УДК 004.732

ПРОТОКОЛ МАРШРУТИЗАЦИИ ДЛЯ AD-HOC СЕТЕЙ

М.Л. Карманов

ROUTING IN AD-HOC NETWORKS

M.L. Karmanov

В статье описывается метод существенного повышения защищенности протоколов маршрутизации ad-hoc сетей от внешних воздействий. Ad-hoc сети - это относительно новое направление, предполагающее построение самоорганизующихся вычислительных сетей на базе беспроводных технологий. Изложенный в статье метод позволяет существенным образом повысить устойчивость алгоритмов маршрутизации от внешних воздействий, при этом, практически не увеличивая вычислительную сложность и объем служебного трафика.

Ключевые слова: вычислительные сети, алгоритмы маршрутизации, ad-hoc сети.

In given article the method of essential increase of security of reports of routeing ad-hoc of networks from external influences is described. Ad-hoc networks is rather new on-board, assuming construction self-organized computer networks on the basis of wireless technologies. The method stated in article allows to raise essentially stability of algorithms of routeing from external influences, thus, practically without increasing computing complexity and volume of the traffic.

Keywords: network, routing, ad-hoc networks.

Введение

В 1990-х годах широкое распространение получили мобильные компьютеры, оснащенные беспроводными интерфейсами. Именно тогда и зародилась идея создания так называемых ad-hoc сетей. Ad-hoc сеть подразумевает под собой объединение нескольких мобильных устройств с беспроводными сетевыми адаптерами в единую сеть передачи данных. При этом предполагается, что мобильные устройства принадлежат различным людям и единое централизованное административное управление отсутствует, кроме того, такие сети должны быть самоорганизующимися (самонастраивающимися). Также, необходимо учитывать мобильность узлов сети и их ограниченность как в вычислительных, так и в энергоресурсах.

Построение ad-hoc сетей порождает множество самых разнообразных проблем. В данной статье рассматривается только вопрос маршрутизации.

В ходе выполненного анализа существующих протоколов маршрутизации, используемых в таких сетях, выяснилось, что все они обладают слабой устойчивостью к ситуациям, при которых один или несколько узлов сети отклоняются от требований протокола. В ряде случаев такое поведение всего лишь одного узла может парализовать работу всей сети. Кроме того, большинство протоколов маршрутизации было так или иначе унаследовано из проводных сетей и слабо адаптировано к особенностям беспроводных ad-hoc сетей.

Был проведен детальный анализ причин неустойчивости протокола к отклонениям отдельных узлов от выполнения протокола. Эти причины были выделены и формализованы. Затем один из существующих протоколов динамической маршрутизации был существенным образом модернизирован. Было проведено моделирование работы нового протокола и проведен сравнительный анализ с другими протоколами.

В результате исследований было установлено, что новый протокол обладает свойством локализации воздействий, при этом вычислительные и энергозатраты возрастают незначительно, кроме того, новый протокол оказался более производительным по ряду параметров.

1. Обзор существующих протоколов маршрутизации

Был проведен анализ следующих протоколов динамической маршрутизации: OSPF, RIP, EBFRP, DSDV, DSR, AODV и ряда других. Для проведения анализа была разработана система критериев. Рассматривались следующие критерии: количество узлов, занимающихся маршрутизацией; уровень знания каждым узлом топологии всей сети; наличие у каждого узла маршрута до любого другого

Карманов Максим Леонидович - аспирант ЮУрГУ; Karmanov.Maxim@gmail.com

Karmanov Maxim Leonidovich - postgraduate student of SUSU; Karmanov.Maxim@gmail.com

узла; возможность использования различных метрик; возможность возникновения «петель»; знание резервных маршрутов до узла; время реакции на изменение топологии сети; объем данных передаваемых по сети для построения маршрута; количество ресурсов, необходимых узлу для построения таблицы маршрутизации; поддержка multicast (групповой рассылки); устойчивость протокола.

В результате проведенных исследований было выяснено, что все протоколы маршутизации, использующиеся на сегодняшний день в ad-hoc сетях, являются не устойчивыми к внешним и внутренним воздействиям. Во многих протоколах отклонение нескольких узлов от протокола может полностью парализовать работу сети.

