Оптимизация числа узлов распределенной PKI-системы

© 2009 Е.Н. Тищенко
доктор экономических наук, доцент
© 2009 Н.В. Коротаев
Ростовский государственный экономический университет "РИНХ"

Инфраструктура открытых ключей является основой для легитимного, надежного и достоверного электронного взаимодействия в сфере информационных технологий. Существующие тенденции ведут к интеграции созданной в России инфраструктуры, что повлечет за собой укрупнение PKI-систем. Важной задачей является обоснованность увеличения структуры и повышение эффективности работы PKI-систем. Ее решение с применением теории массового обслуживания позволит сократить расходы без снижения качества обслуживания.

Ключевые слова: инфраструктура открытых ключей, PKI, система массового обслуживания, эффективность, PKI-система, система высокой готовности.

Современный документооборот, а также любой информационный обмен переходят в сферу электронных коммуникаций. С принятием соответствующих нормативных актов стало возможно легитимное взаимодействие между гражданами, бизнесом и государством в виде электронных документов. Многие услуги, ранее требующие личного присутствия, теперь оказываются дистанционно. В их число входят удаленное управление банковским счетом, интернет-магазины и электронная торговля, регистрация авторских прав в электронном нотариате, подача заявлений в органы исполнительной власти и др.

Для защиты информационных потоков между субъектами электронного взаимодействия используют инфраструктуру открытых ключей (PKI). Электронная цифровая подпись подтверждает авторство и целостность сообщения, придает информации юридическую значимость, а асимметричное шифрование препятствует фальсификации и делает невозможным ее раскрытие.

Во многих случаях PKI-система состоит из нескольких удостоверяющих центров (УЦ), каждый из которых является самостоятельной единицей с определенной структурой. Так что конечный пользователь при обращении к PKI-системе контактирует с распределенной инфраструктурой удостоверяющих центров.

Целью создания такой структуры может быть возросшая нагрузка на PKI-систему в связи с увеличением числа обращений к ней, создание крупного территориального узла, предназначенного для интеграции разрозненных систем или создания совершенно новой инфраструктуры и др.

Объединить физически независимые УЦ в одну PKI-систему позволяет программный кластер. Существуют два вида организации кластера: высокоскоростные системы и системы высокой готовности.

В высокоскоростных системах основным требованием является возможность разбиения исходной задачи (задания для УЦ) на подзадачи, за счет чего достигается максимальное быстродействие. В системах высокой готовности основной целью выступает максимальная отказоустойчивость.

Функции удостоверяющего центра и вытекающие из них функциональные операции не предполагают деления на подзадачи, так как являются последовательным набором команд. В связи с этим единственным видом организации кластера для PKI-системы служит система высокой готовности.

Схема архитектуры PKI-системы изображена на рис. 1. Здесь каждый сегмент УЦ включает в себя внутреннюю реплицируемую с хранилищем сертификатов базу данных, к которой направляются все запросы на выборку. Запросы на добавление и обновление данных отправляются напрямую в хранилище сертификатов, изменения в котором приводят к синхронизации реплик.

Закономерным является вопрос о количестве узлов, необходимых для эффективной работы PKI-системы. На него вполне возможно дать ответ, используя теорию массового обслуживания, целью которой является выработка рекомендаций по рациональному построению систем массового обслуживания (СМО), рациональной организации их работы и регулированию потока заявок для обеспечения высокой эффективности функционирования СМО.

В качестве характеристик эффективности функционирования СМО можно выбрать три основные группы показателей:

1. Показатели эффективности использования СМО:

- абсолютная пропускная способность (A);
- относительная пропускная способность (Q);

Рис. 1. **Архитектура PKI-системы высокой готовности**

2. Показатели качества обслуживания заявок:

- среднее время ожидания заявки в очереди ( );
- среднее время пребывания заявки в СМО ($\overline{T}_{сист}$);
- вероятность отказа в обслуживании без ожидания (p_n или p_{n+m});
- среднее число заявок, находящихся в очереди ($\overline{l}$);
- среднее число заявок, находящихся в СМО ($\overline{k}$).

3. Показатели эффективности функционирования пары “СМО - клиент”. К числу таких показателей относится, например, средний доход, приносимый СМО в единицу времени, и т.п.

Для описания работы кластера PKI-системы наиболее подходят два вида моделей: многоканальная СМО с отказами и многоканальная СМО с ожиданием.

В нашем конкретном случае на предприятии “Гамма” PKI-система состоит из четырех УЦ. Среднее время выполнения функциональной операции, непосредственно связанной с УЦ, согласно измерениям, равняется 15,5 с. В среднем в течение 1 мин в сеть поступает 20 заявок на обслуживание. Требуется определить минимальное количество узлов, чтобы обеспечить 95%-ную пропускную способность для СМО.

