рассматривать атаки повторного воспроизведения. А именно, злоумышленник может оказаться способным повторно воспроизвести недавно аутентифицированные обновления привязки к корреспонденту и, таким образом, направить пакеты на прежнее местоположение мобильного узла. Подобно подложным обновлениям привязки, это может использоваться как для захвата пакетов, так и для атак типа «отказ в обслуживании». Злоумышленник может захватывать пакеты и имитировать мобильный узел, если он запоминает прежний адрес мобильного узла и затем после перемещения последнего повторно воспроизводит предыдущее обновление привязки для переадресации пакетов назад на предыдущее местоположение.

В родственной атаке злоумышленник блокирует обновления привязки от мобильного узла в его новом местоположении, например, путем создания помех в радиоканале или путем организации атаки «затопления», и захватывает его соединения на старом местоположении. Злоумышленник окажется способным захватывать пакеты, посылаемые мобильному узлу, и имитировать мобильный узел до тех пор, пока не истечет время жизни элемента кэша привязок в узле-корреспонденте.

Обе описанные выше атаки, требуют, чтобы злоумышленник находился в той же самой локальной сети, что и мобильный узел, где он может относительно просто наблюдать пакеты и блокировать их, даже если мобильный узел не перемещается на новое местоположение. Поэтому, считается, что эти атаки не настолько серьезны, как атаки, которые могут быть организованы из удаленного местоположения. Ограниченное время жизни элемента кэша привязок и связанных с ним одноразовых номеров ограничивает интервал времени, в течение которого возможны атаки повторного воспроизведения.

5.2. Атаки на другие узлы и сети («затопление»)

Путем посылки подложных обновлений привязки злоумышленник может переадресовать трафик на произвольный IP-адрес. Это может быть использовано для бомбардировки

произвольного Internet-адреса непомерным количеством пакетов. Злоумышленник может также иметь целью целую сеть путем переадресации данных на один или несколько IP-адресов этой сети. Имеется две вариации атак «затопления»: «затопление» временного адреса (basic flooding) и «затопление» домашнего адреса (return-to-the-home flooding). Они будут рассмотрены по отдельности.

5.2.1. «Затопление» временного адреса

В самой простой атаке злоумышленник знает, что имеется интенсивный поток данных от узла A к узлу B, и переадресует его на целевой адрес C. Однако узел A вскоре прекратит посылать данные, поскольку он не получает подтверждений от B.

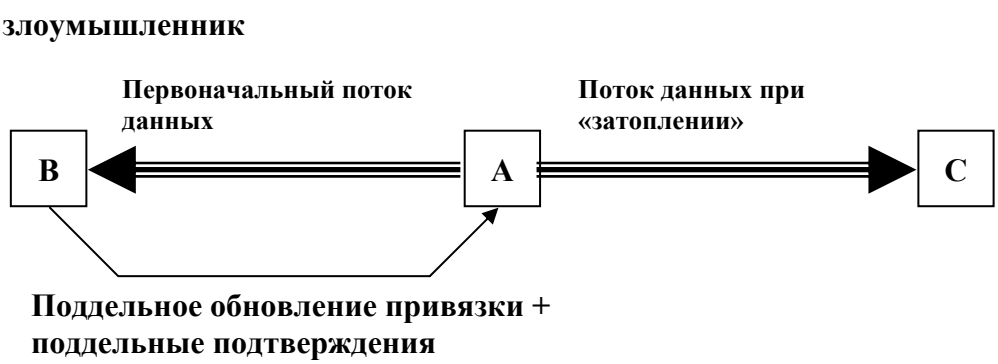

Рис. 9. Атака «затопления» временного адреса.

Более изощренный злоумышленник действует сам как B (см. рис. 9). Сначала он подписывается на поток данных (например, поток видео данных), а затем переадресует его на целевой адрес C. Злоумышленник может оказаться способным подделывать даже подтверждения. Например, рассмотрим поток TCP. Злоумышленник сам выполняет TCP-квитирование и, таким образом, знает начальные порядковые номера. После переадресации данных на C злоумышленник будет посылать подложные подтверждения. Он окажется даже способным увеличить скорость данных путем имитации «толстого канала» (fatter pipe) [7].

Эта атака может оказаться даже проще при использовании UDP/RTP. Злоумышленник может создавать поддельные подтверждения RTCP. В любом случае злоумышленник, не выполняя большой работы, может оказаться способным переадресовать нарастающий поток ненужных данных на целевой адрес. Он может продолжать открывать следующие потоки и обновлять элементы кэша привязок путем посылки нового обновления привязки через каждые несколько минут. Таким образом, одно ограничение времени жизни элемента кэша привязок несколькими минутами здесь не помогает.

В процессе разработки мобильного IPv6 обсуждалась эффективность этой атаки. Ошибочно предполагалось, что целевой узел пошлет источнику ненужного потока данных команду TCP Reset, который затем прекратит посылку данных. В действительности все практические реализации TCP/IP не выполняют посылки Reset. Целевой узел отбрасывает ненужные пакеты на уровне IP, поскольку он не имеет элемента списка обновлений привязки, соответствующего заголовку маршрутизации в поступающем пакете. Таким образом, «затопляющие» данные никогда не обрабатываются уровнем TCP целевого узла, и никакой команды Reset не посылается. Это означает, что атака с помощью потоков TCP является более эффективной, чем первоначально ожидалось.

Эта атака является серьезной, поскольку ее целью может оказаться любой узел или любая сеть, а не только мобильный узел. Что делает ее особенно серьезной по сравнению с другими атаками, так это то, что сама цель не может сделать что-либо для

предотвращения этой атаки. Например, ситуация не меняется, если целевая сеть прекращает использование оптимизации маршрутов. Ущерб наиболее значительный, если эти методы используются для усиления эффекта других атак распределенного отказа в обслуживании (DDoS - distributed denial of service). Входная фильтрация в локальной сети злоумышленника предотвращает подделку адресов источников, но атака все еще возможна путем установки целевого адреса в подопцию Alternate Care-of Address.

