DOI 10.31891/2307-5732-2024-345-6-26
УДК 004.75:004.49:004.5

КАШТАЛЬЯН АНТОНІНА
Хмельницький національний університет
https://orcid.org/0000-0002-4925-9713
e-mail: yantonina@ukr.net

КРИТЕРІЙ ОПЕРАТИВНОСТІ ЩОДО ВАРІАНТІВ ЦЕНТРАЛІЗАЦІЇ В АРХІТЕКТУРІ МУЛЬТИКОМП'ЮТЕРНИХ СИСТЕМ З КОМБІНОВАНИХ АНТИВІРУСНИХ ПРИМАНОК І ПАСТОК ДЛЯ ВИЯВЛЕННЯ ЗЛОВМИСНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА КОМП'ЮТЕРНИХ АТАК

В роботі здійснено аналіз існуючих методів виявлення зловмисного програмного забезпечення та комп'ютерних атак з використанням приманок та пасток. Також, розглянуто системи, які можуть використовуватись для інтеграції в них приманок та пасток. Архітектура таких систем дає змогу, також, здійснювати перебудову в процесі функціонування без залучення адміністратору. В цьому процесі важливими є ознаки та параметри, які впливатимуть на процес перебудови і вибір варіанту перебудови. Тому, в роботі розроблено критерій оперативності щодо наступного варіанту центру системи в архітектурі системи для забезпечення її перебудови.

В розробленому критерії оперативності враховано показники такі, як час для визначення нових компонент з функціоналом центру та компонент без такого функціоналу, час для повідомлення компонентам про наступний стан централізації і їх призначення в новій архітектурі системи, час на повідомлення всім компонентам системи про завершення поточного типу централізації в архітектурі системи, час отримання підтвердження від всіх компонент системи про опрацювання ними повідомлення про завершення поточного типу централізації та перехід до нового типу централізації в архітектурі системи, час надсилання команди всім компонентам системи про початок роботи з новим центром системи та отримання підтвердження від них про успішний перехід, час надсилання повідомлень між компонентами центру системи для узгодження роботи, загальна кількість компонент в системі, кількість активних компонент системи в поточний момент часу, кількість компонент в системі з функціоналом центру системи в поточний момент часу, відомості про компоненти системи в поточний момент часу у вузлах корпоративної мережі, відомості про активні та неактивні компоненти центру системи в поточний момент часу у вузлах корпоративної мережі, кількість неактивних компонент з функціоналом центру системи в поточний момент часу, кількість неактивних компонент без функціоналу центру системи в поточний момент часу, кількість сегментів в корпоративній мережі, в які встановлено компоненти системи, кількість компонент системи в демілітаризованій зоні корпоративної мережі, кількість компонент системи у серверних вузлах, кількість компонент з функціоналом центру системи у вузлах в демілітаризованій зоні, кількість компонент з функціоналом центру системи у серверних вузлах.

В результаті з врахуванням параметрів було розроблено критерій оперативності для визначення наступного варіанту централізації в архітектурі мультикомп'ютерних систем виявлення зловмисного програмного забезпечення та комп'ютерних атак з використанням приманок та пасток. Для перевірки адекватності опису критерію оперативності процесам в системі було проведено експеримент, результати якого підтвердили можливість застосування критерію оперативності для таких систем.

Ключові слова: критерій, оперативність, зловмисне програмне забезпечення, комп'ютерні атаки, приманки, пастки.

KASHTALIAN ANTONINA
Khmelnytskyi National University, Khmelnytskyi

THE CRITERION OF PROMPTNESS IN CENTRALIZATION IN THE ARCHITECTURE OF MULTICOMPUTARY SYSTEMS WITH COMBINED ANTIVIRUS BAITS AND TRAPS TO DETECT MALICIOUS SOFTWARE AND COMPUTER ATTACKS

The work analyzes existing methods of detecting malicious software and computer attacks using baits and traps. Systems that can be used to integrate baits and traps are considered. The architecture of such systems enables to carry out restructuring in the process of functioning without involving the administrator. In this process, the features and parameters that will influence the restructuring process and the choice of restructuring are important. Therefore, the work criterion for the next version of the system of the system in the architecture of the system to ensure its restructuring was developed.

The developed criteria of efficiency takes into account indicators such as time to determine new components with the functionality of the center and component without such functionality, time to notify the components of the next state of centralization and their purpose in the new architecture of the system, time to notify all components of the system about the completion of current type of centralization. in the architecture of the system, the time of receipt of confirmation from all the components of the system about the completion of the current type of centralization and the transition to a new type of centralization in the architecture of the system, the time of sending the team to all components of the system about the start of work with the new center of the system and obtaining confirmation from them about successful Transition, time sending messages between the components of the system of system for work coordination, the total number of components in the system, the number of active components of the system at the current time, the number of components in the system with the functionality of the system of the system at the current time, information about the components of the system at the current point in time in Corporate network nodes, information about the active and inactive components of the system of the system at the current time at the corporate network nodes, the number of inactive components with the functionality of the system center at the current time, the number of inactive components without the functionality of the system at the current time, the number of segments in the corporate network , in which the components of the system, the number of system components in the demilitarized zone of the corporate network, the number of system components in server units, the number of components with the functionality of the center center in the nodes in the demilitarized zone, the number of components with the functionality of the system center in server units.

