Псевдосервіси та теорія конфлікту в стохастичному управлінні інформаційними мережами

Галина Даниліна[1], Наталя Андрусевич[2]

1. Кафедра КСМ, Криворізький коледж Національного авіаційного університету,
Кривий Ріг, вул.Туполєва, 1, УКРАЇНА, e-mail: znk-ur@kk.nau.edu.ua
2. Циклова комісія ПОДПЗ, Криворізький коледж Національного авіаційного університету,
Кривий Ріг, вул.Туполєва, 1, УКРАЇНА, e-mail: dekanat@kk.nau.edu.ua

Анотація: Розроблена математична модель і методика захисту комп'ютерної мережі від атак і вторгнень. Зроблено припущення про апріорну невизначеність стану мережі і ризик виникнення конфлікту з активним (розумним) супротивником. Розроблено стохастичну модель конфлікту з ескалацією супротивника у псевдосервіси з використанням псевдосервісної мережі Honeynet.

Ключові слова: захист інформації, теорія конфлікту, псевдосервіси, процес розвитку конфлікту, керований марківський процес, стохастичне управління.

I. ВСТУП

Аналіз, адаптація та оптимізація методів захисту комп'ютерних мереж від атак і несанкціонованих вторгнень залишається актуальною темою. Використання математичного апарату статистичної теорії ризику, теорії конфлікту, теорії масового обслуговування, дослідження операцій в задачах побудови систем захисту займає достатньо скромне місце. Намітити реальні шляхи постановки та розв'язання згаданих проблем – мета даної роботи.

II. ПОСТАНОВКА ПРОБЛЕМИ

Організація безпеки даних – це як систематизація, виявлення і відображення загроз, так і управління ризиками, своєчасні превентивні заходи для зниження ризику загроз, щоденна робота по системному забезпеченню безпеки. У теперішній час недостатньо просто виявляти і реагувати на дії порушників, треба ще й прогнозувати їхні дії.

Найбільший інтерес привернув метод так званої "медової пастки" (*Honeypot*) – заманювання на хибні інформаційні об'єкти, що демонструють високу вразливість.

В роботі [1] такі медові пастки названі псевдосервісами, в роботах [2 – 5] – облудними, хибними інформаційними системами або мережами-пастками. Цілі колективи працювали над різноманітними проектами медових пасток [6,7]. Однак в результаті пошуку і аналізу численних літературних джерел нами були виявлені лише дві статті, що заслуговують на увагу [2,3]. Зокрема, в роботі [3] глибоко і всебічно опрацьований теоретичний підхід до оцінювання ефективності мережних медових пасток (за термінологією роботи – хибних інформаційних систем).

У цей час все більшого розвитку набувають мережні атаки, яскравим прикладом яких є розподілені атаки типу "відмова в обслуговуванні"(так звані *DDOS*-атаки).

Для швидкого виявлення широко розповсюджених комп'ютерних хробаків розгортається у випадкових місцях ряд систем, які очікують появи зловмисної активності. Якщо кілька систем виявляють подібні дії, дуже ймовірно, що це буде широко розповсюджена атака. Чим більше систем розміщено, тим швидше буде виявлено напад, але своєчасність не є лінійною щодо кількості систем. Швидше за все, ймовірність зростає з кількістю обманів, розміщених пропорційно розміру загального простору, тоді як час на виявлення - це функція від ймовірності зустріти одну або декілька систем обману як функцію, що стосується поширення хробака.

Логічним розвитком методів активної протидії мережним атакам з використанням медових пасток є перехід від однієї *Honeypot* або сукупності автономних *Honeypot* до мережі *Honeypot*, яку називають *Honeynet* [6].

Ці сподівання на проект медоносної мережі та пропозиції внесені до DARPA та інших агентств щодо масштабних масивів виявлення на основі обману для швидкого виявлення великомасштабних хробаків.

Розробка архітектури, топології, протоколів *Honeynet* тощо ведеться у рамках відповідного *Honeynet*-проекту [7]. Однак у рамках цього проекту вивченню розвитку конфлікту між сторонами атаки та захисту приділяється значно менше уваги. Тому це завдання представляється вельми нагальним.