Например, в описании одного из самых популярных протоколов AODV, прямо указано, что разработчики понимают, что их протокол является неустойчивым к внешним и внутренним воздействиям, но менять эту ситуацию пока не собираются [1].

На основании результатов проведенного исследования был выявлен наиболее подходящий протокол для ad-hoc сетей - Ad-hoc On demand Distance-Vector (AODV). Также в пользу этого выбора говорит то, что данный протокол получил отражение в RFC, и то, что многие последние доклады на различных конференциях связаны именно с этим протоколом. В том числе, проведены многочисленные исследования, в которых сравнивалась производительность различных протоколов в смоделированных сетях. По итогам этих исследований протокол AODV по многим параметрам оказался лучше остальных [2, 3, 4]. Кроме того, данный протокол используется во многих программных реализациях для построения ad-hoc сетей [5, 6].

2. Описание протокола AODV

Вкратце, работа данного протокола выглядит следующим образом. Если некоторому узлу, назовем его инициатором, требуется передать данные другому узлу, назовем его узлом назначения, а соответствующий маршрут не известен, то узел инициатор посылает широковещательный запрос RREQ для поиска данного маршрута. Этот запрос передается всем соседям данного узла, которые, в свою очередь, пересылают его своим соседям и так далее. Так как в запросе указана информация об узле инициаторе, то все узлы, получившие данный запрос строят маршруты до узла - инициатора. Через некоторое время данный запрос достигает либо узла назначения, либо некоторого промежуточного узла, которому известен необходимый маршрут. При этом узлу инициатору отправляется ответ RREP, который передается уже не широковещательно, а адресно, по маршруту, построенному при распространении запроса. В результате такой операции выстраивается двунаправленный маршрут между заинтересованными узлами. Правда, в случае ответа на запрос промежуточным узлом он обязан отправить ещё один «беспричинный» ответ уже не инициатору, а узлу назначения. Этот ответ необходим для построения обратного маршрута от узла назначения до инициатора.

Заметим, что информация, находящаяся у различных узлов сети, может иметь разную степень давности, при этом понятно, что для построения маршрутов лучше использовать более новую информацию. Для того чтобы можно было определять степень свежести информации, в данном протоколе введены порядковые номера узлов. Эта идея была взята из протокола DSDV, один из авторов которого C.E. Perkins является также и автором протокола AODV. Суть идеи состоит в следующем. Каждый узел имеет собственный порядковый номер, значением которого он управляет, кроме того, этот номер прикрепляется ко всей информации о маршрутах до данного узла, в том числе хранится и в таблицах маршрутизации. При изменении связей с соседними узлами, узел увеличивает свой порядковый номер. Благодаря этому, появляется возможность выбора более новой информации о маршрутах до данного узла.

При обнаружении нарушения маршрута узел, обнаруживший это нарушение, рассылает информацию об ошибке посредством специального сообщения RERR. При этом маршрут в большинстве случаев заново перестраивается.

На рис. 1 изображена отправка запроса REEQ (пунктирные стрелки) узлом *A,* который желает узнать маршрут до узла *B.* При этом один из промежуточных узлов - узел 5 знает необходимый маршрут и отправляет узлу *A* ответ RREP (сплошные стрелки), он же отправляет ещё один «беспричинный» ответ (сплошные стрелки) узлу *B,* для того, чтобы построился обратный маршрут от узла *B* к узлу *A*.

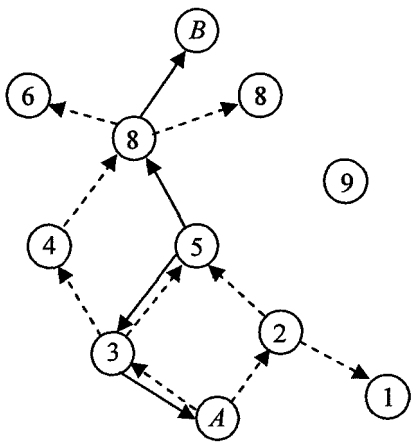

Рис. 1. Установление маршрута от *A* к *B*

При построении маршрутов в ad-hoc сетях, как правило, возможны различные варианты и узел *A* получит несколько ответов с различными маршрутами. При этом в первую очередь выбираются маршруты с большим порядковым номером

узла *B* (как маршруты, построенные на основании более новой информации), а среди маршрутов с одинаковым порядковым номером выбирается более короткий. Узел *A* не ожидает всех ответов, а начинает передачу данных после прихода первого ответа. Получив дополнительные ответы, он может изменить маршрут и следующие пакеты с данными передавать уже по более новому или короткому маршруту.