As a result, the parameters have developed a criterion for promptness to determine the following centralization in the architecture of multicomputer systems detection of malicious software and computer attacks using baits and traps. In order to check the adequacy of the description

of the criterion of efficiency of processes in the system, an experiment was conducted, the results of which confirmed the possibility of applying the criterion of efficiency for such systems.

Keywords: criterion, promptness, malicious software, computer attacks, decoys, traps.

Постановка проблеми

Мультикомп'ютерні системи для виявлення зловмисного програмного забезпечення та комп'ютерних атак можуть бути розроблені з урахуванням їх спроможності до перебудови архітектури в процесі функціонування самостійно без залучення адміністратора [1, 2, 3]. Для організації такого їх функціонування необхідні ознаки, показники та їх поєднання. Ці поєднання можна реалізувати певними функціями, які будуть розглядатись в контексті критеріїв щодо визначених характеристик. Актуальним критерієм для розподілених систем [4, 5] є критерій оперативності. Згідно цього критерію можна було б системі визначати наступні варіанти своєї архітектури, тобто за певними визначеними параметрами оцінити свої спроможності [6] до такої перебудови і здійснити її.

Важливими показниками для критеріїв щодо оперативності в контексті мультикомп'ютерних систем можуть бути такі, як час для визначення нових компонент з функціоналом центру та компонент без такого функціоналу, час для повідомлення компонентам про наступний стан централізації і їх призначення в новій архітектурі системи, час на повідомлення всім компонентам системи про завершення поточного типу централізації в архітектурі системи, час отримання підтвердження від всіх компонент системи про опрацювання ними повідомлення про завершення поточного типу централізації та перехід до нового типу централізації в архітектурі системи, час надсилання команди всім компонентам системи про початок роботи з новим центром системи та отримання підтвердження від них про успішний перехід, час надсилання повідомлень між компонентами центру системи для узгодження роботи, загальна кількість компонент в системі, кількість активних компонент системи в поточний момент часу, кількість компонент в системі з функціоналом центру системи в поточний момент часу, відомості про компоненти системи в поточний момент часу у вузлах корпоративної мережі, відомості про активні та неактивні компоненти центру системи в поточний момент часу у вузлах корпоративної мережі, кількість неактивних компонент з функціоналом центру системи в поточний момент часу, кількість неактивних компонент без функціоналу центру системи в поточний момент часу, кількість сегментів в корпоративній мережі, в які встановлено компоненти системи, кількість компонент системи в демілітаризованій зоні корпоративної мережі, кількість компонент системи у серверних вузлах, кількість компонент з функціоналом центру системи у вузлах в демілітаризованій зоні, кількість компонент з функціоналом центру системи у серверних вузлах.

При врахуванні розглянутих параметрів можна розробити критерій оперативності для визначення наступного варіанту централізації в архітектурі мультикомп'ютерних систем виявлення зловмисного програмного забезпечення та комп'ютерних атак з використанням приманок та пасток.

Аналіз останніх досліджень і публікацій

Розглянемо особливості використання та функціонування систем з приманками та пастками, а також обманних систем.

В роботі [7] пропонується новий тип системи приманок, що ґрунтується на обманній технології захисту. Підхід динамічного обману адаптується для збору невикористаних IP адрес у мережі електромереж із збереженням суті приманки. Невикористані IP адреси використовуються для створення динамічних віртуальних хостів, які забезпечують проактивну взаємодію із зловмисниками та перенаправляють трафік на приманки, таким чином захоплюючи зловмисника в пастку.

Новий метод для кіберобману із використанням локалізації приманки та різноманіття програмного забезпечення [8] для покращення безпеки мережі базується на тому, що засіб захисту мережі обирає, де розташувати приманку, враховуючи обмежені ресурси. Сформульовано теоретико-ігровий підхід для опису політики локалізації приманки, що захищає найбільш цінні ресурси мережі.

Обман з використанням приманок може забезпечити ефективний шлях протидії кібератакам в комп'ютерних мережах. В роботі оцінюється вплив розміру мережі на рішення зловмисника щодо кібератак, використовуючи гру в обман [9]. Гра в обман має дві послідовні стадії, дослідження та атака. На стадії дослідження учасники можуть перевірити декілька веб серверів або не перевіряти мережу. На стадії атаки учасники можуть атакувати один з досліджуваних веб серверів або вирішити не атакувати мережу. Таким чином, було доведено необхідність більшого покриття мережі приманками.

В роботі пропонується архітектура [10] Secure Shell (SSH) приманки із використанням простукування портів та система виявлення вторгнень для вивчення інформації про атаки на SSH сервісі та визначення необхідного механізму безпеки для роботи із зловмисником. SSH сервіси є популярною ціллю серед існуючих вразливостей, атаки на які мають різні характеристики. Вивчення цих характеристик за допомогою приманок необхідне для застосування відповідних механізмів на реальних серверах. Запропоновано ефективну стратегію комбінування простукування портів та системи виявлення вторгнень, яке передбачає, що сервер зберігає сервіс на закритому порту та відкриває її за запитом користувача, надсилаючи попередньо визначену послідовність портів як процес аутентифікації для контролю доступу до сервера. Таким чином, розглянуто особливості архітектури систем з приманками і їх спрямування на різні об'єкти в мережі.

