УДК 004.7

О.П. Ігнатенко

КОНФЛІКТНА ЗАДАЧА ВЗАЄМОДІЇ ДВОХ ГРАВЦІВ У ВІДКРИТОМУ ІНФОРМАЦІЙНОМУ СЕРЕДОВИЩІ

При розробці систем керування мережами нерідко зустрічається ситуація, коли виникає необхідність урахування наслідків зловмисних дій, спрямованих на перешкоджання роботи. В цьому випадку методи побудови керування на основі потокових моделей (fluid models) та дискретних моделей випадкових блукань (controlled random walk models), які зазвичай використовуються, потребують певних змін. В роботі розглядається узагальнення звичайної моделі роботи окремого серверу (single server queue), яке дозволяє описати атакуючі дії та поведінку системи захисту. Проводиться формальна постановка і аналіз отриманої диференціальної гри. Знайдені умови при яких гра може бути закінчена за скінчений час.

Вступ

Інформаційні мережі, телекомунікаційні, газотранспортні або енергетичні системи, розподілені виробничі процеси і, навіть, системи ескалаторів у великих офісних спорудах – все це області застосування моделей мереж. Особливо важливими є інформаційні мережі. Сучасні мережі об'єднують незлічені масиви даних, які належать до практично всіх сторін людської діяльності. В результаті, захищеність і надійність потоків інформації напряму впливають на якість обслуговування, ефективність роботи і загалом на економічний розвиток цілих галузей виробництва. При цьому складність і взаємопов'язаність мереж постійно зростає.

На сьогодні все більше організацій залежать у своїй діяльності від роботи інформаційних мереж. З іншого боку, вразливість мереж також зростає з кожним роком. Це пов'язано, в основному, з тим, що з ростом мереж все більше потенційних нападників отримують доступ до ресурсів. Таким чином, урахування питань захисту від можливих атак, аналіз роботи при різних аномальних навантаженнях при проектуванні мереж стає нагальною необхідністю.

Стандартною процедурою стало імітаційне моделювання мережі на стадії проектування [1]. З появою стандартизованих засобів розробники отримали ефективний інструмент для аналізу майбутньої роботи складної мережі в різних обставинах, що дозволяє значно економити час і кошти. Серед великої кількості програм моделювання роботи мереж, що були створені нещодавно можна відзначити OPNET, Ns-2, NetworkSim, OMNet++ та ін.

В результаті моделювання можуть бути розв'язані такі задачі:

- дослідження часу затримки пакетів у чергах, виявлення вузьких місць, знаходження причин затримок;
- вплив різних моделей маршрутизації на роботу мережі;
- дослідження ефектів змін топології;
- зміни роботи при різних змінах середовища;
- реакція системи на здійснення атак на відмову та при аварійних розривах ланок мережі.

Зрозуміло, що побудова адекватної імітаційної моделі це непроста задача. Досить часто розробнику спочатку необхідно оцінити основні параметри роботи мережі та побудувати схеми маршрутизації і керування мережею. Потім – оцінити стабільність роботи отриманих алгоритмів, оскільки ідеалізована математична модель не може врахувати можливі шуми, недоліки конструкції та зміни у топології мережі. Нарешті слід побудувати імітаційну модель, яка б адекватно описувала результати, отримані при теоретичному моделюванні.

Складовою частиною такої моделі буде система протидії і виявлення атак [2]. При побудові такої системи перед розробником вже на першому етапі виникають фундаментальні проблеми, пов'язані з специфікою предметної області. Серед них можна виділити дві найбільш важливі на наш погляд:

• поява нових видів атак. Як показує практика останніх років, нові атаки виникають постійно. При цьому вони ускладнюються, інтелектуалізуються і стають більш небезпечними;

• зміна характеристик системи, що підлягає захисту, які не пов'язані з діяльністю зловмисників (розширення, реконфігурація та ін.). Як вищеописано, при побудові кожної системи захисту використовуються певні припущення про роботу системи. Якщо відбувається зміна роботи системи, то ці припущення можуть виявитися невірними.

Таким чином, при побудові системи захисту необхідно розв'язати наступні задачі [3].

1. Побудова профілю системи. Здійснюється аналіз роботи системи. Виділяються ключові параметри функціонування. Описуються характеристики нормальної і аномальної роботи.

2. Оцінка сценаріїв атаки. Будується модель взаємодії системи з користувачами. Описується зв'язок характеристик роботи і дій користувачів. Виділяються типові сценарії атаки.

3. Побудова системи виявлення і протидії. Вибираються конкретні алгоритми виявлення, які можуть бути ефективно застосовані для даної системи. Описується основні параметри та їх вплив на достовірність виявлення. Визначаються алгоритми протидії, що можуть бути застосовані.

