Многоадресная рассылка с подтверждениями

Алексей Коваленко
ИППИ РАН
kovalenko@iitp.ru

Анна Цыганова
ИППИ РАН
tsyganova@iitp.ru

Аннотация

В данной статье рассматривается надежная многоадресная рассылка в беспроводной меш-сети. Анализируются варианты реализации надежной рассылки с помощью протоколов, строго гарантирующих доставку сообщений получателям рассылки, вероятностных протоколов, в которых доставка сообщений осуществляется с некоторой вероятностью, а так же гибридных протоколов. В статье предлагается новый протокол DORG (Delay-Oriented Reliable Groupcast), реализующий новый метод опроса получателей рассылки и учитывающий факт частой корелляции ошибок в меш-сети. Произведена аналитическая оценка среднего времени обнаружения ошибки передачи, как важного параметра для многих категорий трафика.

1. Введение

В связи с растущей популярностью приложений групповой коммуникации, работающих в реальном времени или использующих надежное распространение мультимедийной информации, важную роль начинает играть реализация *списочной* передачи (надежной многоадресной передачи, см. [2]). Особенно остро эта проблема встает в случае, когда в качестве среды передачи данных используется не проводная сеть, где потери пакетов невелики, а беспроводная широковещательная среда передачи, где в силу ряда причин, таких как изменение узлами своего местоположения, интерференция между каналами передачи данных и пр., потери пакетов могут быть значительными даже в случае одношаговой передачи данных. Если же приложение, осуществляющее групповую рассылку, работает поверх меш-сети, где передача может осуществляться в несколько шагов, эти нежелательные эффекты накладываются и вероятность потери пакета может возрасти. Также в случае меш-сети существенное влияние оказывает проблема «скрытых станций», приводящая к росту коллизий. Ассиметрия беспроводных соединений может привести к тому, что негативные или позитивные подтверждения (см. 2), передаваемые получателями многоадресных пакетов не достигнут источника сообщений. Традиционные методы обеспечения надежности передачи пакетов, такие как [5], использующиеся в проводных сетях, приводят к дополнительным накладным расходам, недопустимым в беспроводных сетях ввиду их ограниченной пропускной способности. Кроме того, в силу ненадежности беспроводной среды передачи данных, в случае потери пакета данных, либо пакета с подтверждением об успешной доставке время, затраченное на все попытки передачи пакета, может быть значительным, что также недопустимо для приложений реального времени. Соответственно требуется оптимизация стандартных методов, либо новый подход к обеспечению надежности передачи многоадресных пакетов в меш-сетях.

2. Способы обеспечения надежности передачи

Протоколы надежной многоадресной рассылки в зависимости от способа их реализации можно поделить на два больших класса. К первой категории относятся «точные» или «строгие» (deterministic) протоколы, когда источник сообщений получает обратную связь от узлов-получателей рассылки, то есть используется автоматический запрос повторной передачи – ARQ-протокол (Automatic Repeat reQuest). Существует большое количество разновидностей таких протоколов для передачи многоадресных данных на один шаг (см. [9, 8, 10]), также были предприняты попытки применять эти протоколы для меш-сетей [2]. Некоторые из этих протоколов могут требовать обратной связи от всех узлов, которым предназначалось сообщение, что может привести к коллизиям подтверждений в случае, когда они передаются

методом случайного доступа. Другие же протоколы используют различные схемы, позволяющие достичь приемлемой для конкретного приложения надежности, при уменьшении накладных расходов за счет сокращения количества узлов, подтверждающих прием сообщений. Для уменьшения накладных расходов может так же использоваться механизм «негативных подтверждений» (NAK или Negative Acknowledgement) (см. [7]) когда получатели запрашивают переповтор сообщений в случае их потери.

В работе [2] было предложено использовать протокол ELBP (Enhanced Leader-Based Protocol), предложенный в работе [1] для одношаговых беспроводных сетей, обеспечивающий надежную доставку сообщений с помощью механизма многоадресной передачи с мультилидерным подходом, который позволяет достигнуть необходимого уровня надежности в балансе с производительностью. Однако если использовать протокол ELBP с фиксированным выбором лидеров (получателей, ответственных за подтверждение многоадресных пакетов), то гарантированная надежность обеспечивается только для выбранных лидеров. Кроме того, в случае потерь за счет коллизий невозможно обоснованно выбрать лидеров.

