УДК 004.04 (043.3)

КУЛАКОВ Ю.А.,
ДЕРЕВЯНЧУК А.О.

БЕЗОПАСНАЯ ПЕРЕДАЧА ИНФОРМАЦИИ НА ОСНОВЕ МНОГОПУТЕВОЙ МАРШРУТИЗАЦИИ

В данной работе приведен краткий обзор протоколов безопасной маршрутизации для мобильных сетей, а так же приведено новое решение научной задачи, которая использует преимущества распределенных беспроводных сетей вместе с секретным разделением сообщения и применением многопутевой маршрутизации.

In this paper we present a survey of secure routing protocols for mobile wireless network and give a new solution to a scientific problem which is to take advantage of the distributed nature of wireless networks and combine the secret sharing scheme and multipath routing.

1. Введение

Многопутевая маршрутизация является одним из наиболее важных направлений в области маршрутизации. Данная маршрутизация основана на однопутевой маршрутизации между узлом источником и узлом назначения, где с большой вероятностью выбирается путь с минимальность стоимостью, хотя по различным ценовым показателям могут быть различные пути. Таким образом, в хорошо связанной сети может существовать несколько путей между парой узлов источника и назначения. Смысл многопутевой маршрутизации состоит в том, чтобы предоставить узлу источнику выбор одного из нескольких маршрутов в любое время к конкретному узлу назначения, используя преимущество избыточной связности а основной сети. Несколько путей могут использоваться как поочередно (трафик проходит по одному из путей в одно время), так и одновременно (трафик проходит одновременно по нескольким путям).

Мобильные ad hoc сети (MANETs) в последнее время привлекли много внимания. MANET – это набор узлов, которые могут свободно перемещаться и сообщаться друг с другом используя беспроводные устройства. MANET характеризуется динамическими изменениями топологии, ограниченной пропускной способностью, а также ограниченной мощностью батарей (аккумуляторов) в узлах. В последнее время многопутевая маршрутизация широко используется в сетях MANETs. За счет плотности расположения узлов в мобильной сети многопутевая маршрутизация используется как естественная и перспективная технология решения проблемы частых изменений топологии. Так же многопутевая маршрутизация используется в целях повышения надежности доставки данных, балансировки нагрузки трафика, балансировки потребления мощности между узлами, уменьшения сквозных задержек, повышения частоты нахождения маршрутов, а так же для повышения безопасности сети.

Безопасность и надежность связи являются двумя важными аспектами в любой сети, которые с первого взгляда противоречат использованию дополнительной избыточности. С одной стороны, надежность может быть достигнута за счет отправления избыточной информации по нескольким путям. С другой стороны, избыточная информация дает противнику больше шансов для перехвата информации. Для решения этой задачи предложен новый протокол безопасности по надежной доставки данных (SPREAD, Security Protocol for REliable dAta Delivery), который повышает как безопасность, так и надежность. Данный протокол был исследован в мобильных ad hoc сетях. Цель предлагаемого протокола состоит в обеспечении дополнительной защиты передаваемых данных, в частности, в снижении вероятности того, что секретное сообщение будет утеряно в то время, как оно будет передаваться по ненадежной сети. Основная идея состоит в разделении секретного сообщения на несколько частей по секретной схеме разделения и в последующей отправки этих частей по нескольким независимым путям к источнику. Таким образом, если

даже какое-то небольшое количество узлов, используемых для передачи сообщения, будет скомпрометировано, то секретное сообщение в целом не будет рассекречено.

Целью статьи является ознакомление с концепцией и технологией многопутевой маршрутизации в ad hoc сетях и получением значительной выгоды при ее использовании.

2. Надежность

Надежность – вероятность того, что сообщение, сгенерированное в одном месте сети будет доставлено в узел назначения. Надежность является сложной задачей в сетях MANETs/WSNs из-за того, что есть большая вероятность потери пакетов в связи с частыми изменениями топологии, различными помехами, которые влияют на корректность кодирования беспроводных сигналов в беспроводных трансиверах.