4. Визначення поведінки агентів. Визначення алгоритмів роботи агентів: взаємодії, виявлення, протидії. Розробка механізмів оновлення і налаштування.

Існують різні підходи до створення систем виявлення. Перший з цих підходів використовує поняття аномальної поведінки, другий – особливостей поведінки, які ґрунтуються на профілі нормальної роботи. Обидва підходи тісно пов'язані з задачею моделювання поведінки мережевого трафіку. Метою моделювання є визначення поняття нормальної поведінки і, як наслідок, аномалій або особливостей у роботі системи. Побудова моделі включає у себе:

• дослідження роботи системи;

• виділення основних параметрів;

• оцінку меж нормальної поведінки для виділених параметрів.

Розглянемо загальну модель системи (рис. 1) [3]. Виділимо наступні частини системи: зовнішні користувачі, сама мережа і вузли мережі або хости. Природа процесів, які відбуваються в кожній з цих частин суттєво різна, тому і підходи до моделювання мають відрізнятися.

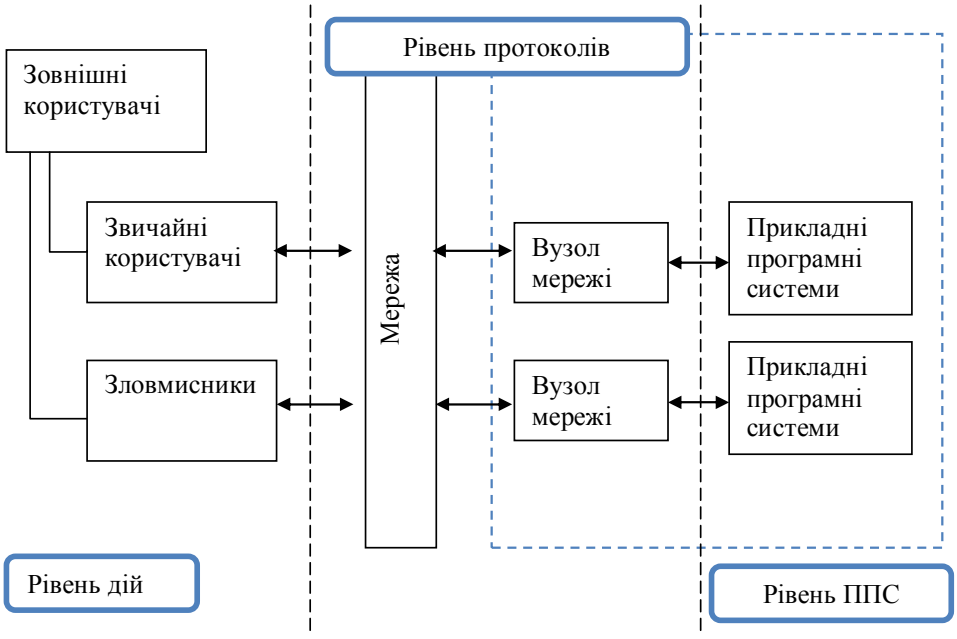

Рис. 1. Загальна модель системи

Зовнішні користувачі – це певні агенти, що мають доступ до системи або користуються її сервісами. Виділяють дві загальні групи: звичайні користувачі та зловмисники. Вплив зовнішніх користувачів на систему відбувається через мережу, але логіка їх поведінки описується певними мотивами та діями. Виділення певних груп користувачів, поведінка яких може бути узагальнена та змодельована є ключовим елементом для визначення поняття нормальної та аномальної поведінки користувачів. Звичайно, оскільки під користувачем ми розуміємо людину, поведінку якої ми не можемо не передбачити, тому побудова такої моделі є складною задачею. Однак, мета поведінки звичайних користувачів принципова відмінна від мети зловмисників, тому і дії їх будуть відрізнятися. Виконуючи декомпозицію намірів на окремі шаблони поведінки ми можемо оцінювати за послідовністю дій користувача його приналежність до одної з груп.

Модель вузла мережі необхідна для відстеження змін, які являються ознаками аномальної поведінки або вторгнення. Широко розповсюдженим підходом у літературі являється побудова моделі на базі характеристичних параметрів. Вибравши множину таких параметрів, які можуть прямо вимірюватися або розраховуватися на основі складних формул, можна побудувати модель. Відхилення від нормальних значень цих параметрів: перевищення порогів значень, швидкості росту, інтегральних обмежень означає появу аномалії. Відмінністю такого підходу є явне, аналітичне визначення моделі, її ясна і проста структура.

