УДК 621

ИСПОЛЬЗОВАНИЕ ЛИНЕЙНЫХ ДИОФАНТОВЫХ УРАВНЕНИЙ ДЛЯ МОДЕЛИРОВАНИЯ МАРШРУТИЗАЦИИ В САМООРГАНИЗУЮЩИХСЯ СЕТЯХ

Д.Ж. Корзун, доцент Петрозаводского государственного университета, к.ф.-м.н.
А.В. Гуртов, с.н.с. Хельсинкского института информационных технологий (Финляндия), Ph.D

Проблема моделирования маршрутизации в самоорганизующихся сетях, частным случаем которых являются сети ad hoc [16], представлена в статье на примере инфраструктуры протокола идентификации сетевых ЭВМ (HIP, Host Identity Protocol [14]). Эта инфраструктура предназначена для обслуживания запросов, обеспечивающих динамическое связывание уникального имени конечной точки с ее текущим местоположением. Для моделирования маршрутизации предлагается подход, основанный на формальных грамматиках, линейных диофантовых уравнениях и базисах Гильберта [1–6]. Такие модели позволяют определить состояние маршрутизации в терминах конечного множества базовых маршрутов. Каждый базовый маршрут агрегирует пути, которыми может следовать заданный набор сообщений. Подход обобщает модели, основанные на графе сети [9].

Инфраструктура динамического связывания конечных точек. Протокол HIP и динамическое связывание. Протокол HIP определяет новый уровень в семействе протоколов Интернета [14, 15], расположенной между уровнем IP и транспортным уровнем. На уровне IP используются адреса для маршрутизации пакетов; на новом уровне – имена конечных точек (сетевых ЭВМ), формируя новое пространство имен Интернета. Эти имена реализуются в виде 128-битовых идентификационных меток (HIT, Host Identity Tag). Новое пространство имен устраняет двойственность роли IP-адресов, определяющих как местонахождение конечной точки, так и ее уникальное имя.

В протоколе HIP за IP-адресом оставляется лишь первая функция – топологическая метка, а вторая функция возлагается на новый уровень. Конечная точка может менять IP-адрес без прерывания соединений транспортного уровня, а соответствие между топологическими и идентификационными метками становится динамическим. Таким образом, протокол HIP обеспечивает дополнительную функциональность, позволяя естественным образом поддерживать мобильность, множественный доступ в Интернет и делегирование сервиса. Кроме того, за счет криптографического механизма формирования идентификационных меток обеспечиваются дополнительные гарантии информационной безопасности.

Для широкого использования HIP необходимо эффективное динамическое связывание между меткой HIT и текущими IP-адресами конечной точки. Для решения этой задачи архитектура HIP включает два механизма [14]. В первом для хранения соответствия "HIT–IP-адрес" используется инфраструктура поддержки имен, например, основанная на системах DNS (domain name system), LDAP (lightweight directory access protocol) или алгоритмах DHT (distributed hash table) [17]. Второй механизм базируется на концепции рандеву-сервера – посредника, перенаправляющего управляющие сообщения HIP между конечными точками. Эта концепция может быть расширена до перенаправляющей инфраструктуры – оверлейной сети HIP рандеву-серверов [11]. В обоих случаях будем использовать термин *инфраструктура динамического связывания*.

Маршрутизация в инфраструктуре. Для реализации инфраструктуры динамического связывания разумно использовать структурированные P2P-оверлеи, определяющие оверлейные (над нижележащей сетью IP) сети узлов. Взаимодействие между узлами обеспечивается алгоритмами DHT, предоставляющими механизм маршрутизации сообщений по линиям связи нижележащей сети [8, 18, 20].

Рассмотрим инфраструктуру из N узлов, $S = \{s_1, s_2, \ldots, s_N\}$. Каждый узел $s \in S$ идентифицируется меткой HIT_s и хранит множество пар $D_s = \{\langle HIT, VAL\rangle\}$, определяющих соответствие меток конечных точек их IP-адресам. Пара $\langle HIT, VAL\rangle$ может реплицироваться на другие узлы. Такие узлы, также как и сам узел s, будем называть *узлом назначения* метки HIT. В узле назначения пара $\langle HIT_d, VAL_d\rangle$ может представлять непосредственное соответствие между меткой HIT_d и IP-адресами конечной точки d. При этом последние хранятся в VAL_d. В перенаправляющей инфраструктуре возможен вариант, когда в VAL_d хранятся метки других узлов или конечных точек, которым перенаправляются сообщения. Это позволяет реализовать делегирование сервиса и обеспечить дополнительный уровень информационной безопасности [7, 19].

