Выводы

Общее понятие динамической системы относится не только к объектам, описываемым дифференциальными уравнениями, но и к дискретным объектам, описываемым разностными уравнениями, а так же к конечным устройствам. Для рассматриваемых задач контроля важным является включение в описание контролируемой динамической системы параметров c, которые характеризуют техническое состояние системы в частности ее работоспособность. Задача контроля динамической системы заключается в формировании входных сигналов $x(t)$, измерении выходных сигналов $y(t)$ на основании этих изменений параметров c и степени работоспособности системы путем сравнения полученных значений параметров с их допустимыми значениями.

004.94:004.7

Яциковська У.О., Касянчук М.М., Трембач Р.Б.

УДОСКОНАЛЕНА СИСТЕМА ЗАХИСТУ КОМП'ЮТЕРНОЇ МЕРЕЖІ НА ПІДСТАВІ АСИМЕТРИЧНОГО ШИФРУВАННЯ

Досліджено залежність кількості ресурсу мережі в децентралізованих мобільних комп'ютерних мереж динамічної структури від обсягу вхідного буфера комп'ютерів. Залежність кількості обчислювальних станцій від пропускної здатності комп'ютерних мереж типу Asynchronous Transfer Mode. Розв'язано науково-технічну задачу створення теоретичних основ оптимального проектування комп'ютерних мереж з технологією Asynchronous Transfer Mode та децентралізованих мобільних комп'ютерних мереж динамічної структури на базі розроблених моделей, методів, алгоритмів оптимізації показників якості.

Постановка проблеми у загальному вигляді

Децентралізовані мобільні комп'ютерні мережі динамічної структури є малодослідженими з точки зору безпеки взаємодії вузлів, а також проведення інформаційної взаємодії на підставі асиметричного шифрування. Поява нової технології ATM обумовила потребу розробити аналітичну модель оцінки показників якості для різних категорій трафіка в залежності від інтенсивності вхідних потоків, перепускних спроможностей каналів зв'язку на підставі асиметричного шифрування.

Зв'язок з важливими науковими або практичними завданнями

Побудова, функціонування та застосування децентралізованих мобільних комп'ютерних мереж динамічної структури для захисту інформації на підставі асиметричного шифрування має більш ніж 30-річну історію. Організації та використання радіомереж з пакетною передачею даних почали проводились ще в 70-х роках XX століття [1].

Однією з найбільш перспективних технологій в комунікаційних мережах є технологія Asynchronous Transfer Mode, асинхронний спосіб передачі даних, яка справедливо вважається технологією XXI сторіччя [2].

Аналіз останніх досліджень і публікацій

Основними відношеннями стійкості є: рівень стійкості та часова функція стійкості. Рівень стійкості визначається як вектор $TV_{ID} = \left[TV_{ID}^{tc_0}, \quad \mathbf{K} \quad , TV_{ID}^{tc_n}, \quad TV_{ID}^{tcr} \right],\ TV_{ID}^{tc_i} \in \left[0 \mathbf{K} 1 \right)$, кожен елемент якого відображає рівень стійкості до об'єкту з ідентифікатором ID стосовно визначеної категорії взаємодії tci [3].

Для різних категорій користувачів мереж в передачі різнорідної інформації , форум ATM ввів наступні категорії сервісу:

CBR (constant bit rate) – передача з постійною швидкістю відео та аудіоінформації;

VBR (variable bit rate) – передача із змінною швидкістю скомпресованої відео та

аудіоінформації;

ABR (available bit rate) – передача із доступною швидкістю файлів даних;

UBR (unspecified bit rate) – передача із невстановленою швидкістю даних електронної пошти, служби новин, тощо [4].

Встановлено такі показники якості обслуговування, які використовуються при оцінці якості передачі по каналах різних типів трафіку:

середня затримка в передачі комірок – Cell Transfer Delay (CTD);

варіація затримки передачі – Cell Delay Variance (CDV);

частка (ймовірність) втрачених комірок – Cell Loss Ratio (CLR) [5].