Інший підхід полягає у спостереженні системи протягом певного періоду часу, в результаті чого поведінка, що повторюється найбільш часто визначається як еталон. При подальшій роботі поточна поведінка системи порівнюється з еталоном. Як правило, при цьому використовуються неявні моделі – нейронні мережі, системи правил тощо. Однак, такий підхід може бути ефективним для систем, що виконують однотипні завдання в умовах чітко визначеної робочої області. Це накладає на тип систем певні обмеження, що не завжди прийнятно. Основним недоліком існуючих моделей є їх фрагментарність, націленість на окремі явища у роботі системи. З одного боку, це дозволяє отримати швидкі алгоритми для створення конкретних систем захисту, з іншого – відсутність єдиної загальної моделі не дозволяє охопити всю сутність процесів, що відбуваються у мережі.

У роботі пропонується застосовувати для моделювання досягнення теорії конфліктних динамічних систем. Такий підхід, який використовуватиме потужний апарат для опису поведінки керованих систем за умов невизначеності і конфлікту дозволить розробити аналітичну модель поведінки системи.

1. Математичні моделі керування мережами

З вищесказаного випливає, що на перший план виходять питання дослідження керованих систем. Однак мережа представляє собою складну нелінійну систему, зі значними невідомими збуреннями. Причому вплив на неї обмежений певними параметрами, на які ми можемо впливати тим чи іншим чином. З іншого боку для визначення керування використовуються скінченно-вимірні, лінійні, детерміністичні моделі. Чим простіша модель, тим легше її аналізувати, але надмірна ідеалізація зашкодить прикладній цінності розв’язку. Ідея, висловлена в [4], полягає у тому, що слід розглядати найпростішу модель, яка відображає сутність процесів, що відбуваються в реальній системі, тоді керування буде мати запас стійкості до різного роду невизначеностей.

Неможливо створити модель, яка б гранично точно описувала картину поведінки мережі. На практиці, ми завжди маємо справу з різними ідеалізованими припущеннями. Статистичні моделі, наприклад, майже завжди вважають, що розподіл довжин інтервалів часу між прибуттям двох пакетів описується незалежними і однаково розподіленими випадковими величинами. Також складно врахувати відмови і збої на машинному рівні, розриви з’єднань, невизначеність у частотах пакетів та ін. Вибір підходящої моделі

роботи мережі має визначатися її призначенням. Потокові моделі [5] погано підходять для довготермінового прогнозу роботи. Для точного прогнозу потрібна точна розгорнута модель. Але точна модель буде занадто складною для визначення керування. Тому загальний підхід полягатиме в наступному. Візьмемо у якості початкової точки детерміністичну потокову модель, яка описується звичайними диференціальними рівняннями. Знайшовши керування, яке розв'язує нашу задачу, необхідно узагальнити його на більш складний випадок (з урахуванням шумів, невизначеності), і завершити процес створенням імітаційної моделі з використанням відповідного середовища.

Таким чином, на першому кроці задача керування мережею може розглядатися у рамках класичної теорії. У даній роботі пропонується узагальнити моделі керування, описані в [4] на ігровий випадок. Дійсно, наявність у мережі різних учасників, що можуть впливати на загальну роботу, призводить до того, що їх взаємний вплив може породжувати конфлікти. В цьому випадку інший учасник або гравець своєю поведінкою буде заважати системі працювати. Ця ситуація може виникнути за різними причинами, яскравий приклад – атаки на відмову [3], коли роботу системи погіршують зі зловмисною метою. Іноді такі дії можна врахувати у якості випадкових збурень, але якщо вплив є значним і цілеспрямованим, така модель не буде адекватною. Тому моделювання систем керування мережами при наявності конфлікту є відкритою проблемою.

Опишемо основні постановки задач. Мережа буде вважатися скінченним набором терміналів, кожний з яких має певну кількість буферів. *Користувачі*, що очікують у такому буфері можуть представляти собою пакети, обсяги енергії або людей, що очікують на обслуговування. Один або декілька *серверів* обслуговують користувачів на даному терміналі , після чого користувач покидає мережу або іде на інший термінал. Користувачі прибувають до буферів терміналу ззовні мережі. Загальна стохастична модель може бути описана у наступному вигляді [4]. Нехай Q – вектор затримок у черзі, що приймає значення з R_+^N. Вектор керування розподілом ресурсів $Z \in R_+^{N_u}$. Компонента $Z_i(t)$ показує сумарний час, протягом якого працював i-ий сервер. Тоді зміна затримок описується рівнянням

$$Q(t) = Q(t_0) + B(Z(t)) + A(t),\ t \ge 0. \qquad (1)$$

Процес A – описує об'єднання зовнішнього прибуття користувачів та зовнішню потребу в матеріалах з мережі. Функція B представляє ефект від маршрутизації і роботи серверів. При цьому на процес (1) накладаються такі обмеження:

1) вектор затримок у черзі не може бути необмеженим, оскільки об'єм буферів обмежений:

$$Q(t) \in X,\ t \ge 0,\ X \subset R_+^N. \qquad (2)$$

2) процес розподілу керування обмежується наступним чином:

$$C(Z(t_1) - Z(t_0)) \le (t_1 - t_0) \cdot e,$$
$$Z(t_1) - Z(t_0) \ge 0,\ 0 \le t_0 \le t_1, \qquad (3)$$

де матриця C розмірністю $N_m \times N_u$, $e = (1,...,1)$ – вектор з простору R^{N_m}. Співвідношення (3) означає обмеженість ресурсів керування.