Как и в предыдущих случаях, применяемым в MIPv6 механизмом защиты является процедура обратной маршрутизируемости. При попытке переадресации потока данных необходимо проверить, что действительно имеется узел на новом временном адресе, и что этот узел является узлом, который запросил переадресацию пакетов именно на этот адрес (см. раздел 6.1.2).

5.2.2. «Затопление» домашнего адреса

Одна из разновидностей атаки бомбардировки нацелена на домашний адрес или на домашнюю сеть, а не на временный адрес или на посещаемую сеть. Злоумышленник заявляет, что он является мобильным узлом с домашним адресом равным адресу цели. Наряду с тем, что злоумышленник заявляет, что находится вне дома, он начинает загрузку потока данных. Затем злоумышленник посылает команду аннулирования ранее посланного обновления привязки (т.е. запрос на удаление привязки из кэша привязок), или просто позволяет истечь времени жизни элемента кэша. Любое из этих действий переадресует поток данных на домашний адрес. Так же, как и при бомбардировке временного адреса, злоумышленник путем подделки подтверждений может поддерживать поток живым и даже увеличить скорость передачи данных. В случае успешного проведения атака бомбардировки домашней сети настолько же серьезна, что и атака бомбардировки временного адреса.

Основным применяемым механизмом защиты в этом случае также является процедура обратной маршрутизируемости. Однако полностью защититься от этой атаки трудно (см. раздел 6.1.1).

5.3. Атаки на протоколы обновления привязки

Протоколы безопасности, которые успешно защищают секретность и целостность данных, иногда могут сделать участников более уязвимыми для атак отказа в обслуживании. В действительности, чем строже аутентификация, тем легче для злоумышленника может оказаться использование свойств протокола для исчерпания ресурсов мобильного узла или узла-корреспондента.

5.3.1. Порождение ненужных обновлений привязки

Когда мобильный узел получает IP-пакет от нового корреспондента через домашнего агента, он может запустить протокол обновления привязки. Злоумышленник может использовать это путем посылки мобильному узлу подложных IP-пакетов (например, пакетов ping или TCP SYN), которые представляются поступившими от нового узла-корреспондента. Поскольку пакет поступает через домашнего агента, мобильный узел может запустить протокол обновления привязки с этим узлом-корреспондентом. Решение о том, запускать или не запускать в этом случае процедуру обновления привязки, зависит от нескольких факторов (включая эвристики, информацию смежных уровней, опции конфигурирования и т.д.), и оно не специфицируется мобильным IPv6. Решение о том, чтобы не инициировать процедуру обновления привязки автоматически, может смягчить эти атаки, но в общем случае не сможет их устранить полностью.

В реальной атаке злоумышленник будет побуждать мобильный узел запускать протоколы обновления привязки с большим количеством узлов-корреспондентов в один и тот же

момент времени. Если адреса корреспондентов являются реальными адресами существующих IP-хостов, то большинство запущенных экземпляров протокола обновления привязки могут даже успешно завершиться. Элементы, созданные в кэшах привязок, являются правильными, но бесполезными. Таким способом злоумышленник может заставить мобильный узел впустую выполнять протокол обновления привязки, что может исчерпать ресурсы мобильного узла.

Узел-корреспондент (т.е. любой IP-узел) также может быть атакован подобным способом. Злоумышленник посылает подложные IP-пакеты большому числу мобильных устройств с целевым адресом узла в качестве адреса источника. Эти мобильные устройства запустят протокол обновления привязки с целевым узлом. И опять, большая часть экземпляров протокола обновления привязки завершится благополучно. Путем порождения большого числа ненужных обновлений привязки злоумышленник способен потреблять ресурсы целевого узла.

Эта атака возможна на любой протокол аутентификации обновления привязки. Чем больше ресурсов потребляет протокол обновления привязки, тем более серьезна атака. Поэтому протокол строгой криптографической аутентификации является более уязвимым к этой атаке, чем протокол слабой аутентификации или вообще не аутентифицированные обновления привязки. Входная фильтрация помогает мало, поскольку она усложняет подделку адреса источника поддельных пакетов, но полностью не устраняет эту угрозу.

Узел должен сам защищать себя от этой атаки путем установки ограничения на количество ресурсов, то есть на время обработки, память и полосу пропускания средств связи, которые он использует для обработки обновлений привязки. Когда ограничение превышается, узел может просто остановить оптимизацию маршрутов. Иногда можно обрабатывать некоторые обновления привязки, даже если узел подвергается атаке. Мобильный узел может иметь локальную политику безопасности, в которой перечислено ограниченное количество адресов, на которые будут посылаться обновления привязки, даже когда мобильный узел подвергается DoS-атаке. Узел-корреспондент (то есть любой IP-узел) может подобным образом иметь локальную политику безопасности, в которой перечислен ограниченный набор адресов, с которых обновления привязки будут признаваться годными, даже если корреспондент подвергается DoS-атаке обновления привязок.

Узел может также распознавать адреса, с которыми он имел осмысленный обмен информацией в прошлом, и посылать обновления привязки или принимать их с этих адресов. Поскольку для уровня IP может оказаться невозможным узнать состояние протокола на более высоких протокольных уровнях, вероятно хорошей мерой осмысленности прошлых обменов информацией является подсчет пакетов для каждого адреса.

Раздел 11.7.2 ("Correspondent Registration") в [2] не специфицирует точно, когда такая процедура оптимизации маршрутов должна инициироваться. Он указывает только, когда целесообразно это делать. Этот вопрос остается той областью, в которой необходимы дополнительные исследования. Очевидно, что поскольку оптимизация маршрутов является дополнительной возможностью, любой узел, который считает нагрузку по ее обработке чрезмерной или неоправданной, может просто ее отключить (либо выборочно, либо полностью).

5.3.2. Принудительное выполнение неоптимизированной маршрутизации

В качестве варианта предыдущей атаки злоумышленник может препятствовать в использовании узлом-корреспондентом оптимизации маршрутов путем наполнения его

кэша привязок ненужными элементами так, что большинство элементов для реальных мобильных устройств отбрасывается.