Конечная точка u, которая хочет связаться с другой конечной точкой w, зная ее метку HIT_w, выполняет запрос к инфраструктуре по этой метке. Запрос инициируется через любой узел инфраструктуры – *инициирующий узел*. Для доставки запроса к узлу назначения решается *задача маршрутизации* – последовательные пересылки от одного узла к другому, пока запрос не достигнет узла назначения. Запрос может быть как запросом от u на получение текущего IP-адреса конечной точки w, так и управляющим сообщением HIP от u к w. В первом случае узел назначения возвращает u текущие IP-адреса для w. Во втором случае сообщение перенаправляется к w по уровню IP.

Самоорганизация инфраструктуры. Инфраструктура протокола HIP должна поддерживать самоорганизацию, сводящуюся к модификации таблиц маршрутизации узлов и обеспечивающую выполнение следующих свойств.

1. Сохранение связности в условиях асинхронного присоединения и выхода узлов, а также отказов узлов и каналов связи нижележащей сети.

2. Задержки, вызываемые инфраструктурой, не должны превышать нескольких RTT между конечными точками HIP-соединения в нижележащей сети.

3. Адаптация и устойчивость к неоднородности нагрузки (узлов и соединяющих их линий связи), включая устойчивость к атакам.

4. Обеспечение гарантий доставки.

5. Затраты на самоорганизацию (управляющий трафик) должны составлять лишь небольшую долю пропускной способности инфраструктуры.

В то же время модификация таблиц маршрутизации в соответствии с этими свойствами является сложной задачей, так как для ее решения необходимо обеспечить узлы информацией о текущем состоянии инфраструктуры.

Подход к моделированию маршрутизации. Рассмотрим подход к моделированию, основанный на формальных грамматиках, линейных диофантовых уравнениях и базисах Гильберта. Получаемые модели предоставляют информацию о состоянии маршрутизации в инфраструктуре. Необходимый математический аппарат взят из [1–6].

Грамматика маршрутизации. Пусть сообщение с меткой HIT получено узлом s. Если s не является узлом назначения, то определяются узлы дальнейшего следования.

Узлы, которые известны s, хранятся *в таблице маршрутизации* T_s.

1. Базовая маршрутизация. Выбирается в точности один узел $v \in T_s$ для дальнейшего следования сообщения.

2. Повторные передачи. Для обеспечения дополнительных гарантий доставки узел s, отправив сообщение, ждет подтверждения. Если его нет, то s выполняет повторную передачу. Максимальное число попыток определяется параметром k.

3. Последовательная рассылка. В повторной передаче используются альтернативные направления. Узел s пытается отправить сообщение через узел v_1, затем через v_2 и так далее до v_k. Для каждого узла v задано число попыток k_v.

4. Параллельная рассылка. Аналогично предыдущему варианту, но s передает сообщение одновременно через v_1, v_2, ... и v_k. Дополнительные гарантии доставки обеспечиваются за счет пропускной способности.

5. Завершение пути. Сообщение достигает узла s и далее не пересылается.

Опишем перечисленные выше варианты с помощью следующих правил. В случае базовой маршрутизации правила определены для всех возможных направлений следования из таблицы маршрутизации T_s:

$$s \to v^{k_v}, v \in T_s, s \in S, \tag{1}$$

где k_v – число попыток передачи. Более компактно это можно представить как

$$s \to v_1^{k_1} v_2^{k_2} \cdots v_j^{k_j}; T_s = \{v_1, v_2, \ldots, v_j\}, s \in S. \tag{2}$$

Правила (2) можно использовать также для описания последовательной и параллельной рассылки. Если требуется явно указать, какая рассылка используется, то пометим правую часть правила дополнительным символом $\sigma \in \Sigma$:

$$s \to \sigma v_1^{k_1} v_2^{k_2} \cdots v_j^{k_j}, s \in S, \tag{3}$$

где $\sigma \in \{a, b, c\}$ определяет классификацию правил для случая базовой ($\sigma = \mathrm{a}$), последовательной ($\sigma = b$) и параллельной ($\sigma = c$) маршрутизации, соответственно.

Завершение пути следования сообщения описывается правилом:

$$s \to \varepsilon, s \in S, \tag{4}$$

где ε – пустая цепочка. Если требуется различать виды завершения, то используются дополнительные символы $\sigma \in \Sigma$ в правой части.

В общем случае, для узла s множество правил R_s задается как

$$s \to Q_s(s_1, s_2, \ldots, s_N; HIT), s \in S, \tag{5}$$

где Q_s – некоторый полином от s_1, s_2, ..., s_N (узлы инфраструктуры). Каждый член $v_1^{k_1} v_2^{k_2} \cdots v_j^{k_j}$ представляет некоторый набор возможных направлений маршрутизации – *вариант маршрутизации*, а коэффициент $\kappa \in \Sigma^*$ описывает дополнительные атрибуты маршрутизации. Таким образом, Q_s определяет классификацию маршрутизации в узле s по вариантам в зависимости от метки HIT, алгоритма маршрутизации и целей моделирования. Эта классификация допускает различные степени детализации. Так, в (1) все возможные направления рассматриваются отдельно, а в (2) они агрегированы в один вариант.