Поток заявок на обслуживание является простейшим в силу ординарности и стационарности, что дает нам право считать его простейшим. В случае, если поток не является стационарным, необходимо найти его пиковое значение и принять его в качестве константы. Так как перед нами стоит задача нахождения эффективного числа узлов при условии уровня пропускной способности не ниже заданного использование пикового значения позволит гарантировать доступность системы.

Рассчитаем интенсивности потоков заявок и обслуживаний:

$$\lambda = \frac{1}{3},\ \mu = \frac{2}{31} \approx 0{,}0645161,\ \rho = \frac{\lambda}{\mu} \approx 5{,}1666667.$$

Рассмотрим многоканальную СМО с отказами. Вероятность того, что система будет бездействовать, равна $p_0 = 0{,}0138519$. Также рассчитаем вероятность отказа и относительную пропускную способность:

$$p_n = \frac{\rho^n}{n!} p_0 = 0{,}4112827,$$

$$Q = 1 - p_n = 0{,}5887173.$$

Вероятность отказа в нашем случае довольно высока - более 41%, или менее 59% заявок на обслуживание будут выполнены. В абсолютном выражении это приблизительно 11,77 заявок в минуту из 20 поступающих.

Для того чтобы достигнуть требуемой пропускной способности, воспользуемся методом последовательного перебора. Это более эффективно, поскольку ограничение для соответствующей задачи имеет нелинейный вид и число вариантов невелико. Для этого будем последовательно перебирать значения n=5, 6, 7, ..., пока не достигнем требуемого результата.

Из табл. 1 видно, что минимальное число узлов, которое необходимо использовать для до-

Таблица 1. **Показатели эффективности для PKI-системы**

Показатели эффективности	Число узлов в PKI-системе					
	4	**5**	**6**	**7**	**8**	**9**
Относительная пропускная способность, *Q*	0,59	0,70	0,80	0,87	0,92	**0,96**
Абсолютная пропускная способность, *A*	11,8	14,0	15,9	17,4	18,4	19,1

Таблица 2. **Относительная пропускная способность в PKI-системе**

Число узлов в PKI-системе	Максимальная длина очереди								
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
4	0,65	0,69	0,71	0,73	0,74	0,75	0,76	0,76	0,76
5	0,76	0,80	0,83	0,85	0,87	0,88	0,89	0,90	0,90
6	0,85	0,89	0,91	0,93	0,94	***0,95***	***0,96***	***0,97***	***0,97***
7	0,91	0,94	***0,96***	***0,97***	***0,98***	***0,98***	***0,99***	***0,99***	***0,99***
8	***0,95***	***0,97***	***0,98***	***0,99***	***0,99***	***0,99***	***1,00***	***1,00***	***1,00***

стижения пропускной способности Q не менее 95%, равно 9. Следовательно число узлов требуется увеличить на 5 ед. При этом среднее число выполненных запросов на обслуживание в среднем будет около 19,1 в минуту, а среднее число заявок в системе (занятых каналов) - 4,95.

Возможно также определить значения других показателей PKI-системы для нахождения их оптимальных значений и повышения эффективности в целом. Например, найти интенсивность потока заявок (а значит, косвенно определить количество пользователей сети) или максимизировать число занятых каналов.

Однако использование СМО с отказами не вполне рационально. Во-первых, запрос нельзя поставить в очередь для дальнейшей обработки. Во-вторых, наличие единственной оптимизируемой переменной - числа узлов - снижает вариативность решения.

Более гибким вариантом является многоканальная СМО с ожиданием. Рассчитаем показатели СМО с ожиданием и длиной очереди $m = 1$.

Вероятность того, что система будет простаивать, равна $p_0 = 0{,}0138519$. Тогда вероятность отказа и относительная пропускная способность окажутся равными:

$$p_{n+m} = \frac{\rho^{n+m}}{n^m n!} p_0 = 0{,}3469346,$$

$$Q = 1 - p_{n+m} = 0{,}6530654.$$

Вероятность отказа высока - более 34,5%, или менее 65%, заявок на обслуживание будут выполнены. В абсолютном выражении это равносильно выполнению 13,06 заявки в минуту из 20 поступающих.

Наличие очереди в модели вводит в число параметров качества среднюю длину очереди $\bar{l}$ и среднее время ожидания в очереди $\bar{t}_{ож}$, а в число параметров эффективности - среднее число заявок в системе $\bar{k}$ и среднее время пребывания в системе $\overline{T}_{сист}$.