III. МЕТА ТА ЗАВДАННЯ ПРОБЛЕМИ

Мета даної роботи – розробити метод управління процесом розподіленого захисту інформаційної системи від розподілених атак з використанням мережі *Honeynet*. Математичною основою цього завдання залишаються теорії

конфлікту [8] і керованих марковських процесів [9].

Основні завдання:

– ідентифікація вторгнення, оцінювання характеристик атаки;

– аналіз можливих стратегій конфлікту й вибір найбільш перспективних стратегій контратак для конкретної задачі;

– розробка методів модифікації стратегії при зміні стану сторін;

– вибір математичного апарату для опису процесів розвитку конфлікту;

– розробка математичної моделі конфлікту;

– отримання асимптотичних характеристик ефективності.

IV. РОЗРОБКА МОДЕЛІ КОНФЛІКТУ

Для комп'ютерних мереж та цифрових інформаційних систем характерні дискретні процеси розвитку конфлікту між сторонами атаки та контратаки, що характерні.

Дискретний випадковий процес конфліктного керування являє собою сукупність, що складається з трьох абстрактних об'єктів:

$$K = \left[S_t, M_{ch}, \Psi\left(S_t, M_{ch}\right) \right], \qquad (1)$$

де S_t – підмножина ресурсів контратаки, M_{ch} – множина стратегій контратаки з результатом res_{ch}, $\Psi(S_t, M_{ch})$: $S_t \rightarrow M_{ch}$ – відображення підмножини стратегій S_t в множині M_{ch}. При повній інформації чи наявності достатньої статистики процесу *j*-му ресурсу S_{tj} відповідає стратегія контратаки M_{chj} з результатом res_{chj}.

Для дискретних систем з запізненням, до яких відносяться комп'ютерні мережі та розподілені інформаційні системи, справедливо припущення, що процеси протиборства між сторонами атаки та контратаки описуються диференційно-різницевими рівняннями або рівняннями з аргументами, що відхиляються [10,11].

У загальному випадку

$$\begin{cases} z'_{ids}(t) = f_1\left(t, z_{ids}(t), \ldots, z_{ids}(t-\tau_1), u_1(t), v_2(t-\tau_2), \xi(t)\right); \\ z'_{icm}(t) = f_2\left(t, z_{icm}(t), \ldots, z_{icm}(t-\tau_2), u_2(t-\tau_2), v_1(t), \eta(t)\right), \end{cases} \qquad (2)$$

де

Z_{ids} та Z_{icm} – вектори стану систем S_{ids} та S_{icm} відповідно;

$u_1(t)$ та $u_2(t)$ – вектори управлінь в S_{ids} та S_{icm} відповідно;

$v_1(t)$ – вектор дій в S_{ids} на S_{icm};

$v_2(t)$ – вектор дій в S_{icm} на S_{ids};

$\xi(t)$ та $\eta(t)$ – вектори випадкових збурень, які діють на S_{ids} та S_{icm} відповідно;

τ_1 та τ_2 – запізнення у векторах S_{ids} та S_{icm} відповідно.

Ефективність E_1 системи S_{ids} й ефективність E_2 системи S_{icm} на інтервалі спостереження T у загальному випадку являють собою нелінійні функціонали станів Z_{ids}, Z_{icm} та векторів $\xi(t)$ та $\eta(t)$ відповідно. З рівняння (1) випливає їх взаємна залежність.