Пусть $R = \bigcup_{s \in S} R_s$. Для упрощения пренебрежем явной зависимостью от метки HIT, отслеживая пути следования любых сообщений (отметим, что эта зависимость может быть учтена косвенно в коэффициентах $\kappa \in \Sigma^*$). В результате приходим к КС-грамматике $G = (S, \Sigma, R, \cdot)$, не имеющей начальный символ и игнорирующей порядок символов в цепочках. Назовем ее *грамматикой маршрутизации*.

Пусть каждый узел $s \in S$ инициирует отправку $b_s^- \in \mathbf{Z}_+$ сообщений, которые маршрутизируются далее. В результате каждый узел назначения $v \in S$ получает $b_v^+ \in \mathbf{Z}_+$ сообщений, а число применений правил с характеристикой σ есть $b_\sigma \in \mathbf{Z}_+$. Множество всех путей, которыми следовали эти сообщения, назовем *маршрутом* и обозначим $(b^-) \overset{b}{\longrightarrow} (b^+)$.

В грамматике G маршруту соответствует вывод $\alpha \Rightarrow^* \gamma\beta$, где $\alpha = (s^{b_s^-})_{s \in S}$ показывает, сколько сообщений изначально послано каждым узлом; $\beta = (v^{b_v^+})_{v \in S}$ дает результирующее распределение сообщений; $\gamma = (\sigma^{b_\sigma})_{\sigma \in \Sigma}$ описывает суммарные характеристики использованных правил. Маршрут назовем *простым*, если в грамматике ему соответствует простой вывод.

Предложенный способ описания маршрутизации в виде грамматики обобщает традиционные графовые модели сети [9, 10, 12, 13], соответствующие (1). Правило (5) позволяет получить агрегированное представление о путях следования сообщений, объединяя несколько путей в один маршрут.

Пример 1. Рассмотрим инфраструктуру из узлов s_1, ..., s_5. Узлы соединены в кольцо по часовой стрелке. Узел s_1 может дополнительно отправлять сообщения параллельно к s_3 и s_5. Узел s_4 также может последовательно посылать сообщения к s_2 и s_5. Получаем грамматику маршрутизации с правилами r_1, ..., r_7:

$$r_1, r_2 : s_1 \to s_2 | \mathrm{c} s_3 s_5; \;\; r_3 : s_2 \to s_3; \;\; r_4 : s_3 \to s_4;$$

$$r_5, r_6 : s_4 \to s_5 | \mathrm{b} s_2 s_5; \;\; r_7 : s_5 \to s_1.$$

Правила, правая часть которых не помечена терминалом, определяют базовую маршрутизацию. Сообщение из s_1 может по часовой стрелке обойти все узлы и вернуться обратно, что соответствует выводу $s_1 \Rightarrow s_2 \Rightarrow s_3 \Rightarrow s_4 \Rightarrow s_5 \Rightarrow s_1$. Для сообщения из s_1 возможен маршрут из двух циклических путей, когда сообщение дублируется из-за параллельной рассылки. Это соответствует выводу $s_1 \Rightarrow \mathrm{c} s_3 s_5 \Rightarrow \mathrm{c} s_4 s_5 \Rightarrow \mathrm{c} s_5^2 \Rightarrow \mathrm{c} s_1 s_5 \Rightarrow \mathrm{c} s_1^2$.

Диофантова модель маршрутизации. Пусть КС-грамматика описывает маршрутизацию в инфраструктуре. Будем сначала игнорировать терминалы и построим по грамматике ассоциированную систему однородных неотрицательных линейных диофантовых уравнении (одАНЛДУ):

$$\sum_{r \in R_s} x_r = \sum_{r \in R} a_{sr} x_r, \;\; s \in S. \tag{6}$$

Каждому узлу s соответствует уравнение. Значения неизвестных x_r равны числу применений правила r в некотором выводе-цикле. Таким образом, описывается точный баланс между прибытием сообщений в узел s и их отправкой далее.

Система (6) представляет линейную диофантову модель маршрутизации в инфраструктуре. В матричном виде она имеет вид:

$$\mathbf{E}(R)x = Ax, \tag{7}$$

где матрица $\mathbf{E}(R) = \mathbf{E}$ определяет распределение правил маршрутизации по узлам инфраструктуры: $E_{sr} = 1$, если узел s использует правило r, иначе $E_{sr} = 0$. Отметим, что $\sum_{s \in N} E_{sr} = 1$, поскольку правило r принадлежит только одному узлу.

Матрица $\mathbf{A}$ отражает специфику маршрутизации, определяемую правыми частями правил (5). Строки соответствуют узлам. Каждый столбец описывает *вариант маршрутизации*: x_r соответствует правилу $r = [s \to Q_s[s_1, \ldots, s_N)]$, узел s передает сообщение в те узлы, для которых элементы столбца ненулевые. Если все столбцы являются единичными векторами, то $\mathbf{E}(R) - \mathbf{A}$ есть матрица инцидентности орграфа маршрутизации, и (7) моделирует закон циркуляции потока в сети [9]. Этот случай возможен, когда используются только правила (1) с $k_v = 1$. По правилам (2) и (3) ненулевые элементы в столбце определяются узлами, используемыми данным вариантом маршрутизации. Значение этих элементов равно числу возможных передач. Правила (4) дают нулевые столбцы.

