

МЕТОД МНОГОУРОВНЕВОЙ ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ

Введение

Развитие компьютерных сетей и информационных технологий требует комплексного решения задачи повышения эффективности передачи информации, совместно с решением задачи защиты передаваемой информации. Необходимость обеспечения информационной безопасности пользователей компьютерных сетей вызвана широким использованием их в государственных и финансовых организациях, в промышленных предприятиях и в организациях оборонного комплекса. Перспективным является направление повышения уровня защищенности компьютерных сетей, которое связано с совершенствованием методов маршрутизации передачи информации в сетях.

Анализ последних исследований и публикаций [1] позволяет сделать вывод о том, что повышение уровня защищенности компьютерных сетей можно достичь методом многокритериальной маршрутизации, который позволяет учесть качество обслуживания и информационную безопасность пользователей компьютерных сетей.

Реализация многокритериальной маршрутизации совместно с поиском нескольких независимых альтернативных маршрутов позволяет увеличить допустимую нагрузку в сети, увеличить надежность передачи данных и снизить риски потери информации или ее модификации.

Метод многопутевой многокритериальной маршрутизации может быть усовершенствован в направлении создания многоуровневой защиты информации в компьютерных сетях.

Основная часть

Цель работы заключается в разработке метода многоуровневой защиты информации в компьютерных сетях.

Метод многоуровневой защиты информации опишем на математической модели компьютерной сети в виде графа, вершины которого моделируют узлы-источники и узлы-приемники информации, а ветви графа соответствуют каналам передачи информации.

Первый уровень защиты информации реализуется на основе решения задачи многокритериальной маршрутизации на графе между узлом-источником и узлом-приемником информации.

Введем систему частных критериев качества, которая, с одной стороны, характеризует качество передачи информации от узла-источника к узлу-приемнику, а с другой стороны, характеризуют уровень защищенности передаваемой информации от несанкционированного доступа.

В общем случае считаем, что качество обслуживания и уровень информационной безопасности пользователя оценивается n минимизируемыми критериями качества I_1, I_2, \dots, I_n . На основании технических характеристик каналов передачи информации, требований к качеству обслуживания и уровню информационной безопасности задаются предельно-допустимые значения частных критериев качества $I_{1m}, I_{2m}, \dots, I_{nm}$. Затем переходим к системе относительных частных критериев качества $I_1/I_{1m}, I_2/I_{2m}, \dots, I_n/I_{nm}$, диапазон изменения которых задаются ограничениями:

$$0 \leq \frac{I_i}{I_{im}} \leq 1, \quad i = \overline{1, n}. \quad (1)$$

Известно, что задача многокритериальной оптимизации является некорректной, так как частные критерии качества конфликтуют между собой. Улучшение одного частного критерия качества ухудшает один или несколько других частных критериев качества. Регуляризация некорректной задачи многокритериальной оптимизации выполним скалярной сверткой частных критериев качества по нелинейной схеме компромиссов [2]:

$$J = \sum_{i=1}^n \frac{\alpha_i}{1 - \frac{I_i}{I_{im}}}, \alpha_i \geq 0, \sum_{i=1}^n \alpha_i = 1, \quad (2)$$

где I_i – i -й частный критерий качества,

α_i – весовые коэффициенты,

I_{im} – предельно-допустимое значение частного критерия качества I_i .

Предлагается присваивать ветвям графа вес (длину) пропорциональный скалярной величине J , которая определяется по нелинейной схеме компромиссов (2).

Математическая модель компьютерной сети в виде графа, веса (длина) ветвей которого рассчитываются по выражению (2) позволяет реализовать многокритериальную оптимизацию маршрутов передачи информации от узла-источника к узлу-приемнику путем минимизации критерия качества:

$$\min_j L = \sum_{j=1}^r \sum_{i=1}^n \frac{\alpha_{ij}}{1 - \frac{I_{ij}}{I_{ijm}}}, \alpha_{ij} \geq 0, \sum_{i=1}^n \alpha_{ij} = 1, \quad (3)$$

где I_{ij} – i -й частный критерий качества в j -й ветви графа;

I_{ijm} – предельно-допустимое значение i -го частного критерия качества в j -й ветви графа;

α_{ij} – весовые коэффициенты;

n – количество частных критериев качества;

r – количество ветвей графа вдоль маршрута от узла-источника к узлу-приемнику.

