

УДК 681.3.06

А.В. СКАТКОВ, А.О. СМАГИНА

Севастопольский национальный технический университет, Украина

ОПТИМИЗАЦИЯ СТРУКТУРНЫХ РЕШЕНИЙ ПО КОНТРОЛЮ ДОСТУПА В СИСТЕМАХ ПЕРЕДАЧИ ДАННЫХ

В статье решается оптимизационная задача размещения точек контроля прав доступа в системах передачи данных с учетом обеспечения гарантоспособности безопасности передаваемых данных. Решена задача методами булева линейного программирования. Получено оптимальное решение с некоторым множеством точек контроля. Приведен пример системы с расстановкой контрольных точек и учетом маршрутов передачи данных в этой системе. Выполнен анализ полученного решения и его устойчивости при введении дополнительных маршрутов.

Ключевые слова: гарантоспособность, системы передачи данных, оптимизационная задача, контроль прав доступа.

Введение

В современной инфраструктуре компьютерных сетей важную роль играют факторы обеспечения гарантоспособности безопасности передаваемых данных. Это такие факторы как целостность, функциональная безопасность, подтверждение авторства, прав доступа к передаваемым данным [1]. Рассмотрим решение данной проблемы на примере специальной системы передачи данных (СПД). СПД состоит из слоев, слои образуются из узлов, слои и узлы упорядочены. Дисциплина функционирования СПД такова, что ее узлы упорядочены по слоям, данные могут передаваться только через соседние слои непосредственно от предыдущего к последующему по указанным маршрутам, направление передачи данных значения не имеет, т.е. речь идет о двусторонней передаче данных. Для каждого сообщения (пользователя) существует входной и выходной узел в сети, кроме того, строго предписанный маршрут, соответствующий праву доступа для этого сообщения. Маршрут задает администратор сети, который контролирует право доступа к этому сообщению, руководствуясь следующими критериями: наиболее кратчайший маршрут от источника к приемнику и равномерная нагрузка на узлы СПД. Под маршрутом понимается путь передачи данных от узла к узлу в каждом слое и соседних слоях. Узел СПД имеет следующую структуру: человек-оператор, техническая часть, программная часть. Функции узла СПД реализуют на основе использования аппаратно-программного комплекса с участием человека-оператора. Принципиально важно, что дополнительно в каждом узле может быть установлено специальное программно-аппаратное устрой-

ство контроля прав доступа – точка контроля доступа (ТКД). Контроль должен быть гарантоспособен, т.е. каждый маршрут должен быть проверен, проверка осуществляется хотя бы однократно в одном из узлов данного маршрута. Процесс проверки прав доступа является трудоемким и требует достаточно больших ресурсов, что само по себе отражается на затратах при проектировании и эксплуатации СПД. Построение оптимальных решений по расстановке ТКД должно основываться на двух моментах: во-первых, ТКД должна устанавливаться в узле, через который проходит несколько маршрутов, во-вторых, число ТКД должно быть минимально при соблюдении основного требования: каждое передаваемое сообщение должно быть проверено. Именно поэтому, с целью минимизации затрат на установку оборудования ТКД актуальна задача оптимизации расстановки ТКД в сети. Функционирование СПД на основе ТКД обеспечивает процесс проверки факторов, отвечающих за гарантоспособность системы в целом.

Целью данной статьи является рассмотрение подхода к защите передаваемых данных в СПД путем оптимальной расстановки ТКД узлов. Предлагаемый подход основан на постановке решения задачи булевого программирования при соответствующих ограничениях.