Пример 2. Для грамматики маршрутизации из примера 1 система одАНЛДУ имеет вид:

$$\begin{cases} x_1 + x_2 = x_7; & x_3 = x_1 + x_6; & x_4 = x_2 + x_3; \\ x_5 + x_6 = x_4; & x_7 = x_2 + x_5 + x_6 \; . \end{cases}$$

Рассмотрим сценарий, при котором любой узел в итоге получает ровно столько сообщений сколько он инициировал, т.е. $b^- = b^+$. Соответствующий маршрут будем называть *контуром* и обозначать $(\mathbf{0}) \to (\mathbf{0})$.

Теорема 1. *Контуру всегда соответствует некоторое решение h системы одАНЛДУ (7) и наоборот. Контур является простым тогда и только тогда, когда решение базисное ($h \in H$).*

Доказательство. Любой вывод $(s^{d_s})_{s\in S} \Rightarrow^* (s^{d_s})_{s\in S}$, $d \in \mathbf{Z}_+^N$, дает некоторое решение системы одАНЛДУ (7). В формуле общего решения [4] $\alpha = \beta = \beta' = \beta'' = \varepsilon$, следовательно $x^{\alpha,\beta'} = x^{\beta''} = \mathbf{0}$. Таким образом, любому базисному решению соответствует простой цикл $s \Rightarrow^* s$ и наоборот. По определению грамматики маршрутизации любой подобный цикл дает простой контур, а конечный набор таких циклов – маршрут $(\mathbf{0}) \to (\mathbf{0})$. Верно и обратное: если предположить, что некоторый контур соответствует выводу, который нельзя представить в виде набора $\{s \Rightarrow^* s\}$, то получим решение системы (7), не удовлетворяющее теореме А.

Рассмотрим сценарий, когда исходное и итоговое распределение $b^-, b^+ \in \mathbf{Z}_+^N$, $b^- \neq b^+$ зафиксировано. Обозначим такой маршрут $(b^-) \to (b^+)$. Рассмотрим следующую неоднородную систему *АНЛДУ:*

$$E(R)x + b^+ = Ax + b^-. \tag{8}$$

Теорема 2. *Маршруту $(b^-) \to (b^+)$ всегда соответствует некоторое решение x системы (8). Если маршрут простой, то решение базисное ($x \in \mathbf{N}$). В частности, маршрут является простым, если $\forall s \in S$ $b_s^+ b_s^- = 0$. По произвольному решению системы (8) всегда можно построить маршрут $(c + c' + c'') \to (b' + c' + b'' + c'')$, где $c, c', c'', b', b'' \in \mathbf{Z}_+^N$; $c_s = b_s^- - \min(b_s^-, b_s^+)$; $c_s b_s' = 0$; $b_s' + b_s'' = b_s^+ - \min(b_s^-, b_s^+)$.*

Доказательство. В грамматике маршрутизации маршруту $(b^-) \to (b^+)$ соответствует вывод $(s^{b_s^+})_{s\in S} \Rightarrow^* (s^{b_s^-})_{s\in S}$, который по определению системы АНЛДУ дает некоторое ее решение. Для простого маршрута вывод не содержит циклов, определяя базисное решение. Условие $b_s^+ b_s^- = 0$ исключает случай, когда сообщение, инициированное узлом s, приходит обратно. В частности, если нет циклов $s \Rightarrow^* s$, то решение является базисным.

Однако могут быть решения, не соответствующие маршруту $(b^-) \to (b^+)$. По произвольному решению x всегда можно построить [4] маршрут для вывода $\alpha\alpha'\alpha'' \Rightarrow^* \beta'\alpha'\beta''\alpha''$. Подвывод $\alpha \Rightarrow^* \beta'$ ($\alpha = (s^{c_s})_{s\in S}$, $\beta' = (s^{b_s'})_{s\in S}$) содержит пути, для которых инициирующие узлы и узлы назначения не пересекаются. Подвывод $\alpha' \Rightarrow^* \alpha'\beta''$ ($\alpha' = (s^{c_s'})_{s\in S}$, $\beta'' = (s^{b_s''})_{s\in S}$) содержит пути, в которых среди узлов назначения всегда есть инициирующие узлы. Подвывод $\alpha'' \Rightarrow^* \alpha''$ ($\alpha'' = (s^{c_s''})_{s\in S}$) содержит простые циклы $\{s \Rightarrow^* s\}$. Полученный маршрут соответствует искомому из второй части условия теоремы.

