УДК 658.012.011.56:681.3.06
[1]М.П. Карпінський, докт. техн. наук, проф., [1]Я.І. Кінах, канд. техн. наук, доц.
[3]І.З. Якименко канд. техн. наук, доц., [3]М.М. Касянчук, канд. фіз.-мат. наук, доц.
[1]Академія технічно-гуманістична, Польща
[2]Тернопільський національний технічний університет імені Івана Пулюя, Україна
[3]Тернопільський національний економічний університет, Україна

ВИКОРИСТАННЯ ПОТОКОВИХ МОДЕЛЕЙ ДЛЯ ЗАДАЧ КРИПТОАНАЛІЗУ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

M.P. Karpinsky – Dr., Prof., I.I. Kinakh – Ph.D, Assoc. Prof., I.Z. Yakymenko – Ph.D, Assoc. Prof., M.M. Kasyanchuk – Ph.D, Assoc. Prof.

USING OF STREAMING MODELS FOR CRYPTANALYSIS TASKS IN COMPUTER NETWORKS

Для задачі криптоаналізу найважливішими системними характеристиками є швидкодія та пропускна здатність мережі. З огляду на характерні особливості сучасних комп'ютерних мереж, доцільно на початковому етапі дослідження доцільно зробити декомпозицію мережі з урахуванням таких параметрів, як щільність розподілу інформаційних потоків у комунікаційній підсистемі, живучість, максимально припустимий діаметр кожної під мережі.

Більшість відомих способів вибору структури мережі й пропускної спроможності каналів зв'язку використовують потокові моделі, засновані на інтенсивностях $F_{i,j}$ трафіка в каналах $e_{i,j}$ мережі. Як функцію оптимізації в більшості випадків вибирають зростаючою. При цьому для обчислення $D_{i,j}$ ($F_{i,j}$) вибирають зважені функції вигляду [1]: $\sum_{\substack{i=1 \\ j=1}}^{N} D_{i,j}(F_{i,j})$, де кожна функція $D_{i,j}$ є монотонною.

Враховується пропускна спроможність каналу зв'язку, затримка обробки і поширення даних. Передбачається, що трафік потоку, що надходить у будь-який канал $e_{i,j}$, змінюється тільки через відновлення маршрутів. Таке припущення є коректним [1], коли зміна трафіка відбувається відносно повільно в порівнянні з середнім часом, необхідним для зменшення черг у мережі, і коли потоки в лініях виміряються шляхом часового усереднення.

Дослідження показали, що найбільш перспективний напрямок організації обчислювального процесу в криптоаналізі є концепція віртуальної підмережі, що дозволяє значно скоротити часову складність процедури формування і реконфігурації віртуального з'єднання, пов'язаного з переміщенням абонентських систем. Як критерій оптимальності розглядається часова складність реконфігурації шляху. При цьому враховується характер переміщення й імовірність перебування мобільного абонента у тій чи іншій локальній мережі.

Такі моделі дозволяють на практиці вибирати комп'ютерні мережі на яких розв'язок задач криптоаналізу є найпродуктивнішим.

Література

1.Кулаков Ю.А., Гайдукова Л., Халиль Х. А. Аль Шкерат. Способы повышения эффективности качества обслуживания (QoS) в многофункциональных сетях // Вісник НТУУ "КПІ" Інформатика, управління та обчислювальна техніка. – 2002. - № 39. - С. 132 - 141.