Формулювання мети статті та постановка завдання (досліджень)

Метою роботи є розробка математичних моделей та методів для побудови адаптивних засобів формування реакцій вузлів децентралізованих мобільних комп'ютерних мереж динамічної структури та оптимального розподілу інформаційних ресурсів серед вузлів обчислювальних мобільних мереж динамічної структури та мереж типу АТМ на підставі асиметричного шифрування.

Основний матеріал дослідження

Децентралізована модель визначення адекватного рівня стійкості, має властивість адаптивності ,що формується з двох складових:

забезпечує механізми для встановлення відношень стійкості в результаті взаємодії самих об'єктів та модифікації наявних відношень в залежності від зміни структури системи;

дає змогу виявляти зміни у поведінці об'єктів та модифікувати рівні довіри до них.

Для забезпечення ефективного функціонування ДМКМДС необхідно використати засоби формування реакцій, що здатні адаптуватись при швидкій зміні структури мережі. На основі аналізу моделей стійкості, що застосовуються при побудові адаптивних систем формування реакцій, проведемо наступні дослідження. Для побудови відношення стійкості асиметричного шифрування елементи вектора рівнів стійкості, що визначається за такою формулою:

$$TV_{O_n}^{tc_i} = \begin{cases} 0, & \text{якщо } R < TV_{MIN}^{tcr_i}; \\ \left[\prod_{k=0}^{n-1} TV_{O_k}^{tcr}\right] TV_{O_n}^{tc_i}, & \text{якщо } R \geq TV_{MIN}^{tcr_i}, \end{cases} \quad (1)$$

де $R = \prod_{k=0}^{n} TV_{O_k}^{tcr}$, $i = \overline{0, \mathbf{K}, |TC|}$.

Проведемо чисельний експеримент для моделі (1), в якій значення Т належить проміжку [0;8*1020], а $TV_{o_n}^{tc_i}$ - стійкість криптоалгоритму з використанням математичного апарату ЕК. Графічне представлення результату подане на рисунку (1).

Дослідження показали, що система працює стабільно. Лише в краєвих умовах досягається локальний максимум, це відповідає послідовному виконанню алгоритму, тому цей випадок не беремо до уваги.

Місткість вхідного буферу N повинна задовольняти такій нерівності

$$N > \sum_{k=1}^{m}\left[l_k \sum_{i=1}^{m} l_i \left(E_i^2(t) + \mathrm{var}_i(t)\right) \Big/ 2\left(1 - S_{k-1}\right)\left(1 - S_k\right)\right], \quad (2)$$

де $E_i\{t\}$ та $\mathrm{var}_i(t)$ – відповідно, середнє значення та дисперсія функції розподілу часу обробки запиту, l – інтенсивність поступлення заявок у систему, $r_k = l_k E_k(t)$, $S_k = \sum_{i=1}^{k} r_i < 1$, $S_0 = 0$.

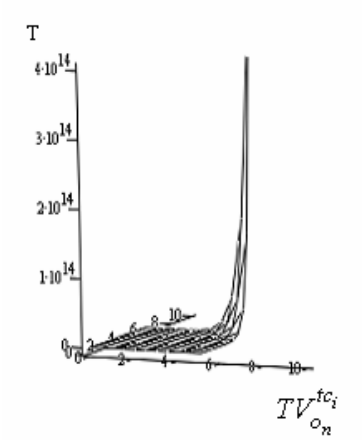

Рис. 1. Рівні стійкості асиметричного шифрування в мобільній комп'ютерній мережі

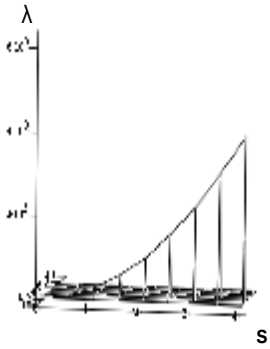

Рис. 2. Залежність кількості ресурсу мережі від обсягу вхідного буфера комп'ютерів

Дослідження показали, що із збільшенням кількості ресурсу мережі значно збільшується обсяг вхідного буфера окремого комп'ютера.