Многопутевая маршрутизация в MANET была изначально разработана как средство обеспечения защиты маршрута от сбоев. Например, протокол динамической маршрутизации от источника (Dynamic Source Routing – DSR) [1] может запоминать несколько маршрутов к определенному узлу назначения. Когда возникают проблемы на основном маршруте, будут использоваться альтернативные маршруты для того, чтобы доставить пакет к узлу назначения. Так же было предложено "многопутевое" расширение некоторых протоколов, которые первоначально использовали для маршрутизации один путь, как, например AODV-BR, APR (Alternative Path Routing) и SMR (Split Multipath Routing), что значительно улучшило однопутевые протоколы за счет предложения альтернативных путей. В этом случае, разные маршруты используются не одновременно. Трафик проходит по одному из путей. Остальные маршруты хранятся в качестве резервных для случая, если на используемом маршруте возникнут проблемы. Когда все известные маршруты сталкиваются с проблемами, запускается новая процедура поиска маршрутов. Выбор маршрута осуществляется на канальном уровне, когда доступно несколько последующих хопов, и пакет посылается по маршруту с наилучшим состоянием канала [2].

Другой способ использования многопутевой маршрутизации – одновременно отправлять поток данных по нескольким путям. Параллельно многопутевая маршрутизация в MANET была разработана для повышения пропускной способности, надежности и балансировки нагрузки.

В [3] и [4] за счет объедения пороговой схемы разделения секрета и многопутевой маршрутизации мы предложили новый протокол – SPREAD, который обеспечивает более высокую надежность и более безопасную доставку данных в MANET. Алгоритм порогового (T;N) разделения секрета делит и всю информацию на N сегментов. Исходную информацию можно восстановить из любого T, состоящего из N сегментов. Кроме того, схема разделения секрета является достаточно безопасной, то есть, менее чем из T частей, невозможно узнать никакой информации, тем более восстановить первоначальное сообщение. Таким образом, в ad hoc сетях повысилась надежность доставки, так как при использовании протокола SPREAD допускается потеря определенного количества пакетов или путей, в то время как надежность каждого пути в целом не повышается.

3. Качество обслуживания

Одной из основных целей многопутевой маршрутизации является качество обслуживания, а именно, уменьшение задержек, избежание или снижение перегрузок, а так же повышение пропускной способности. Было доказано, что многопутевая маршрутизация повышает качество обслуживания за счет уменьшения задержек при доставки пакетов. На уменьшение задержек влияет несколько факторов. Задержка – это время, за которое пакет проходит от узла источника к узлу назначения. Кроме обычной задержкой передачи, задержкой распространения и задержкой в очереди, которые присутствуют во всех IP сетях, еще существует 2 типа задержек, которые встречаются только в ad hoc протоколах маршрутизации по требованию. Первый вид задержек – это время поиска первого маршрута к узлу назначения. Многопутевая маршрутизация существенно снижает время поиска маршрута, поэтому время такой задержки снижается. Второй вид задержек связан с восстановлением маршрута в случае нарушений в маршруте. В этом случае задержка – это

сумма трех задержек (время, которое потратил пакет при прохождении маршрута до обнаружения поломок; время обнаружения поломки; время, затраченное на прохождение сообщения об ошибке к узлу источнику). Многопутевая маршрутизация помогает избежать или уменьшить возникновение ошибок в маршруте, следовательно, снижается и этот вид задержек.

4. Безопасность

Для повышения безопасности сети предложено несколько способов на основе многопутевой маршрутизации. Многопутевая маршрутизация в данном случае часто применяется с шифрованием секрета. При пороговом разделении (T, N) секрет делится на N частей, которые называются часть (share) или тень (shadow). Секрет может быть восстановлен не менее чем из T частей (share). Таким образом, при объединении многопутевой маршрутизации с методом порогового разделения секрета происходит следующее – разделение секрета и доставка его частей при использовании многопутевой маршрутизации. Тем самым, при распределении по нескольким путям сети, система становится более устойчивой к атакам противника.

