УДК 004.713, 004.27

Р.Б. Дунець
Національний університет “Львівська політехніка”,
кафедра спеціалізованих комп’ютерних систем

МЕТОД ПЕРЕДАЧІ ПАКЕТІВ У МЕРЕЖАХ НА КРИСТАЛІ З МАТРИЧНОЮ ТОПОЛОГІЄЮ

Описано метод маршрутизації передачі пакетів даних у матричних топологіях мереж на кристалі, що ґрунтується на введенні у заголовок пакета поля інформації про елементи мінімальних шляхів топології та застосуванні булевих операцій над цією інформацією.

The method of routing packet data in a matrix topology networks on a chip, based on the type of packet header field information about the elements of minimal paths topology and applying Boolean operations on the information.

Постановка проблеми. Останнім часом завдяки досягненням мікроелектроніки стало можливим створення мереж на кристалі (МНК). За своєю суттю мережа на кристалі є певним підходом до організації обміну пакетами даних між процесорами, пам’яттю та іншими вузлами, тобто ядрами (IP-core) у системах на кристалі. Тут слід зазначити, що мережі на кристалі практично не масштабуються, тобто кількість елементів таких систем є незмінною після створення кристала. На відміну від звичайних мереж, зокрема глобальних, топологія мереж на кристалі теж є фіксованою і є “відомою” для всіх її компонентів. Крім того, до мереж на кристалі ставиться вимога мінімальної затримки передавання пакетів, мінімальних обсягів буферної пам’яті та простоти алгоритму маршрутизації.

Аналіз останніх досліджень та публікацій. Створення мереж на кристалі велося в різних напрямах. Особлива увага приділялася дослідженню та розробленню архітектури таких мереж [1–3], топологій мереж [4–6], структурним елементам: адаптерам, рутерам, комутаторам [7, 8], питанням буферизації [9, 10] та оптимізації часу передавання пакетів [11].

Попри те, більшість запропонованих рішень практично вдосконалювали можливості класичних комп’ютерних мережі й не повною мірою враховували особливості та вимоги до мереж на кристалі.

Мета дослідження. Підвищення продуктивності мереж на кристалі на основі зменшення затрат часу на передавання пакетів.

Загальний алгоритм передачі пакета. Загальний алгоритм передавання одного пакета в комунікаційному середовищі мережі на кристалі, від передавача до приймача, містить такі кроки (рис. 1):

1. Елемент-передавач пакета на підставі інформації про номер елементу-приймача пакета та про топологію комунікаційного середовища одним із відомих методів визначає ті елементи топології, які утворюватимуть мінімальні шляхи передавання пакета. Залежно від місця елемента-передавача в топології та місця елемента-приймача може бути не один мінімальний шлях, а кількість елементів, що утворюють мінімальні шляхи, може становити від 2-х до всього числа елементів топології. Перелік номерів цих елементів, але без номера елемента-передавача, утворює окреме поле заголовка пакета.

2. Для кожного елементу топології перелік номерів елементів сусідів є наперед відомий і є незмінним впродовж роботи системи. Сусідній елемент, до якого необхідно передати пакет,

визначають шляхом виявлення номерів елементів-сусідів серед тих, що утворюють мінімальні шляхи. Якщо таких елементів виявиться більше одного, то потрібно вибрати один із них. Для цього серед кандидатів на передавання їм пакета визначають їх завантаженість (зайнятість). Зайняті у цей момент елементи теж вилучаються із розгляду за умови, що залишається хоч би один незайнятий елемент, який готовий прийняти. Якщо вільних не виявиться, то серед зайнятих вибирається, наприклад, випадковим чином, один із них, якому буде переданий пакет. У цьому випадку пакет має бути буферизований за допомогою вхідної чи вихідної буферизації, наприклад так, як показано в роботах [9, 10]. Аналогічним чином вибирають один елемент серед вільних.