Стохастичні моделі типу (1) останнім часом стали найбільш популярними у теорії черг. Ідеалізацією моделі (1) є лінійна потокова модель, яка описується рівнянням

$$q(t) = q(t_0) + Bz(t) + \alpha(t - t_0),\ t \ge 0,\ x \in R_+^N, \qquad (4)$$

де стан системи q належіть фазовому простору $X \subset R_+^N$, вектор розподілу $z(t)$ належить простору $R_+^{N_u}$. Щодо вектора $z(t)$ вважається, що $z(0) = 0$, і для кожного $0 \le t_0 \le t_1$ виконується

$$C[z(t_1) - z(t_0)] \le (t_1 - t_0) \cdot e,$$
$$z(t_1) - z(t_0) \ge 0. \qquad (5)$$

Потокову модель можна також представити у вигляді диференціального рівняння

$$\frac{dq}{dt} = Bu + \alpha, \qquad (6)$$

де керування $u(t)$ – взагалі кажучи вимірна функція, на яку накладається обмеження $Cu \le e$, $u(t) \ge 0$. Система керування вибирає функцію $u(t)$ з метою зменшення значення $q(t)$ при виконанні певних умов (наприклад, за найкоротший час).

Розв'язок рівняння (6) знаходиться за наступною формулою:

$$q(t) = q(t_0) + \int_{t_0}^{t} Bu(\tau)d\tau + \alpha(t - t_0)$$

з урахуванням заміни $z(t) = \int_{t_0}^{t} u(\tau)d\tau$ співпадає з (4). При цьому, очевидно, виконуються обмеження (5). Оскільки моделі (6) і (1) описують один процес, то вони мають бути пов'язані одна з одною. Потокова модель (1) може розглядатись як усереднений потік стохастичної моделі:

$$Q(t) = Q(t_0) + A(t) + B(Z(t)) =$$
$$= Q(t_0) + BZ(t) + \alpha(t - t_0) + N(t),\ t \ge 0, \qquad (7)$$

де α і B є середніми значеннями випадкових величин A і B, і

$$N(t) = [A(t) - \alpha(t - t_0)] + [B(Z(t)) - BZ(t)].$$

Типові припущення моделі (7) полягають у тому [4], що процес $N(t)$ обмежений у часі і його дисперсія росте лінійно за відношенням до t. У цьому разі процес (1) можна вважати потоковою моделлю з додатковим адитивним збуренням $N(t)$. Приклад поведінки процесів (1) і (6) показані на рис. 2.

Керовані диференціальні рівняння (6) дозволяють розглядати процеси, що відбуваються у мережах з точки зору теорії оптимального керування. Однак на практиці нерідко виникає ситуація, коли в системі присутні фактори, що погіршують роботу, тобто збільшують значення $q(t)$. Ці фактори можуть мати різну природу (технічні поломки, недоліки топології, нападники, що організовують атаку на відмову), однак їх спільною характеристикою є конфліктна націленість за відношенням до першого гравця.

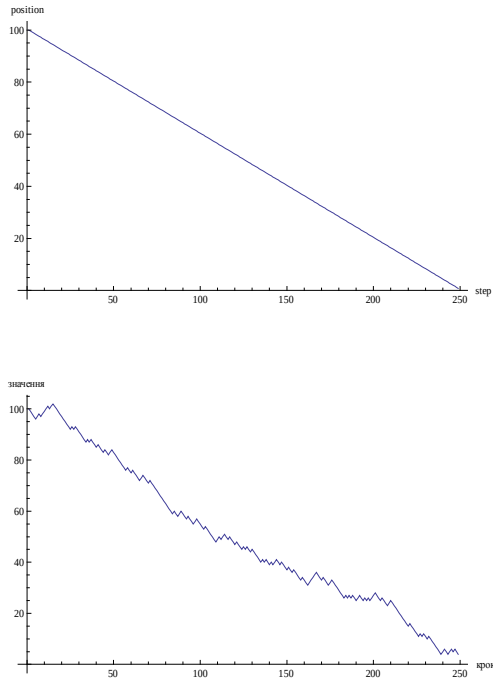

Рис. 2. Стохастична та потокова моделі

Для опису такого роду систем, буде використовуватися теорія конфліктно-керованих процесів [6]. Розглянемо динамічну систему, поведінка якої описується лінійним диференціальним рівнянням:

$$\frac{dq(t)}{dt} = Aq(t) + Bu(t) - Cv(t) + \alpha(t), \qquad (8)$$

де фазовий вектор $q(t) \in R_+^n$, керування гравців – вимірні функції які приймають значення з компактних множин U і V відповідно: $u(t) \in U \subset R^m$, $v(t) \in V \subset R^l$. Векторна функція $\alpha(\cdot): R \to R^n$ описує потік користувачів у момент часу t і вважається невідомою обом гравцям і обмеженою у часі величиною $\alpha_{\max}$. A, B, C – дійсні матриці розмірністю $n \times n$, $n \times m$ і $n \times l$, відповідно. Умовою закінчення гри будемо вважати виконання рівності

$q(t)=0$. Гра відбувається наступним чином: у кожний момент часу $t\ge 0$ гравці обирають свої керування $v(t)$ і $u(t)$, причому перший гравець прагне збільшити черги в мережі, а другий якомога швидше звести їх до нуля. Якщо $\alpha(t)\equiv 0$, тоді рівняння перетворюється на звичайний конфліктно-керовний процес [6]

$$\frac{dq(t)}{dt}=Aq(t)+Bu(t)-Cv(t). \qquad (8')$$

Задачі конфлікту двох учасників започаткували створення теорії диференціальних ігор. Дослідженню процесів типу (8′) присвячені численні роботи починаючи з Р. Айзекса, Л.С. Понтрягіна та М.М. Красовського. В даній роботі буде використовуватися ідея першого прямого методу Л.С. Понтрягіна [7, 8], який був розроблений у 1965 р. Особливість цього методу полягає у тому, що він вимагає суттєвої переваги одного гравця над іншим та фактично зводить гру до задачі оптимального керування.

2. Лінійна ігрова модель окремого сервера

Модель окремого сервера (single server queue) – одна з базових моделей у теорії черг. Ця модель відображає поведінку широкого класу прикладних систем. У даному розділі досліджується узагальнення класичної потокової моделі на випадок конфліктного процесу. Розглянемо динамічну систему (рис. 3), поведінка якої описується наступним чином:

$$\dot q_1(t)=\alpha(t)+k\cdot q_2(t)-u_1(t),$$
$$\dot q_2(t)=v(t)-u_2(t),\ t\ge 0. \qquad (9)$$

Фазовий стан системи описується вектором $q(t)=(q_1(t),q_2(t))\in R^2$, де $q_1(t)$ – довжина черги в момент часу t, $q_2(t)$ – потужність атаки. При цьому слід урахувати фізичну природу процесів – довжина черги і потужність атаки не можуть бути від'ємними, а довжина черги не може також перевищувати об'єм буфера. Тобто мають місце фазові обмеження

$0\le q_1(t)\le q_1^{\max}$, $0\le q_2(t)$ для всіх $t\ge 0$.

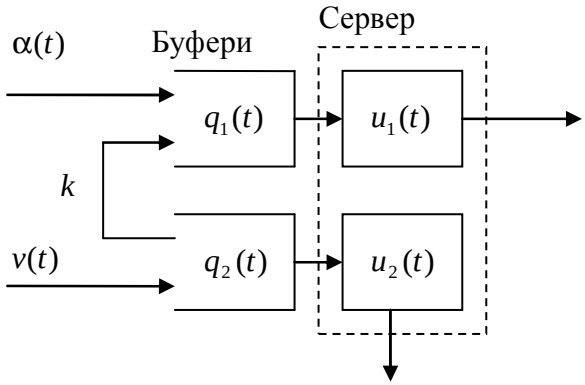

Рис. 3. Модель окремого сервера з протидією

Потужність атаки впливає на загальну чергу лінійно з коефіцієнтом $k\ge 0$. Гравець, якого будемо називати нападником, має у своєму розпорядженні керування $v(t)$, $v(t)\ge 0$, $v(t)\le \nu$ за допомогою якого він може посилювати початкову потужність атаки $q_2(0)$. Початкова умова $q(0)=(q_1(0),q_2(0))$. Інший гравець – захисник, розподіляє свої ресурси керування за двома напрямками $u_1(t)$ – для обробки поточних запитів користувачів і пакетів атаки (будемо вважати що вони завантажують мережу однотипними пакетами) та $u_2(t)$ – для виявлення і відсічення джерел атаки.

На керування захисника накладається природне обмеження $u_1(t)\ge 0$, $u_2(t)\ge 0$, $u_1(t)+u_2(t)\le \mu$. При цьому вважається, що захисник у момент часу t володіє інформацією про $\alpha(t)$, $v(t)$ і $q(t)$.