Ко второй категории относятся «вероятностные» протоколы, гарантирующие доставку сообщений с определенной вероятностью. При этом отправитель не имеет обратной связи с получателями о дошедших сообщениях. Один из интересных методов, применяющийся в таких протоколах – FEC (Forward Error Correction). При этом используются коды, исправляющие ошибки, которые добавляют избыточность к каждому пакету либо генерирует избыточные пакеты. Тогда получатель может восстановить исходную информацию даже в том случае, если получил лишь часть отправленной информации. Однако достичь приемлемой надежности в случае больших потерь возможно только с использованием длинных кодов, что приводит к росту задержки передачи. FEC-протоколы приводят к возрастанию нагрузки на сеть независимо от количества потерь, что в случае меш-сетей может привести к росту коллизий. Получатели рассылки могут также помогать друг другу в востановлении потерянной информации. Примером такого подхода может служить протокол AG (Anonymous Gossip) [3]. Узел, получающий сообщения, случайным образом выбирает соседа и отправляет ему информацию о полученных/потерянных сообщениях. Далее эти узлы синхронизируют полученные сообщения. Как и в случае FEC-протоколов, таким образом нельзя обеспечить 100%-ю надежность; кроме того, в этом случае невозможно предсказать величину задержки/вариации задержки для приложений реального времени.

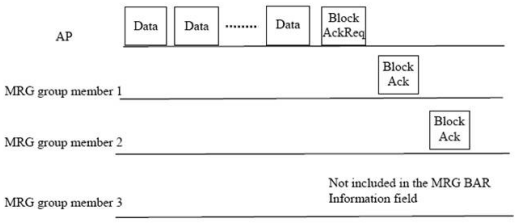

Рис. 1. MRG-Block-Ack.

Большим преимуществом вероятностных протоколов является их масштабируемость, они хорошо работают в больших группах. Однако невозможность обеспечить предсказуемую задержку не позволяет использовать их для работы с приложениями реального времени. Поэтому в ряде статей [6] предлагается использовать гибридные протоколы, совмещающие преимущества первой и второй категории для работы в меш-сетях.

В настроящий момент ведется разработка дополнения 802.11aa [4] к стандарту IEEE 802.11 в котором описывается протокол MRG (More Reliable Groupcast), позволяющий повысить надежность передачи групповых аудио- и видео- данных при рассылке на один шаг. При этом предлагаются 4 политики или механизма такой передачи, различающиеся соотношением между степенью надежности передачи информации и объемом служебного трафика. Самым интересным представляется механизм блочного подтверждения (MRG-Block-Ack). Станция-передатчик многоадресного потока передает пакет Block-Ack Request (BAR) с указанием упорядоченного списка участников группы, в котором они должны отправлять пакеты подтверждения Block Ack на уже принятые пакеты – см. рис. 1. Таким образом каждым из получателей, включенным в список, подтверждаются все принятые пакеты. Дополнение 802.11aa не определяет порядок смены получателей в списке опроса в зависимости от накопленной истории ошибок. Кроме того, пакет BAR отправляется после блока пакета данных, поэтому время до реакции на потерю пакета может быть значительным для приложений реального времени. Сам пакет BAR может быть потерян, и тогда потребуется дополнительное время на его перепосылку, что так же увеличивает задержку передачи данных.

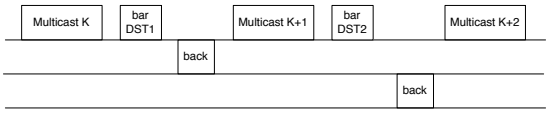

Рис. 2. Подтверждение многоадресного потока данных.

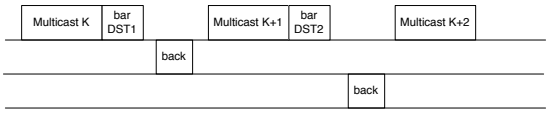

Рис. 3. Подтверждение многоадресного потока данных с агрегацией запроса.

3. Основная идея протокола DORG

В качестве основного критерия пригодности механизма подтверждения в многоадресной рассылке возьмем обязательное подтверждение о получении каждого пакета каждым получателем. Под данный критерий попадает много [9, 8, 10] механизмов подверждений, однако большинство из них страдают от больших накладных расходов или приводят к относительно длительным задержкам. С другой стороны, механизмы подтверждения, основанные на выделении лидера, не удовлетворяют данному критерию, но вносят существенно меньше накладных расходов. Однако сушествует способ объединить сильные стороны этих механизмов, как снизив накладные расходов, так и удовлетворив критерию надежности многоадресной рассылки.

