

Перегрузки и мониторинг сети сигнализации ОКС-7

Б.С. ГОЛЬДШТЕЙН, заместитель директора ЛОНИИС, доктор технических наук, профессор, заведующий кафедрой систем коммутации ГУТ им. М.А. Бонч-Бруевича, В.И. ЦЫБАКОВ, технический директор по эксплуатации ЗАО "МТУ-Информ"

От перегрузок локальных к сетевым

В середине 90-х годов прошлого века с проблемой перегрузок, вызванных внедрением новых видов услуг связи (и не только), первой, вероятно, столкнулась Московская городская телефонная сеть (МГТС), обслуживающая свыше 4 млн. абонентов. В частности, серия передач Александра Гурно-ва, позиционированных как своего рода "интерактивное ТВ" и подразумевающих звонки телезрителей в студию, оказалась вдруг столь привлекательной и пробудила такой единовременный интерес, что целые районы города остались без телефонной связи.

Очевидно телефонисты, не сталкивавшиеся с такими масштабными проблемами даже при обрыве своих коммуникаций, в сердцах посоветовали тогда телевизионщикам "звонить через телевизор". Передачу сняли, но проблема не исчезла. Как-то под 8 марта лавиной телефонных поздравлений была остановлена даже DX-200, одна из первых в стране цифровых АТС. Такую причину перегрузки удалить невозможно, поэтому наступало время других решений.

Все эти ситуации носили сугубо локальный характер, в связи с чем авторы данной статьи в то время не посчитали актуальным обсуждение этой проблемы на страницах журнала. Тем временем, перегрузки старались не только предотвратить, но и "обезопасить" от них МГТС.

Создавая во второй половине 90-х годов в Москве интеллектуальную сеть (IN) компания "МТУ-Информ" постаралась по максимуму увеличить пропускную способность своей "интеллектуальной платформы" (с быстроедействием там и так все в порядке), прежде всего, за счет чисто сетевых аспектов.

В частности, транспортная сеть SDH МТУ-Информ предусматривала наличие мультиплексоров на каждом узле исходящего сообщения (УИС), через которые осуществлялся выход на услуги IN. Это позволяло разгрузить транспортную сеть МГТС от дополнительной нагрузки, инициированной услугами IN и, в первую очередь, таких, как телеголосование (televoting).

Одновременно увеличивалась и учтенная при опросе аудитория, поскольку в противном случае множество звонков просто отсекалось бы в ТФОП (как это обычно и происходит). Это обстоятельство повышало "ценность" опроса в глазах заказчика. Например, использовавший в то время услуги МТУ-Информ канал НТВ успевал собирать за час - полтора до 50 - 70 тыс. "откликов с мест".

Сегодня такими услугами пользуются уже многие телеканалы и радиостанции. В частности, "Эхо Москвы" в ежедневной интерактивной программе "Рикошет" успевают за несколько минут "собрать" до 3 - 5 тыс. звонков. В результате мониторинг мест возможных перегрузок - ежедневная забота таких операторов, как "МТУ-Информ".

Сегодня, в связи с широким внедрением общекабельной сигнализации № 7 проблема общесетевых перегрузок заслуживает самого пристального внимания. Именно поэтому с нее начинается статья. Главным признаком перегрузок является, как правило, большой объем неоднократно передаваемых между пунктами сигнализации сообщений.

Причиной может стать, например, заказанная двумя абонентами услуга переадресации вызова друг на друга. Первый же звонок к любому из этих номеров приведет к лавинообразному росту сообщений между соответствующими АТС. Причем это может быть отнюдь не злонамеренным сговором двух хулиганов. Для подобной шутки достаточно и одного человека, утром переадресовавшего вызовы с домашнего телефона на рабочий, а вечером сделавшего обратную переадресацию и забывшего отменить предыдущую.

Сколько же неприятностей может произойти в сети ОКС-7, пока забывчивый абонент добирается с работы домой. Впрочем, с такой ситуацией в ее упрощенной формулировке читатель знаком с раннего детства и безусловно помнит ее печальную концовку: "в этой речке утром рано утонули два барана".

Очевидность и высокая вероятность появления именно этой причины перегрузки привели к включению средств защиты от нее в более поздние версии протокола ISUP. Но множество других, отнюдь не столь очевидных ситуаций не могут быть априорно заблокированы и требуют оперативного внимания со стороны системы мониторинга сети ОКС-7.

Такая система, называемая СПАЙДЕР, установлена, в частности, на сети "МТУ-Информ" и выполняет целый ряд функций, включая как контроль, так и предотвращение перегрузок в сети.

Разные аспекты этой, пока единственной российской системы мониторинга уже рассматривались в журнале "Вестник связи" № 4 за 2001 и за 2002 г. Сейчас же сосредоточимся на проблеме перегрузок.