Обратим внимание на ряд особенностей данного протокола. Узел инициатор всегда выбирает более новый маршрут (с большим порядковым номером), даже если тот является существенно длиннее. Узел назначения при ответе на запрос может увеличивать свой порядковый номер только на единицу. Протокол AODV работает на прикладном уровне, используя в качестве транспортного протокола UDP. Получение узлом ответа RREP без отправки соответствующего запроса является нормальной ситуацией и получивший такой ответ узел должен его обработать.

3. Анализ устойчивости протокола AODV

Теперь перейдем к рассмотрению устойчивости данного протокола. Возможны два вида воздействий на протоколы маршрутизации. Первый вид воздействий может быть отнесен к классу man-in-the-middle. Своей целью данные воздействия ставят прокладку маршрута между двумя узлами через определенный третий узел, с целью прослушивания трафика между интересующими узлами. Второй вид воздействий принадлежит классу deny-of-service и ставит своей целью нарушение работы сети, путем создания неверных маршрутов, чрезмерного увеличения нагрузки на сеть или блокирования возможности создания верных маршрутов.

После тщательного изучения спецификации протокола AODV были разработаны способы реализации воздействий обоих видов. Важно отметить, что эти воздействия являются возможным не из-за ошибок в конкретных реализациях протокола, а из-за особенностей самого протокола маршрутизации.

Воздействия первого вида реализуются одним из двух способов. Узел *Z* отправляет узлам жертвам *A и B* «беспричинные» ответы, содержащие либо заниженное расстояние до второго узла, либо завышенный порядковый номер. При этом маршрут от узла *A* к узлу *B* выстраивается через узел *Z* и наоборот. Более выигрышной является стратегия завышения порядкового номера узла, так как при этом созданные маршруты обладают большей устойчивостью.

Поясним это с помощью рис. 2. На нем сплошными стрелками изображен «беспричинный» ответ RREP узлу *A,* содержащий завышенный порядковый номер узла *B.* То есть узлы 2 и *A* будут иметь неверную завышенную информацию о порядковом номере узла *B.* Также, сплошными стрелками обозначен «беспричинный» ответ RREP узлу *B.* При этом узлы 9, 8 и *B* будут иметь неверную завышенную информацию о порядковом номере узла *A.* Так как сами узлы *A и B* могут увеличивать свои порядковые номера не более чем на единицу при каждом запросе, то в течение некоторого времени вся информация, приходящая узлам *2 та A,* относительно маршрута до узла *B* будет иметь порядковый номер меньший, чем записан у этих узлов и, соответственно, будет игнорироваться. Аналогично с маршрутом от *X* до *B.* Заметим, что при реализации данного воздействия нарушается одно из двух соотношений, которые выполняются для произвольного маршрута ($A \to \ldots \to N \to \ldots \to B$) при нормальном функционировании протокола AODV:

$$D_B(A) > \ldots > D_B(N) > \ldots > D_B(B),$$

$$S_B(A) \le \ldots \le S_B(N) \le \ldots \le S_B(B),$$

где $D_B(N)$ – это расстояние до узла *B*, известное узлу *N*, а $S_B(N)$ – это порядковый номер узла *B*, известный узлу *N*.

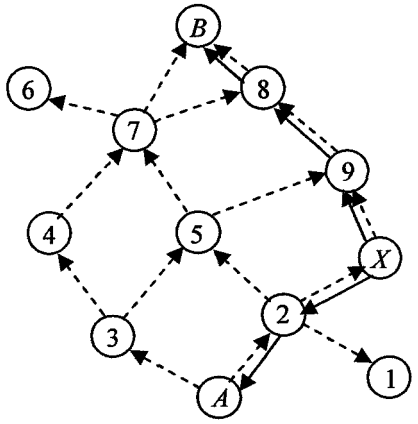

Рис. 2. Узел *B* отправляет ответы $RREP_A$ и $RREP_E$

Если модернизировать протокол таким образом, что бы он мог контролировать выполнение данных соотношений, то такие воздействия станут невозможными.