1. Постановка задачи

Пусть задана структура СПД, состоящая из N узлов, соединенных каналами связи, по которым могут передаваться данные по известным M маршрутам от i -го узла к j -ому и не могут передаваться от i узла к $j+1$ минуя слой j . Каждый узел может

быть инициатором сообщения, т.е. автором (с этого узла начинается маршрут передачи данных) и приемником сообщения (пользователь этого узла является получателем сообщения). Максимальное количество ТКД в системе будет равно мощности множества маршрутов $|M|$ в случае, если маршруты не пересекаются, т.е. $K = |M|$, где K – число контрольных точек. $N(M_i)$ – число контрольных точек на маршруте, которое должно быть минимальным, $K(M_i)$ – контрольные точки на i -м маршруте. Если маршруты пересекаются, тогда максимальное количество маршрутов равно M' , $M' < |M|$, т.к., например, можно установить ТКД в точке пересечения маршрутов. Дизъюнкция $K(M_i)$ должна быть равна $D(M_i) = 1$. С целью минимизации затрат требуется поставить минимальное количество аппаратуры, контролирующей права доступа, т.е. найти такую расстановку контрольных точек, чтобы $M' = \min$ и каждый маршрут имел точку контроля. Вариант расстановки называется допустимым, если все дизъюнкции для каждого маршрута равны 1. Иными словами, среди всех допустимых вариантов расстановки следует выбрать минимальный. Качество решения задачи можно оценить с помощью функционала $E(S, M, \Sigma, X)$, где S – структура сети, M – матрица маршрутов, Σ – стратегия расстановки маршрутов, X – вектор расстановки ТКД. Качество решения – $\text{extr}_{X^0 \in X} E(S, M, \Sigma, X)$

Фрагмент структуры СПД показана на рис. 1. Сообщения могут передаваться от любого узла – источника сообщения к любому узлу – приемнику сообщения. Передача осуществляется двусторонним способом, т.е. направление передачи сообщения роли не играет.

На рис. 1 S_i – i -й узел СПД.

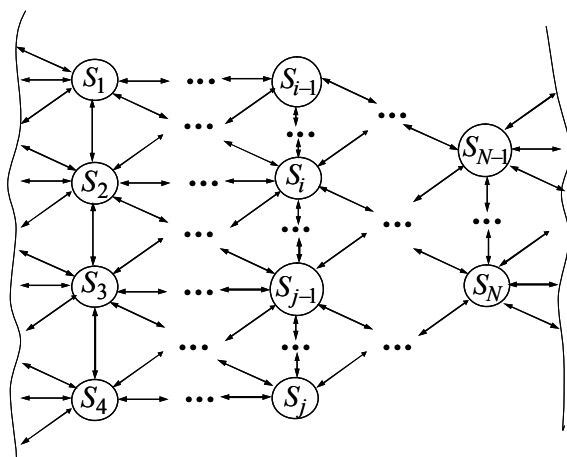


Рис. 1. Фрагмент структуры СПД

В СПД заданы маршруты передачи данных, их ограниченное число $|M|$. Маршруты представлены матрицей, в которой строки – номера маршрутов, столбцы – номера узлов. Элемент сети – x_{ij} , где первый индекс определяет номер маршрута, второй индекс – номер узла, в матрице $x_{ij} = 1$, если $x_{ij} \in M_i$, и $x_{ij} = 0$ в противном случае. В общем виде матрица может быть представлена в табл. 1.

Таблица 1
Множество маршрутов в СПД

| Маршруты \ Узлы | 1 | ... | j | ... | N |
|-----------------|----------|-----|----------|-----|----------|
| M_1 | x_{11} | ... | x_{1j} | ... | x_{1N} |
| \vdots | \vdots | ... | \vdots | ... | \vdots |
| M_i | x_{i1} | ... | x_{ij} | ... | x_{iN} |
| \vdots | \vdots | ... | \vdots | ... | \vdots |
| M_M | x_{M1} | ... | x_{MJ} | ... | x_{MN} |

Множество вершин – $x : \{x_i, \dots, i = \overline{1, |N|}\}$,

Множество маршрутов – $M \{m_i, \dots, i = \overline{1, |M|}\}$.

Маршрут M_i может быть описан следующим образом: $M_i : \langle x_{i1}, x_{i2}, \dots, x_{i|M_i|} \rangle$.

Необходимо найти такой вариант расстановки ТКД, который обеспечит $M' = \min$.