В статті [11] розглянуто типові методи, що використовуються в приманках та засобах захисту рухомих цілей, що охоплює період з кінця 1980-х до 2021 року. Методи з цих трьох галузей доповнюють одна одну і можуть бути використані для побудови цілісного захисту на основі обману. В роботі досліджено інтегроване

використання цих трьох напрямків для організованого обману. Використовуючи адаптовану модель кіберланцюга знищення, яка може відображати поточний ландшафт загроз, і чотирирівненвий стек обману, розроблено двовимірну таксономію, на основі якої класифікуються методи обману.

Представлено модель в роботі [12], яка може буде використана для планування та інтегрування обманних систем в захист безпеки комп'ютера. Представлено огляд фундаментальних причин, чому обманні системи працюють та основних принципів використання цього підходу. Показано, як запропонована модель може бути вбудована в багато частин комп'ютерних систем та як це зробити ефективно.

В роботі [13] проведено огляд 24 робіт 2008-2018 років, які використовують теорію ігор для моделювання захисного обману для кібербезпеки та приватності. Запропонована класифікація, яка виділяє шість типів обману: збурення, захист рухомої цілі, заплутування, змішування, приманка, залучення зловмисника. Ці типи характеризуються своїми інформаційними структурами, діями та тривалістю, та концепцією теорії ігор.

Обманні рішення в роботі [14] можуть виявляти, аналізувати та захищати веб застосунки від вдосконалених атак, від яких не можуть захистити існуючі рішення на основі пошуку аномалій та методи запобігання атакам. Наявні обманні рішення викликають сумнів щодо протоколів прикладного рівня та відсутності досліджень застовування обману на цьому рівні. Робота спрямована на вивчення можливого використання методів обману, які можуть бути включені в контекст трафіку рівня веб застосунків з метою виявлення атак.

Вважається в роботі [15], що розташування приманок в різних георграфічних локаціях збільшує їх ефективність, однак цей факт не є достатньо дослідженим, особливо для систем раннього виявлення вторгнень. В роботі досліджено патерни атак великого публічного датасету географічно розподілених приманок та створено профілі зловмисників. Результати показують, що розташування приманок допомагає виявити патерни атак та побудувати профілі зловмисників. Зроблено висновок, що не всі дані, зібрані з георафічно розподілених приманок є однаково цінними, і можна створити систему раннього попередження вторгнень за допомогою двох розподілених приманок та робочого серверу.

Важливим шляхом знаходження вразливостей в сучасних мережах [16] для зловмисників є розвідка, через яку вони ідентифікують конфігурації певних мережевих хостів. Для підвищення невизначеності системний адміністратор (засіб захисту) може додавати обман у відповіді на мережеве сканування, зокрема приховувати певні характеристики системи. В роботі представлено нову теоретику-ігрову модель оманливої взаємодії між засобом захисту та зловмисником, яку в роботі названо кіберобман. Розглянуто випадки потужного зловмисника, якому відомо про обманну стратегію засобу захисту, та наївного зловмисника, якому це невідомо. Показано що обчислення оптимальної стратегії для обох типів зловмисників має NP-складність. Для випадку потужного зловмисника надано лінійне програмне рішення, а також швидкий і ефективний жадібний алгоритм. Так само запропоновано точні та евристичні підходи для випадку наївного зловмисника.

Розвідка IP-адреси та порту зв'язку є необхідною умовою для мережевих атак [17]. Статичні налаштування дають велику перевагу зловмисникам у виявленні мережевих цілей та запуску атак. В роботі запропоновано новий метод, який перетворює кінцеві хости на непередбачувані рухомі цілі шляхом прозорого інтелектуального та випадкового перетворення їх IP-адрес або портів без зменшення продуктивності мережі.

Розширені цільові кібератаки часто використовують розвідувальні заходи для збору інформації про потенційні цілі, їх характеристики та розташування [18] для виявлення вразливостей у мережевому середовищі. З цією метою часто використовують вдосконалені методи сканування мережі, які автоматично виконуються хостами, зараженими зловмисними програмами. В роботі визначено мережевий обман для захисної розвідки та розроблено систему розвідувального обману, яка грунтується на програмно визначеній мережі, щоб досягти обману шляхом імітації віртуальних топологій.

В аналізованих роботах вказується на механізми активізації систем з приманками та обманних систем. Але деталізації їх активізації не подано. Тому, необхідна деталізація механізмів та правил для перебудови систем під час їх функціонування з метою забезпечення ними ефективних обманних дій з приманками та пастками.

Метою роботи є розроблення критерію щодо оперативності для оцінювання наступних варіантів централізації для вибору одного з варіантів централізації з врахуванням попереднього досвіду функціонування систем.

