DOI 10.31891/2307-5732-2025-347-73
УДК 004.75:004.49:004.3

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

МУЛЬТИКОМП'ЮТЕРНА СИСТЕМА З КОМБІНОВАНИХ АНТИВІРУСНИХ ПРИМАНОК І ПАСТОК ДЛЯ ВИЯВЛЕННЯ ЗЛОВМИСНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА КОМП'ЮТЕРНИХ АТАК НА ОСНОВІ МУЛЬТИАГЕНТНИХ ТЕХНОЛОГІЙ

В роботі реалізовано комплексний підхід до захисту комп'ютерної мережі шляхом створення мережі приманок, що забезпечує ефективне виявлення зловмисного трафіку та аналіз патернів нових атак. Впроваджено інноваційну систему, яка включає приманки, здатні моніторити виключно ворожий трафік, що дозволяє значно скоротити час реакції на потенційні загрози та забезпечує високоточне виявлення атак на мережу. Реалізовано мультиагентну систему приманок, яка об'єднує в собі множину різнорідних приманок, кожна з яких виконує певні функції, спрямовані на протидію загрозам. Розроблено високоефективні інтелектуальні приманки, що мають властивості автономних агентів і характеризуються адаптивною поведінкою, що дає їм змогу швидко та ефективно реагувати на зміни в мережевому середовищі. Вони здатні самостійно визначати особливості атак, адаптувати свою поведінку під загрози та передавати відповідну інформацію іншим компонентам системи, що значно підвищує ефективність функціонування всієї мережі приманок.

Забезпечено інтеграцію ключових характеристик, таких як реактивність, проактивність і соціальна взаємодія приманок. Реактивність реалізована через здатність приманок аналізувати навколишнє середовище, своєчасно реагувати на зміну мережевого трафіку та швидко адаптуватися до нових атак. Проактивність забезпечує можливість приманок не лише реагувати на вже існуючі загрози, а й передбачати потенційні атаки, моделюючи поведінку зловмисників і відповідно змінюючи свої алгоритми роботи. Соціальні можливості розробленої системи дозволяють приманкам взаємодіяти між собою, обмінюватися інформацією про потенційні загрози, координувати дії та формувати єдину стратегію захисту мережі. Завдяки цьому реалізовано гнучку, адаптивну та ефективну систему кібербезпеки, яка не лише захищає мережу від атак, але й активно вивчає поведінкові моделі зловмисників.

Розгорнуто мультикомп'ютерну систему, яка включає в себе приманки та пастки, інтегровані у вузлах корпоративної мережі. Це дозволяє створити масштабоване середовище для всебічного аналізу загроз та ефективного управління ризиками. Завдяки модульному підходу реалізовано як централізовану, так і децентралізовану архітектуру мультиагентної системи приманок. У централізованій версії всі зібрані дані передаються на центральний пристрій мережі, де здійснюється їхній комплексний аналіз, у тому числі статистичний та поведінковий. Для цього розроблено систему збору, обробки та кореляції даних, що дозволяє отримувати цілісну картину кіберзагроз у мережі. На основі цих даних реалізовано механізм навчання моделей машинного навчання, які дозволяють прогнозувати потенційні вектори атак і автоматично адаптувати систему безпеки до нових загроз.

Запроваджено гнучку систему управління приманками, що дає змогу легко змінювати параметри роботи, адаптувати поведінку окремих елементів мережі та оперативно реагувати на нові загрози. Вся система функціонує у режимі постійного самонавчання, що дозволяє їй удосконалювати алгоритми роботи без втручання адміністратора. Завдяки цьому створено динамічну систему захисту корпоративної мережі, яка здатна не лише виявляти загрози в режимі реального часу, але й проактивно запобігати потенційним атакам.

Ключові слова: зловмисне програмне забезпечення, комп'ютерні атаки, приманки, пастки, мультиагентна система, мультикомп'ютерна система.

KASHTALIAN ANTONINA
Khmelnytskyi National University, Khmelnytskyi, Ukraine

A MULTI-COMPUTER SYSTEM OF COMBINED ANTIVIRUS DECOYS AND TRAPS FOR DETECTING MALWARE AND COMPUTER ATTACKS BASED ON MULTI-AGENT TECHNOLOGIES

The work has a comprehensive approach to protecting the computer by creating a network of baits, which ensures effective detection of malicious traffic and analysis of new attacks. An innovative system is introduced, which includes baits capable of monitoring exclusively hostile traffic, which can significantly reduce the response time to potential threats and ensures high detection of attacks on the network. A multi -agent bait system is implemented, which combines a set of heterogeneous baits, each of which performs certain functions aimed at counteracting threats. Highly effective intellectual lures have been developed, which have the properties of autonomous agents and are characterized by adaptive behavior, which enables them to respond quickly and effectively to changes in the network environment. They are able to independently determine the features of attacks, adapt their behavior to threats and transmit relevant information to other components of the system, which significantly increases the efficiency of the entire network of baits.