Предположим также, что каждый пакет содержит порядковый номер и каждая станция поддерживает механизм блочного подтверждения. Тогда существует возможность организовать опрос станций получателей многоадресного потока данных таким образом, чтобы каждый пакет был подтвержден. Станция-передатчик многоадресного потока пакетов составляет расписание опроса и по этому расписанию опрашивает получателей потока данных, отправляя по одному запросу после каждого пакета данных. По получении запроса станция отправляет блочное подтверждение на ранее полученые сообщения, в котором указывается номер последнего полученного пакета и карта с информацией о получении пакетов: см. рис.2. В этой схеме можно сократить накладные расходы, агрегировав запрос на подтверждение с пакетом данных – см рис.3. На основании полученного блочного потверждения от запрашиваемой станции станция-отправитель определяет и переповторяет неподтвержденные пакеты. Таким образом на каждую передачу многоадресного пакета приходится ровно один пакет подтверждения, что по накладным расходам сравнимо с одноадресной передачей данных при отсутствии блочного подтверждения.

В отличие от метода надежной многооадресной рассылки, предлагаемого в дополнении к стандарту [4], подтверждения от всех станций не идут одним блоком пакетов, а рассредоточены во времени, что потенциально позволяет добиться существенно меньшей задержки перед переповтором искаженного пакета, при условии использования адаптивного алгоритма опроса получателей для получения подтверждения.

4. Алгоритм опроса в DORG

Так как каждый пакет подтверждается каждой станцией-получателем, то вероятность потери пакета при достаточном большом ограничении на количество переповторов мала. Однако для многих категорий трафика важной характеристикой является еще и задержка, в которую, в случае ненадежной среды передачи, вносит существенный вклад время, прошедшее до обнаружения потери пакета. В дальнейшем будем рассматривать это время в качестве основного показателя производительности.

Рассмотрим такие расписания запроса подтверждения, в которых в каждом цикле опроса станция опрашивается ровно один раз. Пусть множество станций-получателей многоадресной рассылки – M, тогда расписание опроса подтверждения (последовательность номеров станций множества M, в соответствии с которым происходит опрос) $S : M \to M$. k – дискретное «время», увеличивающееся при каждой следующей передаче станцией-отправителем. $\xi_i(k) = 0,1$ указывает на потерю пакета k i-той станцией (1 – пакет потерян, 0 – пакет получен). Тогда до момента получения информации о потере пакета любой из станций-получателей пройдет время:

$$d(k) = \delta \min_{l>0}\{l : \xi_s(k+l) = 1\}, \qquad (1)$$

где δ – время между двумя последовательными передачами пакетов. Будем считать, что это время постоянно, поскольку джиттер, вносимый случайным методом доступа, значительно меньше интервала между поступлениями пакетов. При этом при каждой передаче пакета реализуется один из возможных вариантов списка станций, не принявших этот пакет. Будем обозначать такой список с количеством участников n $\{i_1, i_2, \cdots, i_n\}$ с упорядочиванием по расписанию опроса – $S(i_1) < S(i_2) < \cdots < S(i_n)$. Чем больше количество станций, потерявших пакет, тем

большее влияние оказывает возникшая ошибка передачи на качество оказания услуг групповых сервисов. Таким образом показателем будет являться не $d(k)$ а D, которое учитывает кратность ошибки:

$$D^{(n)} = d(k) \cdot n. \quad (2)$$

Верхний индекс указывает на кратность ошибки доставки пакета (кратность ошибки– количество станций, не получивших пакет). Тогда, произведя усреднение формулы (1) по циклу опроса (на каком шаге k цикла опроса произошла ошибка, характеризуемая списком станций, не принявших пакет):

$$\langle d^{(n)}_{i_1 \cdots i_n} \rangle = \frac{\delta}{2M}((S(i_2) - S(i_1))^2 + \\ +(S(i_3) - S(i_2))^2 + \cdots + (M - (S(i_n) - S(i_1)))^2). \quad (3)$$

Тогда усредняя по всем возможным вариантам списка станций, не получившим пакет:

$$D = 0 \cdot P^{(0)} \quad + \quad 1 \cdot \frac{M}{2} \sum_i P^{(1)}_i + 2 \cdot \sum_{S(i)<S(j)} P^{(2)}_{ij} \langle d^{(2)}_{ij} \rangle + \\ + \quad 3 \cdot \sum_{S(i)<S(j)<S(k)} P^{(3)}_{ijk} \langle d^{(3)}_{ijk} \rangle \cdots \quad (4)$$