Виклад основного матеріалу

Визначимо критерій щодо оперативності функцією $f_{1,kr}^{centr}\left(p_{1,kr}^{centr}\right)$. Оскільки оперативність характеризується швидкістю передачі інформації та своєчасністю її отримання, то для визначення відповідного їй критерію будемо враховувати час, а також з урахуванням розподілення системи будемо враховувати кількість компонент, які будуть залучені в процес передачі та отримання інформації.

Деталізуємо визначення критерію $f_{1,kr}^{centr}\left(p_{1,kr}^{centr}\right)$ щодо оперативності з урахуванням співвідношень між певними параметрами, які задані у векторі $p_{i,kr}^{centr}$. Нехай показник $p_{1,1,kr}^{centr} = t_1^{p_{1,kr}^{centr}}$ – час для підготовки рішення центром системи щодо певного наступного типу централізації. Для різних типів централізації цей час буде різним, оскільки різні типи централізації передбачають залучення різної кількості компонент для формування центру системи. Процес безпосередньої зміни типу централізації в системі вимагатиме певного часу для проведення різних його етапів і, при цьому, може бути так, що частина цих етапів буде виконуватись

паралельно, що зменшить час реалізації всього процесу. Тому, введемо для подання показники, які відображатимуть етапи процесу зміни типу централізації:

1) $p_{2,1,kr}^{centr} = t_2^{p_{1,kr}^{centr}}$ – час для визначення нових компонент з функціоналом центру та компонент без такого функціоналу;

2) $p_{3,1,kr}^{centr} = t_3^{p_{1,kr}^{centr}}$ – час для повідомлення компонентам про наступний стан централізації і їх призначення в новій архітектурі системи;

3) $p_{4,1,kr}^{centr} = t_4^{p_{1,kr}^{centr}}$ – час на повідомлення всім компонентам системи про завершення поточного типу централізації в архітектурі системи;

4) $p_{5,1,kr}^{centr} = t_5^{p_{1,kr}^{centr}}$ – час отримання підтвердження від всіх компонент системи про опрацювання ними повідомлення про завершення поточного типу централізації та перехід до нового типу централізації в архітектурі системи;

5) $p_{6,1,kr}^{centr} = t_6^{p_{1,kr}^{centr}}$ – час надсилання команди всім компонентам системи про початок роботи з новим центром системи та отримання підтвердження від них про успішний перехід;

6) $p_{7,1,kr}^{centr} = t_7^{p_{1,kr}^{centr}}$ – час надсилання повідомлень між компонентами центру системи для узгодження роботи;

7) $p_{8,1,kr}^{centr} = k_8^{p_{1,kr}^{centr}}$ – загальна кількість компонент в системі;

8) $p_{9,1,kr}^{centr} = k_9^{p_{1,kr}^{centr}}$ – кількість активних компонент системи в поточний момент часу;

9) $p_{10,1,kr}^{centr} = k_{10}^{p_{1,kr}^{centr}}$ – кількість компонент в системі з функціоналом центру системи в поточний момент часу;

10) $p_{11,1,kr}^{centr} = u_{11}^{p_{1,kr}^{centr}}$ – вектор, координатами якого є відомості про компоненти системи в поточний момент часу у вузлах корпоративної мережі для підмножин $A_{1,u}^{\Subset}, A_{2,u}^{\Subset}$;

11) $p_{12,1,kr}^{centr} = v_{12}^{p_{1,kr}^{centr}}$ – вектор, координатами якого є відомості про компоненти системи в поточний момент часу у вузлах корпоративної мережі для підмножин $A_{1,v}^{\Subset}, A_{2,v}^{\Subset}$;

12) $p_{13,1,kr}^{centr} = u_{13}^{p_{1,kr}^{centr}}$ – вектор, координатами якого є відомості про компоненти центру системи в поточний момент часу у вузлах корпоративної мережі для підмножини $A_{1,u}^{\Subset}$, які відображають активні компоненти центру і неактивні, але які були означені як такі, що вони є частиною центру системи;

13) $p_{14,1,kr}^{centr} = k_{14}^{p_{1,kr}^{centr}}$ – кількість неактивних компонент з функціоналом центру системи в поточний момент часу;

14) $p_{15,1,kr}^{centr} = k_{15}^{p_{1,kr}^{centr}}$ – кількість неактивних компонент без функціоналу центру системи в поточний момент часу;

15) $p_{16,1,kr}^{centr} = k_{16}^{p_{1,kr}^{centr}}$ – кількість сегментів в корпоративній мережі, в які встановлено компоненти системи;

16) $p_{17,1,kr}^{centr} = k_{17}^{p_{1,kr}^{centr}}$ – кількість компонент системи в демілітаризованій зоні корпоративної мережі;

17) $p_{18,1,kr}^{centr} = k_{18}^{p_{1,kr}^{centr}}$ – кількість компонент системи у серверних вузлах;

18) $p_{19,1,kr}^{centr} = k_{19}^{p_{1,kr}^{centr}}$ – кількість компонент з функціоналом центру системи у вузлах в демілітаризованій зоні;

19) $p_{20,1,kr}^{centr} = k_{20}^{p_{1,kr}^{centr}}$ – кількість компонент з функціоналом центру системи у серверних вузлах.