The integration of key characteristics, such as reactivity, proactivity and social interaction of baits, is ensured. Reactivity is realized through the ability to analyze the environment, respond in a timely manner to change network traffic and adapt quickly to new attacks. Proactivity provides the possibility of baits not only to respond to existing threats, but also to anticipate potential attacks, modeling the behavior of the intruders and accordingly changing their work algorithms. The social capabilities of the developed system allow the lures to interact, exchange information about potential threats, coordinate actions and form a single network protection strategy. This implemented a flexible, adaptive and effective cybersecurity system that not only protects the network from attacks, but also actively studies the behavioral models of malefactors.

The multi -computer system is deployed, which includes baits and traps integrated at the corporate network nodes. This allows you to create a scaled environment for comprehensive threat analysis and effective risk management. Thanks to the modular approach, both

centralized and decentralized architecture of the multi -gault system of baits have been implemented. In the centralized version, all collected data are transmitted to the central device of the network, where their comprehensive analysis is carried out, including statistical and behavioral. For this purpose, a data collection, processing and correlation system has been developed, which allows you to get a holistic picture of cyber threats in the network. On the basis of these data, the mechanism of training of machine learning models is implemented that allow you to predict potential attack vectors and automatically adapt the security system to new threats.

A flexible bait management system is introduced, which makes it easy to change the parameters of work, adapt the behavior of individual elements of the network and respond promptly to new threats. The whole system operates in constant self -study mode, which allows it to improve the algorithms of work without administrator intervention. This has created a dynamic corporate network protection system that is capable not only of real -time threats, but also proactively prevent potential attacks.

Keywords: malicious software, computer attacks, baits, traps, multi-agent system, multi-computer system

Постановка проблеми

Розроблення нових комп'ютерних вірусів та нових типів комп'ютерних атак продовжує здійснюватись. Напрями застосування зловмисного програмного забезпечення (ЗПЗ) та комп'ютерних атак (КА) змінюються. Зокрема, в мобільні пристрої [1], в пристрої IoT [2]. Все це демонструє розширення напрямів атак для зловмисників. Одним з напрямів є створення ботнет [3]. Така різноманітність не тільки типів ЗПЗ та КА, але й типів комп'ютерних систем, на які спрямовують свої зусилля зловмисники вимагає винахідливості від розробників систем попередження, виявлення та протидії ЗПЗ та КА. Одним з перспективних напрямів на фоні зростання загроз є розроблення обманних систем з приманками та пастками [4, 5].

При розробленні приманок та пасток для їх застосування в корпоративних мережах потрібно розроблення ефективних методів та засобів їх організації та синтезу [4]. Одним із перспективних напрямів при їх розробленні є розроблення мереж інтелектуальних приманок та пасток, при розробленні яких би використовувались технології мультиагентних систем.

Аналіз останніх досліджень і публікацій

Виявлення ЗПЗ та комп'ютерних атак КА потребує подальшого удосконалення систем. Для корпоративних мереж проблема виявлення ЗПЗ та КА залишається актуальному і перспективним для них є застосування систем кіберобману [4, 5] на основі приманок і пасток з використанням технологій мультиагентних систем. Сучасні системи захисту повинні бути інтелектуальними, адаптивними та здатними випереджати зловмисників.

В роботі [6] представлено високорівневу архітектуру системи захисту, яка використовує кіберобман для забезпечення стійкості та живучості системи в умовах наявності атак, помилок та інших інцидентів. Не існує єдиної deception стратегії, яка відповідала б усім конфігураціям та цілям цільової системи. В роботі [7] система захисту із централізованим підходом на основі приманок із програмно визначеним перемиканням. В роботі [8] запропоновано проактивну deception систему, яка складається з пасток різних типів, мережевої системи приманок та операційного центру безпеки. В роботі [9] для забезпечення динамічної конфігурації та зменшення ефективності неперервних розвідувальних атак зловмисників розроблену удосконалену систему захисту рухомих цілей на основі програмно визначених мереж, яка використовує топологію віртуальної мережі для заплутування цільової мережі. В роботі [10] подано розроблену гнучку систему керування віртуальною мережею приманок, яка динамічно створюється, конфігурується та розгортається з приманками низького та високого рівня взаємодії, які емулюють декілька операційних систем.