"Безотбойность" в сети ОКС-7

Прежде всего напомним, что простой успешный вызов по ОКС-7 начинается с передачи начального адресного сообщения IAM. В ответ поступает сообщение о принятии полного адреса ACM, а затем, когда вызываемый абонент ответит, - сообщение ответа ANM.

Когда вызывающий абонент кладет трубку, в сторону вызываемого абонента передается сообщение освобождения REL, которое подтверждается сообщением завершения освобождения канала RLC. В этой процедуре возможны варианты, но приведенный алгоритм вполне достаточен для описания еще одной, вполне легальной ситуации перегрузки сообщениями освобождения (Release).

Такой лавинообразный рост числа сообщений освобождения REL может возникнуть, когда критический элемент сети препятствует доставке сообщения освобождения к пункту его назначения.

Протокол ISUP требует, чтобы пункты сигнализации повторно передавали сообщения освобождения, которые не были подтверждены до истечения таймера освобождения, составляющего 4 - 6 с.

Пункт сигнализации может продолжать попытки освобождения соединительной линии путем передачи сообщений освобождения в течение минуты, после чего с интервалом в одну минуту он будет передавать заменяющее сообщение сброса канала Reset Circuit.

Высокая интенсивность сообщений освобождения вкупе с большим числом разрешенных протоколом попыток повторной их передачи на каждый вызов означает, что как только сообщения освобождения или подтверждающие их сообщения завершения освобождения канала Release Complete не будут попадать в свои пункты назначения, объем трафика сообщений освобождения может начать быстро возрастать.

По мере его роста их неуспешная передача из-за ограниченных ресурсов сети сигнализации приведет к еще большему числу неудачных передач сообщений освобождения или завершения освобождения канала и, как следствие, - к еще большему числу повторных передач этих сообщений.

Таким образом, трафик сообщений освобождения может принять лавинообразный характер. Эта лавина может "сметать" на своем пути сообщения запроса установления соединения, что будет приводить к низкой производительности по обслуживанию вызовов. Кроме того, недозвонившиеся вызывающие абоненты могут предпринимать повторные попытки установления соединения, что еще больше усугубит перегрузку.

Лавины сообщений освобождения наблюдались в имитационных испытаниях системы СПАЙДЕР, где причиной их появления была искусственно созданная перегрузка звена сигнализации. Эта ситуация спровоцировала перегрузку в сети сигнализации, что привело к снижению качества обслуживания вызовов.

Существуют два очевидных пути борьбы с такими перегрузками: ограничить число повторных передач сообщения освобождения или удлинить таймер освобождения.

К сожалению, накопленная с помощью системы СПАЙДЕР статистика показала, что оба эти подхода слабо улучшают показатель производительности сети при перегрузках такого рода.