Вероятности реализации ошибки передачи кратности n со списком $\{i_1, \cdots, i_n\}$ станций, на которых произошла ошибка, обозначены $P^{(n)}_{i_1 \cdots i_n}$. Заметим, что зависимость от расписания в формуле (4) появляется только начиная с члена с кратностью ошибки равной двум. Также легко показать, что

$$\langle d^{(2)}_{ij} \rangle > \langle d^{(3)}_{ijk} \rangle, \ \langle d^{(2)}_{ij} \rangle > \langle d^{(3)}_{ikj} \rangle, \ \langle d^{(2)}_{ij} \rangle > \langle d^{(3)}_{kij} \rangle, \quad (5)$$

где индексы упорядочены по расписанию S, аналогичные неравенства возможно написать и для $\langle d^{(n)}_{i_1 \cdots i_n} \rangle$ и $\langle d^{(n+1)}_{i_1 \cdots i_{n+1}} \rangle$.

5. Примеры

5.1. Независимый прием станциями-получателями

Рассмотри случай независимости вероятности приема станциями-получателями, с вероятностью ошибки P_0 для каждой станции. Тогда вероятность реализации ошибки приема ровно на i станциях:

$$V^{(n)} = P_0^i (1 - P_0)^{M-i} \binom{M}{i}. \quad (6)$$

Тогда в случае MRG с размером блока M получаем для D:

$$D_r^{mrg} = \frac{M\delta}{2} \sum_{i=1}^{M} iV^{(i)} = \frac{\delta M^2 P_0}{2} \quad (7)$$

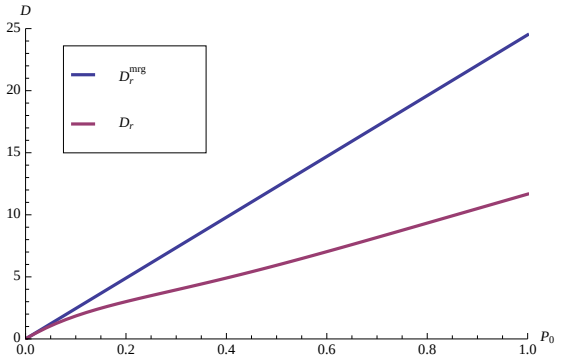

Рис. 4. Величина D в зависимости от вероятности потери пакета P_0 для $M = 7$

Для протокола DORG произведем оценку сверху величины D. Исходя из неравенств (5) для $\langle d^{(n)} \rangle$ и формулы (4) можно для оценки сверху заменить все $\langle d^{(n)} \rangle$ для $n > 2$ на $\langle d^{(2)} \rangle$. Тогда из формулы 4 получаем:

$$D_r^{dorg} = \frac{M\delta}{2} V^{(1)} + \bar{D}^{(2)} \sum_{i=2}^{M} iV^{(i)} = \quad (8)$$
$$= \frac{M\delta}{2} V^{(1)} + \bar{D}^{(2)} (MP_0 - V^{(1)}),$$

где $\bar{D}^{(2)}$ – усредненная по всем возможным расписаниям формула (3):

$$\bar{D}^{(2)} \quad = \quad \frac{\delta}{2M(M-1)} \ \times$$
$$\times \quad \sum_{l=0}^{M-2} [l(l+1) + (M-l-2)(M-l-1)] \ =$$
$$= \quad \frac{\delta}{3}(M-2). \quad (9)$$

Тогда:

$$D_r^{dorg} = \frac{P_0 M\delta}{6} \left(2M - 4 + (4+M)(1-P_0)^{M-1}\right), \quad (10)$$

что меньше чем D_r^{mrg} при $0 \le P_0 \le 1$. Еще раз стоит подчеркнуть, что была произведена оценка сверху, реальное значение D_r^{dorg} будет еще меньше. Соотношение между D_r^{mrg} и оценкой сверху D_r^{dorg} приведено на рис.4.