Отметим, что $b_s' + b_s''$ равно числу сообщений, завершивших путь в узле s, без учета путей, где s является и инициирующим узлом, и узлом назначения.

Пример 3. В условиях примера 1 рассмотрим вариант, когда узел s_1 отправляет одно, а получает два сообщения (маршруты $s_1 \Rightarrow^+ s_1^2$). Этот случай можно описать системой АНЛДУ:

$$\begin{cases} x_1 + x_2 + 2 = x_7 + 1; & x_3 = x_1 + x_6; \quad x_4 = x_2 + x_3; \\ x_5 + x_6 = x_4; & x_7 = x_2 + x_5 + x_6, \end{cases}$$

где $b^- = (1,0,0,0,0)^{\mathrm{T}}$; $b^+ = (2,0,0,0,0)^{\mathrm{T}}$. Маршрут $s_1 \Rightarrow s_3 s_5 \Rightarrow s_4 s_5 \Rightarrow s_5^2 \Rightarrow s_1 s_5 \Rightarrow s_1^2$ определяется базисным решением $x = (0,1,0,1,1,0,2)^{\mathrm{T}}$ ($\alpha = \beta' = \alpha'' = \varepsilon$, $\alpha' = \beta'' = s_1$).

Обобщением системы (8) является система АНЛДН:

$$\sum_{r\in R_s} x_r + z_s^+ + b_s^+ \bullet \sum_{r\in R} a_{sr} x_r + z_s^- + b_s^-, \quad s \in N, \tag{9}$$

где $\bullet \in \{=, \leq, \geq\}$. Число сообщений, для которых s – инициирующий узел, и число сообщений, для которых s – узел назначения, связаны не точным равенством, а отношением $\bullet$. Узел s в процессе маршрутизации дополнительно отправляет z_s^- сообщений и в s завершают путь z_s^+ сообщений. Такие маршруты будем обозначать $(b^-, z^-) \to (b^+, z^+)$. В грамматике маршрутизации вспомогательные переменные z_s^+ и z_s^- соответствуют правилам $s \to \varepsilon$ и $\varepsilon \to s$, а сам маршрут – выводу $(s^{b_s^-})_{s\in S} \Rightarrow^* (s^{b_s^- + z_s^-})_{s\in S} \Rightarrow^* (s^{b_s^+ + z_s^+})_{s\in S} \Rightarrow^* (s^{b_s^+})_{s\in S}$.

Теорема 3. *Маршруту $(b^-, z^-) \to (b^+, z^+)$ всегда соответствует некоторое решение x системы (9). Если маршрут простой, то решение базисное (если $b^- \neq b^+$, то $x \in \mathbf{H}$; если $b^- = b^+$, то $x \in \mathbf{H}$). По произвольному решению системы (9) всегда можно построить маршрут $(c + c' + c'') \to (b' + c' + b'' + c'')$, где $c, c', c'', b', b'' \in \mathbf{Z}_+^N$; $c_s = b_s^- - \min(b_s^-, b_s^+)$; $c_s b_s' = 0$; $b_s' + b_s'' \bullet b_s^+ - \min(b_s^-, b_s^+)$.*

Доказательство. Аналогично теоремам 1 и 2.

Пример 4. В условиях примера 1 рассмотрим те случаи для узла s_1, когда входящих сообщений не меньше, чем исходящих. В остальных узлах предполагается точный баланс:

$$\begin{cases} x_1 + x_2 + z_1^+ \geq x_7 + z_1^-; & x_3 = x_1 + x_6; \quad x_4 = x_2 + x_3; \\ x_5 + x_6 = x_4; & x_7 = x_2 + x_5 + x_6. \end{cases}$$

Базис Гильберта состоит из пяти решений $(x_1, \ldots, x_7; z_1^+, z_1^-)$. Два из них дают вырожденные случаи $(0, \ldots, 0; z_1^+, z_1^-)$:

1) $z_1^+ = z_1^- = 1$; 2) $z_1^+ = 1$, $z_1^- = 0$.

Остальные решения: $h^{(1)} = (1,0,1,1,1,0,1;0,0)^{\mathrm{T}}$ – контур полного обхода инфраструктуры; $h^{(2)} = (0,1,0,1,1,0,2;1,0)^{\mathrm{T}}$ – контур $s_1 \Rightarrow s_3 s_5 \Rightarrow s_4 s_5 \Rightarrow s_5^2 \Rightarrow s_1 s_5 \Rightarrow s_1^2 \Rightarrow s_1$, равносильный решению из примера 4; $h^{(3)} = (0,0,1,1,0,1,1;1,0)^{\mathrm{T}}$ – контур $s_2 \Rightarrow s_3 \Rightarrow s_4 \Rightarrow s_2 s_5 \Rightarrow s_2 s_1 \Rightarrow s_2$, в котором узел s_1, выступая промежуточным узлом, не отправляет далее прибывающее от s_2 сообщение.