Разделение секрета было предложено для управления ключами в системе информационной безопасности. Управление ключами является сложной задачей, когда мы говорим о безопасности в MANET или WSN. Возможность использования других сервисов безопасности, как, например, конфиденциальность и аутентификация, зависит от эффективного и рационального управления ключами. В [5] автора используют репликацию и пороговое шифрование и, таким образом, они смогли построить более защищенную и более доступную систему управления ключами для отклонения атак в MANET. Идея состоит в том, чтобы распределить функции центра сертификации по управлению ключами на несколько серверов (доверенных узлов). Таким образом повышается безопасность центра сертификации. В предложенной модели пороговое шифрование используется для разделения системного секрета на части, каждая часть будет удерживаться на своем сервере; сервера вместе выполняют такие функции, как подписание сертификата и обновление распределенных ключей. Многопутевая маршрутизации подразумевает под собой маршрутизацию частей от нескольких серверов к одному объединителю (сумматору). Данный подход был исследован в [6], где центры сертификации локализированы путем распределения серверов по сети таким образом, что совместные криптографические операции могли бы выполняться соседями запрашивающих узлов. Другой подход к управлению ключами на основе многопутевой маршрутизации – это вероятностный подход с установлением парных секретных ключей [7, 8]. Из-за вычислительной сложности вычисления, основанные на алгоритмах открытого ключа, являются достаточно дорогими для сетей MANET/WSN. Проектирование данного подхода основывается на вероятностном разделении ключа и на методе порогового разделения секрета. При вероятностном разделении ключа, каждый узел сети будет предварительно содержать начальный ключ. С большой вероятностью, любая пара узлов будет обладать общими ключами. Затем, используя общие ключи в качестве начальных, узел источник генерирует новый секретный ключ и разбивает его на несколько частей используя секретную схему разделения. После этого части секретного ключа доставляются к узлу назначения при использовании многопутевой маршрутизации. Многопутевая маршрутизация в такой схеме логична – части ключа могут проходить по одинаковым физическим каналам, но при этом каждый будет зашифрован различными открытыми ключами. Схема SPREAD аналогична подходам описанным выше – схема базируется на объединение многопутевой маршрутизации и разделении секрета. Однако, схема SPREAD направлена на защиту доставляемого по незащищенной сети потока данных, предполагая, что сквозное шифрование является небезопасным и ненадежным. Многопутевая маршрутизация в схеме SPREAD использует физически разделенные пути и предлагает алгоритм поиска заданного пути. Схема SPREAD может быть использована для доставки ключей вместо потока данных. Тем не менее, при доставке потока данных, схема SPREAD повышает не только безопасность, но и надежность, что

является большой проблемой в сетях MANETs/WSNs.

5. Протокол SPREAD

Впервые схема SPREAD была предложена в [8], а затем была изучена в качестве дополнительного механизма повышения безопасности доставки данных в MANET в [3]. Основная идея и работа SPREAD представлена на рис. 1.

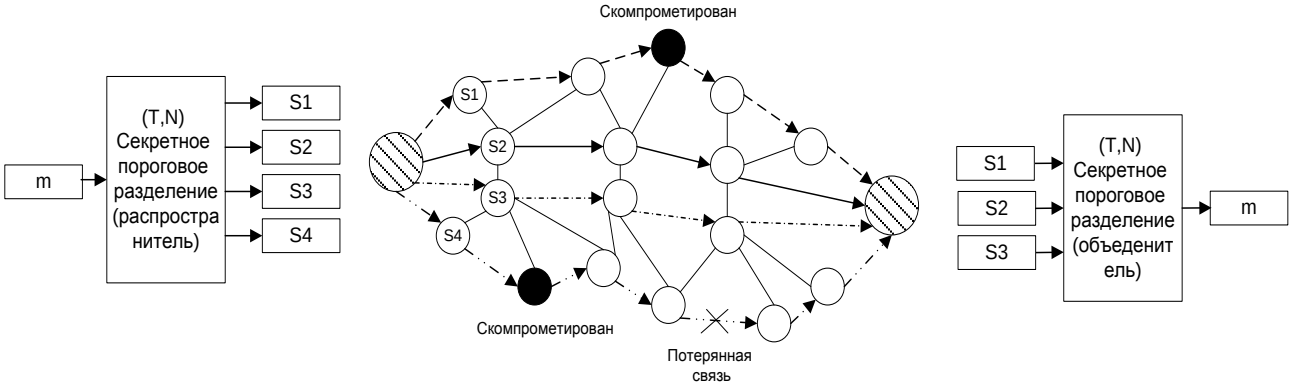

Рис. 1 Принцип работы SPREAD

Секретное сообщение m разделяется на несколько частей – S1, S2,..., по секретной схеме разделения, а затем, доставляются к узлу назначения по разным независимым путям.

Из-за характерных особенностей секретного разделения и доставки сообщения по разным путям, алгоритм SPREAD показал хорошую устойчивость при отказах узлов, а именно, даже если отказало небольшое количество узлов, частей сообщения или путей, целостность не нарушалась. В целях повышения надежности могут использоваться различные схемы кодирования для разделения трафика при многопутевой маршрутизации. Примерами могут служить код Рида-Соломона, разнесенный код и др. В нашей схеме SPREAD мы использовали пороговую секретную схему для обеспечения дополнительно безопасности.