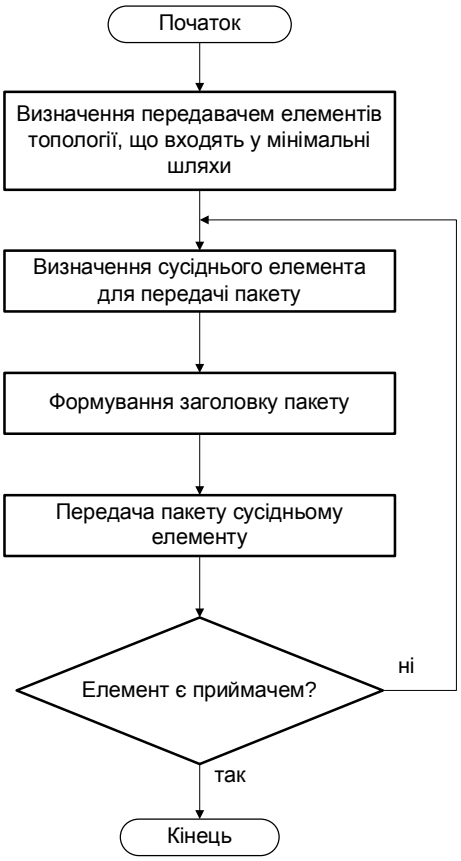

Рис. 1. Загальний алгоритм передавання одного пакета

3. Суть формування заголовка пакета зводиться до вилучення номерів елементів, що зв'язані з елементом, який надсилає пакет, зі списку у відповідному полі заголовка. Отже, у цьому полі заголовка після кожного передавання пакета від елемента до елемента число номерів буде зменшуватися.

4. Останній крок зводиться власне до пересилання пакета. Елемент, який передав пакет, стає незадіяним.

5. Якщо пакет досяг елемента-приймача, то процес передавання пакета завершується, в іншому випадку процес повторюється з п.2.

Приклад передавання пакета. Розглянемо процес передавання пакетів у матричній топології, що наведена на рис. 2. Нехай елемент 9 є передавачем, елемент 8 – приймачем (на рис. 2 вони позначені жирнішою лінією). Елементи 5, 11, що затушовані, є елементами, які зайняті на момент передавання їм пакета.

Після визначення елементом-передавачем всіх елементів, що утворюють мінімальні шляхи, формують матрицю-рядок, у якій позиції зліва направо відповідають номерам елементів топології. Самі ж елементи цієї матриці набувають значення 1 або 0. Значення 1 відповідає приналежності відповідного елементу топології до мінімального шляху, а 0 – коли даний елемент не утворює

мінімальний шлях. У нашому прикладі мінімальні шляхи утворюють елементи 5, 6, 7, 8, 9, 10, 11, 12 топології, а матриця матиме такий вигляд:

$$M = \left|0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0\right|.$$

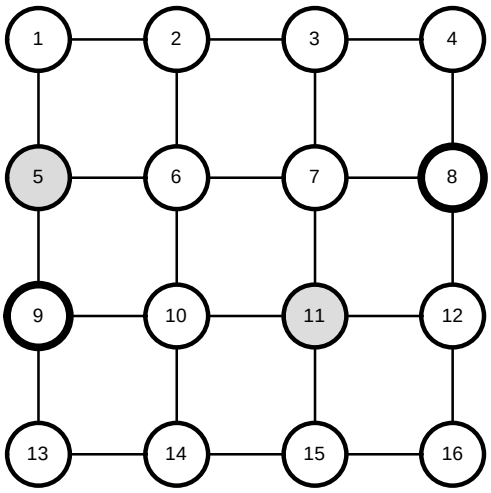

Рис. 2. Приклад матричної топології

Далі у цій матриці елемент, що відповідає номеру елемента-передавача, встановлюється в 0. Тобто матриця *M* стане такою:

$$M = \left|0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 1 \quad 1 \quad 1 \quad 0 \quad 1 \quad 1 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0\right|.$$

Елемент-передавач 9 має безпосередні зв'язки з елементами 5, 10, 13. У роботах [12, 13] доведено, що наявність зв'язків із сусідніми елементами топології найкраще подавати у вигляді бінарної матриці-рядка, оскільки для подальших процедур виявлення елементів-кандидатів на передавання їм пакета можна застосовувати операції алгебри логіки, виконання яких є принципово швидшим порівняно з арифметичними операціями.

