УДК 004.75; 004.056.3

МЕТОДЫ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ РАСПРЕДЕЛЕННЫХ СИСТЕМ

Е.А. Микрин
ПАО «РКК Энергия»
Россия, 141070, Московская обл., г. Королев, ул. Ленина, д. 4А
E-mail: Eugeny.Mikrin@rsce.ru

В.В. Кульба
Институт проблем управления им. В.А. Трапезникова РАН
Россия, 117997, Москва, Профсоюзная ул., 65
E-mail: kulba@ipu.ru

С.К. Сомов
Институт проблем управления им. В.А. Трапезникова РАН
Россия, 117997, Москва, Профсоюзная ул., 65
E-mail: ssomov2016@ipu.ru

Ключевые слова: распределенные системы, безопасность распределенных систем, репликация массивов данных, оперативное и восстановительное резервирование массивов данных.

Аннотация: Рассматривается проблема повышения безопасности работы распределенных систем, работающих на основе ненадежных компьютерных сетей. Представлены три эффективных метода повышения безопасности работы таких систем: репликация массивов данных, оперативное резервирование данных в узлах системы и восстановительное резервирование. Все три метода дополняют друг друга и обеспечивают хорошую защищенность используемых в системе данных от воздействия различных негативных факторов. Приведена формулировка задачи оптимального размещения реплик массивов данных в распределенной системе и представлен алгоритм решения этой задачи.

1. Введение

На основе компьютерных сетей создано и функционирует множество распределенных систем обработки данных (РСОД) различного масштаба и назначения. В этих системах каналами связи объединяются множество компьютеров, удаленных друг от друга на сотни и тысячи километров. РСОД обслуживают сотни и тысячи пользователей, расположенных в разных часовых поясах. РСОД представляют собой крупномасштабные, сложные системы, в рамках которых между собой взаимодействует огромное количество информационных, программных и технических компонент. Под влиянием негативных факторов различной природы каждая из этих компонент может выйти из строя. В свою очередь это может привести к искажению или потере используемой в системе информации, и, в конечном счете, к простою, нарушению безопасности или к отказу отдельных элементов или всей системы. В работе рассмотрены методы, сущест-

венно повышающие безопасность распределенных систем: репликация массивов данных, их оперативное и восстановительное резервирование.

2. Репликация массивов данных

Эффективным и широко используемым методом повышения безопасности работы РСОД является метод репликации массивов данных по нескольким узлам компьютерной сети. Данный метод заключается в том, что некоторое количество N идентичных копий (реплик) массива данных размещается в N узлах компьютерной сети. Узлы компьютерной сети для размещения реплик выбираются с помощью специального алгоритма, который решает задачу отбора подмножества узлов. Подмножество узлов отбирается таким образом, чтобы достигалось оптимальное (или близкое к оптимальному) значение критерия оптимальности размещения реплик. В качестве критериев оптимальности, как правило, используются следующие: минимум стоимости эксплуатации системы, минимум среднего времени отклика системы на запрос к данным, максимум вероятности получения ответа на запрос.

Реплики размещаются в узлах сети, как правило, таким образом, чтобы данные реплик были максимально приближены к их потребителям (прикладным процессам и пользователям системы). При этом сокращается время и увеличивается вероятность успешной обработки запросов к данным реплик. Кроме того, при наличии в нескольких узлах сети идентичных реплик одного массива данных повышается надежность работы РСОД. Это обеспечивается тем, что в случае потери работоспособности одним узлом с репликой запросы к реплике могут быть переадресованы для обработки в другой работоспособный узел с идентичной репликой массива данных.

Для поиска оптимального варианта размещения реплик применяются различные методы [1,2]. В итоге счете эти методы сводятся к оптимизационной задаче, в которой необходимо из множества всех N узлов сети выбрать такое подмножество узлов M $(M<N)$ для размещения реплик, которое обеспечит наилучшее значение используемого критерия оптимальности. Задачи такого класса обладают большой вычислительной сложностью, поэтому для их решения применяются специальные методы, например эвристики, которые позволяют уменьшить вычислительную сложность таких задач.

3. Оперативное резервирование массивов данных

Для уменьшения количества случаев потери информации по причине разрушения реплик под влиянием тех или иных негативных факторов можно использовать два метода: метод оперативного резервирования реплик массивов данных, а также метод восстановительного резервирования.

При использовании первого метода в узлах компьютерной сети помимо реплик массивов данных размещается и дополнительный оперативный резерв (далее - ОР), который состоит из копий и/или предысторий массивов данных [3]. Это позволяет в случае разрушения реплики во время обработки запроса не переадресовывать запрос для обработки в другой узел сети с репликой, а продолжить обработку запроса в этом же узле с помощью размещенного в узле оперативного резерва из копий и/или предысторий массива данных. Оперативный резерв данных в узлах РСОД с репликами создается при помощи трех стратегий организации резерва:

Стратегия 1. Стратегия 1 используется для создания резерва массивов постоянных данных. В этом случае оперативный резерв создается из некоторого количества копий

реплики массива данных. При разрушении основной реплики обработка запроса продолжается с использованием первой из копий реплики, при ее разрушении обработка запроса продолжается с использованием второй копии реплики и так далее.