Воздействия типа deny-of-service могут быть реализованы двумя способами. Первый способ состоит в регулярной рассылке «беспричинных» ответов RREP различным узлам. При этом все маршруты будут выстраиваться к одному узлу. Второй способ состоит в отправке сообщений об ошибке RERR различным узлам от имени других узлов сети.

Нужно отметить, что с 2000 года на различных конференциях стали появляться работы, связанные с безопасностью и устойчивостью протоколов маршрутизации в ad-hoc сетях [7, 8]. В них предлагаются различные модификации, призванные увеличить защищенность протоколов. Однако все предложенные модернизации опираются на криптографию с асимметричными ключами и предполагают наличие некоторого удостоверяющего центра, либо регулярную генерацию сеансо-

вых ключей. При этом, как признаются сами авторы модификаций, возможности для воздействий все равно остаются. Кроме того, применение криптографических средств, особенно асимметричной криптографии, существенно увеличивает требование к вычислительным мощностям узлов, а также увеличивает энергопотребление.

В данной статье рассматривается другой подход - модернизировать протокол так, чтобы воздействия на него если и были возможны, то носили локальный характер. Локальный, либо по времени воздействия, либо по области воздействия.

4. Модернизированный протокол AODV

Для решения проблем устойчивости протокола AODV в него был внесен ряд изменений. В данной статье приводятся только наиболее существенные из них.

1. Все служебные пакеты инкапсулируются не в протокол UDP, а в протокол канального уровня. Это позволяет локализовать область, в которой могут подделываться адреса отправителей в сообщениях.

2. Введен механизм периодического обмена таблицами маршрутизации между соседними узлами. Тем самым к знаниям узла о топологии сети добавляются также знания его соседей. Это позволяет в большинстве случаев выявлять нарушение неравенств (1) и (2) и блокировать связь с узлом-нарушителем на длительное время.

3. Благодаря периодическому обмену таблицами маршрутизации между соседними узлами, был также введен механизм быстрого восстановления маршрутов в случае нарушения одной из промежуточных связей. При этом многократно сократилось время на восстановление нарушенного маршрута, а также уменьшился объем трафика, передаваемого по сети для восстановления нарушенного маршрута.

4. Изменена метрика сети. Под длиной связи понимается остаточная пропускная способность канала. Это позволило ввести в протокол AODV функции балансировки нагрузки. И избавиться от проблемы протокола AODV, связанной с повышенной нагрузкой на каналы передачи данных, находящиеся в центральной части вычислительной сети.

5. Добавлена возможность включения блока данных в пакет запроса построения маршрута, что позволило в случае использования протокола TCP передавать в месте с запросом на построение маршрута и запрос на установление соединения, что примерно на 35 % снизило задержку при установлении соединения с новым узлом, маршрут до которого был ранее не известен.

Также было внесено множество других изменений, некоторые из которых не влияли на защищенность протокола, но увеличивали его эффективность. Общее количество внесенных изменений равно шестнадцати.

5. Основные результаты и достижения

Была проведена классификация большинства протоколов динамической маршрутизации. Протоколы были проанализированы на предмет их устойчивости к внутренним и внешним воздействиям.

На основании проведенного анализа был модернизирован протокол AODV, что позволило сделать его существенно более устойчивым к внутренним и внешним воздействиям, а также оптимизировать его работу.

Было проведено изучение модернизированного протокола в смоделированной вычислительной сети. Наиболее показательными являются следующие результаты, полученные в сравнении со стандартным протоколом AODV.

1. Объем служебного трафика увеличился всего на 13 %.

2. Среднее время построения маршрута осталось неизменным.

3. Среднее время восстановления маршрута сократилось на 81 %.

4. Количество операций полного восстановления маршрута (инициированных одним из конечных узлов) сократилось на 98 %.

5. Средняя задержка в установлении TCP-соединения с новым узлом сократилась на 36 %.

6. Воздействие типа Deny-of-service на вычислительную сеть локализовано зоной покрытия приемо-передающего устройства, осуществляющего воздействие.

