УДК 654.02:519.246
© Р. Бурачок, Б. Коваль[1], 2011

МОДЕЛЮВАННЯ ПАРАМЕТРІВ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ З ВИКОРИСТАННЯМ ГЕНЕРАТОРА ПСЕВДОВИПАДКОВИХ ЧИСЕЛ ANSI X9.17

Розглянуто питання застосування генераторів псевдовипадкових чисел для генерування процесів, які відбуваються в телекомунікаційних мережах або вузлах зв'язку.

This paper considers the problem of using pseudorandom numbers generators to generate processes that occur in telecommunication networks or nodes of communication.

1. ВСТУП

Сучасні телекомунікаційні мережі характеризуються значною складністю структури та процесів, які відбуваються у вузлах зв'язку та у мережі в цілому. І тим не менше існує потреба точного математичного опису структури і процесів, які відбуваються у мережах або вузлах зв'язку, з метою визначення їх впливу на характеристики трафіку між окремими напрямками передавання.

Структуру та ієрархію мережі, організацію взаємозв'язків між вузлами можна описати використовуючи теорію графів, або будь-яку іншу, яка дозволить отримати достатньо точний математичний опис структури мережі або зв'язків між вузами. Процеси у мережі або у вузлах, які дозволяють отримати такі характеристики трафіку як часова затримка пакетів та джиттер у заданому напрямку передавання інтенсивність поступлення викликів чи пакетів у вузол і т.д., з їх точними числовими значеннями, отримуються за допомогою використання ряду відомих розподілів. І оскільки визначення характеристик трафіку в складних моделях вузла чи структури мережі відбувається на основі моделювання, то кожен з таких розподілів можна отримати одним із двох шляхів: перший – формувати для кожного процесу індивідуальний генератор, другий – використовувати спільний генератор рівномірного розподілу з якого далі формується необхідний розподіл для опису кожного процесу. Кожен з таких шляхів застосування генераторів має свої переваги і недоліки. Для першого головним недоліком є потреба використання значної кількості генераторів спеціалізованих на якомусь окремому процесі: генеруванні пакетів, визначенні напрямку передавання, перерозподілі послідовності пакетів у випадку використ-

[1] Національний університет „Львівська політехніка"

тання єдиної черги, яка працює з пріоритетами і т.д., а також значна складність програмної або апаратної реалізації такого виду генераторів, але перевагою є висока швидкість роботи генератора. Складність реалізації генераторів веде до введення ряду спрощень, які в кінцевому результаті ведуть до пониження точності результатів і різниці між реальними і отриманими при моделюванні значеннями. Для другого шляху недоліком є відносно низька швидкодія та потреба застосування додаткових блоків перетворення рівномірного розподілу у необхідні. Але значною перевагою є застосування універсального генератора придатного для будь-яких цілей у моделюванні процесів у мережі чи вузлі, а також зміна внутрішньої структури вузла, мережі чи процесів не веде до потреби формування нового генератора із новим видом розподілу, а отже і зміни всієї схеми моделювання, а тільки до введення нового блоку – кількох рядків у програмі, які будуть здійснювати перетворення рівномірного розподілу у заданий. Структурні схеми кожного із шляхів застосування генераторів показано на рис.1.

І саме послідовність дій: використання генератора рівномірного розподілу випадкових величин і перетворення рівномірного розподілу у необхідний для використання (рис.1.б) дозволить отримувати найбільш наближені до реальних умов результати моделювання роботи вузла зв'язку чи мережі та уникнути ряду спрощень. Тому саме таку схему і пропонується використовувати при моделюванні процесів у телекомунікаційних вузлах та мережах.