Математическая постановка оптимизационной задачи:

Целевая функция:

$$\sum x_i^k \rightarrow \min_{x \in \Delta\beta}, \quad (1)$$

где x_i^k – множество ТКД, $\Delta\beta$ – множество допустимых вариантов их расстановки, формируется из следующей системы ограничений:

$$\begin{cases} \sum_{j=1}^N x_{ij}^k \geq 1, & i \in M_1, x_i \neq 0 \\ \dots \\ \sum_{j=1}^N x_{ij}^k \geq 1, & i \in M_i, x_i \neq 0 \\ \dots \\ \sum_{j=1}^N x_{ij}^k \geq 1, & i \in M_M, x_i \neq 0 \\ x_{ij}^k \in \{0, 1\} & (\forall i \in \{1, 2, \dots, N\}) \end{cases}, \quad (2)$$

Система ограничений (2) формируется следующим образом: в уравнение входят все узлы маршрута M_i , т.е. переменные $x_{ij} = 1$. Каждому

узлу, вошедшему в уравнение ставится индекс k , отвечающий за то, что в нем устанавливается ТКД x_{ij}^k . Переменная x_{ij}^k может принимать два значения: 0 – аппаратура не устанавливается в i -м узле, 1 – устанавливается. Изначально все переменные x_{ij}^k равны 1, т.е. в каждом узле маршрута стоит точка контроля.

Система (2) обеспечивает выполнение ограничения конъюнкция дизъюнкций равна 1. Решая задачу методами булева линейного программирования, получаем оптимальное решение с некоторым множеством точек контроля.

2. Пример оптимизации структурных решений в СПД

Для примера рассмотрим СПД из 16 узлов. Известны маршруты передачи данных. Структура СПД изображена на рис. 2. Известны 6 маршрутов передачи данных. Одна ТКД устанавливается в одном узле. Необходимо расставить ТКД таким образом, чтобы контролировать все маршруты.

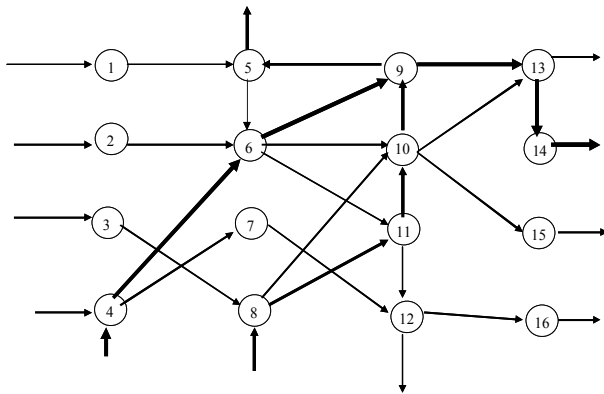


Рис. 2. Структура СПД

Выпишем все узлы маршрутов:

Маршрут № 1 – {1,5,6,11,12};

Маршрут № 2 – {2,6,10,15};

Маршрут № 3 – {3,8,10,13};

Маршрут № 4 – {4,7,12,16};

Маршрут № 5 – {4,6,9,13,14};

Маршрут № 6 – {8,11,10,9,5}.

Переменная x_i ($i \in \{1,2,\dots,16\}$), $x_i = 1$ – если в данном узле устанавливается ТКД, $x_i = 0$ – если не устанавливается.

Целевая функция (1):

$$\sum x_i^k \rightarrow \min_{x \in \Delta B},$$

где ΔB – множество допустимых вариантов их расстановки, формируется из следующей системы ограничений (2):

$$\begin{cases} x_1 + x_5 + x_6 + x_{11} + x_{12} \geq 1; \\ x_2 + x_6 + x_{10} + x_{15} \geq 1; \\ x_3 + x_8 + x_{10} + x_{13} \geq 1; \\ x_4 + x_7 + x_{12} + x_{16} \geq 1; \\ x_4 + x_6 + x_9 + x_{13} + x_{14} \geq 1; \\ x_8 + x_{11} + x_{10} + x_9 + x_5 \geq 1. \\ x_i \in \{0,1\} \quad (\forall i \in \{1,2,\dots,16\}) \end{cases}$$

Каждому маршруту соответствует одно ограничение, имеющее следующий смысл: для контроля прав доступа к отправленному сообщению на каждом маршруте достаточно одной ТКД.