7. Воздействие типа man-in-the-middle локализовано зоной диаметром в 1-2 узла от источника воздействия.

Заключение

В ходе проделанной работы был существенно модернизирован протокол динамической маршрутизации для ad-hoc сетей.

Было проведено моделирование работы протокола, результаты которого показали более высокую эффективность модернизированного протокола по сравнению с базовым. Также моделирование показало более высокую устойчивость протокола к внешним воздействиям и локализацию последствий воздействия относительно небольшой областью.

В настоящее время ведутся работы по реализации данного протокола и его полевым испытаниям.

Литература

1. Perkins, CE. Ad hoc On-Demand Distance Vector (AODV) Routing/C.E. Perkins, C.E. Belding-Royer // RFC 3561. - July 2003.

2. Shin, KG. Performance Analysis of Distributed Routing Strategies Free of Ping-Pong-Type Looping / K.G. Shin, M. Chen // IEEE Trans. Computers. - February 1987. - V. COMP-36, M 2. - P. 129-137.

3. Broch, J. A performance comparison of multi-hop wireless ad hoc network routing protocols /

J. Broch, D.A. Maltz, D.B. Johnson, Y.-C. Hu, J. Jetcheva//Proc. ofMOBICOM'98. -1998.

4. Basagni, S. Mobility- Adaptive Protocols for Managing Large AD Hoc Network / S. Basagni, D. Turgut, S.K. Das // Proceedings of the IEEE International Conference on Communications (ICC). - 2001.-P. 1539-1543.

5. Kawadia, V. System services for implementing Ad-Hoc routing: Architecture, Implementation and Experiences/ V. Kawadia, Y. Zhang, B. Gupta//Proceedings of the 1st International Conference on Mobile Systems, Applications and Services (MobiSys). San Francisco, CA. - June 2003. - P. 99-112,

6. Kernel AODV from National Institute of Standards and Technology (NIST). Режим доступа: http://w3.antd.nist.gov/wctg/aodvJcernel/, свободный.

7. Zhou, L. Securing Ad Hoc Networks / L. Zhou, Z.J. Haas // IEEE Networks Special Issue on Network Security. —November/December 2000.

8. Brinkley, J. Authenticated Ad Hoc Routing at the Link Layer for Mobile Systems / J. Brinkley, W. Trost// WirelessNetworL· 7. -2001. -P. 139-145.

9. Карманов, МЛ. Mesh networks: проблемы безопасности [Текст] /МЛ. Карманов // Снежинск и наука-2006: сб. науч. тр. междунар. науч.-практ. конф. - Снежинск: СГФТА, 2006. - С. 158-159.

10. Карманов, М.Л. Системы дистанционного обучения: вопросы безопасности [Текст] / П.В. Збицкий, М.Л. Карманов // Математика. Механика. Информатика: сб. тез. Всерос. науч. конф. - Челябинск: ЧелГУ, 2006. - С. 58.

11. Карманов, М.Л. Маршрутизация в ad-hoc сетях: вопросы безопасности [Текст] / М.Л. Карманов // Безопасность информационного пространства: материалы междунар. науч.-практ. конф. - Екатеринбург: УрГУПС, 2006. - С. 62—66.

12. Карманов, М.Л. Протоколы маршрутизации для ad-hoc сетей [Текст] / М.Л. Карманов // Безопасность информационного пространства: материалы межвузовской науч.-практ. конф. — Тюмень: ТюмГУ, 2007. - С. 19-26.

13. Карманов, М.Л. «Защита беспроводных сетей» [Электронный ресурс] / М.Л. Карманов // Цифровые радиоэлектронные системы. - Режим доступа: http://www.drts.susu.ac.ru/niires/. Зарегистрирован в Комитете РФ по печати № 0146611 от 20.03.1996. Твердая копия № 7, 2007-2008. - Челябинск: ЮУрГУ, 2008. - С. 108-115.

14. Карманов, М.Л. Самоорганизующиеся беспроводные сети: алгоритмы маршрутизации [текст] / М.Л. Карманов // Наука ЮУрГУ: материалы 60-й юбилейной науч. конф. Секция технических наук. - Челябинск: Изд-во ЮУрГУ, 2008. - Т. 2. - С. 64-68.

Поступила в редакцию 10 апреля 2009 г.