Секретная схема (T,N) разделения делит секретное сообщение на N частей, называемых частями. Особенность такого разделения состоит в том, что меньше чем из T частей невозможно что-либо узнать о сообщении. В то же время при использовании соответствующего алгоритма можно восстановить секретное сообщение из любого числа *T* (или больше) частей. Затем, используя многопутевую маршрутизацию, части сообщения доставляются к адресату по N различным путям, где у *T* путей нет пересекающихся узлов. Процесс разделения на части очень простой – вычисление многочлена степени *(T-1)*.

$$f(x) = \left(a_0 + a_1 x + \ldots + a_{T-1} x^{T-1}\right) \bmod p$$

в точке $x = i$ получаем *i*–ю часть:

$$S(i) = f(i)$$

где $a_0, a_1, a_2, \ldots, a_{T-1}$ – части секретного сообщения, а p – большое простое число, которое больше любого из коэффициентов и которое является открытым.

Согласно основной теореме алгебры, при известный *T* значениях многочлена степени *(T - 1)* можно решить многочлен (т.е. определить все его коэффициенты). Таким образом, зная значение любых T частей, можно восстановить секретное сообщение. Эффективность $\left(O\left(T \log^2 T\right)\right)$ алгоритма была исследована для определения многочлена и интерполяции [7]. Кроме того, в зависимости от количества доступных путей, значение (T,N) в SPREAD будет небольшим. Для практического применения достаточно даже обычных квадратичных алгоритмов.

Многопутевая маршрутизация является перспективной технологией в мобильных сетях с ненадежной передачей данных. Такая маршрутизация хорошо применима из-за плотного расположения узлов в сетях MANETs. SPREAD – это новая схема, которая включает в себя многопутевую маршрутизацию и технологию разделения сообщения с целью обеспечения надежности

и безопасности. Применение SPREAD схемы позволяет одновременную маршрутизацию по нескольким путям и обеспечивает более безопасную передачу данных при прохождении данных по незащищенной сети. Избыточность не влияет на безопасность за счет оптимального расположения частей на каждом выбранном пути.

6. Повышение эффективности алгоритма SPREAD

Алгоритм SPREAD будет работать эффективно в том случае, когда получает не меньше чем *T* частей сообщения. Для уменьшения вероятности потери пакетов могут использоваться дополнительные буферы в каждом из узлов. При таком подходе необходимо, чтобы в каждом узле поддерживалось по 2 небольших буфера – один для маршрутов, а второй – для сообщений.

Кэш маршрутов содержит несколько маршрутов к активному адресату, а кэш сообщений содержит последний отправленный пакет. Таким образом, в случае отказа канала связи или узла по основному маршруту и при наличии в узле альтернативного маршрута, сообщение может быть передано повторно.

7. Выводы

Многопутевая маршрутизация – перспективный метод в сетях MANET. Преимущества при использовании многопутевой маршрутизации: повышение отказоустойчивости, безопасности, надежности, эффективности, уменьшение потерь при маршрутизации, балансировка нагрузки по потоку сообщений и потреблению энергии, снижение задержек.

Список литературы

1. D. B. Johnson, D. A. Maltz, Y-C. Hu, J. G. Jetcheva, “The dynamic source routing protocol for mobile ad hoc networks”, IETF Internet Draft, draft-ietfmanet-dsr-06.txt, Nov 2001
2. S. Jain, Yi Lv, S. R. Das, “Exploiting path diversity in the link layer in wireless ad hoc networks,” Technical Report, SUNY at Stony Brook, CS department, WINGS Lab, July 2003.
3. W. Lou, W. Liu, Y. Fang, “SPREAD: Enhancing data confidentiality in mobile ad hoc networks”, IEEE INFOCOM 2004, HongKong, China, March 2004
4. W. Lou, Y. Zhang, W. Liu, Y. Fang, “A multipath protocol for secure and reliable data collection in wireless sensor networks”, technical report, ECE department, Worcester Polytechnic Institute, June 2004
5. J. Kong, P. Zerfos, H. Luo, S. Lu and L. Zhang, “Providing robust and ubiquitous security support for manet,” Proceedings of the 9th IEEE International Conference on Network Protocols(ICNP), pp. 251 - 260, 2001.
6. H. Chan, A. Perrig, D. Song, “Randon key predistribution schemes for sensor networks”, IEEE Symposium on Security and Privacy (SP’03), Oakland, CA, May 2003
7. S. Zhu, S. Xu, S. Setia, S. Jajodia, “Establishing pairwise keys for secure communication in ad hoc networks: A probabilistic approach”, 11th IEEE International Conference on Network Protocols (ICNP’03), Atlanta, GA, November 2003
8. W. Lou, Y. Fang, “A multipath routing approach for secure data delivery”, IEEE Military Communications Conference (MILCOM 2001), Mclean, VA, USA, Oct 2001

Поступила в редакцию 4.12.2009