Теперь построим модель, учитывающую терминалы грамматики маршрутизации. Пусть $a_{\sigma r}$ – число появлений $\sigma \in \Sigma$ в правой части r. Рассмотрим маршруты $(b^-) \overset{b}{\longrightarrow} (b^+)$ и $(b^-, z^-) \overset{b}{\longrightarrow} (b^+, z^+)$, в которых количество применений правил, содержащих σ в правой части, ограничено $(=, \leq, \geq)$ величиной b_σ. Добавим к любой из предыдущих систем уравнения или неравенства вида:

$$\sum_{r\in R} a_{\sigma r} x_r \bullet b_\sigma, \quad \sigma \in \Sigma. \tag{10}$$

Для решений получаемых систем АНЛДН справедливы ранее установленные теоремы с учетом того, что выводы, соответствующие маршрутам, содержат терминальные цепочки. По произвольному решению всегда можно построить вывод:

$$\alpha\alpha'\alpha'' \Rightarrow^* \gamma'\beta'\gamma''\alpha'\beta''\alpha'',$$

где $\alpha = (s^{c_s})_{s\in S}$; $\beta' = (s^{b_s'})_{s\in S}$; $\alpha' = (s^{c_s'})_{s\in S}$; $\beta'' = (s^{b_s''})_{s\in S}$; $\alpha'' = (s^{c_s''})_{s\in S}$; $\gamma' = (\sigma^{d_\sigma'})_{\sigma\in\Sigma}$, $\gamma'' = (\sigma^{d_\sigma''})_{\sigma\in\Sigma}$; $\forall s \in S$; $c_s = b_s^- - \min(b_s^-, b_s^+)$; $c_s b_s' = 0$; $b_s' + b_s'' \bullet b_s^+ - \min(b_s^-, b_s^+)$; $\forall \sigma \in \Sigma d_\sigma' + d_s'' \bullet b_\sigma$.

Пример 5. В условиях предыдущих примеров рассмотрим маршруты, использующие параллельную r_2 или последовательную r_6 рассылку. Получаем систему АНЛДН:

$$\begin{cases} x_1 + x_2 + z_1^+ = x_7 + z_1^-; & x_3 = x_1 + x_6; \quad x_4 = x_2 + x_3; \\ x_5 + x_6 = x_4; & x_7 = x_2 + x_5 + x_6; \quad x_2 + x_6 \geq 1. \end{cases}$$

Общее решение определяется базисными решениями $h^{(2)}$ и $h^{(3)}$ из примера 4:

$$x = \left(x_1, x_2, x_3, x_4, x_5, x_6, x_7, z_1^+, z_1^-\right)^{\mathrm{T}} =$$

$$= C_1(0,1,0,1,1,0,2,1,0)^{\mathrm{T}} + C_2(0,0,1,1,0,1,1,1,0)^{\mathrm{T}} =$$

$$= (0, C_1, C_2, C_1 + C_2, C_1, C_2, 2C_1 + C_2, C_1 + C_2, 0)^{\mathrm{T}},$$

где C_1 и C_2 – произвольные неотрицательные целочисленные константы.

Приложения к самоорганизующимся сетям. Предложенная линейная диофантова модель дает математический аппарат для анализа маршрутизации в сети и получения

важной информации для выполнения самоорганизации. Базис Гильберта модели определяет базовые маршруты – конечный агрегированный набор всех возможных путей прохождения порции сообщений через инфраструктуру. Любой другой маршрут может быть получен как комбинация базовых. Таким образом, базовые маршруты определяют состояние связности инфраструктуры, и узлы могут использовать их для оптимизации таблиц маршрутизации.

Если время прохождения сообщений по некоторому базовому маршруту велико, то длинные пути этого маршрута можно сократить, транзитивно замыкая некоторые пути или их части. Для этой цели можно использовать контуры, определяющие, какие узлы и каким образом достижимы из исходного узла.

Модель допускает анализ различных сценариев нагрузки на инфраструктуру. Например, если $b_s^- = 1$ для $s \in N$, то все узлы одновременно отправляют сообщение. Исследуя ненулевые компоненты базисных решений, можно оценить равномерность нагрузки на узлы инфраструктуры и определить узкие места. Аналогичным образом, можно оценить насколько хорошо инфраструктура распределяет нагрузку, если только часть узлов $M \subset N$ посылает сообщения ($b_s^- = 1,\ s \in M$). В частности, это позволяет оценить устойчивость к атакам на группу узлов.

Использование модели может быть полезным для владельца группы узлов инфраструктуры. Модифицируя таблицы маршрутизации своих узлов, владелец может пытаться достичь распределения нагрузки на его узлы, например, в соответствии с объемом сообщений, которые инициируются его узлами, или в зависимости от имеющихся мощностей узлов. Это достигается за счет управления балансом входящих и исходящих сообщений.