2. ТЕОРЕТИЧНА ЧАСТИНА

Основним питанням є спосіб реалізації генератора рівномірного розподілу. В якості такого генератора можна використати будь-який генератор псевдовипадкових чисел. Одними з кращих генераторів псевдовипадкових чисел рівномірного розподілу є генератори BBS [1], ANSI X9.17 [2], OFB/DES [3] та OFB/AES [3,4], але згідно [5], кращим із них вважається генератор ANSI X9.17, в основі якого використовується алгоритм шифрування DES. Робота генератора описується:

$$R_i = E_{K1}D_{K2}E_{K1}\left[V_i \oplus E_{K1}D_{K2}E_{K1}\left(DT_i\right)\right], \quad (1)$$

$$V_{i+1} = E_{K1}D_{K2}E_{K1}\left[R_i \oplus E_{K1}D_{K2}E_{K1}\left(DT_i\right)\right], \quad (2)$$

де DT_i – значення дати і часу на початку і-ої стадії генерування, V_i – початкове значення для і-ої стадії генерування, R_i – псевдовипадкове число отримане в результаті і-ої стадії генерування, E – шифрування, D – дешифрування, K_1, K_2 – ключі для алгоритму DES, які

використовуються на кожній стадії генерування, $\oplus$ – операція сумування по модулю 2.

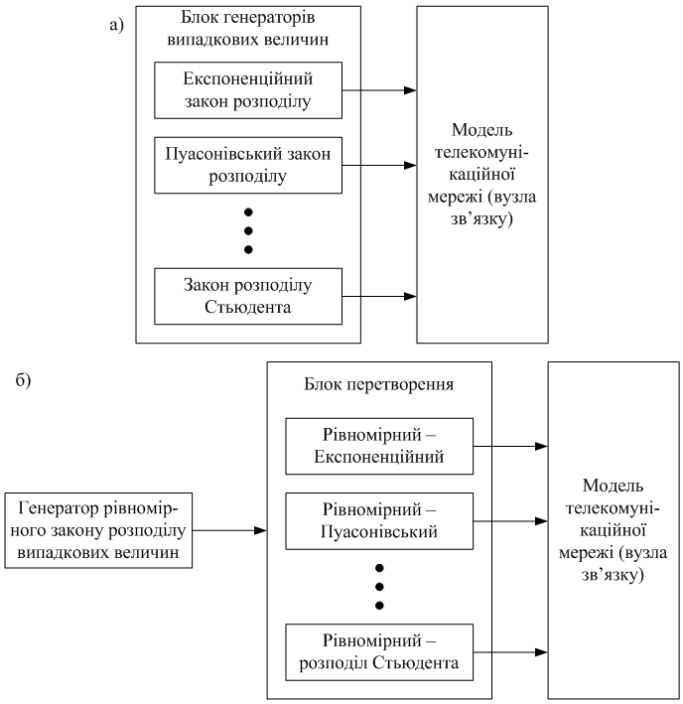


Рис. 1. Шляхи використання генераторів випадкових процесів у моделюванні процесів телекомунікаційних мереж: а) застосування індивідуальних генераторів; б) застосування єдиного генератора рівномірного розподілу випадкових величин та блоку перетворення

Структурна схема генератора ANSI X9.17 приведена на рис. 2.

Даний генератор використовується для генерування псевдовипадкових чисел в широких діапазонах – від 0 до 2^{64}. Для отримання чисел меншого діапазону пропонується використовувати ділення згенерованого випадкового числа довжиною 64 біти на відповідну кількість частин. Так наприклад, для отримання 8-ми випадкових чисел, які можуть представляти 8 виходів комутатора, кожен з яких нумерується 000, 001, …, 111, 64-ох бітову послідовність створену генератором розбивається по 3 біти – номер виходу комутатора. В результаті такту роботи генератора ANSI X9.17 можна отримати 21 випадкове число – номер виходу комутатора на який відбулося передавання пакету з його входу. Останній біт – 64-ий може бути відкинутим, або ж використа-

ним для формування послідовності у наступних тактах роботи генератора. Результати роботи генератора ANSI X9.17 для діапазону 1÷8 та 1÷256 виходів комутатора при рівномірному законі розподілі вибору виходів комутатора показано на рис. 3.