Функція $\alpha(\cdot):R\to R^n$, яка описує потік користувачів у момент часу t, вважається додатною і обмеженою числом $\alpha_{\max}$. Задача полягає у знаходженні умов які б гарантували приведення вектора $q(t)$ в точку $(0,0)$ зі стану q_0 при будь-яких протидіях суперника не пізніше ніж за час $T(q_0)<\infty$.

Якщо $q_2(0)=0$ і $v(t)\equiv 0$, $\alpha(t)\equiv\alpha_{\max}$, то система (9) зводиться до відомої задачі керування [4], яка має розв'язок при виконанні умови $\mu>\alpha_{\max}$. Оптимальне (у сенсі задачі швидкодії)

керування задається формулою $u(t)=(u_1(t),0)$, де

$$u_1(t)=\begin{cases}\mu, & q_1(t)>0\\ 0, & q_1(t)=0\end{cases}.$$

Час вичерпання черги дорівнює $\dfrac{q_1(0)}{\mu-\alpha_{\max}}$.

Для дослідження задачі (9) методами теорії диференціальних ігор приведемо її до загального вигляду. Позначимо $A=\begin{pmatrix}0 & k\\ 0 & 0\end{pmatrix}$, тоді

$$\dot q(t)=Aq(t)+\begin{pmatrix}\alpha(t)\\ \nu(t)\end{pmatrix}-\begin{pmatrix}u_1(t)\\ u_2(t)\end{pmatrix}. \quad (10)$$

Множини керування мають вигляд

$$U=\{u\in R_+^2: u_1+u_2\le\mu\},$$
$$V=\{v\in R_+^2: v_1\le\alpha_{\max}, v_2\le\nu\}.$$

Термінальна множина $M=\{(0,0)\}$. Застосуємо для розв'язання задачі (10) ідею першого прямого методу Л.С. Понтрягіна [7, 8]. Введемо відображення Понтрягіна $\omega(t)=\bigcap\limits_{v\in V}\left(e^{At}U-e^{At}v\right)$, та обчислимо його:

$$\bigcap_{v\in V}(U-v)=\{x\in R^2: x_1+x_2\le\mu-v-\alpha_{\max}\}=$$
$$=co\{(0,0),(\mu-v-\alpha_{\max},0),(0,\mu-v-\alpha_{\max})\}.$$

Оскільки e^{At} – лінійний оператор, то

$$\bigcap_{v\in V}\left(e^{At}U-e^{At}v\right)=e^{At}\bigcap_{v\in V}(U-v),$$
$$\omega(t)=co\{(0,0),(R,0),(kt(R),R)\},$$

де $R=\mu-\nu-\alpha_{\max}$.

Умова 1. Відображення $\omega(t)\ne\varnothing$ для всіх $t\ge0$.

Умова 1 виконується для всіх $t\ge0$, якщо $\mu>\nu+\alpha_{\max}$.

Як показано в роботі Нікольского [7] (для гри (10) без фазових обмежень) якщо виконується умова 1 та існує час $T\ge0$, такий, що вірне включення $e^{AT}q_0\in\int\limits_0^T\omega(\tau)d\tau$ і виконується умова 1, то існує стратегія переслідування (захисту в термінах задачі про моделювання мережі), яка гарантує закінчення гри за час T при будь-яких протидіях суперника. Покажемо, що для задачі (10), при виконанні певних умов, можна конструктивно побудувати стратегію, яка гарантує закінчення гри не пізніше моменту часу $T(q(0))$.

Умова 2. Для початкової умови $(q_1(0),q_2(0))$ виконується співвідношення

$$q_1^{\max}-q_1(0)\ge\frac{k}{2(\mu-\nu-\alpha_{\max})}(q_2(0))^2.$$

Теорема. Нехай для системи (10) виконуються умови 1, 2. Тоді існує стратегія $u(t)$, яка гарантує закінчення гри не пізніше моменту часу $T(q(0))$.

Доведення. Побудуємо стратегію, яка забезпечує приведення траєкторії процесу (10) в нуль. Будемо вважати, що $q(0)\ne(0,0)$. Визначимо моменти часу

$$T_1=\min\{t>0: q_1(t)=0\},$$
$$T_2=\min\{t\ge0: q_2(t)=0\}, \text{ тоді}$$

$$u(t)=\begin{cases}(\alpha(t),\mu-\alpha(t)), & t\in[0,T_2],\\ (\mu-v(t),v(t)), & t\in[T_2,T_1].\end{cases} \quad (11)$$

Покажемо, що стратегія $u(t)$, допустима. Дійсно, $u(t)$ визначена для всіх $t\ge0$ і на проміжку часу $[0,T_1]$ виконується $u_1(t)+u_2(t)=\mu$. При цьому $u_1(t)\ge0$, $u_2(t)\ge0$ для всіх $t\ge0$, оскільки виконується умова 1. Підставимо керування (11) в систему (10).