Любая успешная DoS-атака на мобильный узел или на узел корреспондента может также препятствовать обработке обновлений привязки. Разработчики MIPv6 предложили, чтобы целевой узел, подвергающийся DoS-атаке, мог отвечать путем остановки оптимизации маршрутов для всех или некоторых обменов информацией. Очевидно, злоумышленник может использовать этот запасной механизм и заставить целевой узел использовать менее эффективную, базирующуюся на домашнем агенте маршрутизацию. Злоумышленнику нужно только организовать заметную DoS-атаку на мобильный узел или на узел корреспондента, и цель по умолчанию перейдет на неоптимальную маршрутизацию.

Целевой узел может ослабить последствия атаки путем резервирования большего пространства для кэша привязок, путем перехода к неоптимальной маршрутизации только когда он не может иным способом справиться с DoS-атакой, путем попытки активно вернуться к оптимальной маршрутизации или путем оказания поддержки тем мобильным узлам, с которыми он имеет установленные отношения. Эта атака не так серьезна, чем описанная ранее, но приложения, которые полагаются на оптимизацию маршрутов, все еще могут быть затронуты. Например, разговорные мультимедийные сеансы могут сильно пострадать из-за дополнительных задержек, вызванных треугольной маршрутизацией (маршрутизацией через домашнего агента).

5.3.3. Отражение и усиление

Иногда злоумышленники пытаются скрыть источник атаки «затопления» пакетами путем отражения трафика от других узлов [8]. А именно, вместо того, чтобы посылать поток пакетов непосредственно цели, злоумышленник посылает данные другим узлам, втягивая их обманным путем в посылку цели того же или большего числа пакетов. Такое отражение может скрыть адрес злоумышленника, даже когда входная фильтрация предотвращает подмену адреса источника. Отражение особенно опасно, если пакеты могут отражаться по несколько раз, если они могут быть посланы по зацикленному пути, или если узлы могут быть втянуты обманным путем в посылку намного большего числа пакетов, чем они получают от злоумышленника, поскольку такие свойства могут использоваться для увеличения объема трафика с существенным коэффициентом усиления. Поэтому при разработке протоколов необходимо обходить сервисы, которые могут быть использованы для отражения и усиления.

Треугольная маршрутизация просто создает возможности для отражения: узел-корреспондент получает пакеты (например, TCP SYN) от мобильного узла и отвечает на домашний адрес, заданный мобильным узлом в опции Home Address (HAO). Реально мобильный узел может оказаться не мобильным узлом, а домашний адрес в действительности может быть адресом цели. Цель будет видеть только пакеты, посланные корреспондентом, и не может видеть адреса злоумышленника (даже если входная фильтрация не дает возможности злоумышленнику подменить его адрес источника).

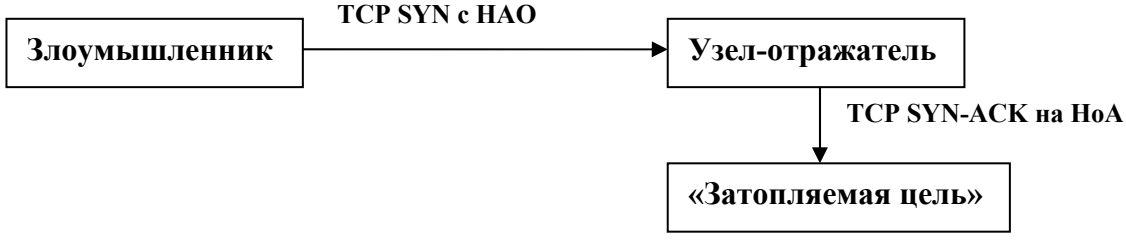

Рис. 10. Атака «отражения».

Плохо разработанный протокол обновления привязки также может использоваться для отражения: корреспондент отвечает на пакет данных инициализацией протокола аутентификации обновления привязки, который обычно вызывает посылку пакета на домашний адрес. В этом случае, атаке отражения можно воспрепятствовать путем копирования в сообщения адреса мобильного узла, посланного мобильным узлом корреспонденту (для мобильного узла адрес источника обычно совпадает с временным адресом, но в подопции Alternative Care-of Address может указываться другой временный адрес). В некоторых начальных предложениях по безопасности MIPv6 использовался этот подход, который был подвержен атакам отражения.

В некоторых предложениях для протокола аутентификации обновлений привязки, узел-корреспондент отвечал на начальное сообщение, полученное от мобильного узла двумя пакетами (одним на домашний адрес, другим на временный адрес). Это может быть использовано для усиления атаки «затопления» с коэффициентом два. Более того, при аутентификации с открытым ключом пакеты, посланные корреспондентом, могут быть значительно большего размера, чем пакеты, их инициирующие.

Этих типов отражения и усиления можно избежать, если корреспондент будет отвечать только на тот же адрес, от которого он получил пакет, и только одним пакетом того же размера. Эти принципы были применены при разработке системы безопасности MIPv6.

5.4. Классификация атак

На рис. 11 представлена сводка рассмотренных атак. На сегодня, атаки затопления домашнего адреса и порождения ненужных обновлений привязки рассматриваются как угрозы, которые имеют наименьшую степень защиты, по сравнению с их серьезностью.

Раздел	Название атаки	Цель атаки	Степень серьезности	Средство смягчения
5.1.1	Основной вариант атаки хищения адреса	MN	Средняя	RR
5.1.2	Хищение адресов стационарных узлов	Любая	Высокая	RR
5.1.3	Хищение «будущего» адреса	MN	Низкая	RR, Время жизни
5.1.4	Атаки на секретность и целостность	MN	Низкая	RR, IPsec
5.1.5	Основной вариант атаки «отказа в обслуживании»	Любая	Средняя	RR
5.1.6	Повторное воспроизведение и блокирование обновлений привязки	MN	Низкая	Время жизни, идентифицирующие цепочки
5.2.1	«Затопление» временного адреса	Любая	Высокая	RR
5.2.2	«Затопление» домашнего адреса	Любая	Высокая	RR
5.3.1	Порождение ненужных обновлений привязки	MN,CN	Средняя	Эвристики
5.3.2	Принудительная неоптимальная маршрутизация	MN	Низкая	Эвристики
5.3.3	Отражение и усиление	-	Средняя	Разработка протокола BU

Рис. 11. Основные виды атак на MIPv6.