Якщо врахувати фактор нормалізації випадкових процесів у великих системах [9], то можна застосувати для вирішення рівнянь (1) метод гаусовської апроксимації в малій околиці точок екстремуму E_1 і E_2. У цьому разі вирази для ефективностей мають вигляд

$$E_1 = \int_0^T z_{ids}(t)\,dt, \quad E_1 \rightarrow \max_{v_1}, \qquad E_2 = \int_0^T z_{icm}(t)\,dt, \quad E_2 \rightarrow \max_{v_2} \qquad (3)$$

Мета кожної системи при рішенні конфлікту - максимально підвищити свою ефективність за рахунок зниження ефективності супротивної сторони. Однак результат докладених зусиль стане відомий тільки в момент часу t. На інтервалі спостереження $0 \le t \le T$ можна виробляти найкращі управління $u_1(t)$, дії $v_1(t)$ та прогнозувати кінцевий результат, тільки спираючись на припущення про стратегії поведінки супротивника й дані про поточні стани Z_{ids} та Z_{icm}. Включення в рівняння (1) функцій $v_1(t)$ означає відволікання частини ресурсу на формування захисних впливів або контратак. Задачу конфлікту необхідно вирішувати або з додатковим критерієм мінімізації частки ресурсу, що відводиться на захист, або з обмеженням на допустимі витрати цієї частки ресурсу.

Схема моделі конфлікту [1] між сторонами атаки S_{icm} та захисту S_{ids}, модифікована для випадку застосування стратегій ескалації в псевдосервіси (пастки, хибні інформаційні системи), наведена у роботі [12]. Модель реального конфлікту, як правило, є нелінійною, але для отримання асимптотичних оцінок при досить великому інтервалі спостереження (і, відповідно, при великому числі кроків розвитку конфлікту) є припустимим робити покрокову стохастичну лінеаризацію моделі з екстраполяцією на основі методів кореляції та регресії [13]. Для пошуку коефіцієнтів екстраполяції лінеаризованої моделі розроблено модифіковану покрокову процедуру з заміною та примусовим включенням незалежних змінних. При цьому усунення з вибірки незалежних змінних $X_1, X_2, \ldots, X_p$ (активні ресурси та псевдосервіси) відсутнього значення X_i, $1 \le t \le p$ не є необхідним, оскільки воно може приводити до втрати про змінні $X_1, X_2, \ldots, X_i, \ldots X_p$ інформації, яка доставляється елементом X_i. Теоретично можна залишити цей елемент у вибірці та використати виміри, що містяться в ньому, для обчислення вектора середніх значень $\bar{\mathbf{X}}$ та матриці коваріацій R_x.

У реальній ситуації для отримання цих даних приходиться використовувати наближені методи:

– видалення елементів, лишаючи тільки комплектні елементи, тобто елементи з повністю присутніми значеннями;

– підстановку середнього: замість відсутнього значення X_i підставляється середнє значення $\bar{x}_i$,

завдяки чому результуюча вибірка комплектується до повного об’єму n;

– попарного викреслювання, підстановки регресії тощо.

На жаль, для будь-якого зі згаданих методів їх статистичні властивості частіше за все невідомі, тому немає гарантій, що отримані оцінки будуть незміщеними. Якщо елемент містить багато пропусків, його треба усунути. Якщо значення будь-якої змінної невідомо для більшості елементів, цю змінну треба видалити. Тоді можна застосовувати стандартні методи множинного регресійного аналізу [13].

На рис. 1 зображено мережну модель процесів розвитку конфлікту з передбаченням та виправленням помилкових припущень [8].

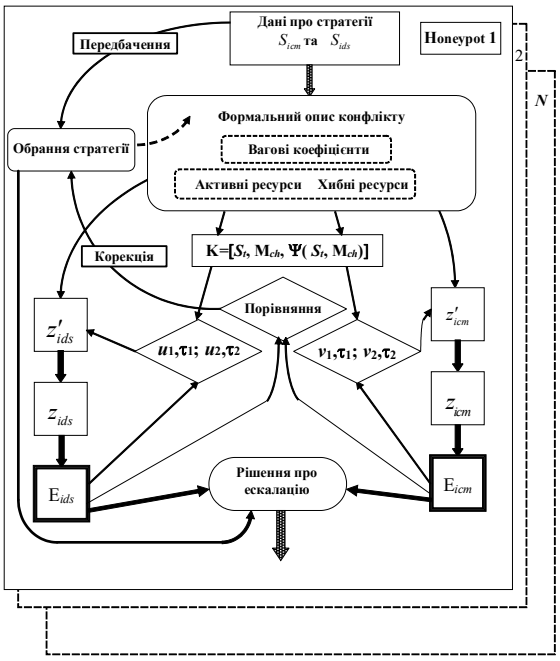

Рис. 1 Схема стохастичної мережної моделі конфлікту з можливою ескалацією в псевдосервіси