Теперь задача увеличения эффективности и качества обслуживания состоит в оптимизации двух переменных - числа узлов n и максимальной длины очереди m, также как и в предыдущем случае необходимо достичь пропускной способности не менее 95%, с тем отличием, что мы можем менять не только число узлов, но и длину очереди.

Воспользуемся тем же методом последовательного перебора: будем последовательно перебирать значения n и m, пока не достигнем требуемого результата (табл. 2).

Таким образом, лицо, принимающее решение, может выбрать две стратегии для увеличения эффективности работы PKI-системы: увеличить число узлов, что влечет за собой повышение расходов, или увеличить длину очереди, что при большом времени ожидания снизит качество обслуживания.

Так, например, в отличие от СМО с отказами, если пойти по пути минимизации затрат, число узлов понадобится увеличить всего на 3, а не на 6. При этом длина очереди должна быть увеличена на 5 ед.

Если же пойти по пути максимизации числа узлов, то здесь понадобится всего 8 узлов, а не 9, как в первом случае. Снижение количества узлов позволит сократить расходы на приобретение нового оборудования, его развертывание и эксплуатацию.

Описанная задача более всего напоминает задачу линейного целочисленного программирования с тем отличием, что ограничение имеет нелинейный вид и не может быть представлено в непрерывном виде (из-за присутствия факториала).

Применение целочисленного программирования позволит составить целевую функцию,

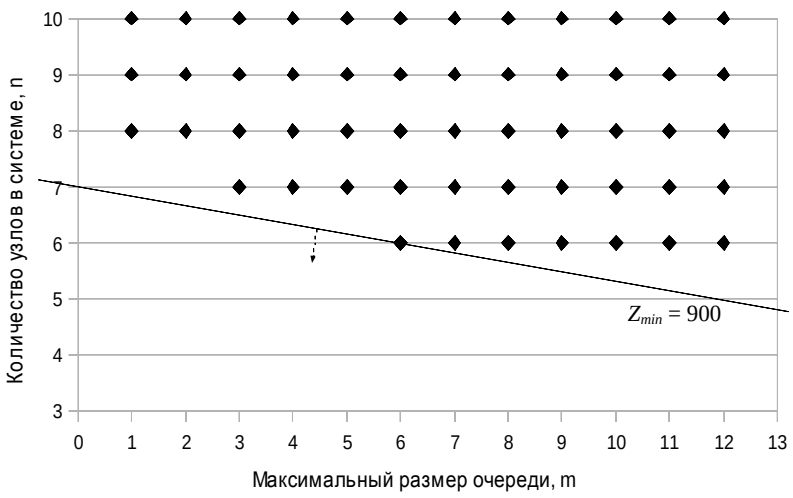

Рис. 2. **Линия Z_{min}**

учитывающую расходы на увеличение числа узлов, а также учесть потери, связанные с увеличением размера очереди.

Составим целевую функцию. Средняя стоимость современного сервера равна 300 тыс. руб. Именно на эту величину увеличатся общие единовременные затраты при увеличении числа узлов на единицу. Исследуемая PKI-система уже имеет 4 узла, поэтому значение соответствующей переменной в модели уменьшено на эту величину.

Также здесь следует учесть величину штрафа за увеличение размера очереди на одну единицу. Эти затраты могут быть связаны с модернизацией аппаратного и программного обеспечения, оттоком клиентов в связи с увеличением времени ожидания в очереди, а также служит фиктивным ограничением на длину очереди.

Тогда получим следующую модель:

$$Z = 300(n-4) + 50m \to \min$$
$$\begin{cases} Q \geq 0{,}95 \\ n \geq 4 \\ n, m \in \boldsymbol{N} \end{cases},$$

где Z - оптимизируемая функция;

Q - относительная пропускная способность;

n,m - количество узлов в системе и мест в очереди, соответственно.

Решение предложенной задачи графическим способом наиболее приемлемо, поскольку позволяет избежать сложных расчетов в ограничениях на область допустимых значений. Для этого мы построили линию, соответствующую Z = const, и указали направление ее убывания. На рис. 2 изображена линия Z_{min}, которая проходит через точку (6,6), достигая при этом минимального значения.

Достаточно увеличить количество узлов на 2, а размер очереди на 5 мест, чтобы решить поставленную задачу. При этом затраты составят 600 тыс. руб.

Таким образом, с помощью теории массового обслуживания можно определить эффективное число узлов для PKI-системы, состоящей из нескольких удостоверяющих центров. Для организации такой инфраструктуры наиболее подходит система высокой готовности, преимущество которой заключается в максимальной надежности.

Поступила в редакцию 05.08.2009 г.