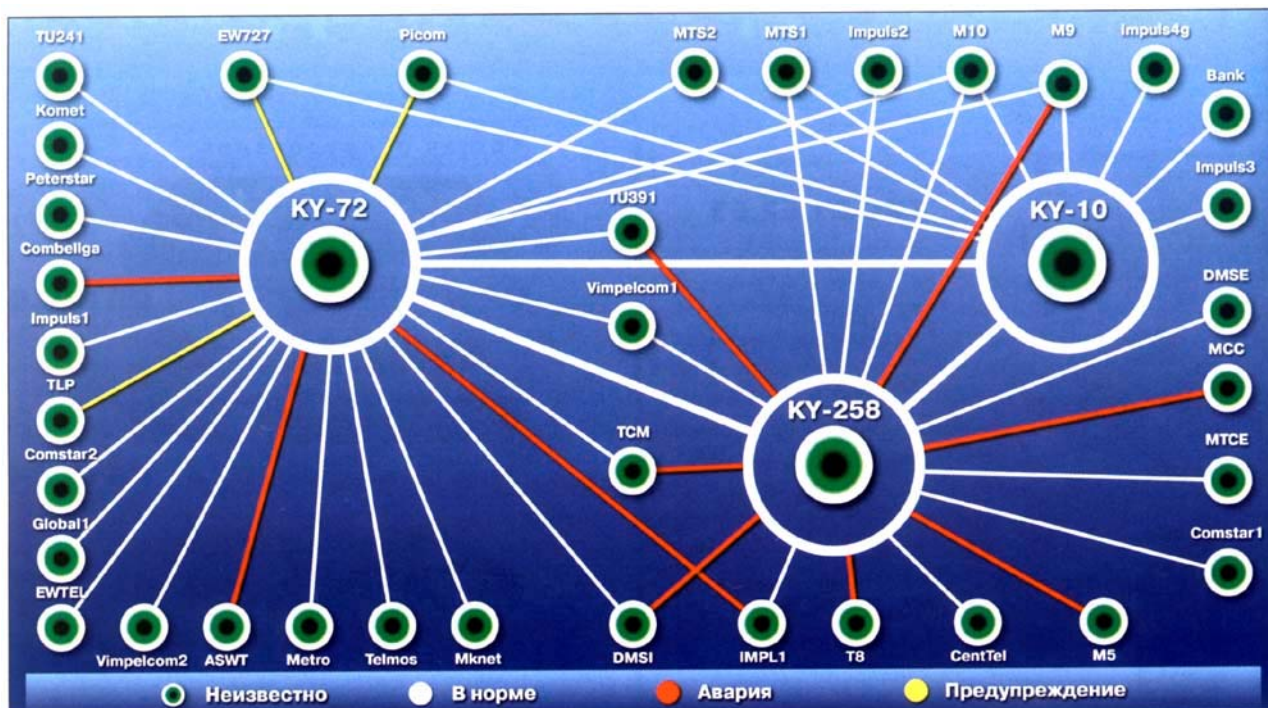
Модель BeSleore для сети ОКС-7

Рассмотренная выше ситуация, кстати, анализировалась компанией Bellcore в 2000 г., где в качестве решения предлагался динамический алгоритм управления для регулирования поступления сообщений освобождения в сеть ОКС. Предложенный алгоритм является распределенным в том смысле, что каждый источник регулирует свой собственный трафик сообщений освобождения, не зная о соответствующем трафике от других источников (полная картина известна только центральному модулю СПАЙДЕР).

Источники используют местные измерения на уровне удаленных модулей СПАЙДЕР/RU для того, чтобы оценить, в какой степени им следует изменить частоту посылки сообщений освобождения.

Это позволяет изменить совместное поведение источников таким образом, что они выдают только такую суммарную нагрузку, которую в состоянии обработать перегруженный коллективно используемый ресурс. Предварительные результаты имитации на сети компании "МТУ-Информ" (в качестве испытательного полигона для СПАЙДЕРА это более чем достойный объект) показали, что динамическое управление дает значительно более высокую производительность по обслуживанию вызовов, чем статическое управление. Происходит это за счет значительного снижения числа повторных передач сообщений освобождения.

На рисунке показана сеть общеканальной сигнализации "МТУ-Информ", используемая для имитационного моделирования описанной выше ситуации.



Исследуемая сеть ОКС-7

Сеть состоит из пяти гетерогенных (неоднородных) пунктов сигнализации ("источников"), которые направляют трафик к одному транзитному пункту сигнализации STR с интенсивностями попыток установления соединений $X.1$, где $1=1,2, \dots,5$.

Для сообщений: IAM, ACM, ANM, REL и RLC выбраны приоритеты 0, 1,2, 1, 1, соответственно, согласно модели Belcore, а для сообщения сброса канала (Reset Circuit) - приоритете.

Длина сообщений в октетах составляет: IAM=48, ACM=20, ANM=16, REL=22 и RLC=17, время обслуживания звена пропорционально длинам сообщений, а сами сообщения IAM поступают от источников и адресата согласно распределению Пуассона.

Последующие сообщения ISUP, относящиеся к одному вызову, уже не являются независимыми пуассоновскими, а моделируются так называемым кластер-пуассоновским потоком, исследованным одним из авторов данной статьи в 1990 г.

Вызов считается успешным тогда и только тогда, когда его сообщения IAM и ANM доходят до своих пунктов назначения. Моделируются и поведение абонентов при повторных попытках установления соединения путем генерирования повторных попыток согласно схеме Бернулли с вероятностью 0,7 после соответствующей задержки, а также дополнительные сетевые задержки, равные 250 мс на каждом узле.

Сетевая задержка в данном контексте - это время, которое требуется пунктам сигнализации для реагирования на начало перегрузки в сети, и это время обусловлено задержками, связанными с обработкой данных в пунктах сигнализации и STP.

Численному анализу роста трафика во времени при различных конфигурациях нагрузки, приводящих к перегрузке, хотелось бы посвятить отдельную статью, а здесь приходится ограничиться только некоторыми качественными результатами моделирования.

Они свидетельствуют, что большой объем неуспешных сообщений, которые запускаются в сеть ОКС во время перегрузки, и их негативное влияние на качество обслуживания вызовов делает очевидной потребность в системе сетевого мониторинга СПАЙДЕР. Это позволяет согласовывать, в частности, интенсивность трафика сообщений REL с пропускной способностью того критического элемента в сети, который работает во время возникновения перегрузки.

Применение СПАЙДЕРА дает возможность значительно улучшить показатель обслуживания вызовов при различных уровнях перегрузки и, таким образом, лучше управлять повторными передачами сообщений освобождения. Что, собственно, и наблюдается.