Стратегії протидії та атак, розроблені відповідно до класичної теорії конфлікту [8] і модифіковані для конкретної розглянутої задачі, наведені в роботі [12]. Тут же розглянемо набір найбільш наочних стратегій захисту:

– ешелонування рубежів захисту типу "зовнішня – демілітаризована – внутрішня зони безпеки";

– відмова від отримання – просте повернення підозрілого трафіку;

– розподілена відмова від отримання – трансляція підозрілого трафіку на кілька точок і повернення трафіку з усіх цих точок;

– насичення рубежів захисту псевдосервісами з відтворенням добре відомих вразливостей – затягування противника в ескалаційну пастку – один з елементів мережі *Honeynet*.

В системі захисту, заснованої на теорії конфлікту, передбачаються активні дії по відбиттю атаки. Тут розглядаються теоретичні моделі і методи аналізу, прогнозу розвитку конфлікту і оптимізації послідовностей захисних дій. Щодо правових аспектів адекватності заходів контратаки передбачається лише, що оцінка цієї адекватності в технічних системах може бути зроблена досить точно і об'єктивно.

Розглянемо алгоритмічну модель конфлікту між розподіленими системами атаки і захисту. Схема процесу моделювання атакуючих і контратакуючих потоків зображена на рис. 2.

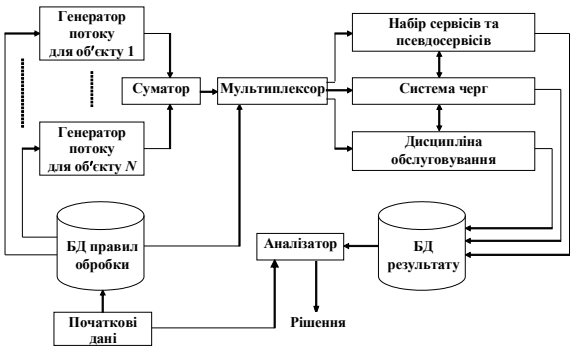

Рис. 2. Алгоритмічна модель

Як видно з рис. 2, рішення про вибір напрямку розвитку конфлікту приймаються на підставі результатів повного аналізу параметрів і стану системи, наявних вихідних даних і поточної інформації про характеристики мережного трафіку.

Припустимо, що в результаті атаки ймовірність штатного функціонування об'єкта знижується, можливо, до нуля, а в результаті застосування відповідної захисного заходу ймовірність функціонування об'єкта підвищується, можливо, аж до вихідної величини. Процес розвитку конфлікту є розгалуженим напівмарківським процесом, перехідні і фінальні ймовірності якого залежать від співвідношення стратегічних (S_{ids},S_{icm}) й енергоінформаційних (E_{ids},E_{icm}) ресурсів сторін.

Напівмарківський процес [8] – це марківський процес з випадковими інтервалами між переходами. При входженні процесу у певний стан, обираються наступний стан і тривалість затримки відповідно до імовірностей переходів і функцій щільності розподілу тривалості затримок. Після затримки в стані і на час τ_{ij}, процес переходить в стан j, а потім процедура повторюється.

V. ВИСНОВКИ

Стратегія відволікання ресурсів противника на мережні псевдосервіси дозволяє залишати ресурс захисту достатнім, що дає виграш навіть коли ресурси атаки мають перевагу над ресурсами захисту.

Тема використання розгалужених ескалаційних пасток з імітацією активної боротьби з супротивником шляхом управління еволюцією вразливостей псевдосервісів (медових пасток), тобто заманюванням супротивника на хибні сервіси зі змінними вразливостями, залишається актуальною і буде розширена в наступній роботі.