Для $t\in[0,T_2]$

$$\dot q_1(t)=k\cdot q_2(t),$$
$$\dot q_2(t)=v(t)+\alpha(t)-\mu.$$

Для $t\in[T_2,T_1]$

$$\dot q_1(t)=v(t)+\alpha(t)-\mu,$$
$$\dot q_2(t)=0.$$

Нехай $\varepsilon=\mu-\alpha_{\max}-\nu>0$, тоді

$$\dot q_2(t)\le-\varepsilon,$$
$$q_2(t)\le q_2(0)-\varepsilon t.$$

Отже не пізніше за час $T_2^* = \frac{q_2(0)}{\varepsilon}$ виконується $q_2(t) = 0$. Або, інакше $T_2 \le T_2^*$. При цьому виконуються наступні співвідношення:

$$q_1(t) = q_1(0) + \int_0^t k q_2(\tau) d\tau,$$

$$q_1(0) + k q_2(0) t - \int_0^t k(v(\tau) + \alpha(\tau) - \mu) d\tau,$$

$$q_1(t) \le q_1(0) + k q_2(0) t - k\varepsilon \frac{t^2}{2},$$

$$q_1(T_2) \le q_1(0) + k \frac{(q_2(0))^2}{\varepsilon} - k\varepsilon \frac{1}{2}\left(\frac{q_2(0)}{\varepsilon}\right)^2,$$

$$q_1(T_2) \le q_1(0) + \frac{k}{2} \frac{(q_2(0))^2}{\varepsilon},$$

$$q_1(T_2) \le q_1^{\max}.$$

Остання нерівність випливає з умови 2. В момент часу T_2 відбувається переключення керування. Оскільки $q_2(t) = 0$, $t \ge T_2$, то розглядаємо далі тільки $q_1(t)$

$$q_1(t) = q_1(T_2) - \int_{T_2}^t (v(\tau) + \alpha(\tau) - \mu) d\tau,$$

$$q_1(t) \le q_1(T_2) - \varepsilon(t - T_2),$$

$$t \le \frac{q_1(T_2) + \varepsilon T_2}{\varepsilon}.$$

Таким чином, має місце наступна оцінка для T_1

$$T_1 \le \frac{q_1(0)}{\varepsilon} + \frac{k}{2}\left(\frac{q_2(0)}{\varepsilon}\right)^2 + T_2 \le$$

$$\le \frac{q_1(0)}{\varepsilon} + \frac{q_2(0)}{\varepsilon} + \frac{k}{2}\left(\frac{q_2(0)}{\varepsilon}\right)^2.$$

Отже, не пізніше як у момент часу T_1 гру буде завершено при будь-яких діях суперника $v(t)$. Теорема доведена.

3. Чисельне моделювання

Проілюструємо результати теореми на прикладі. Розглянемо модель

$$\dot{q}_1(t) = \alpha + q_2(t) - u_1(t),$$
$$\dot{q}_2(t) = v - u_2(t),\ t \ge 0.$$

На рис. 4 показана динаміка фазових змінних $q_1(t)$, $q_2(t)$. У початковий момент часу $q_1(t) > 0$, $q_2(t) > 0$, тобто система завантажена чергою $q_1(t)$ і відбувається атака з потужністю $q_2(t)$. За відсутності керування відбувається експоненціальний ріст значення $q_1(t)$ (рис. 4).

Застосування керування

$$u(t) = \begin{cases} (\alpha, \mu - \alpha), & t \in [0, T_2], \\ (\mu - v, v), & t \in [T_2, T_1]. \end{cases}$$

забезпечує приведення системи в точку (0,0) не пізніше за момент часу T_1 (рис. 5). На часовому інтервалі $[0, T_2]$ відбувається