Для децентралізованої архітектури показники часу $t_7^{p_{1,kr}^{centr}}$ будуть більшими порівняно з іншими типами архітектури. Для централізованого типу архітектури без розподілення центру системи $t_7^{p_{1,kr}^{centr}} = 0$. Якщо тип централізації в архітектурі системи відмінний від децентралізованого типу, тоді на показник часу $t_7^{p_{1,kr}^{centr}}$ буде впливати кількість компонент з центром системи. Із збільшенням їх кількості зростатиме час для узгодження роботи між ними.

Для децентралізованої архітектури показник $t_2^{p_{1,kr}^{centr}} = 0$, оскільки рішення щодо часу для визначення нових компонент з функціоналом центру та компонент без такого функціоналу приймати не потрібно, оскільки всі ці компоненти будуть компонентами центру. Але в такій архітектурі час $t_7^{p_{1,kr}^{centr}}$ надсилання повідомлень між компонентами центру системи для узгодження роботи буде найбільшим порівняно з рештою типів архітектури.

Визначимо $f_{1,kr}^{centr}\left(p_{1,kr}^{centr}\right)$ для критерію щодо оперативності так:

$$f_{1,kr}^{centr}\left(p_{1,kr}^{centr}\right) = 1 - \frac{1}{9}\cdot\left(\frac{\sum_{i=1}^{7} t_i^{p_{1,kr}^{centr}}}{\sum_{i=1}^{7} t_{i,max}^{p_{1,kr}^{centr}}} + \frac{k_8^{p_{1,kr}^{centr}}}{k_9^{p_{1,kr}^{centr}}} + \frac{k_{10}^{p_{1,kr}^{centr}}}{k_{10}^{p_{1,kr}^{centr}} + k_{14}^{p_{1,kr}^{centr}}} + \frac{k_8^{p_{1,kr}^{centr}} - \left(k_{15}^{p_{1,kr}^{centr}} + k_{16}^{p_{1,kr}^{centr}}\right)}{k_8^{p_{1,kr}^{centr}}} + \frac{k_{16}^{p_{1,kr}^{centr}} - 1}{k_{16}^{p_{1,kr}^{centr}}} + \frac{k_8^{p_{1,kr}^{centr}} - k_{17}^{p_{1,kr}^{centr}}}{k_8^{p_{1,kr}^{centr}}} + \frac{k_{17}^{p_{1,kr}^{centr}} - k_{19}^{p_{1,kr}^{centr}}}{k_{17}^{p_{1,kr}^{centr}}} + \frac{k_8^{p_{1,kr}^{centr}} - k_{18}^{p_{1,kr}^{centr}}}{k_8^{p_{1,kr}^{centr}}} + \frac{k_{18}^{p_{1,kr}^{centr}} - k_{20}^{p_{1,kr}^{centr}}}{k_{18}^{p_{1,kr}^{centr}}}\right), \quad (1)$$

де $t_{i,max}^{p_{1,kr}^{centr}}$ – найбільше значення часу за і-тою характеристикою, яке було отримано в процесі функціонування системи, починаючи з першого самостійного рішення системою; $i = 1, \dots, 7$.

Таким чином, критерій щодо оперативності може бути визначений за формулою (1) і значення обчислені з його визначення можуть бути використані в цільовій функції оцінювання наступних варіантів централізації для вибору одного з варіантів з чотирьох типів централізації. В формулі (1) враховано досвід функціонування системи в частині самостійного прийняття рішень щодо наступного варіанту централізації і збереження отриманих показників для використання в подальших кроках їх найбільших значень.

Експеримент

Для проведення експерименту використаємо прототип системи, в якому реалізовано вибір наступного варіанту централізації з використанням критерію оперативності. Мультикомп'ютерна система функціонувала 90 діб. З а цей час вона самостійно перебудувала центр системи в своїй архітектурі 311 разів. На графіку на рис. 1 зображено значення функції, які визначено за формулою (1) та точки якої з'єднано відрізками. На графіку зображено розміщення точок в інтервалі (0;0,1), для яких перебудова центру системи була успішною. Для точок з інтервалу (0;0,25) процес перебудови центру системи не відбувся і далі були повторні ітерації з іншими варіантами, які були підготовлені в центрі системи.