Для нашого прикладу матриця зв'язків із сусідніми елементами 9-го елемента-передавача буде такою:

$$C = \left|0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 0 \quad 0 \quad 1 \quad 0 \quad 0 \quad 0\right|.$$

Визначення матриці *T* претендентів на отримання пакетів від 9-го елемента визначимо за допомогою операції кон'юнкції матриць *M* і *C*, тобто:

$$T = M \,\&\, C\,.$$

У нашому прикладі ця операція буде реалізована так:

$$T = \begin{array}{l} 0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 1 \quad 1 \quad 1 \quad 0 \quad 1 \quad 1 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0 \\ \underline{0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 0 \quad 0 \quad 1 \quad 0 \quad 0 \quad 0} \\ 0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0. \end{array}$$

Аналіз вмісту матриці *T* показує, що є два сусідні елементи, що можуть прийняти пакет. Оскільки 5-й елемент є зайнятий передаванням іншого пакета, то для передавання пакета вибирається елемент 10. Перед відправкою пакету елементу 10 необхідно відкоригувати матрицю *M* так:

$$M := M \,\&\, \overline{C}\,.$$

Тобто

$$M := \begin{array}{l} 0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 1 \quad 1 \quad 1 \quad 0 \quad 1 \quad 1 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0 \\ \underline{1 \quad 1 \quad 1 \quad 1 \quad 0 \quad 1 \quad 1 \quad 1 \quad 1 \quad 0 \quad 1 \quad 1 \quad 0 \quad 1 \quad 1 \quad 1} \\ 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 1 \quad 1 \quad 0 \quad 0 \quad 1 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0. \end{array}$$

Відкоригована матриця M розміщується у відповідному полі пакета.

В елементі 10 після надходження пакета проводять такі процедури. Спочатку визначають матрицю T претендентів на отримання пакетів від 10-го елемента із врахуванням сусідства цього елемента так:

$$T = \&\begin{array}{cccccccccccccccc} 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0. \end{array}$$

Виявилося, що кандидатами на приймання пакета є два елементи: 6 і 11. Оскільки елемент 11 є зайнятим, то для передавання пакета вибирається елемент 6. Залишилося відкоригувати матрицю M так:

$$M := \&\begin{array}{cccccccccccccccc} 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0. \end{array}$$

В елементі 6 будуть проведені такі дії визначення елемента, куди буде напрямлений пакет.

$$T = \&\begin{array}{cccccccccccccccc} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0. \end{array}$$

Таким елементом буде елемент 7. Інших варіантів немає. Далі коригується матриця M.

$$M := \&\begin{array}{cccccccccccccccc} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0. \end{array}$$

І, нарешті, в елементі 7 будуть проведені такі дії.

$$T = \&\begin{array}{cccccccccccccccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0. \end{array}$$

Наступним елементом, який прийматиме пакет, буде елемент 8. Цей елемент є останнім, оскільки йому власне адресований пакет.

$$M := \&\begin{array}{cccccccccccccccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0. \end{array}$$

Висновки. Отже, враховуючи той факт, що мережа на кристалі має фіксоване число елементів топології, що, своєю чергою, дає змогу визначити всі елементи мінімальних шляхів та помістити цю інформацію у заголовку пакета, забезпечують передавання пакетів у мережі з матричною топологією з мінімальними затратами часу. Крім того, застосування операцій алгебри логіки додатково зменшує затрати часу в процесі маршрутизації пакетів.

1. Chrysostomos N., Vijaykrishnan N., Chita R. Das. Network-on-Chip Architectures. A Holistic Design Exploration // Lecture Notes in Electrical Engineering, Vol. 45. - Hardcover 2010. - 223 p. 2. Kumar S., Jantsch A., Soininen J.-P., Forsell M., Millberg1 M., Oberg1 J., Tiensyrja K, Hemani A. A Network on Chip Architecture and Design Methodology // Proc. IEEE Computer Society Annual Symposium on VLSI (ISVLSI.02). - P. 105 - 112 3. Vincenzo R., Atienza D. A Reconfigurable Network-on-Chip Architecture for Optimal Multi Processor SoC Communication // 16th IFIP/IEEE International