Данная задача относится к классу задач булева линейного программирования.

Решение задачи с использованием среды MS Excel [2]:

Установка ТКД в узлах $N(6) = 3$:

– 4 (контроль маршрутов 4 и 5);

– 5 (контроль маршрутов 1 и 6);

– 10 (контроль маршрутов 2, 3 и 6).

Таким образом, все маршруты покрыты контрольными точками.

Добавим в k заданному множеству маршрутов следующие маршруты:

Маршрут № 7 – {4,8,11,15};

Маршрут № 8 – {3,7,10,14};

Маршрут № 9 – {2,5,10,16}.

Установка ТКД в узлах (контрольные точки не добавляются) $N(9) = 3$:

– 4 (контроль маршрутов 4, 5 и 7);

– 5 (контроль маршрутов 1 и 6);

– 10 (контроль маршрутов 2, 3, 6, 8 и 9).

Таким образом, на всех маршруты осуществлен контроль.

Добавим в существующую структуру следующие маршруты:

Маршрут № 7 – {2,6,9,14};

Маршрут № 8 – {4,7,11,14,15};

Маршрут № 9 – {3,6,7,9,16}.

Установка ТКД в узлах (контрольные точки добавляются не существенно) $N(9) = 4$:

– 6 (контроль маршрутов 1, 2, 5, 7 и 9);

– 10 (контроль маршрутов 2, 3 и 6);

– 12 (контроль маршрутов 1 и 4);

– 14 (контроль маршрутов 5, 7 и 8).

Таким образом, все маршруты покрыты точками контроля.

Изменим маршруты передачи сообщений:

Маршрут № 1 – {1,5,9,13};

Маршрут № 2 – {2,6,10,14};

Маршрут № 3 – {3,7,11,15};

Маршрут № 4 – {4,8,12,16};

Маршрут № 5 – {4,7,10,13};

Маршрут № 6 – {3,8,12,15}.

Установка контрольных точек в узлах (контрольные точки добавляются не существенно) $N(6) = 4$:

- 1 (контроль маршрута 1);
- 3 (контроль маршрутов 3 и 6);
- 4 (контроль маршрутов 4 и 5);
- 10 (контроль маршрутов 2 и 10).

Таким образом, все маршруты покрыты контрольными точками.

Изменим маршруты передачи сообщений:

- Маршрут № 1 – {1,5};
- Маршрут № 2 – {2,6,9};
- Маршрут № 3 – {3,7};
- Маршрут № 4 – {4,8};
- Маршрут № 5 – {10,13,14};
- Маршрут № 6 – {11,15,16};
- Маршрут № 7 – {12,16};
- Маршрут № 8 – {9,10,11}.

Установка ТКД в узлах (контрольные точки добавляются существенно) $N(8) = 6$:

- 1 (контроль маршрута 1);
- 3 (контроль маршрута 3);
- 4 (контроль маршрута 4);
- 9 (контроль маршрутов 2 и 8);
- 10 (контроль маршрутов 5 и 8);
- 16 (контроль маршрутов 6 и 7).

Таким образом, контроль прав доступа осуществлен на всех маршрутах.

3. Анализ полученных результатов

Выполним анализ полученного решения и его устойчивости при введении дополнительных маршрутов.

Множество типов изменения маршрутов в рассматриваемой структуре данных можно разбить на три класса:

- 1) ТКД не добавляются;
- 2) ТКД добавляются не существенно;
- 3) ТКД добавляются существенно.

Введем понятие меры близости маршрутов M_B . Между маршрутами M_i и M_j мера близости равна 0, если у них нет ни одного общего узла. Если есть хотя бы один общий узел, то мера близости полагается равной 1.

Таким образом, относительная оценка меры близости – в скольких узлах пересекаются маршруты M_i и M_j .

К первому классу можно отнести добавление тех маршрутов, которые пересекают уже имеющиеся в структуре маршруты и, главное, установленные ТКД. В таком случае расположение контрольных

точек не изменится. Если добавлять маршруты, которые не пересекают уже проставленные точки контроля, но существенно пересекаются с уже имеющимися в структуре маршрутами, то количество контрольных точек не изменится, поменяется только их расположение. Иными словами, внося изменения в маршруты передачи сообщений к этому классу можно отнести маршруты, для которых мера близости с уже имеющимися относительно высока, например, M_B больше 1.