5.2. Скрытая станция

Рассмотрим случай передачи, когда существует одна скрытая станция, соседствующая с N_h станциями из списка получателей M. На рис.5 схематически изображен случай $N_h = 2$, окружность с станциями схематически отображает расписание опроса. Пусть с вероятностью P_h передаваемый пакет попадает в коллизию с каким-либо пакетом скрытой станции, такая коллизия приводит к потере пакета на всех

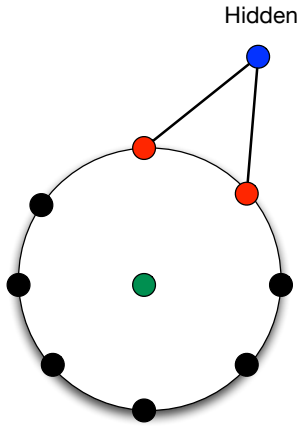

Рис. 5. Скрытая станция $N_h = 2$

N_h станциях-получателях. Предполагается, что эти коллизии являются единственным источником ошибок. Тогда по формуле (4):

$$D = \frac{N_h \delta}{2M} P_h(\lambda_1^2 + \lambda_2^2 + ... + \lambda_{N_h}^2), \quad (11)$$
$$\sum_{i=1}^{N_h} \lambda_i = M, \lambda_i > 0,$$

где λ_i – расстояния по циклу опроса между i-й и $i+1$-й станциями из списка станций, потерявших пакет. Очевидно, что минимум D достигается в при $\lambda_i = M/N_h$ и в случае использования DORG равен:

$$D_{min}^{dorg} = \frac{\delta M}{2} P_h \quad (12)$$

и не зависит от N_h. Для сравнения, в случае MRG:

$$D_{min}^{mrg} = \frac{\delta M}{2} P_h N_h. \quad (13)$$

6. Заключение

Рассмотренные выше примеры показывают, что предложенный протокол DORG существенно уменьшает время реакции на потерю пакета по сравнению с предлагаемым к стандартизации методом MRG [4] даже в случае использования некоррелированных ошибок приема станциями-получателями многоадресной рассылки. При этом накладные расходы сравнимы с одноадресной передачей данных и не превышают расходов, возникающих в MRG. В случае корреляции между ошибками приема пакетов станциями-приемниками время реакции на ошибку для протокола MRG пропорционально кратности ошибки, тогда как для протокола DORG оно не зависит от кратности ошибки. Более того, если провести оптимизацию расписания опроса, среднюю задержку до первого переповтора потерянного пакета можно снизить еще больше. Однако задача оптимизации расписания опроса NP-сложна и требует разработки новых приближенных алгоритмов.

Список литературы

[1] Якимов М.Ю., Сафонов А.В. Поддержка надежной многоадресной передачи в беспроводном протоколе ieee 802.11. *Труды конференции "Информационные технологии и системы"(ИТИС-2007)*, pages 54–58, 2007.

[2] Цыганова А.М. Надежная многоадресная рассылка в беспроводной меш-сети. *Труды конференции "Информационные технологии и системы"(ИТИС-2009)*, 2009.

[3] R. Chandra, V. Ramasubramanian, and K. P. Birman. Anonymous gossip: Improving multicast reliability in mobile ad-hoc networks. *Distributed Computing Systems, International Conference on*, 0:0275, 2001.

[4] *Draft STANDARD for Information Technology Telecommunications and information exchange between systems Local and metropolitan area networks Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 8: MAC Enhancements for Robust Audio Video Streaming*, 2010.

[5] I. S. Institute. RFC 793, 1981. Edited by Jon Postel. Available at http://rfc.sunsite.dk/rfc/rfc793.html.

[6] N. Jörg, B. Ernst, and T. Don. Parity-based loss recovery for reliable multicast transmission. In *SIGCOMM'97 Proceedings*. ACM, 1997.

[7] K. Tang, K. Obraczka, S.-J. Lee, M. Gerla. Congestion controlled adaptive lightweight multicast in wireless mobile ad hoc networks. *Proceedings of ISCC*, 2002.

[8] M.-T. Sun, L. Huang, A. Arora, and T.-H. Lai. Reliable mac layer multicast in ieee 802.11 wireless networks. In *ICPP '02: Proceedings of the 2002 International Conference on Parallel Processing*, page 527, Washington, DC, USA, 2002. IEEE Computer Society.

[9] K. Tang and M. Gerla. Random access mac for efficient broadcast support in ad hoc networks. pages 454–459, 2000.

[10] K. Tang and M. Gerla. Mac reliable broadcast in ad hoc networks. volume 2, pages 1008–1013 vol.2, 2001.