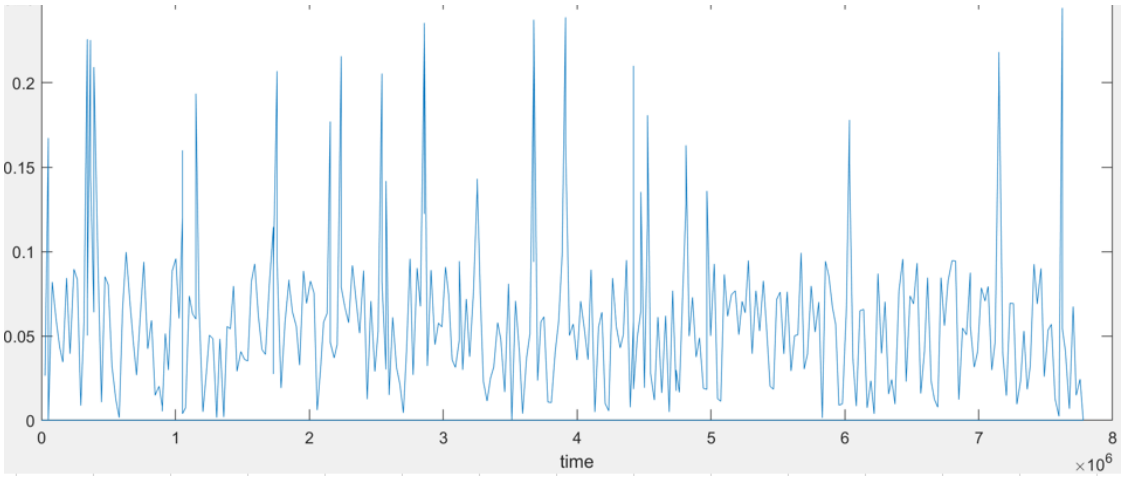

Рис. 1. Графік функції критерію оперативності

Таким чином, розроблений критерій оперативності в контексті його використання для визначення наступного варіанту централізації в системі адекватно відображає стани, в яких процес перебудови завершився успішно або не відбувся.

Висновки

Розроблено критерій щодо оперативності для оцінювання наступних варіантів централізації для вибору одного з варіантів централізації. В формулі (1) враховано досвід функціонування системи в частині самостійного прийняття рішень щодо наступного варіанту централізації і збереження отриманих показників для використання в подальших кроках їх найбільших значень.

Проведено експеримент для розробленого критерію щодо оперативності в контексті його використання для визначення наступного варіанту централізації в системі. Він адекватно відображає стани, в яких процес перебудови завершився успішно або не відбувся.

Напрямами подальших досліджень є розроблення критеріїв щодо стійкості, безпеки та цілісності систем в контексті вибору наступного варіанту централізації в архітектурі систем.

Література

1. Savenko, O., Sachenko, A., Lysenko, S., Markowsky, G., & Vasylkiv, N. (2020). BOTNET DETECTION APPROACH BASED ON THE DISTRIBUTED SYSTEMS. *International Journal of Computing*, *19*(2), 190-198. https://doi.org/10.47839/ijc.19.2.1761

2. Lysenko S, Bobrovnikova K, Kharchenko V, Savenko O. IoT Multi-Vector Cyberattack Detection Based on Machine Learning Algorithms: Traffic Features Analysis, Experiments, and Efficiency. *Algorithms*. 2022; 15(7):239. https://doi.org/10.3390/a15070239

3. Kashtalian, A., Lysenko, S., Savenko, O., Nicheporuk, A., Sochor, T., & Avsiyevych, V. (2024). Multi-computer malware detection systems with metamorphic functionality. Radioelectronic and Computer Systems, 2024(1), 152-175. doi:https://doi.org/10.32620/reks.2024.1.13

4. D. Denysiuk, O. Savenko, S. Lysenko, B. Savenko and A. Kashtalian, "Method for Detecting Steganographic Changes in Images Using Machine Learning," 2023 13th International Conference on Dependable Systems, Services and Technologies (DESSERT), Athens, Greece, 2023, pp. 1-6, doi: 10.1109/DESSERT61349.2023.10416453.

5. B. Savenko, A. Kashtalian, S. Lysenko and O. Savenko, "Malware Detection By Distributed Systems with Partial Centralization," 2023 IEEE 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Dortmund, Germany, 2023, pp. 265-270, doi: 10.1109/IDAACS58523.2023.10348773.

6. Kashtalian, A., Lysenko, S., Savenko, B., Sochor, T., & Kysil, T. (2023). Principle and method of deception systems synthesizing for malware and computer attacks detection. *Radioelectronic and Computer Systems, 0*(4), 112-151. doi:https://doi.org/10.32620/reks.2023.4.10

7. Feng, M. et al. (2022). A Novel Deception Defense-Based Honeypot System for Power Grid Network. In: Qiu, M., Gai, K., Qiu, H. (eds) Smart Computing and Communication. SmartCom 2021. *Lecture Notes in Computer Science*, vol 13202. Springer, Cham. https://doi.org/10.1007/978-3-030-97774-0_27

8. H. Anwar and C. A. Kamhoua, "Cyber Deception using Honeypot Allocation and Diversity: A Game Theoretic Approach," *2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC*), Las Vegas, NV, USA, 2022, pp. 543-549 doi: 10.1109/CCNC49033.2022.9700616.