Стратегия 2. Вторая стратегия применяется для резервирования массивов с переменными данными. При этом в узле сети с размещенной в нем репликой создается резерв из предысторий массива данных. Предистории массива данных это некоторое количество предыдущих версий массива и соответствующих им журналов изменений. В случае разрушения реплики ее восстановление производится специальной программой на основе первой предыстории массива данных и соответствующего журнала изменений. При разрушении очередной предыстории, ее восстановление производится на основе предшествующей ей предыстории и так далее.

Стратегия 3. Данная стратегия является смешанной стратегией, в которой используются как копии, так и предыстории реплик. При этом сначала используются копии реплики (согласно стратегии 1), а при разрушении копий используются предыстории массива данных (согласно стратегии 2).

Детальное описание и анализ характеристик этих стратегий изложен в работе [3].

4. Восстановительное резервирование массивов данных

Размещение в узлах сети оперативного резерва в дополнение к репликам массивов данных значительно повышает безопасность функционирования распределенных систем. Тем не менее, остается возможность разрушения, как реплики массива данных, так и оперативного резерва в узле сети. В таком случае необходимо предпринять меры для восстановления работоспособности узла с разрушенным резервом и репликой. С этой целью используется метод восстановительного резервирования [4].

Суть метода восстановительного резервирования состоит в том, что для восстановления работоспособности узла сети с разрушенной репликой и ОР используется специальный резерв – восстановительный резерв (далее – ВР). ВР состоит из копий и/или предысторий массива данных, которые используются только для целей восстановления разрушенной в узле сети реплики и разрушенного ОР. Используется два вида восстановительного резервирования:

– Во-первых, в качестве восстановительного резерва используется ОР работоспособного узла сети, наиболее близко расположенного к узлу с разрушенной репликой и ОР.

– Согласно второму типу восстановительного резервирования восстановление разрушенных массивов данных и реплик производится путем использования специального резерва данных - архива магнитных носителей (далее АМН). АМН предназначен для надежного хранения массивов данных. Он используется только для обработки запросов на восстановление разрушенной информации.

Восстановление разрушенных данных производится с помощью стратегий восстановления: В-1 и В-2. Стратегия В-1 предполагает, что при помощи АМН последовательно восстанавливаются разрушенная реплика массива и все копии разрушенного ОР. Согласно стратегии В-2 при восстановлении очередной копии массива или реплики, наравне с копиями из АМН используются ранее восстановленные копии массива данных. Подробное описание и анализ характеристик данных стратегий приведен в [4].

5. Пример алгоритма решения задачи оптимального размещения реплик

Предположим, что распределенная система построена и работает на основе компьютерной сети, которая состоит из *N* узлов. Топология сети задана неориентированным графом $G = (X, \Gamma)$. Необходимо найти подмножество $\tilde{X}_p$ из *p* узлов множества *X* узлов сети такое, размещение в котором *p* реплик обеспечит минимальное значение стоимости функционирования распределенной системы. Используются следующие обозначения:

- $\Lambda_n^e = \|\lambda_n^e\|$ и $\Lambda_n^u = \|\lambda_n^u\|$ – векторы размерности N, в которых λ_n^e – интенсивность информационных запросов, а λ_n^u интенсивность запросов на модификацию, генерируемых в узле x_n.
- $dis(x_n, x_j)$ – длина кратчайшего пути между узлом x_n и узлом x_j.
- *s* - стоимость передачи единицы данных по пути единичной длины.
- d^e, d^u–средний объем данных, передаваемый по каналам сети при обработке информационного запроса и запроса на модификацию данных. $d^e = d^u$.
- $cost\_S(x_n)$ – стоимость хранения одной реплики в узле x_n.
- $cost\_E(x_n)$, $cost\_U(x_n)$ – стоимость обработки в узле x_n информационного запроса и запроса на модификацию данных.
- $V = \{v_1, \dots, v_n, \dots, v_N\}$ – вектор с «весами» узлов компьютерной сети, где $v_n = (\lambda_n^e d^e + p\lambda_n^u d^u)$.
- X_p - подмножество номеров вершин из *X*, в которых размещено *p* реплик.
- $d(X_p, x_n) = \min_{x_j \in X_p} dis(x_n, x_j)$ – минимальное расстояние от вершины x_n множества *X* до одной из вершин множества X_p.
- $\sigma(X_p)$ – передаточное число для подмножества вершин X_p, равное