Весовые коэффициенты α_{ij} в (3) позволяют задать приоритет тех каналов передачи информации, которые имеют больший уровень защищенности информации, чем другие. Весовые коэффициенты α_{ij} также дают возможность повысить уровень информационной безопасности за счет уступок в качестве обслуживания компьютерной сети.

Задача минимизации критерия качества (3) известна как задача о кратчайшем пути между узлом-источником и узлом-приемником. Следовательно, применение для расчета весов графа математической модели компьютерной сети свертки по нелинейной схеме компромиссов (3) сводит задачу многокритериальной маршрутизации к известной задаче о кратчайшем пути, которая может быть решена алгоритмом Дейкстры либо параллельными средствами маршрутизации [3].

В случае увеличения нагрузки на компьютерную сеть влияние частных критериев, характеризующих риски потери информации на общий интегральный критерий качества (3) уменьшается.

Проблему снижения чувствительности общего интегрального критерия качества (3) решим методом иерархической многокритериальной оптимизации на основании вложенных скалярных свертки по нелинейным схемам компромиссов [4]. Метод основан на формировании из системы n частных критериев качества (1) многоуровневой иерархической структуры в виде пирамиды, в основание которой лежит система n частных критериев качества, каждый $S+1$ -й уровень пирамиды формируется из частных критериев качества нижнего S -го уровня пирамиды, а вершина пирамиды определяет иерархический общий скалярный критерий качества. На каждом S -м уровне пирамиды все частные критерии качества разбиваем на K групп, по $n_k^{(s)}$ частных критериев качества в каждой группе. Скалярная свертка $n_k^{(s)}$ частных критериев выполняется по нелинейной схеме компромиссов (2) согласно выражению:

$$I_K^{(S+1)} = \sum_{i=1}^{n_k^{(s)}} \frac{\alpha_{ik}^{(s)}}{1 - \frac{I_{ik}^{(s)}}{I_{ikm}^{(s)}}}, \alpha_{ik}^{(s)} \geq 0, \sum_{i=1}^{n_k^{(s)}} \alpha_{ik}^{(s)} = 1, \quad (4)$$

где $\alpha_{ik}^{(s)}$ – весовые коэффициенты;

$I_{ik}^{(s)}$ – i -й частный критерий качества на S -м уровне в K -й группе;

$I_{ikm}^{(s)}$ – предельно-допустимые значения i -го частного критерия качества на S -м уровне в K -й группе:

$$0 \leq I_{ik}^{(s)} \leq I_{ikm}^{(s)}, i = \overline{1, n_k^{(s)}}. \quad (5)$$

Предположим, что пирамида частных критериев качества содержит S уровней. Тогда вершину пирамиды образует иерархический общий критерий качества $I^{(s+1)}$. Согласно методу иерархической многокритериальной маршрутизации предлагается присваивать ветвям графа, моделирующего компьютерную сеть, вес (длину) пропорциональный скалярной величине иерархического общего критерия качества $I^{(s+1)}$ формируемого в вершине пирамиды частных критериев качества (4), (5). Такая математическая модель компьютерной сети позволяет реализовать иерархическую многокритериальную оптимизацию маршрутов передачи информации от узла-источника к узлу-приёмнику путём минимизации длины маршрута

$$\min L = \sum_{j=1}^r I_{j0}^{(s+1)}, \quad (6)$$

где $I_{j0}^{(s+1)}$ – иерархический общий критерий качества j -й ветви графа,

r – количество ветвей графа вдоль маршрута от узла-источника к узлу-приёмнику.

Применение метода вложенных скалярных сверток по нелинейным схемам компромиссов (4), (5) встречает затруднения связанные с выбором предельно-допустимых значений частных критериев качества $I_{ikm}^{(s)}$ на всех уровнях, кроме нижнего (первого) уровня. Выше указывалось, что предельно- допустимые значения частных критериев качества на нижнем уровне известны из технических характеристик каналов передачи информации, требований к качеству обслуживания и уровню информационной безопасности. На более высоких уровнях иерархии при $S > 1$, предельные значения частных критериев на каждом S -м уровне $I_{ikm}^{(s)}$ неизвестны. В работе [4] предлагается при $S > 1$ преодолеть это затруднение путём нормировки в свёртке (4) частных критериев качества $I_{ik}^{(s)}$ не к максимальному значению $I_{ikm}^{(s)}$, а к минимальному значению свёртки частных критериев качества (4). Определим по выражению (4) минимальное значение $I_k^{(s+1)}$. Предположим, что минимизируемые частные критерии качества $I_{ik}^{(s)}$ достигают идеальные нулевые значения.