9. Harsh Katakwar. Influence of Network Size on Adversarial Decisions in a Deception Game Involving Honeypots/ Harsh Katakwar, Palvi Aggarwal, Zahid Maqbool, Varun Dutt Front. Psychol., 25 September 2020 Sec. Cognition Volume 11 – 2020. https://doi.org/10.3389/fpsyg.2020.535803 https://www.frontiersin.org/articles/10.3389/fpsyg.2020.535803/full

10. Sven Schindler. Hyhoneydv6: A hybrid Honeypot Architecture for Ipv6 Networks/ Sven Schindler, Bettina Schnor, Thomas Scheffler// International Journal of Intelligent Computing Research (IJICR), Volume 6, Issue 2, June 2015, P. 562-570 http://www.infonomics-society.org/wp-content/uploads/ijicr/published-papers/volume-6-2015/Hyhoneydv6-A-hybrid-Honeypot-Architecture-for-IPv6-Networks.pdf

11. Li Zhang, Vrizlynn L. L. Thing. Three Decades of Deception Techniques in Active Cyber Defense -- Retrospect and Outlook. https://doi.org/10.48550/arXiv.2104.03594 https://arxiv.org/pdf/2104.03594.pdf

12. Mohammed H. Almeshekah and Eugene H. Spafford. 2014. Planning and Integrating Deception into Computer Security Defenses. In Proceedings of the 2014 New Security Paradigms Workshop (NSPW '14). Association for Computing Machinery, New York, NY, USA, 127–138. https://doi.org/10.1145/2683467.2683482

13. Pawlick, J., Colbert, E., & Zhu, Q. (2017). A Game-theoretic Taxonomy and Survey of Defensive Deception for Cybersecurity and Privacy. ACM Computing Surveys (CSUR), 52, 1 - 28. https://www.semanticscholar.org/paper/A-Game-theoretic-Taxonomy-and-Survey-of-Defensive-Pawlick-Colbert/47e558cd6c72e7292d7d686cdffaefe0e6e5fba2 https://arxiv.org/abs/1712.05441

14. Efendi, M.A., Ibrahim, Z.B., Zawawi, M.N., Rahim, F.A., Pahri, N.A., & Ismail, A. (2019). A Survey on Deception Techniques for Securing Web Application. 2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity*), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, 328-331. https://www.semanticscholar.org/paper/A-Survey-on-Deception-Techniques-for-Securing-Web-Efendi-Ibrahim/d2c9acbda2145fe8860e81cdcc870486a560a3e6

15. Valeros V., Rigaki M., Garcia S. Attacker Profiling Through Analysis of Attack Patterns in Geographically Distributed Honeypots. https://doi.org/10.48550/arXiv.2305.01346

16. Aaron Schlenker, Omkar Thakoor, Haifeng Xu, Fei Fang, Milind Tambe, Long Tran-Thanh, Phebe Vayanos, and Yevgeniy Vorobeychik. 2018. Deceiving Cyber Adversaries: A Game Theoretic Approach. In Proceedings of the 17th International Conference on Autonomous Agents and MultiAgent Systems (AAMAS '18). *International Foundation for Autonomous Agents and Multiagent Systems,* Richland, SC, 892–900. https://dl.acm.org/doi/10.5555/3237383.3237833 https://www.ifaamas.org/Proceedings/aamas2018/pdfs/p892.pdf

17. Li Kechao and Xiong Xinli. 2019. OpenHIP Random Host Hopping in Network Layer. *In International Conference on Education, Management and Information Technology (ICEMIT 2019)* https://webofproceedings.org/proceedings_series/ESSP/ICEMIT%202019/ICEMIT19048.pdf

18. S. Achleitner, T. F. La Porta, P. McDaniel, S. Sugrim, S. V. Krishnamurthy and R. Chadha, "Deceiving Network Reconnaissance Using SDN-Based Virtual Topologies," *in IEEE Transactions on Network and Service Management*, vol. 14, no. 4, pp. 1098-1112, Dec. 2017, doi: 10.1109/TNSM.2017.2724239

References

1. Savenko, O., Sachenko, A., Lysenko, S., Markowsky, G., & Vasylkiv, N. (2020). BOTNET DETECTION APPROACH BASED ON THE DISTRIBUTED SYSTEMS. *International Journal of Computing*, *19*(2), 190-198. https://doi.org/10.47839/ijc.19.2.1761

2. Lysenko S, Bobrovnikova K, Kharchenko V, Savenko O. IoT Multi-Vector Cyberattack Detection Based on Machine Learning Algorithms: Traffic Features Analysis, Experiments, and Efficiency. *Algorithms*. 2022; 15(7):239. https://doi.org/10.3390/a15070239

3. Kashtalian, A., Lysenko, S., Savenko, O., Nicheporuk, A., Sochor, T., & Avsiyevych, V. (2024). Multi-computer malware detection systems with metamorphic functionality. Radioelectronic and Computer Systems, 2024(1), 152-175. doi:https://doi.org/10.32620/reks.2024.1.13

4. D. Denysiuk, O. Savenko, S. Lysenko, B. Savenko and A. Kashtalian, "Method for Detecting Steganographic Changes in Images Using Machine Learning," 2023 13th International Conference on Dependable Systems, Services and Technologies (DESSERT), Athens, Greece, 2023, pp. 1-6, doi: 10.1109/DESSERT61349.2023.10416453.