На основі апарату систем та мереж масового обслуговування в роботі отримані такі аналітичні моделі для оцінки Q_0S (Quality of Service):

$$CTD_{CBR}(\{m_{rs}\}) = \frac{1}{H^{(0)}_{\Sigma CBR}} \sum_{(r,s)\in E} \frac{f^{CBR}_{rs}}{n'_{rs}m - f^{CBR}_{rs}} \qquad (3)$$

$m^{(1)}_{rs}$ – перепускна спроможність КЗ, виділена під трафік CBR, n'_{rs} – число базових

цифрових каналів (64 кбіт/с), виділених під трафік CBR у локальній мережі (r, s) ; f_{rs}^{CBR} – потік трафіка CBR у КЗ (r, s) .

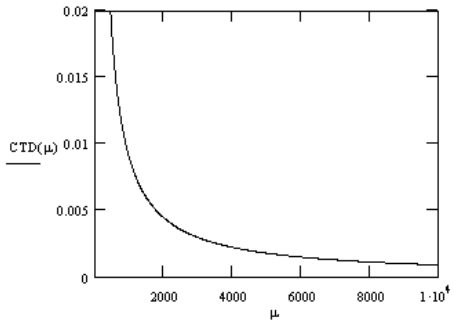

Рис. 3. Залежність кількості обчислювальних станцій від перепускної здатності комп'ютерних мереж

Дослідження показали, що із зростанням кількості обчислювальних станцій зменшується перепускна здатність комп'ютерних мереж. Тому, недоцільно значно збільшувати кількість комп'ютерів в мережі.

Висновки, рекомендації та перспективи подальшого розвитку даного напрямку

Сучасні комп'ютерні мережі типу АТМ є швидкісними і забезпечують високий рівень стійкості криптоалгоритмів на підставі асиметричного шифрування. Тому, на практиці доцільно використати мережі типів ДМКМДС та АТМ для захисту інформації, оскільки вони забезпечують високу якість обробки даних.

Список літератури

1. Шиллер Й. Мобільні комунікації : Пер. с англ. / Й. Шиллер. - М.: Издат. дом «Вильямс», 2002. – 384 с.
2. Зайченко Е.Ю. Оптимизация характеристик сетей с технологией АТМ / Е.Ю. Зайченко // Системні дослідження та інформаційні технології. – 2002. – №3.
3. Сокіл В.М. Мобільні мережі довільної структури – сучасні технології та застосування / В.М. Сокіл // Комп'ютерні науки та інженерія CSE2006 : Міжнародна наукова конференція студентів, аспірантів та молодих науковців тези доп. – Львів, 2006. – С. 72–75.
4. Zaychenko Y. The models and methods of surviveabilty analysis and structural synthesis of regional computer networks / Y. Zaychenko, H. Zaychenko // Information Networks and Systems : Intern. conference ICINAS-96, 1996 : Proceedings of Conference. St. Petersburg, 1996. – P. 112- 123.
5. Traffic contract. – Режим доступу : http://en.wikipedia.org/wiki/Traffic_contract

УДК 658.012.011.56:681.3.06

Кінах Я.І., Якименко І.З.

УДОСКОНАЛЕННЯ МЕРЕЖЕВИХ КРИПТОАНАЛІТИЧНИХ АЛГОРИТМІВ НА ЕЛІПТИЧНИХ КРИВИХ

В даній статті досліджено паралельну реалізацію r - Поларда метода та алгоритму Шуфа на основі використання телекомунікаційної мережі (ТМ). В результаті досліджень автори скористалися аналітичною моделлю ТМ, що дозволило проаналізувати продуктивність криптоаналітичних алгоритмів на еліптичній кривій.