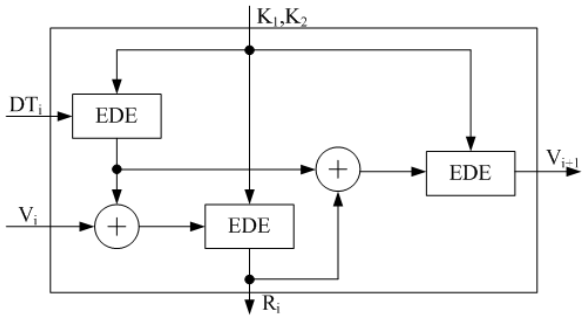
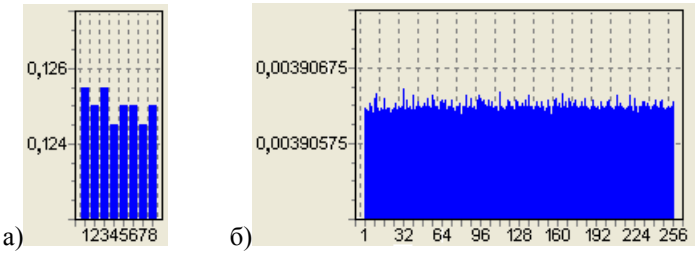


Рис. 2. Генератор псевдовипадкових чисел ANSI X9.17



а) б)

Рис. 3. Результати роботи генератора ANSI X9.17: а) при генеруванні діапазону чисел від 1 до 8 при кількості тактів 256; б) при генеруванні діапазону чисел від 1 до 256 при кількості тактів 1024

Тепер, очевидно було б доцільно провести порівняння роботи двох схем використання генераторів (рис.1) при моделюванні роботи телекомунікаційних пристроїв, або активного обладнання мережі. Для цього пропонується вибирати відомі розподіли, якими описані такі процеси як імовірності поступлення телефонних викриків у систему, імовірність звільнення вихідної лінії комутатора, імовірність затримки пакету у черзі при умові використання черги з абсолютним пріоритетом обслуговування пакетів, процес старіння і виходу з ладу активного обладнання мережі та ін. Так для прикладу роботи і порівняння генераторів буде використано наступні закони розподілів:

- Експоненційний (рис.4.а): $P(t) = e^{-\lambda \cdot t}$, де t – час тривання процесу, λ – інтенсивність виникнення події. Даним законом розподілу

описується надійність роботи системи, інтенсивність виходу з ладу обладнання, затримки пакетів у черзі з абсолютним пріоритетом обслуговування та ін.;

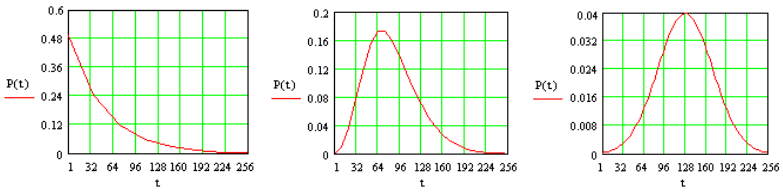
- Пуасонівський (рис.4.б): $P(t)=\frac{(\lambda\cdot t)^i}{i!}e^{-\lambda\cdot t}$. Даним законом розподілу описується процес поступлення викликів у комутаційну систему. Також даний розподіл є основою для формування і опису потоку звільнення комутатора;

- Нормальний (Гауса) розподіл (рис.4.в): $P(t)=\frac{1}{\sigma\cdot\sqrt{\pi}}e^{-\frac{(t-m)^2}{2\cdot\sigma^2}}$,

де σ – середньоквадратичне відхилення, m – математичне очікування. Даним законом розподілу описуються, як правило, шуми в радіотехнічних системах, надійність роботи системи, інтенсивність виходу з ладу обладнання та ін.

Відповідні закони розподілу: експоненційний, Пуасонівський та нормальний також були отримані за допомогою генераторів випадкових чисел. На рис.5 показані отримані результати розподілу випадкової величини згідно двох шляхів використання генераторів випадкових процесів: а, в, д – використання генераторів випадкових величин при їх індивідуальній реалізації, б, г, е – використання генератора рівномірного розподілу і формуванні на онові нього будь-яких інших з використанням блоку перетворень.