Використання контейнерів є ефективним для створення гнучкої інфраструктури для приманок [11]. В роботі [12] фреймворк, що використовує методи контейнеризації та призначений для динамічного створення мереж приманок, забезпечує оманливе середовище для зловмисника.

Розробка адаптивних методів кіберобману в реальних мережах є надзвичайно складним завданням через суттєві зусилля, необхідні для реалізації основних функцій конфігурування мережевої інфраструктури, необхідних для підтримки проактивного обману, що включає в себе аналіз, планування та розгортання ресурсів обманних об'єктів в реальному часі. В роботі [13] розроблено фреймворк активного кіберобману, який має розширений API та механізми синтезу для розробки засобів захисту із обманними об'єктами та дозволяє спостерігати за діями зловмисника, створювати стратегії обману та розгортати їх шляхом автоматичного керування конфігурацією мережі. В роботі [14] подано адаптивну систему кіберобману, що генерує унікальні мережеві представлення віртуальної мережі, яка не відображає конфігурацію фізичної мережі кожному хосту корпоративної мережі та змінює вигляд мережі хостів в реальному часі, що запобігає розвідці скомпрометованих зловмисником вузлів.

В роботі [15] розглянуто ефективний кіберобман, що включає як активні, так і пасивні методи. Засоби пасивного обману використовують інфраструктуру та системи приманок для виявлення розвідки та атак зловмисників. Оскільки дослідження інформаційної системи є першими кроками зловмисника в процесі атаки на інформаційну систему, її виявлення дає можливість активним засобам захисту швидко ідентифікувати зловмисні дії та вжити заходів. Засоби активного кіберобману застосовують стратегії обману та виконують дії у відповідь на дії зловмисників, передбачають поведінку зловмисників та запобігають успішному завершенню атак. В роботі [16] система активного захисту на основі технології приманок з високим рівнем взаємодії та модульного дизайну, що відокремлює середовище приманки від центрального вузла, який керує додаванням, видаленням, зміною приманок, завдяки чому їх легко підтримувати та оновлювати.

Застосування штучного інтелекту є перспективним при створенні обманних систем. В роботі [17] в сучасних deception системах використовуються більш точні способи розпізнавання зловмисної діяльності на основі технологій поведінкової аналітики користувачів, великих даних, штучного інтелекту. В роботі [18] запропоновано комплексний deception фреймворк, який має декілька рівнів, призначених для впровадження та підтримки deception механізмів, що забезпечує використання методів штучного інтелекту на всіх етапах захисту системи, а саме запобіганні, виявленні та реагуванні на зловмисні дії.

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 мультикомп'ютерних систем інтелектуальних приманок та пасток з використанням мультиагентних технологій для забезпечення автоматизації їх використання в процесах виявлення ЗПЗ та КА.

Виклад основного матеріалу

Мережа приманок здійснює комплексний захист комп'ютерної мережі. Вона включає приманки, які моніторять тільки зловмисний трафік, тому може забезпечити максимально швидке його виявлення, а також виявлення патернів нових атак. Мультиагентна система приманок представляє собою множину приманок різного типу. Приманки системи є інтелектуальними, мають ознаки інтелектуального агенту, володіють автономною та гнучкою поведінкою, що передбачає наявність таких характеристик:

1) реактивність – інтелектуальна приманка здатна сприймати середовище, в якому вона працює, та своєчасно реагувати на зміни, які в ньому відбуваються, відповідно до цілей функціонування;

2) проактивність – інтелектуальна приманка здатна проявляти цілеспрямовану поведінку, що передбачає прояв ініціативи, відповідно до цілей функціонування;

3) соціальні можливості – інтелектуальна приманка здатна взаємодіяти з іншими приманками (та іншими пристроями) системи відповідно до цілей функціонування.