5.5. Проблемы с авторизацией, базирующейся на инфраструктуре

На начальных стадиях процесса разработки MIPv6 предполагалось, что для защиты обновлений привязки может использоваться простой протокол IPsec. Однако это оказалось невозможным по двум причинам. Первая причина может быть выведена из приведенных выше описаний атак: протокол IPsec не разрабатывался для защиты от таких видов атак «отказа в обслуживании», которые станут возможными при использовании MIPv6. Защита с помощью простого протокола IPsec от атак «затопления» была бы очень сложной или даже невозможной. Второй причиной является масштабируемость.

Протокол IPsec требует управления ключами, а управление ключами требует инфраструктуры для распределения ключей. Более того, в MIPv6 важно показать, кому принадлежит IP-адрес, т.е. кто имеет полномочия контролировать, куда могут переадресоваться пакеты, предназначенные для заданного адреса. Только «владелец» адреса может посылать обновления привязки для переадресации пакетов на временный адрес.

Для обеспечения глобальной инфраструктуры ключей для мобильного IP предполагалось использование системы DNSSEC. Если бы существовала безопасная инверсная система DNS, которая обеспечивала бы открытый ключ для каждого IP-адреса, она могла бы использоваться для проверки того, что обновление привязки действительно подписано авторизованной стороной. Однако для того, чтобы эта система была безопасной, каждый линк в такой системе должен быть безопасным. А именно, должна существовать цепочка ключей и подписей на всем пути от корня до данного IP-адреса. Более того, не достаточно, чтобы каждый ключ был подписан ключом более высокого уровня, необходимо также, чтобы каждая подпись переносила смысл авторизации ключа нижнего уровня на управление блоком адресов, расположенным ниже его.

Например, рассмотрим элемент инверсной DNS e.f.f.3.ip6.arpa. Он может быть ассоциирован с ключом, скажем K_3ffe. Чтобы этот ключ был действительным, он должен быть подписан ключом более высокого уровня, скажем K_3ff, и т.д. до самого верхнего уровня. Подобным образом, любой поддиапазон адресов ниже 3ff0::/16 должен быть подписан ключом K_3ffe. Дополнительно, когда человек, управляющий ключом K_3ffe, подписывает подключи, он должен убедиться в том, что подписываемый подключ действительно принадлежит стороне, которая авторизована распределять блоки адресов в указанном диапазоне адресов. Другими словами, ключи и подписи должны принимать форму дерева, отражающего действительное распределение адресов.

Даже если теоретически можно было бы построить инфраструктуру инверсной DNS в соответствии с указанными выше контурами, практические проблемы оказались бы неодолимыми. А именно, в то время как делегирование ключей и их подписывание могли бы работать близко к корню дерева, они, вероятно, не смогут работать где-то между корнем и индивидуальными узлами. Более того, проверка всех подписей вверх по дереву создаст на корреспондента значительную нагрузку, делая оптимизацию маршрутов вычислительно очень дорогой. Помимо всего прочего, проверки только того, что мобильный узел авторизован на посылку обновлений привязки, содержащих данный домашний адрес, не достаточно, поскольку злонамеренный мобильный узел все еще окажется способным организовывать атаки «затопления». С другой стороны, опора на такую инфраструктуру для назначения и проверки «владения» временными адресами окажется даже еще более сложной, чем проверка «владения» домашним адресом.

6. Проектные решения по безопасности MIPv6

С целью предотвращения или ослабления угроз, которые обсуждались в разделе 5, средствам безопасности оптимизации маршрутов мобильного IPv6 было уделено серьезное внимание. Разработчики MIPv6 ставили задачу достижения такого уровня безопасности, который близок к уровню безопасности сети Internet, базирующейся на статическом IPv4. При этом считалось, что издержки в пересчете на пакеты, задержку и обработку не должны быть чрезмерными. Созданный протокол не является криптографическим протоколом в традиционным понимании. Он в значительной степени основывается на предположении о неповрежденной инфраструктуре маршрутизации, и строится на идее проверки того, что подозрительный мобильный узел действительно достижим как по своему домашнему, так и по своему временному адресу. Более того, чтобы ограничить потенциальную возможность сдвига атаки во времени, время жизни состояния, создаваемого в узлах-корреспондентах, сознательно ограничивается

несколькими минутами. Ниже дано краткое описание работы созданных средств безопасности.

6.1. Обратная маршрутизируемость

Обратная маршрутизируемость (RR - Return Routability) – это название основного механизма, который был применен для обеспечения безопасности оптимизации маршрутов мобильного IPv6. По существу она означает проверку того факта, что имеется узел, который способен отвечать на пакеты, посланные по заданному адресу. Вообще говоря, такая проверка ничего не гарантирует, если компрометируется инфраструктура маршрутизации, или если на пути между проверяющим узлом и адресом, который должен быть проверен, имеется злоумышленник. С этими исключениями предполагается, что успешный ответ указывает на то, что действительно имеется узел на заданном адресе, и что узел готов отвечать на посылаемые ему пробные сообщения.

Основной механизм обратной маршрутизируемости состоит из двух проверок, проверки домашнего адреса (см. раздел 6.1.1) и проверки временного адреса (см. раздел 6.1.2). Порядок посылки пакетов показан на рис. 12. Сначала мобильный узел посылает узлу-корреспонденту два пакета: пакет Home Test Init (HoTI) посылается через домашнего агента, а пакет Care-of Test Init (CoTI) посылается прямо. Узел-корреспондент отвечает на оба этих пакета независимо путем посылки сообщения Home Test (HoT) в ответ на сообщение Home Test Init и сообщения Care-of Test (CoT) в ответ на сообщение Care-of Test Init. В заключение, когда мобильный узел получил оба пакета Home Test и Care-of Test, он посылает узлу-корреспонденту сообщение Binding Update.