Применение последовательной и параллельной рассылки увеличивает нагрузку на инфраструктуру. Анализ базовых маршрутов позволяет оценить степень возрстания нагрузки. Использование альтернативных путей усиливает гарантии доставки и информационную безопасность. Анализ базовых маршрутов позволяет оценить степень надежности доставки, определяя выход каких узлов приводит к ухудшению производительности или даже к невозможности доставки. Так, число контуров определяет "степень связности" инфраструктуры.

Пример 6. В примере 5 найдены три маршрута-контура, использующие s_1. Два из них ($h^{(1)}$, $h^{(2)}$) обеспечивают достижимость из s_1 за один шаг узлов s_2, s_3 и s_5, но до s_4 требуется два шага ($h^{(2)}$). Следовательно, узел s_1 может включить s_4 в таблицу маршрутизации.

Маршруты $h^{(1)}$ и $h^{(2)}$ используют s_5, т.е. этот узел критичен для обеспечения гарантий доставки из s_1. Часть нагрузки можно передать узлу s_3, если он добавит s_1 в таблицу маршрутизации. Это также увеличит производительность, поскольку s_3 в рассматриваемых маршрутах порождает длинные пути.

В примере 6 константы C_1 и C_2 определяют число маршрутов-контуров, использующих соответственно параллельную и последовательную рассылку. Параллельная рассылка в два раза увеличивает нагрузку на узел s_5, который в результате получает $2C_1 + C_2$ сообщений. Если применяется только базовая маршрутизация ($h^{(1)}$), то все узлы загружаются равномерно.

Вопросы реализации модели. Рассмотрим их в условиях широкого внедрения HIP. Соответствующая инфраструктура состоит из сотен и более узлов, обслуживающих миллионы конечных точек [11].

1. Сбор информации о таблицах маршрутизации. Для больших сетей полный сбор затруднителен. Кроме того, подобная информация быстро устаревает. Для построения модели можно использовать лишь доступные правила маршрутизации. Узлы, о существовании которых нет информации, можно учитывать как один источник/приемник сообщений. В зависимости от целей моделирования, правила маршрутизации можно брать выборочно. Таким образом, модель настраиваема на уровни имеющейся и существенной информации.

2. Нахождение базиса Гильберта. В общем случае, эта задача сложна для вычислений (overNP). В то же время, для ряда систем АНЛДУ существуют эффективные алгоритмы, сложность которых полиноминальна от числа уравнений, неизвестных и базисных решений [4, 5]. Это позволяет выполнять вычисления для сетей из сотен и тысяч узлов при небольшом числе базисных маршрутов.

3. Случай большого базиса Гильберта. Количество возможных путей может быть велико. Так, протокол Chord определяет инфраструктуры, в которых имеются $O((\log_2 N)!)$ возможных циклических путей из заданного узла [10]. В предлагаемой модели в маршруте агрегируется несколько путей, что дает более компактное описание. Более того, как правило, решение практических задач требует анализа не всех возможных маршрутов, а лишь небольшого их числа. Рассматриваемая модель позволяет отбирать нужные маршруты, используя ограничения вида (7)–(10). Применение модели целесообразно и в случае, когда известна лишь часть базиса (анализ на основе частичной информации о маршрутах). В частности, модель допускает вычисления с фиксированным временем на решение.

4. Место выполнения вычислений. Нахождение базиса Гильберта и его анализ могут выполнять сами узлы инфраструктуры. Из-за ограничений на ресурсы, эти узлы могут производить лишь небольшой объем вычислений на основе информации о близких узлах (локальная самоорганизация инфраструктуры). Для построения и решения модели в рамках всей инфраструктуры можно использовать дополнительные серверы – суперузлы. Отметим, что получение информации о маршрутизации не требует агрессивного опроса узлов. Сбор информации может быть организован в механизме маршрутизации сообщений – сообщение, проходя через инфраструктуру, собирает информацию о пути следования. Отметим также, что это дает возможность отслеживать наиболее часто используемые варианты маршрутизации.

5. Адаптация к изменениям. Инфраструктура подвержена динамичным изменениям, что требует быстрого перестроения модели. Эти события находят четкую интерпретацию в модели. Например, присоединение (выход) узла – это появление (исчезновение) уравнения в системе. Добавление (удаление) правила маршрутизации – появление (исчезновение) неизвестной. Изменение правила маршрутизации – соответствующее изменение коэффициентов в столбце матрицы $\mathbf{A}$. Кроме того, синтаксический алгоритм нахождения базиса Гильберта допускает использование информации о решениях систем, близких к исходной [4]. Таким образом, построение модели и ее решение могут наследовать информацию.

Заключение. В общем случае самоорганизация сети на примере инфраструктуры динамического связывания протокола HIP является сложной задачей. Для ее адекватного решения узлы сети необходимо регулярно снабжать данными о текущем состоянии маршрутизации. Предлагаемая линейная диофантова модель дает базовые маршруты в сети для различных сценариев отправки, маршрутизации и получения сообщений. Эти маршруты описывают искомое состояние маршрутизации. Представляется, что это позволит узлам модифицировать таблицы маршрутизации рациональнее, чем в существующих алгоритмах самоорганизации.