Розглянемо формування мережевого середовища та його використання. Мультиагентна система приманок володіє колективною поведінкою, яка передбачає, що приманки, як інтелектуальні агенти, схильні до кооперування. Кожна приманка мережі відслідковує мережевий трафік (кількість запитів, відкритих з'єднань, спроб несанкціонованого доступу, об'єм переданих пакетів тощо). Це є середовище, в якому функціонує конкретна приманка (рис. 1). Це середовище є розподіленим і, тому, потребує розроблення системи підтримки та організації функціонування. Така сукупність приманок розгортається в багатьох вузлах корпоративної мережі і, таким чином, формується мультикомп'ютерна система з приманками і пастками.

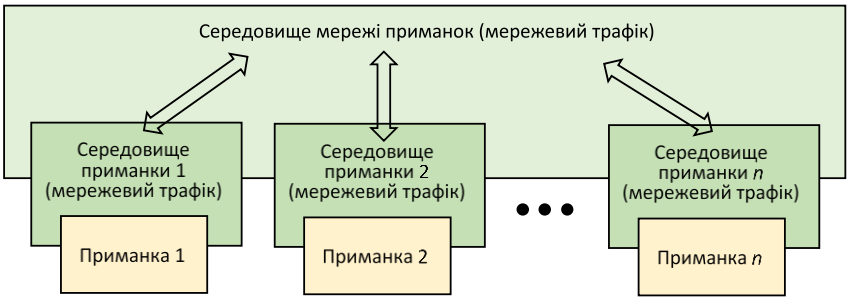

Рис. 1. Середовище мережі приманок

Сумарний мережевий трафік приманок складається з трафіку індивідуальних приманок і представляє собою середовище, в якому функціонує мережа приманок. Для формування сумарного трафіку передбачається взаємодія між приманками. Тобто, приманка фіксує мережевий трафік, який надходить на неї, далі передає його мережі та використовує локально (рис.2).

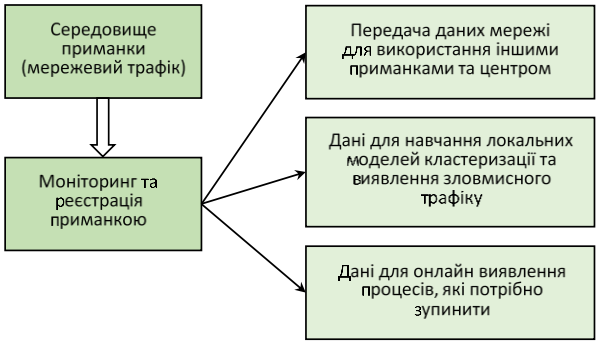

Рис. 2. Схема моніторингу та реєстрації даних приманкою

Локальне використання даних мережевого трафіку передбачає навчання моделей кластеризації патернів атак, навчання моделей виявлення процесів, які необхідно зупинити, онлайн виявлення процесів, які потрібно зупинити. Тобто, приманка сама визначає критерії, що процес потрібно зупинити.

Мультиагентна система приманок може бути як централізована, так і децентралізована. У випадку централізованої мультиагентної системи приманок мережевий трафік передається на центральний пристрій мережі (рис. 3). В центральному пристрої виконується організація і аналіз даних, в тому числі статистичний. Ці дані використовуються для навчання моделей, які працюють з даними всієї мережі.