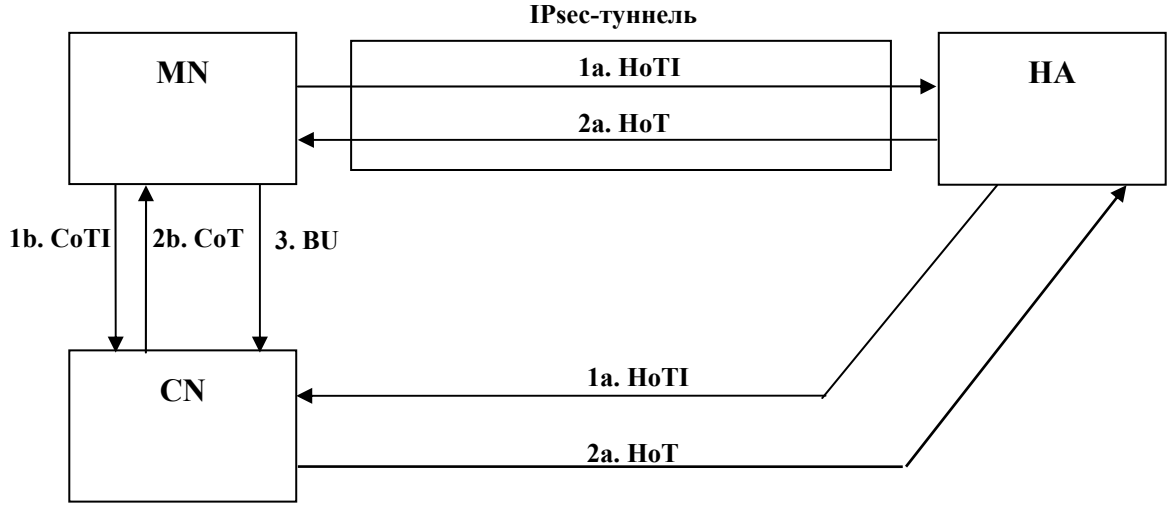

Рис. 12. Выполнение проверки обратной маршрутизируемости.

Может показаться, что такая проверка оказывается слишком запутанной. А именно, реальными проверками обратной маршрутизируемости являются пары < Home Test, Binding Update > и < Care-of Test, Binding Update >. Пакеты Home Test Init и Care-of Test Init нужны только для инициирования проверочных пакетов, а сообщение Binding Update фактически является объединенным ответом на эти обе проверки.

За таким замыслом стоят две основные причины:

- предотвращение отражения и усиления (см. раздел 5.3.3), и
- предотвращение атак отказа в обслуживании, направленных на исчерпание состояния (см. раздел 6.2).

Причина посылки двух инициализирующих пакетов Init вместо одного заключается в предотвращении эффекта усиления. Узел-корреспондент ничего не знает о мобильном узле, и поэтому он просто неожиданно для себя самого получает IP-пакет с некоторого произвольного IP-адреса. В некотором отношении его можно сравнить с сервером, получающим пакет TCP SYN от ранее неизвестного клиента. Если в ответ на инициирование узел-корреспондент посылал бы два пакета, то это бы создавало эффект усиления отказа в обслуживании, как обсуждалось в разделе 5.3.3.

С такой реализацией прямо связано и предотвращение отражения. Если узел-корреспондент отвечал бы на другой адрес, а не на адрес источника пакета, то это создавало бы эффект отражения. Таким образом, поскольку узел-корреспондент не знает ничего более лучшего, единственным надежным способом является ответ на полученный пакет только одним пакетом, и посылка ответа на адрес источника принятого пакета. Именно поэтому вместо одного инициализирующего пакета нужны два.

Теперь рассмотрим две проверки обратной маршрутизируемости по отдельности. Ниже трансформация криптографического материала для каждой из этих проверок показана в упрощенном виде (реальные формулы и более подробное описание даны в [2]).

6.1.1. Проверка домашнего адреса

Проверка домашнего адреса состоит из пакета Home Test (HoT) и последующего сообщения Binding Update (BU). Она инициируется поступлением пакета Home Test Init (HoTI). Узел-корреспондент отвечает на пакет Home Test Init посылкой пакета Home Test на адрес источника пакета Home Test Init. Предполагается, что адресом источника должен быть домашний адрес мобильного узла, и поэтому предполагается, что пакет Home Test должен туннелироваться домашним агентом мобильному узлу. Пакет Home Test содержит криптографически генерируемый маркер, home keygen token, который формируется путем вычисления хэш-функции от конкатенации секретного ключа Kcn, известного только узлу-корреспонденту, адреса источника пакета Home Test Init и одноразового номера.

```
home keygen token = hash(Kcn | home address | nonce | 0)
```

В пакет Home Test включается также индекс одноразового номера, который впоследствии позволяет узлу-корреспонденту проще найти соответствующий одноразовый номер.

Сам маркер позволяет узлу-корреспонденту убедиться в том, что полученное впоследствии обновление привязки создается узлом, который видел пакет Home Test (см. раздел 6.2).

В большинстве случаев пакет Home Test пересылается через два различных сегмента сети Internet. Сначала он проходит от узла-корреспондента к домашнему агенту. В этом переходе он не защищен и любой подслушивающий, находящийся на его пути, может узнать его содержимое. Затем домашний агент пересылает этот пакет мобильному узлу. Этот путь проходит внутри защищенного IPsec ESP туннеля, что делает невозможным для находящихся снаружи узнать содержимое пакета.