В табл. 1 наведено значення максимального відхилення та середнє значення відхилення отриманих результатів генерування випадкових величин двома способами відносно істинного за яке прийнято значення отримані згідно відповідних співвідношень.



а) *б)* *в)*

Рис. 4. Закони розподілу випадкових величин: а) експоненційний, б) Пуасонівський та в) нормальний (Гаусівський)

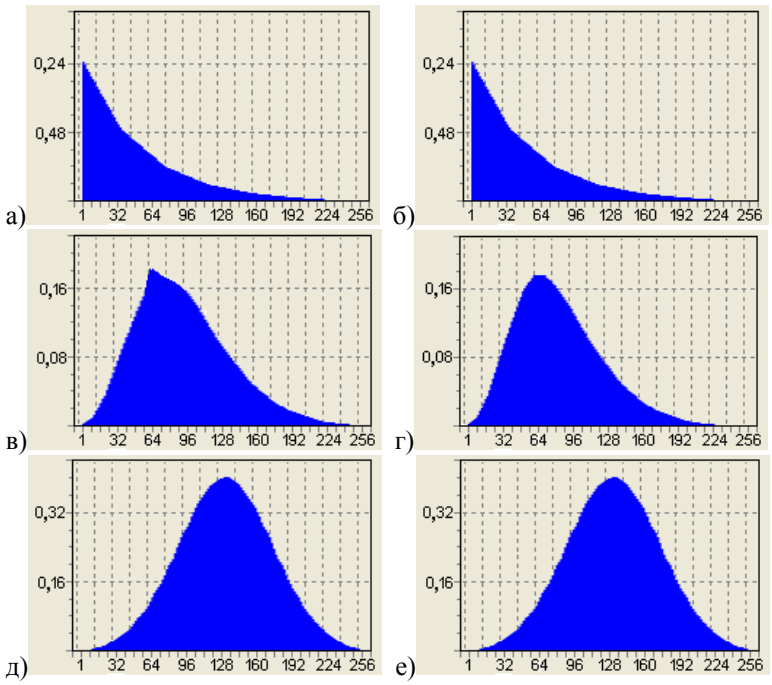


Рис. 5. Закони розподілу випадкових величин отримані експерементально

Таблиця 1

Відхилення результатів генерування від істинних

	I-ий шлях формування випадкової величини		II-ий шлях формування випадкової величини	
	$\left\|\overline{\sigma}\right\| = \frac{\sum_{i=1}^{256}\left\|\Delta_i\right\|}{256}$	$\left\|\Delta_{\max}\right\|$	$\left\|\overline{\sigma}\right\| = \frac{\sum_{i=1}^{256}\left\|\Delta_i\right\|}{256}$	$\left\|\Delta_{\max}\right\|$
Експоненційний	0,0384	0,0458	0,0382	0,0421
Пуасонівський	0,0789	0,0981	0,0267	0,0301
Нормальний	0,0287	0,0322	0,0286	0,0298

3. ВИСНОВКИ

Виходячи з результатів генерування випадкових величин, можна зробити наступні висновки: чим складніший закон розподілу, тим

складніше програмно, або апаратно реалізувати генератор випадкових величин, також спостерігається неточність генерування випадкових величин особливо у точках екстремуму при реалізації індивідуальних генераторів випадкових величин, що у свою чергу веде до неточності у моделюванні і отриманні кінцевих результатів.

1. Blum L., Blum M., Shub M. A Simple Unpredictable Pseudo-Random Number Generator. SIAM Journal on Computing, No.2, 1986. 2. John W. Lyons Key Management Using ANSI X9.17. U.S. Department of Commerce, National Institute of Standard and Technology, 1987. 3. В. Столлингс Криптография и защита сетей. Принципы и практика. Издательский дом «Вильямс», Москва 2001, 672 с. 4. Specification for the Advanced Encryption Standard (AES). Federal Information Processing Standards Publication 197. November 26, 2001. 5. Burn R. A. Pathway to Number Theory. Cambridge, England: Cambridge University Press, 2005.