Второй класс изменения маршрутов. Число контрольных точек изменяется не существенно, если добавляются маршруты, которые пересекаются с уже существующими и в них входит какой либо узел, не входящий ранее в установленный маршрут. В этом случае меняется расположение контрольных точек и происходит добавление еще одной точки. Иными словами, происходит изменение или добавление маршрутов к уже существующим, таким образом, чтобы мера близости M_B была в заданных пределах.

Третий класс изменения маршрутов. Если изменить маршруты в существующей структуре полностью и причем так, что они имеют длину не более трех узлов, то такое изменение внесет существенную расстановку контрольных точек в узлах сети. Иначе говоря, относительная оценка M_B близка к 0.

Заключение

В целом можно сделать вывод, что чем больше M_B , то тем меньше ТКД необходимо расставить в узлах сети. И наоборот, чем меньше M_B , тем больше ТКД необходимо расставить, что приводит к существенному увеличению затрат на контроль прав доступа к передаваемым данным.

Направлением дальнейших исследований можно считать решение данной задачи с условием введения ограничения на стоимость аппаратуры контроля и с учетом временных задержек работы аппаратуры контроля доступа.

Литература

1. Бахмач Е.С. Отказобесопасные информационно-управляющие системы на программируемой логике / Е.С. Бахмач, А.Д. Герасименко, В.А. Головир, А.А. Сиора, В.В. Скляр, В.И. Токарев, В.С. Харченко / Под. ред. Харченко В.С., Скляра В.В. – Национальный аэрокосмический университет «ХАИ», Научно-производственное предприятие «Радий», 2008. – 380 с.

2. Леоненков А.В. Решение задач оптимизации в среде MS Excel / А.В. Леонков – СПб.: БХВ-Петербург, 2005. – 704 с.

Поступила в редакцію 21.01.2010

Рецензент: д-р техн. наук, проф., директор інститута С.Г. Антошук, Одеський національний політехнічний університет, Одеса.

ОПТИМІЗАЦІЯ СТРУКТУРНИХ РІШЕНЬ З КОНТРОЛЮ ДОСТУПУ В СИСТЕМАХ ПЕРЕДАЧІ ДАНИХ

О.В. Скатков, Г.О. Смагіна

У статті вирішується оптимізаційне завдання розміщення точок контролю прав доступу в системах передачі даних з урахуванням забезпечення гарантоздатності та безпеки даних для передачі. Вирішено завдання методами булева лінійного програмування. Отримано оптимальне рішення з деякою безліччю точок контролю. Наведено приклад системи з розстановкою контрольних точок і урахуванням маршрутів передачі даних у цій системі. Виконаний аналіз отриманого рішення і його стійкості при введенні додаткових маршрутів.

Ключові слова: гарантоздатність, системи передачі даних, оптимізаційне завдання, контроль прав доступу.

OPTIMIZATION OF STRUCTURAL SOLUTIONS FOR ACCESS CONTROL IN SYSTEMS OF DATA

A.V. Skatkov, A.O. Smagina

Article optimization problem solved by placing control points of access rights to systems, data transmission based dependability ensure security of data transferred. A task is solved via boolean methods of linear programming. An optimum decision is obtained with some number of control points. An example of a system with an arrangement of control points is provided taking into account the routes of transmission in this system. The analysis of the decision and its stability is provided using introduction of additional routes.

Keywords: dependability, data transmission systems, optimization problem, control of access rights.

Скатков Александр Владимирович – д-р техн. наук, проф., заведуючий кафедрою кібернетики і висчислительной техніки Севастопольського національного технічного університету, Севастополь, Україна, e-mail: kvf@sevgtu.sebastopol.ua.

Смагіна Анна Олеговна – асистент кафедри кібернетики і висчислительной техніки Севастопольського національного технічного університету, Севастополь, Україна, e-mail: gorevaanna@rambler.ru.