Тогда из выражения (4) следует, что $I_{k \min}^{(s+1)} = 1$, так как $\sum_{i=1}^{n_k^{(s)}} \alpha_{ik}^{(s)} = 1$. Введём в рассмотрение относительные частные критерии качества вида:

$$\overline{I_{ok}^{(s+1)}} = \frac{I_{k \min}^{(s+1)}}{I_k^{(s+1)}} = \frac{1}{\sum_{i=1}^{n_k^{(s)}} \alpha_{ik}^{(s)} [1 - I_{ik}^{(s)} / I_{ikm}^{(s)}]^1}. \quad (7)$$

Введённые относительные частные критерии качества (7) преобразуются в максимизируемые критерии качества $\overline{I_{ok}^{(s+1)}}$ на $S+1$ -м уровне. Действительно, если $I_{ik}^{(s)}$ стремится к своему максимальному значению $I_{ikm}^{(s)}$, то $\overline{I_{ok}^{(s+1)}}$ обращается в ноль. В том случае, когда $I_{ik}^{(s)}$ стремится к идеальному нулевому значению, относительный частный критерий качества $\overline{I_{ok}^{(s+1)}}$ на $S+1$ -м уровне стремится к единице, так как $\sum_{i=1}^{n_k^{(s)}} \alpha_{ik}^{(s)} = 1$. Преобразуем максимизируемый относительный частный критерий качества (7) в минимизируемый

$$I_{ok}^{(s+1)} = 1 - \overline{I_{ok}^{(s+1)}}. \quad (8)$$

Подстановка (7) в (8) даёт выражение для расчёта относительных частных критериев качества на $S+1$ уровнях без знания на уровнях $S > 1$ их предельных значений

$$I_{ok}^{(s+1)} = 1 - \left[\sum_{i=1}^{n_k^{(s)}} \frac{\alpha_{ik}^{(s)}}{1 - I_{oik}^{(s)}} \right]^{-1}, \quad (9)$$

где $I_{oik}^{(1)} = I_{ik}^{(1)} / I_{ikm}^{(1)}$.

Таким образом, на втором уровне иерархии критериев качества при $S=1$ расчёт относительных частных критериев качества выполняются по выражению (4), а для остальных уровней при $S>1$ вычисления относительных частных критериев качества реализуются согласно выражению (9).

Метод иерархической многокритериальной маршрутизации реализует второй уровень защиты информации и может быть усовершенствован, если его сочетать с многопутевой маршрутизацией, которая позволяет найти несколько независимых параллельных маршрутов передачи информации с близкими оценками по выражению (6). В этом случае увеличивается надёжность передачи данных и снижаются риски потери информации или ее модификации. Поэтому предлагается на третьем уровне защиты информации перейти к решению задачи многопутевой маршрутизации по оценкам (6). В задаче многопутевой маршрутизации требуется найти несколько параллельных и независимых маршрутов передачи данных между узлом-источником и узлом-приемником информации, имеющие наименьшие характеристики длины маршрутов по оценкам (6). Известно, что время решения задачи о кратчайшем пути при однопутевой маршрутизации алгоритмом Дейкстры растёт пропорционально $O(N^2)$, где N – количество узлов компьютерной сети. В случае многопутевой маршрутизации время решения задачи маршрутизации увеличивается пропорционально количеству искомым путей. В сложных компьютерных сетях существует проблема реализации многопутевой маршрутизации из-за существенного увеличения времени маршрутизации, которое пропорционально оценке $K O(N^2)$, где K – количество искомым маршрутов. Решим эту проблему на основе параллельного алгоритма однопутевой маршрутизации и последовательного поиска альтернативных маршрутов в компьютерной сети. Параллельные алгоритмы однопутевой маршрутизации имеют оценку времени решения задачи о кратчайшем пути $O(N)$ [3]. Последовательный поиск альтернативных маршрутов параллельными алгоритмами маршрутизации хотя и увеличивают время поиска K маршрутов в K раз, но сохраняет линейный характер зависимости времени маршрутизации $K O(N)$ от сложности компьютерной сети, оцениваемой количеством узлов N компьютерной сети.