Может показаться, что необязательно защищать пакет между домашним агентом и мобильным узлом, поскольку он передавался незащищенным между узлом-корреспондентом и мобильным узлом. Если все линки в Internet были бы одинаково небезопасными, то ситуация была бы действительно такой, что это было бы необязательным. Однако в большинстве практических ситуаций сеть, вероятно, является более безопасной вблизи домашнего агента, а не вблизи мобильного узла. Например, если домашний агент размещается на виртуальном домашнем линке, а мобильные узлы в действительности никогда не бывают дома, то подслушивающий должен находиться рядом с узлом-корреспондентом, или на пути между узлом-корреспондентом и домашним агентом, поскольку он не может подслушивать за домашним агентом. Если узел-

корреспондент представляет собой большой сервер, то все линки на пути между ним и домашним агентом, вероятно, достаточно безопасны. С другой стороны, мобильный узел, вероятно, использует беспроводную технологию доступа, которая иногда позволяет тривиальным способом прослушивать его линк доступа. Таким образом, довольно просто прослушивать пакеты, которые поступают в мобильный узел. Следовательно, защита пути HA-MN, вероятно обеспечивает реальный эффект безопасности, даже когда путь CN-HA остается незащищенным.

6.1.2. Проверка временного адреса

С точки зрения узла-корреспондента проверка временного адреса очень похожа на проверку домашнего адреса. Единственная разница заключается в том, что теперь предполагается, что адресом источника принятого пакета Care-of Test Init является временный адрес мобильного узла. Более того, маркер формируется в немного измененной форме, чтобы было невозможно использовать маркеры home token для маркеров care-of token и наоборот.

```
care-of keygen token = hash(Kcn | care-of address | nonce | 1)
```

Пакет Care-of Test передается только по одному этапу пути прямо от узла-корреспондента мобильному узлу. Он остается незащищенным на протяжении всего пути, что делает его уязвимым для подслушивающих, находящихся рядом с узлом-корреспондентом, на пути от узла-корреспондента к мобильному узлу, или находящихся рядом с мобильным узлом.

6.1.3. Формирование первого обновления привязки

Когда мобильный узел получил оба сообщения Home Test и Care-of Test, он создает ключ привязки Kbm, вычисляя хэш-функцию от конкатенации полученных маркеров.

Этот ключ используется для защиты первого и последующих обновлений привязки до тех пор, пока не истечет срок годности этого ключа.

Заметим, что ключ Kbm доступен любому, кто способен получать сообщения Care-of Test и Home Test. Однако обычно эти сообщения маршрутизируются через сеть по различным маршрутам, и сообщение Home Test передается через зашифрованный туннель от домашнего агента к мобильному узлу (см. также раздел 7.4).

6.2. Безопасное создание состояния

Узел-корреспондент может оставаться бесконтекстным (не создавать состояния) до тех пор, пока он не получит первое сообщение Binding Update. А именно, ему не нужно что-либо запоминать при получении и ответе на сообщения Home Test Init и Care-of Test Init. Обмены сообщениями Home Test Init/Home Test и Care-of Test Init/Care-of Test выполняются параллельно, но независимо друг от друга. Таким образом, корреспондент может отвечать на каждое сообщение немедленно и не должен помнить, что сделал это. Это помогает в ситуациях потенциального отказа в обслуживании: при обработке сообщений Home Test Init и Care-of Test Init не требуется никакой памяти. Более того, сама обработка сообщений Home Test Init и Care-of Test Init достаточно легковесна, и если необходимо, может быть ограничена скорость передачи сообщений.

При получении первого обновления привязки узел-корреспондент выполняет достаточно сложную процедуру. Целью этой процедуры является проверка того, что действительно имеется мобильный узел, который недавно получил сообщения Home Test и Care-of Test, посланные на заявленные домашний и временный адреса, соответственно, и гарантия того, что узел-корреспондент при выполнении этой проверки не напрасно расходует CPU и другие ресурсы.

Поскольку узел-корреспондент при поступлении обновления привязки не имеет никакого состояния, само обновление привязки должно содержать достаточно информации для того, чтобы можно было создать соответствующее состояние. Для этого обновление привязки содержит следующие части информации:

Временный адрес, указанный в сообщении Binding Update должен быть равен адресу источника, использовавшегося в сообщении Care-of Test Init. Заметим, что это правило применяется к эффективному временному адресу сообщения Binding Update. В частности, если сообщение Binding Update включает альтернативный временный адрес (AltCoA - Alternate Care-of Address) [2], то эффективным временным адресом, конечно, является этот AltCoA. Таким образом, источником сообщения Care-of Test Init должен был быть этот AltCoA.

Домашний адрес, указанный в сообщении Binding Update, должен быть равен адресу источника, использовавшемуся в сообщении Home Test Init.

Эти адреса вместе с другой информацией позволяют узлу-корреспонденту восстановить маркеры, посланные в сообщениях Home Test и Care-of Test и использовавшиеся для создания ключа Kbm.

Обновление привязки аутентифицируется путем вычисления кода MAC от временного адреса, адреса узла-корреспондента и самого сообщения обновления привязки. Формирование кода MAC управляется ключом Kbm.

Имея адреса, индексы одноразовых номеров, а значит и сами одноразовые номера, и ключ Kcn, узел-корреспондент может заново создать маркеры home token и care-of token ценою нескольких обращений к памяти и вычисления одного кода MAC и одной хэш-функции.

После того, как узел-корреспондент восстановил маркеры, он вычисляет от них хэш-функцию, получая ключ Kbm. Если сообщение Binding Update аутентично, то Kbm кэшируется вместе с привязкой. Затем этот ключ используется для проверки кода MAC, который защищает целостность и источник действительного сообщения Binding Update. Заметим, что один и тот же ключ Kbm может использоваться в течение некоторого времени до тех пор, пока либо не переместится мобильный узел (и ему необходимо получить новый маркер care-of-address token), либо не истечет время жизни маркера care-of token, либо не истечет время жизни маркера home token.

6.2.1. Повторные передачи и автомат состояний

Заметим, что поскольку узел-корреспондент может оставаться бесконтекстным до тех пор, пока он не получит годного обновления привязки, то за повторные передачи полностью отвечает мобильный узел. Т.е., мобильный узел должен хранить посланные сообщения Home Test Init / Care-of Test Init до тех пор, пока он не получит сообщения Home Test / Care-of Test, соответственно. Подобным образом, он будет вынужден несколько раз посылать обновление привязки в случае, если оно теряется во время пересылки.