ПЕРЕЛІК ПОСИЛАНЬ

[1] Виноградов Н. А. Управление псевдосервисами в защищенных информационных системах на основе теории конфликта // Н. А. Виноградов, Г. В. Данилина, Д. В. Домарев, Я. В. Милокум – Наукові записки Українського науково-дослідного інституту зв'язку. – 2014. – №6(34). – с. 5 - 12.

[2] Котенко И. В., Степашкин М. В. Обманные системы для защиты информационных ресурсов в компьютерных сетях // Труды СПИИРАН, Вып. 2, т. 1. – СПб.: СПИИРАН, 2004. с. 211 – 230.

[3] Язов Ю. К., Сердечный А. Л., Шаров И. А. Методический подход к оцениванию эффективности ложных информационных систем // Вопросы кибербезопасности №1(2), 2014. – с. 55 – 60.

[4] Шматова Е.С. Выбор стратегии ложной информационной системы на основе модели теории игр. // Вопросы кибербезопасности №5(13) – 2015 с. 36 –40.

[5] Максин И.С. Распределенная динамическая Honeynet (сеть-ловушка) на основе скрытой модели Маркова //И.С. Максин, В.А. Малышев. – Параллельные вычисления и задачи управления (PACO 2012), шестая международная конференция, М.: ИПУ РАН, 2012. – с. 162 – 168.

[6] Spitzner L. Honeynets and Digital Forensics // The Digital Forensic Research Conference DFRWS 2004 USA Baltimore, MD (Aug 11th – 13th). – 25 pp.

[7] www.honeynet.org

[8] Дружинин В.В., Конторов Д.С., Конторов М.Д. Введение в теорию конфликта. – М.: Радио и связь, 1989. – 288 с.

[9] Дынкин Е.Б., Юшкевич А.А. Управляемые марковские процессы и их приложения. – М.: Наука, 1975. – 338 с.

[10] Bellman R. Differential-Difference Equations. / R. Bellman, K.L. Cooke. – Academic Press, 1963. – 482 p.

[11] Pinney E. Ordinary Difference-Differential Equations. – University of California Press, 1958. – 262 p.

[12] Даниліна Г.В. Віноградов М.А., Савченко А.С. Процеси конфліктного управління мережним комутаційним вузлом з функцією фільтрації шкідливого трафіку. Науково-технічна конференція молодих учених «Актуальні проблеми інформаційних технологій», Київ 2018, 20-21.11.2018. Матеріали доповідей, с.11-12.

[13] Afifi A. Statistical Analysis, Second Edition: A Computer Oriented Approach 2nd Edition / A. A. Afifi, S. P. Azen. – Academic Press; 2 edition, 1979. – 442 pp.

Управління автоматизованою системою керування освітленням NURE Energy з використанням мікросервісів

Сергій Новоселов, Юрій Олександров, Оксана Сичова, Сергій Теслюк

Кафедра Комп'ютерно-інтегрованих технологій автоматизації та мехатроніки, Харківський національний університет радіоелектроніки, Україна, Харків, проспект Науки 14, nsoft72@gmail.com

Реферат: В даній статті описується метод керування освітленням за допомогою автоматизованої системи управління NURE-Energy. В якості ядра системи використовуються мікросервіси. Програма управління автоматизованою системою здійснює облік, контроль, відображення інформації у вигляді діаграм, функції обміну і передачі інформації за допомогою Web технологій. Використання IoT Cloud дозволяє обробляти велику кількість даних, що надходить від багатьох датчиків, які розповсюджені на об'єкті керування. В якості системи керування та зберігання даних використовуються Elasticsearch.

Ключові слова: автоматизована система керування освітленням, NureEnergy, мікросервіси, Elasticsearch, IoT Cloud.

I. ВСТУП

Впровадження автоматизованих систем керування освітленням сприяє вирішенню актуальної проблеми енергозбереження при збереженні якості освітлення.

На даний момент є безліч організацій з відсутньою системою контролю і обліку