$$\sigma(X_p) = \sum_{n=1}^{N} v_n sd(X_p, x_n)$$

  Величина $\sigma(X_p)$ равна сумме затрат на обмен данными между узлами из X_p и узлами множества *X* при обработке запросов.
- $\tilde{X}_p$ – *p*-медиана графа G, если для множества $\tilde{X}_p$ достигается минимум значения передаточного числа: $\sigma(\tilde{X}_p) = \min_{X_p \subseteq X}[\sigma(X_p)]$.
- $COST(X_p)$ – стоимость функционирования РСОД за единицу времени, зависящая от распределения реплик X_p, равная:

$$\mathrm{COST}(X_p) = \sum_{j=1/x_j \in X_p}^{p} cost\_S(x_j) + \sum_{j=1/x_j \in X_p}^{p} cost\_E(x_j) \left(\sum_{n=1/x_n \to x_j}^{N} \lambda_n^e \right) +$$

$$+ \sum_{n=1}^{N} \lambda_n^u \left(\sum_{j=1/x_j \in X_p}^{p} cost\_U(x_j) \right).$$

Величина стоимости $COST(X_p)$ состоит из трех компонент: затраты на хранение реплик, затраты на обработку информационных запросов и запросов на модификацию данных во всех узлах с репликами.

Задача оптимального размещения *p* реплик массива данных имеет следующую формулировку: для графа $G = (X, \Gamma)$ необходимо найти подмножество $\tilde{X}_p$ из *p* вершин графа, для которого достигается минимум функционала: $F_p(\tilde{X}_p) = COST(\tilde{X}_p) + \sigma(\tilde{X}_p)$.

Для решения сформулированной задачи используется эвристический алгоритм, являющийся модификацией метода поиска p-медиан графа, описанного в работе [5]. Краткое описание алгоритма:

1) Задается количество p медиан графа. Случайным образом из множества X выбирается p вершин, образующих множество X_p. Вершины из X, не включенные в X_p, отмечаются как «не протестированные».
2) Случайным образом из множества $\{X \backslash X_p\}$ выбирается «не протестированная» вершина x_j. Если таких вершин нет, то выполняется переход к шагу 6.
3) В цикле по каждой вершине x_i из X_p вычисляется величина Δ_{ij}, на которую изменится функционал F_p, если вершину x_i из X_p заменить на вершину x_j, отобранную на шаге 2):
$$\Delta_{ij} = F_p(X_p) - F_p({X_p}^i), \text{ где } {X_p}^i = (X_p \cup \{x_j\}) \backslash \{x_i\}$$
Запоминаем индекс i^* вершины из X_p, при замене которой на x_j достигается максимальное изменение функционала, т.е. $\Delta_{i^*j} = \max_{x_i \in S} \Delta_{ij}$
4) Если $\Delta_{i^*j} \leq 0$, то замена на вершину x_j любой из вершин множества X_p не производится. Маркируем вершину x_j как «протестированная» и возвращаемся к пункту 2.
5) При $\Delta_{i^*j} > 0$ замена вершины x_{i^*} из X_p на вершину x_j улучшает значение функционала. Производим замену вершин и маркируем обе вершины x_j и x_{i^*} как «протестированные». Получено новое множество $X_p = (X_p \cup \{x_j\}) \backslash \{x_i\}$. Возврат к пункту 2.
6) Завершение работы алгоритма.

6. Заключение

В статье представлены три эффективных метода повышения сохранности информации и повышения безопасности функционирования распределенных систем. Методы основаны на размещении в узлах системы реплик массивов данных, оперативного и восстановительного резерва данных. Оптимальное размещение реплик в узлах системы позволяет также увеличить производительность и надежность работы системы. В работе приведено описание эвристического алгоритма, позволяющего с достаточной точностью и за приемлемое время находить решение задачи оптимального размещения реплик. Оптимизация размещения реплик с помощью данного алгоритма позволяет на 10-12% снизить затраты на функционирование распределенной системы.

Список литературы

1. Сомов С.К. Репликация как инструмент повышения надежности функционирования распределенных систем // Информационные технологии и вычислительные системы. 2018. № 3. С. 69-79.
2. Loukopoulos T., Ahmad I., Papadias D. An Overview of Data Replication on the Internet // Proceedings of the International Symposium on Parallel Architectures, Algorithms and Networks ISPAN ’02. 2002. 6 p.
3. Микрин Е.А., Сомов С.К. Оптимальное оперативное резервирование информации в системах обработки данных на базе вычислительных сетей // Проблемы управления. 2016. № 5. С. 47-56.
4. Микрин Е.А., С.К. Сомов. Анализ эффективности стратегий восстановления информации в распределенных системах обработки данных // Информационные технологии и вычислительные системы. 2016. № 3. С.5-19.

5. Teitz M. B., Bart P. Heuristic methods for estimating the generalized vertex median of a weighted graph // Operations Research. 1968. Vol. 16. P. 955-961.