Однако, многопутевая иерархическая многокритериальная маршрутизация утрачивает эффективность в режиме перегрузки компьютерной сети, когда пропускная способность отдельных направлений кратчайших маршрутов не может обслуживать возрастающий поток информации в этих направлениях. В таких ситуациях кроме рисков потери информации и ее модификации вследствие несанкционированного доступа к ней возрастает вероятность потери пакетов информации из-за перегрузки каналов передачи информации в компьютерной сети. В таких случаях предлагается сформировать четвёртый уровень защиты информации в компьютерной сети на основе многопутевой двухкритериальной маршрутизации. Из всей системы частных критериев качества I_1, I_2, \dots, I_n предлагается выбрать два критерия качества: скорость передачи информации J_1 и риск J_2 потери информации и ее модификации, диапазон изменения которых задаются ограничениями

$$0 \leq J_1 \leq J_{1m}, \quad 0 \leq J_2 \leq J_{2m}, \quad (10)$$

где J_{1m} и J_{2m} – предельно-допустимые значения J_1 и J_2 соответственно. Оба критерия качества J_1 и J_2 минимизируются при выборе маршрутов. Поэтому предлагается в ветвях графа моделирующей компьютерную сеть сменить веса (6) на новые значения, которые рассчитываются по выражению

$$J^* = \left(1 - \frac{J_1}{J_{1m}} \right)^{-1} + \left(1 - \frac{J_2}{J_{2m}} \right)^{-1}. \quad (11)$$

В рассматриваемом случае задача о кратчайших маршрутах решается согласно выражению:

$$\min_j L^* = \sum_{j=1}^R \left[\left(1 - \frac{J_{1j}}{J_{1jm}} \right)^{-1} + \left(1 - \frac{J_{2j}}{J_{2jm}} \right)^{-1} \right], \quad (12)$$

где J_{1j} и J_{2j} – частные критерии качества j -й ветви графа,

J_{1jm} и J_{2jm} – предельно-допустимые значения частных критериев качества j -й ветви графа,

R – количество ветвей графа вдоль маршрута от узла-источника к узлу-приемнику,

L^* – длина кратчайшего маршрута.

Маршрутизация по выражению (12) позволяет найти наименее загруженные каналы передачи информации в компьютерной сети, в которых риски потери информации и ее модификации минимальны. Такая маршрутизация реализует четвертый уровень защиты информации в компьютерной сети до определенного уровня ее перегрузки.

В случае предельной перегрузки компьютерной сети, когда начинается процесс потери пакетов информации целесообразно реализовать пятый уровень защиты информации в компьютерной сети на основе многопутевой маршрутизации по одному критерию качества – скорости передачи информации с целью выявления наименее загруженных маршрутов.

Выводы

Предложен метод многоуровневой защиты информации в компьютерных сетях на основе многопутевой и иерархической многокритериальной маршрутизации, состав критериев качества в которой адаптируется к режиму нагрузки компьютерной сети. Метод многоуровневой защиты информации позволяет повысить информационную безопасность пользователей компьютерной сети в условиях несанкционированного доступа к информации и в режимах перегрузки компьютерной сети.

Список литературы

1. Мартынова О.П. Применение многокритериальной маршрутизации для повышения информационной безопасности компьютерных сетей / О.П. Мартынова, А.А. Засядько, В.Л. Баранов // Проблеми інформатизації та управління: зб.наук.пр. – К.: НАУ, 2007. – Вип. 3(21). – С. 109-113.
2. Воронин А.Н. Многокритериальный синтез динамических систем / Воронин А.Н.– К.:Наук. думка, 1992. – 160 с.
3. Мартынова О.П. Параллельный алгоритм маршрутизации на графах и сетях / О.П. Мартынова // Проблеми інформатизації та управління: зб. наук. пр. – К.: НАУ, 2005. – Вип. 12. – С. 113-119.
4. Воронин А.Н. Декомпозиция и композиция свойств альтернатив в многокритериальных задачах принятия решений / А.Н. Воронин // Кибернетика и системный анализ. – 2009. – № 1. – С. 117-122.

Рецензент: д.т.н., проф. Петров О.С.

Надійшла 24.04.2010 р.