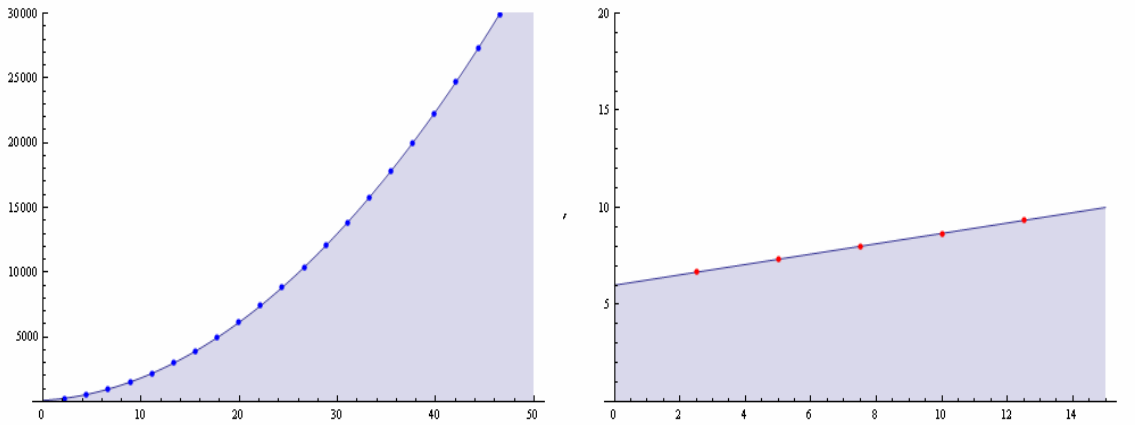

Рис. 4. Потокова модель за відсутності керування

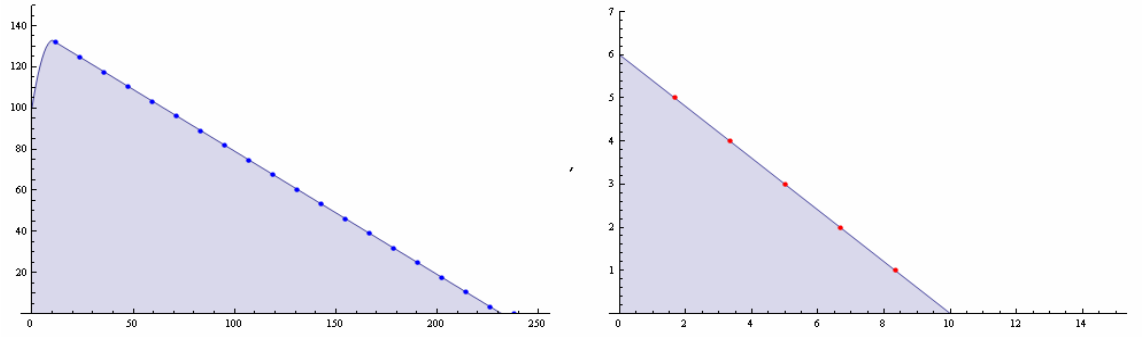

Рис. 5. Керована потокова модель

розподілення ресурсів захисника – стримування зростання $q_1(t)$ на величину α та максимально швидке зменшення $q_2(t)$.

При цьому за рахунок початкового значення $q_2(0)$ початкове значення черги зросте на величину $\frac{k}{2}\frac{(q_2(0))^2}{(\mu-\nu-\alpha_{\max})}$.

На інтервалі $[T_2, T_1]$ захисник стримує нападника не дозволяючи йому збільшувати потужність атаки і, користуючись своєю перевагою у ресурсах, зменшує чергу.

Висновки

У роботі досліджувалась модель окремого сервера з протидією. За основу взято звичайну потокову модель, та узагальнено її для врахування атакуючих дій. Описана поведінки нападника і захисника у термінах диференціальної гри. Проведена формальна постановка й аналіз отриманої гри. Знайдені умови на можливості гравців і початковий стан системи, при яких гра може бути закінчена за скінчений час. Проведене чисельне моделювання отриманої стратегії поведінки.

1. *Chlamtac I., Jain R.* Methodology for Building a Simulation Model for Efficient Design and Performance Analysis of Local Area Networks // Simulation, February 1984. – Vol. 42, N. 2. – P. 57 – 66.
2. *Андон П.І, Ігнатенко О.П.* Протидія атакам на відмову в мережі Інтернет: концепція підходу // Проблеми програмування. – 2008. – № 2-3. – С. 564 – 574.
3. *Андон П.І., Ігнатенко О.П.* Атаки на відмову в мережі Інтернет: опис проблеми та підходів щодо її вирішення. – Київ, 2008. – 50 с. – Препринт / НАН України. Ін-т програмних систем.
4. *Meyn S.* Control Techniques for Complex Networks. – Cambridge University Press, 2007. – 582 p.
5. *Bertsekas D.* Network optimization: continuous and discrete models. – Athena Scientific, Belmond, 1998. – 270 p.
6. *Чикрий А.А.* Конфликтно управляемые процессы. – Киев: Наук. думка, 1992. – 384 с.
7. *Никольский М.С.* Первый прямой метод Л.С. Понтрягина в дифференциальных играх. – М.: Изд-во МГУ, 1984. – 65 с.
8. *Понтрягин Л.С.* Избранные научные труды. – М.: Наука, 1988. – **2**. – 576 с.

Отримано 06.03.2009

Про автора:

Ігнатенко Олексій Петрович,
кандидат фізико-математичних наук,
старший науковий співробітник,
докторант.

Місце роботи автора:

Інститут програмних систем НАН України, 03187, Київ 187,
Проспект академіка Глушкова, 40,
Тел.: 526 6025,
e-mail: o.ignatenko@gmail.com