6.3. Ограничение срока годности элементов кэша привязок

Элемент кэша привязок вместе с ключом Kbm представляет состояние обратной маршрутизируемости сети на тот момент времени, когда были высланы сообщения Home Test и Care-of Test. Теперь возможно конкретный злоумышленник способен подслушать сообщение Home Test в некоторый момент времени, но не позже. Если бы сообщение Home Test имело бы бесконечное или большое время жизни, то это позволило бы злоумышленнику организовать атаку со сдвигом во времени (см. раздел 4.2). А именно, в текущей архитектуре IPv4 злоумышленник, находящийся на пути между узлом-корреспондентом и домашним агентом, способен осуществлять атаки только до тех пор, пока он способен подслушивать (и возможно разрывать) обмены информацией на этом

конкретном пути. Долго живущее сообщение Home Test и, следовательно, способность постоянно посылать годные обновления привязки, позволили бы злоумышленнику продолжать свою атаку даже после того, как он станет неспособным прослушивать путь.

Чтобы ограничить серьезность этой и других подобных угроз сдвига атак во времени, срок годности маркеров ограничивается несколькими минутами. Это действенно ограничивает срок годности ключа Kbm, время жизни получающихся обновлений привязки и элементов кэша привязок.

Хотя короткие времена жизни делают все необходимое для других аспектов системы безопасности, для эффективности и устойчивости протокола они, очевидно, являются вредными. А именно, обмен парой сообщений Home Test Init / Home Test должен осуществляться через домашнего агента через каждые несколько минут. Чисто с функциональной точки зрения эти сообщения не являются необходимыми и создают тем самым накладные расходы. Однако еще хуже то, что они делают домашнего агента единственной точкой отказа. Т.е., если бы сообщения Home Test Init / Home Test были бы не нужны, то существующие соединения от мобильного узла к другим узлам могли бы продолжаться даже в случае отказа домашнего агента, но принятое проектное решение вынуждает делать так, чтобы срок привязки истек через несколько минут.

Таким образом, в основе проекта безопасности MIPv6 лежат идеи обратной маршрутизируемости в сообщениях Home Test, Care-of Test и Binding Update, возможность для узла-корреспондента оставаться бесконтекстным до тех пор, пока не получено годное сообщение Binding Update, и ограничение времени жизни привязок несколькими минутами. Далее коротко обсуждаются оставшиеся угрозы и другие проблемы, присущие проекту.

7. Безопасность MIPv6

В данном разделе дается краткий анализ проекта безопасности MIPv6 главным образом в свете того, что было известно в момент, когда осенью 2002 года его разработка завершилась. Следует отметить, что в данном разделе не представляется настоящий анализ безопасности протокола, а лишь обсуждаются некоторые проблемы, которые были известны на момент завершения разработки.

Необходимо иметь в виду, что никогда не предполагалось, что режим оптимизации маршрутов MIPv6 будет полностью безопасным. Вместо этого, как отмечалось ранее, главной целью было достижение примерно того же уровня безопасности, которым на момент разработки обладал не мобильный IPv4. Как выяснилось, представленный в спецификации протокол немного менее безопасен, чем IPv4, но разница невелика и вероятнее всего будет не существенной в реальной жизни.

7.1. Оставшиеся угрозы в сравнении с IPv4

Как упоминалось в разделе 4.2, время жизни привязки создает потенциальную угрозу сдвига атаки во времени. А именно, злоумышленник, который способен создать поддельную привязку, может этим воспользоваться до тех пор, пока привязка существует, или, альтернативно, может задержать атаку «затопления» (раздел 5.2.2) домашней сети до тех пор, пока не истечет срок годности привязки. Это отличие от IPv4, в котором злоумышленник может продолжать атаку только до тех пор, пока он находится на пути между двумя узлами.

Поскольку в текущей спецификации время жизни привязок жестко ограничено, то соответствующим образом ограничена и способность реализации сдвига атаки во времени.

Конечно, в базовой линии IPv4 internet (раздел 3.3) угрозы, возможные благодаря введению режима оптимизации маршрутов, отсутствуют. В частности, порождение ненужных обновлений привязки потенциально может оказаться тяжелой атакой, но это скорее будет связано с неправильными реализациями. В качестве экстремальной меры узел-корреспондент может защититься от этих атак путем полного выключения режима оптимизации маршрутов. Если это сделать, то единственной оставшейся возможной атакой является упомянутая выше атака сдвига во времени, которую не ясно, как предотвратить (иначе, чем жестко ограничить в соответствии с принятой спецификацией).

7.2. Взаимодействие с IPsec

Главной мотивацией текущей спецификации протокола обновления привязкок была масштабируемость, способность выполнения протокола без наличия какой-либо существующей инфраструктуры безопасности. Альтернативный вариант должен был бы рассчитывать на существующие отношения доверия, возможно в форме специальной инфраструктуры открытых ключей и IPsec. Это ограничило бы масштабируемость, сделав режим оптимизации маршрутов доступным только в таких средах, где имеется возможность между мобильными узлами и узлами-корреспондентами создавать соответствующим образом авторизованные контексты безопасности IPsec.

Очевидно, имеются ситуации, когда существуют соответствующие отношения между мобильным узлом и узлом-корреспондентом. Например, именно таким случаем будет ситуация, если узел-корреспондент представляет собой сервер, который имеет предустановленные ключи с мобильным узлом. Однако для признания годными обновлений привязки, одной аутентификации объектов или одного аутентифицированного сеансового ключа не всегда достаточно. Если кто-то хочет заменить проверку домашнего адреса какими-либо криптографическими мандатами, то в этих мандатах должна передаваться соответствующая авторизация для конкретного домашнего адреса. Например, если мобильный узел выдает узлу-корреспонденту сертификат, и они впоследствии создают пару контекстов безопасности IPsec, то не совсем понятно, могут ли эти контексты безопасности использоваться для замены проверки домашнего адреса. Проверки домашнего адреса могут быть опущены, если и только если сертификат явно устанавливает, что представляет собой домашний адрес мобильного узла, и что мобильный узел авторизован для создания привязок для своего домашнего адреса. Более того, необходимо соблюдать осторожность, чтобы удостовериться в том, что выпускающий сертификат имеет право на выражение такой авторизации.