5. B. Savenko, A. Kashtalian, S. Lysenko and O. Savenko, "Malware Detection By Distributed Systems with Partial Centralization," 2023 IEEE 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Dortmund, Germany, 2023, pp. 265-270, doi: 10.1109/IDAACS58523.2023.10348773.

6. Kashtalian, A., Lysenko, S., Savenko, B., Sochor, T., & Kysil, T. (2023). Principle and method of deception systems synthesizing for malware and computer attacks detection. *Radioelectronic and Computer Systems, 0*(4), 112-151. doi:https://doi.org/10.32620/reks.2023.4.10

7. Feng, M. et al. (2022). A Novel Deception Defense-Based Honeypot System for Power Grid Network. In: Qiu, M., Gai, K., Qiu, H. (eds) Smart Computing and Communication. SmartCom 2021. Lecture Notes in Computer Science, vol 13202. Springer, Cham. https://doi.org/10.1007/978-3-030-97774-0_27

8. H. Anwar and C. A. Kamhoua, "Cyber Deception using Honeypot Allocation and Diversity: A Game Theoretic Approach," 2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 2022, pp. 543-549 doi: 10.1109/CCNC49033.2022.9700616.

9. Harsh Katakwar. Influence of Network Size on Adversarial Decisions in a Deception Game Involving Honeypots/ Harsh Katakwar, Palvi Aggarwal, Zahid Maqbool, Varun Dutt Front. Psychol., 25 September 2020 Sec. Cognition Volume 11 – 2020. https://doi.org/10.3389/fpsyg.2020.535803 https://www.frontiersin.org/articles/10.3389/fpsyg.2020.535803/full

10. Sven Schindler. Hyhoneydv6: A hybrid Honeypot Architecture for Ipv6 Networks/ Sven Schindler, Bettina Schnor, Thomas Scheffler// International Journal of Intelligent Computing Research (IJICR), Volume 6, Issue 2, June 2015, P. 562-570 http://www.infonomics-society.org/wp-content/uploads/ijicr/published-papers/volume-6-2015/Hyhoneydv6-A-hybrid-Honeypot-Architecture-for-IPv6-Networks.pdf

11. Li Zhang, Vrizlynn L. L. Thing. Three Decades of Deception Techniques in Active Cyber Defense -- Retrospect and Outlook. https://doi.org/10.48550/arXiv.2104.03594 https://arxiv.org/pdf/2104.03594.pdf

12. Mohammed H. Almeshekah and Eugene H. Spafford. 2014. Planning and Integrating Deception into Computer Security Defenses. In Proceedings of the 2014 New Security Paradigms Workshop (NSPW '14). Association for Computing Machinery, New York, NY, USA, 127–138. https://doi.org/10.1145/2683467.2683482

13. Pawlick, J., Colbert, E., & Zhu, Q. (2017). A Game-theoretic Taxonomy and Survey of Defensive Deception for Cybersecurity and Privacy. ACM Computing Surveys (CSUR), 52, 1 - 28. https://www.semanticscholar.org/paper/A-Game-theoretic-Taxonomy-and-Survey-of-Defensive-Pawlick-Colbert/47e558cd6c72e7292d7d686cdffaefe0e6e5fba2 https://arxiv.org/abs/1712.05441

14. Efendi, M.A., Ibrahim, Z.B., Zawawi, M.N., Rahim, F.A., Pahri, N.A., & Ismail, A. (2019). A Survey on Deception Techniques for Securing Web Application. 2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), 328-331. https://www.semanticscholar.org/paper/A-Survey-on-Deception-Techniques-for-Securing-Web-Efendi-Ibrahim/d2c9acbda2145fe8860e81cdcc870486a560a3e6

15. Valeros V., Rigaki M., Garcia S. Attacker Profiling Through Analysis of Attack Patterns in Geographically Distributed Honeypots. https://doi.org/10.48550/arXiv.2305.01346

16. Aaron Schlenker, Omkar Thakoor, Haifeng Xu, Fei Fang, Milind Tambe, Long Tran-Thanh, Phebe Vayanos, and Yevgeniy Vorobeychik. 2018. Deceiving Cyber Adversaries: A Game Theoretic Approach. In Proceedings of the 17th International Conference on Autonomous Agents and MultiAgent Systems (AAMAS '18). International Foundation for Autonomous Agents and Multiagent Systems, Richland, SC, 892–900. https://dl.acm.org/doi/10.5555/3237383.3237833 https://www.ifaamas.org/Proceedings/aamas2018/pdfs/p892.pdf

17. Li Kechao and Xiong Xinli. 2019. OpenHIP Random Host Hopping in Network Layer. In International Conference on Education, Management and Information Technology (ICEMIT 2019) https://webofproceedings.org/proceedings_series/ESSP/ICEMIT%202019/ICEMIT19048.pdf

18. S. Achleitner, T. F. La Porta, P. McDaniel, S. Sugrim, S. V. Krishnamurthy and R. Chadha, "Deceiving Network Reconnaissance Using SDN-Based Virtual Topologies," *in IEEE Transactions on Network and Service Management*, vol. 14, no. 4, pp. 1098-1112, Dec. 2017, doi: 10.1109/TNSM.2017.2724239.