Conference on Very Large Scale Integration (October 2008). – Rhodes, Greece. – P. 321-326. 4. Pande P.P., Grecu C., Jones M., Ivanov A., Saleh R. Performance Evaluation and Design Trade-Offs for Network-on-Chip Interconnect Architectures // IEEE TRANSACTIONS ON COMPUTERS, 2005, V. 54, № 8, p.1025-1040 5. Gebali F., Elmiligi H., Watheq El-Kharashi M. Networks-on-Chip: Theory and Practice.– Boca Raton (USA): CRC Press/Taylor and Francis Group LLC, 2009. – 307p. 6. Дунець Р.Б. Топології комп'ютерних систем. – Львів: ІППТ при НУ „Львівська політехніка", 2007. – 50 с. 7. Dally W., Towles B. Route packets, not wires: on-chip interconnection networks // Proceedings of the 38th annual Design Automation Conference (June 2001). – Las Vegas, USA. – P.684-689. 8. Bjerregaard T., Mahadevan S. A survey of research and practices of Network-on-chip // ACM Computing Surveys. – 2006. –Vol.38, 51. – P.1–51. 9. Дунець Б.Р. Базові архітектури пристроїв комутації пакетів з багатоканальною вхідною буферизацією Комп'ютерні технології друкарства. – Львів: Укр. акад. друкарства. – 2004. – №11. – С. 43–49. 10. Дунець Б.Р. Архітектура пристрою планування комутацією // Вісник Тернопільського державного технічного університету. – 2003. – Т. 8. – №4. – С. 85–91. 11. Jingcao Hu, Radu Marculescu, "Energy-Aware Communication and Task Scheduling for Network-on-Chip Architectures under Real-Time Constraints," date, vol. 1, pp.10234, Design, Automation and Test in Europe Conference and Exhibition Volume I (DATE'04), 2004. 12. Дунець Р.Б. Аналіз та синтез топологій комп'ютерних видавничо-поліграфічних систем: Монографія. – Львів: НВФ "Українські технології", 2003. – 192 с. 13. Дунець Р.Б. Визначення часу та маршрутів критичних шляхів топологій спеціалізованих комп'ютерних систем // Вісн. Хмельницького національного університету. – Хмельницький, 2007. – Т.1. – № 2. – С.70–74.

УДК 004.382

Р. Еліас
Національний університет "Львівська політехніка",
кафедра електронних обчислювальних машин

ВБУДОВАНИЙ КОНТРОЛЬ СЕКЦІОНОВАНИХ ПОМНОЖУВАЧІВ ЕЛЕМЕНТІВ ПОЛІВ ГАЛУА GF(2^M)

Розглядається секціонований помножувач елементів полів Галуа GF(2^m). Помножувач обробляє 521-бітні елементи поля Галуа GF(2^{521}), представлені з використанням гауссівського нормального базису типу 2 і формує 521-бітний добуток порціями по 16 бітів. Якщо під час обчислення добутку виникає помилка, помножувач формує відповідну ознаку. Помножувач використовується в процесорах оброблення цифрових підписів, які ґрунтуються на використанні еліптичних кривих.

Scalable multiplier for Galois field GF(2^m) elements is examined. The multiplier processes presented with the use of type 2 Gaussian normal basis 521-bit Galois field GF(2^{521}) elements and forms 521-bit result by 16 bits portions. The multiplier forms the error sign in case error during the calculation. The multiplier is used in the processors for digital signatures which are based on the use of elliptic curves.

Вступ. На сучасному етапі математичною основою цифрових підписів є еліптичні криві. В одному з варіантів реалізації цифрових підписів оброблення точок еліптичних кривих відбувається за правилами оброблення елементів полів Галуа *GF*(2^m). Розрядність елементів поля *m* може сягати 2048 бітів. Апаратна реалізація помножувача для таких полів вимагає більш ніж мільйона транзисторів. Помножувачі можуть бути паралельними, послідовними та паралельно-послідовними – секціонованими. У роботах останніх років звертається увага на вбудовані методи виявлення