Рассмотренные приложения далеко не исчерпывают весь потенциал предложенной модели. Детальный анализ модели и ее применение к самоорганизации различных классов сетей и распределенных систем являются предметом дальнейших исследований.

ЛИТЕРАТУРА

1. **Ахо А., Ульман Д.** Теория синтаксического анализа, перевода и компиляции: Пер. с англ. Т. 1: Синтаксический анализ. – М.: Мир, 1978. – 612 с.
2. **Богоявленский Ю.А., Корзун Д.Ж.** Общий вид решения системы линейных диофантовых уравнений, ассоциированных с контекстно-свободной грамматикой. – Тр. Петрозаводского госуниверси-

тета. Сер. "Прикладная математика и информатика". Вып. 6. – Петрозаводск: Изд-во ПетрГУ, 1997. – С. 79-94.
3. **Корзун Д.Ж.** Об одной взаимосвязи формальных грамматик и систем линейных диофантовых уравнений// Вестник молодых ученых. – СПб: Изд-во СПбГТУ. – 2000. – № 3. – С. 50–56.
4. **Korzun D.** Grammar-Based Algorithms for Solving Certain Classes of Nonnegative Linear Diophantine Systems/ Proceedings of Finnish Data Processing Week at the University of Petrozavodsk (FDPW'2000): Advances in Methods of Modern Information Technology, Vol. 3. – Petrozavodsk, 2001. – P. 52-67.
5. **Korzun D.** Syntactic Methods in Solving Linear Diophantine Equations/ Proceedings of Finnish Data Processing Week at the University of Petrozavodsk (FDPW'2004): Advances in Methods of Modern Information Technology, Vol. 6. – Petrozavodsk, 2005. – P. 151-156.
6. **Схрейвер А.** Теория линейного и целочисленного программирования: Пер. с англ. Т. 2. – М.: Мир, 1991. – 342 с.
7. **Adkins D., Lakshminarayanan K., Perrig A. and et al.** Towards a More Functional and Secure Network Infrastructure/ Report No. USB/CSD-03-1242. Computer Science Division, University of California, Berkeley. – 2003, 16 p.
8. **Androutsellis-Theotokis S., Spinellis D.** A Survey of Peer-to-Peer Content Distribution Technologies// ACM Computing Surveys. – 2004. – Vol. 36, № 4. – P. 335-371.
9. **Bertsekas D.P.** Network Optimization: Continuous and Discrete Models. Athena Scientific: Belmont (USA), 1998. 593 p.
10. **Gummadi K., Gummadi R., Gribble S. and et al.** The Impact of DHT Routing Geometry on Resilience and Proximity/ Proceedings of the ACM SIGCOMM. – 2003. – P. 381-394.
11. **Gurtov A.V., Korzun D.G., Nikander P.** Hi3: An Efficient and Secure Networking Architecture for Mobile Hosts/ HIIT Technical Report, TR-2005-2. – 2005. – 17 p.
12. **Kleinberg J.** The Small-World Phenomenon: An Algorithmic Perspective/ Cornell Computer Science Technical Report 99-1776, 1999. – 14 p.
13. **Loguinov D., Kumar A., Rai V. and et al.** Graph-Theoretic Analysis of Structured Peer-to-Peer Systems: Routing Distances and Fault Resilience// IEEE/ACM Transactions on Networking. – 2005. – Vol. 13, № 5. – P. 1107–1120.
14. **Moskowitz R., Nikander P.** Host Identity Protocol Architecture: draft-ietf-hip-arch-03// IETF Internet draft. – 2005.
15. **Moskowitz R., Nikander P., Jokela P. and et al.** Host Identity Protocol: draft-ietf-hip-base-04// IETF Internet draft. – 2005.
16. **Perkins C.E.** Ad Hoc Networking. Addison Wesley Professional, 2001. – 384 p.
17. **Roost L.J., Toft P. N., Haraldsson G.** The Host Identity Protocol – An Experimental Evaluation/ Report ComNet6-05gr680. – Aalborg University, 2005. – 124 p.
18. **Rowstron A., Druschel P.** Pastry: Scalable, distributed object location and routing for large-scale peer-to-peer systems/ Proceedings of IFIP/ ACM International Conference on Distributed Systems Platforms (Middleware). – 2001. – P. 329-350.
19. **Shanmugam M., Muenz F., Tschofenig H., Gurtov A.** On Supporting Multicast and Delegation in Hi3/ Proceedings of the 8th International Symposium on Wireless Personal Multimedia Communications (WPMC'05). – 2005. http://www.iws2005.org.
20. **Stoica I., Morris R., Karger D. and et al.** Chord: A scalable peer-to-peer lookup service for Internet applications// IEEE/ACM Transactions on Networking. – 2003. – Vol. 11, № 1. – P. 17-32.

Получено 15.02.06