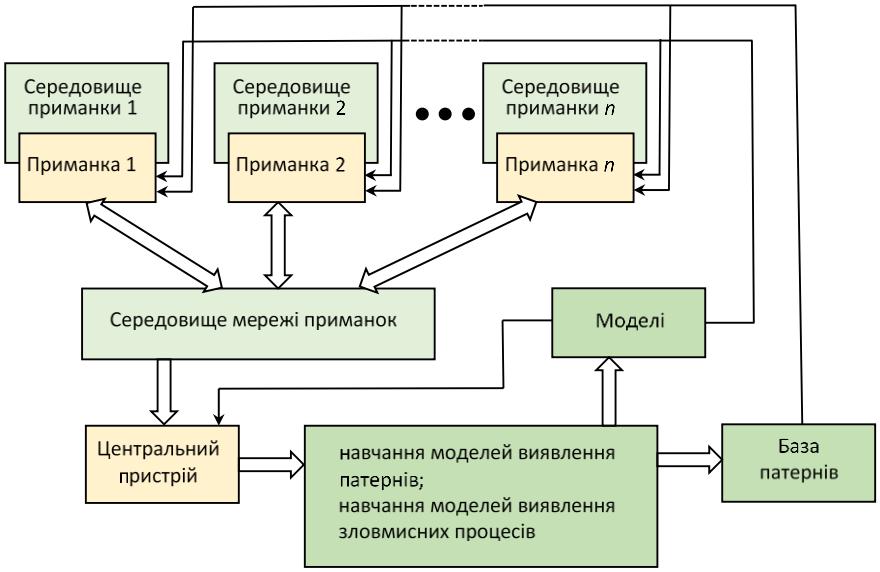

Рис. 3. Архітектура мультиагентної системи інтерактуальних приманок

Цілі функціонування мережі приманок визначаються при її проектуванні. У випадку автономної роботи, тобто роботи без втручання оператора, робота приманки характеризується інтегральною цільовою функцією, яка відображає стан приманки. Кожна подія, яка відбувається в середовищі, впливає на цю цільову функцію. Інтегральна цільова функція (функція винагороди) розраховується на основі набору показників. Наприклад, інтегральна функція у вигляді вектору, яка враховує ряд показників:

$$R_H = (N_d, N_i, t_d, t_i, M, P), \quad (1)$$

де N_d - кількість виявлених зловмисних подій; N_i - кількість ідентифікованих зловмисних подій; t_d - середній час виявлення зловмисної події; t_i - середній час ідентифікації зловмисної події; M - пам'ять, яка використовується приманкою, для виявлення зловмисної події; P - потужність процесора, яка використовується приманкою, для виявлення зловмисної події.

Функціонування приманки повинно бути ефективним, необхідно витримувати компроміс між кількістю виявлених подій та споживаними ресурсами. При визначені набору показників слід також враховувати ступень захищеності комп'ютерної мережі, якого необхідно досягти. Критично важливі сервіси та збереження конфіденційності інформації потребують високого ступеню захищеності комп'ютерної мережі, тому витрати надлишкових обчислювальних ресурсів виправдані.

Цільова функція мережі приманок формується на основі цільових функцій окремих приманок:

$$R_{NH} = R_{H1} + R_{H1} + \cdots R_{Hn}, \quad (2)$$

де R_{NH} - цільова функція мережі, R_{Hn} - цільова функція n-ої приманки.

Цільова функція кожної приманки в мультиагентній системі формується таким чином, щоб сумарна цільова функція була максимальна.

Кількість приманок мережі та їх тип може змінюватися, конфігурування системи відбувається відповідно до цільової функції. Конфігурування системи відбувається на всіх етапах функціонування та передбачає визначення:

1) кількості активних приманок системи;
2) типів активних приманок системи;
3) конфігурацію зв'язків між приманками.

Задачі, які ставляться перед приманкою:

1) збір та аналіз виключно зловмисного трафіку на приманці;
2) робота в режимі тіньової приманки – аналіз трафіку робочого сервісу.

Мережа містить приманки, які виконують ці функції. Одна приманка може виконувати тільки одну з цих функцій або всі. Частина приманок є активними постійно, частина активується за певних умов, відповідно до індикаторів мережі приманок. Функціонування мережі приманок відбувається відповідно до цільової функції, яка включає набір індикаторів, наприклад, з переліку в табл. 1.

Таблиця 1

Індикатори мережі приманок

Індикатори рівня небезпеки середовища	
N_{at_s}	Кількість зловмисних джерел
N_{at_ns}	Кількість нових зловмисних джерел
$N_{at\_ns\_IP}$	Кількість зловмисних джерел в певній IP агрегації
N_{at_r}	Кількість зловмисних запитів
N_{at_p}	Кількість пакетів, прийнятих від зловмисних джерел
N_{at_em}	Кількість електронних повідомлень, отриманих від зловмисних джерел
V_{at_em}	Об'єм електронного повідомлення, отриманого від зловмисного джерела
N_{at_sess}	Кількість сесій зловмисного джерела
t_{at_sess}	Тривалість сесії зловмисного джерела
t_{at_l}	Час «життя» зловмисного джерела
t_{at_p}	Кількість атакованих портів
Індикатори рівня захищеності системи	
$N_{id\_at\_s}$	Кількість виявлених зловмисних джерел
$t_{id\_at\_s}$	Час виявлення зловмисного джерела
Індикатори споживання ресурсів	
L_{cpu}	Завантаження центрального процесора
L_{gpu}	Завантаження графічного процесора
V_m	Обсяг пам'яті, що використовується

До цих індикаторів входять такі, що відображають ступінь захищеності системи (кількість виявлених зловмисних дій, швидкість їх виявлення тощо), а також рівень небезпеки середовища (трафіку), відсоток кількості зловмисних запитів відносно нормальних, швидкість надходження зловмисних запитів тощо.