На практике, кажется маловероятным, чтобы узлы были способны заменить мандатами даже проверку временного адреса. Временные адреса недолговечны, и маловероятно, что мобильный узел окажется способным представить мандаты, которые показывали бы, что он авторизован для использования временного адреса без какой-либо проверки.

Спецификация мобильного IPv6 [2] не указывает, как использовать IPsec вместе с процедурами мобильности между мобильным узлом и узлом-корреспондентом. Поэтому в настоящее время отсутствуют стандартные способы замены проверки домашнего адреса. С другой стороны, спецификация написана достаточно тщательно, что позволяет создавать ключ управления привязкой Kbm с помощью разных средств.

7.3. Атака на соседние узлы

Одной из возможных атак на безопасность MIPv6 является претензия на роль соседнего узла. Чтобы запустить эту атаку, мобильный узел устанавливает оптимизацию маршрутов с некоторым произвольным узлом-корреспондентом. Во время выполнения проверок обратной маршрутизируемости и создания ключа управления привязкой Kbm,

злоумышленник использует свой реальный домашний адрес, но фальшивый временный адрес. В действительности временным адресом будет адрес какого-либо соседнего узла на локальном линке. Злоумышленник способен создать привязку, поскольку он нормально получает годное сообщение Home Test, и способен прослушивать сообщение Care-of Test, поскольку он находится на локальном линке.

Эта атака позволит мобильному узлу направлять нежелательный трафик в направлении соседнего узла, что приводит к атаке «затопления».

Однако на практике такая атака не очень серьезна. Во-первых, она ограничена в терминах местоположения, поскольку возможна только на соседей. Во-вторых, атака работает также против самого злоумышленника, поскольку он и цель атаки находятся на одном и том же локальном линке. В-третьих, подобная атака возможна подделкой протокола Neighbor Discovery.

7.4. Взаимодействие двух мобильных узлов

Когда два мобильных узла хотят установить друг с другом режим оптимизации маршрутов, должна быть проявлена некоторая осторожность, чтобы не открыть злоумышленнику обратные маркеры. В этой ситуации оба мобильных узла играют и роль мобильного узла и роль узла-корреспондента. В роли узла-корреспондента узлы уязвимы для злоумышленников, которые размещаются на том же самом линке. Такой злоумышленник способен узнать оба сообщения Home Test и Care-of Test, посылаемые мобильным узлом, и поэтому способен подделать местоположение другого мобильного узла на соседнее. Но хуже то, что злоумышленник сам может получить законное сообщение Care-of Test, объединить его с сообщением Home Test, и заявить соседнему узлу, что другой узел только что прибыл на тот же самый линк.

Имеется простой способ избежать этой атаки. В роли узла-корреспондента мобильный узел должен туннелировать посылаемые сообщения Home Test через своего домашнего агента. Это не позволяет размещающемуся рядом злоумышленнику узнать содержимое каких-либо законных сообщений Home Test.

8. Заключение

В данном обзоре рассмотрены основные принципы функционирования протокола мобильного IPv6, а также принципы реализации безопасности этого протокола. В основе безопасности MIPv6 лежат идеи обратной маршрутизируемости в сообщениях Home Test, Care-of Test и Binding Update, возможность для узла-корреспондента оставаться бесконтекстным до тех пор, пока не получено годное сообщение Binding Update, а также ограничение времени жизни привязок несколькими минутами. По существу этот протокол обеспечивает почти тот же самый уровень безопасности, что и уровень безопасности современной сети Internet, базирующейся на протоколе IPv4. Наиболее важным отличием представляется возможность организации атак со сдвигом во времени. Именно поэтому в спецификации жестко ограничено время жизни привязок, что, вообще говоря, отрицательно сказывается на эффективности протокола.

Следует отметить, что хотя спецификация MIPv6 получила статус проекта стандарта, работы над ней еще далеки от полного завершения. В частности в ней намечены направления будущих исследований. А именно, разработчики протокола продолжат работы в следующих направлениях:

1. Возможность комбинированной передачи сообщений управления привязками с передачей данных.

2. Возможность организации треугольной маршрутизации, т.е. передачи пакетов от мобильного узла узлу-корреспонденту с опцией Home Address без проверки наличия в кэше привязок узла-корреспондента предварительно установленной привязки.

3. Разработка новых методов авторизации, которые обеспечивают более высокий уровень безопасности, чем принятая процедура обратной маршрутизируемости.

4. Возможность динамического формирования новых домашних адресов мобильного узла без предварительной установки контекстов безопасности и сертификатов.

5. Возможность удаленного конфигурирования домашнего адреса.

6. Расширение протокола Neighbor Discovery для обеспечения быстрой передачи обслуживания при перемещениях мобильного узла.

Список литературы

[1] IETF Mobile IPv6 Working Group, http://www.ietf.org/html.charters/mip6-charter.html

[2] D. Johnson, C. Perkins, J. Arkko, «Mobility Support in IPv6», RFC 3775, June, 2004.

[3] P. Nikander, J. Arkko, T. Aura, G. Montenegro, E. Nordmark, draft-nikander-mobileip-v6-ro-sec-02 «Mobile IP version 6 Route Optimization Security Design Background», December 1, 2003

[4] Johnson, D. and S. Deering, «Reserved IPv6 Subnet Anycast Addresses», RFC 2526, March 1999.

[5] Bush, R. and D. Meyer, "Some Internet Architectural Guidelines and Philosophy", RFC 3439, December 2002.

[6] T. Narten and R. Draves. «Privacy extensions for stateless address autoconfiguration in IPv6», RFC 3041, January 2001.

[7] Savage, S., Cardwell, N., Wetherall, D. and T. Anderson, "TCP Congestion Control with a Misbehaving Receiver", Computer Communication Review 29:5, 1999.

[8] P. Savola. «Security of IPv6 routing header and home address options». Technical report, IETF, November 2002.