Множина індикаторів приманки, яка відображає рівень загрози середовища включає ряд показників, зокрема $R_{H_{at}} = \{N_{at}, t_{at}, \dots\}$, де N_{at} – кількість зловмисних запитів в трафіку приманки, t_{at} – середній час надходження зловмисного запиту. Ця множина є підмножиною цільової функції приманки R_H. Для кожного індикатора встановлюються порогові рівні, досягнення яких потребує відповідних дій приманки.

Мережа приманок складається з N приманок, з яких N_{base} – число основних постійно діючих приманок. Постійно діючі приманки є багатофункціональними приманками (агентами) високого рівня взаємодії. Передбачається, що мережа може функціонувати як централізована або децентралізована. В якості центрального пристрою обирається одна з постійно діючих приманок. У випадку наявності постійно діючих приманок більше однієї, центр може мігрувати між цими приманками.

Розглянемо приманки в контексті інтелектуальних агентів.

Приманка як агент працює в швидко змінюваному та непередбачуваному середовищі.

Тіньова приманка працює паралельно з основним сервісом. Робота може бути організована в 2 варіантах:

1) на приманку надходить той же трафік, який надходить на робочий сервіс;

2) на приманку надходить тільки той трафік, який визначений СВВ (IDS) як підозрілий (зловмисний).

На приманці проводиться аналіз трафіку для виявлення аномалій в онлайн режимі. Приманка містить множину моделей, призначених для виявлення аномалій (детекторів аномалій) $M_a = \{m_{a1}, m_{a2}, \dots, m_{an}\}$. Моделі можуть працювати одночасно або вибірково. В результаті роботи набору детекторів аномалій отримують множину виявлених аномалій $O = \{o_1, o_2, \dots, o_n\}$. Приманка може працювати в таких режимах: автономний; режим керування адміністратором; змішаний режим.

На приманці зберігається попередня інформація про множину патернів атак $P = \{p_1, p_2, \dots, p_n\}$. Патерни атак отримують з різних джерел:

1) автоматичної системи виявлення патернів (різного типу моделі кластеризації даних, отриманих приманками, які працюють тільки із зловмисним трафіком);

2) інструкції адміністратора.

Середовище, в якому функціонує приманка, характеризується мережевим трафіком, і представляє собою множину послідовностей станів $S^* = \{S_1^*, S_2^*, \dots, S_n^*\}$. Передбачається, що в будь-який момент часу середовище знаходиться в одному з цих станів.

Приманка приймає рішення з множини рішень $D = \{d_1, d_2, \dots, d_n\}$. Приклади рішень: d_1 – нормальний трафік; d_2 – аномальний трафік, є збіги з екземплярами множини патернів; d_3 – аномальний трафік, немає збігів з множиною патернів, і т.п.

На основі рішень приманка виконує відповідну дію/дії з множини дій $A = \{a_1, a_2, \dots, a_n\}$. Приклади дій: a_1 – продовжити виконання процесу; a_2 – призупини процес для подальшого аналізу; a_3 – зупинити процес, і т.п.

Таким чином, функціонування приманки розглядається як функція:

$$S^* \to D \to A. \quad (3)$$

Рішення приймаються на основі досвіду, який враховує власний досвід. На основі власного досвіду приманки можливі таки варіанти рішень:

1) оптимальне рішення на основі власного досвіду;

2) неоптимальне рішення на основі власного досвіду;

3) неможливо прийняти будь-яке рішення на основі власного досвіду.

Кожній окремій приманці, як агенту, може не вистачати досвіду (набору знань), яким вона володіє для прийняття оптимального рішення, або рішення взагалі. Тому, доцільна взаємодія з іншими приманками мереж.

Важливо визначити кінцеву ціль, якої повинна досягати приманка. Оптимальним рішенням та оптимальною дією є ті, які підвищують функцію винагороди приманки. Цільова функція винагороди відображає що приманка як агент функціонує в оптимальний спосіб. В процесі роботи на кожному кроці функція винагороди є числом R_t. Робота приманки оптимізується таким чином, щоб забезпечити максимум цільової функції винагороди при тривалій роботі приманки. Приріст функції винагороди має відображати кінцевий результат роботи приманки (наприклад, виявлення аномального трафіку).

Інтегральна функція винагороди на тривалому проміжку роботи приманки отримується з цільових функцій винагороди на кожному кроці. Для інтеграції можуть бути використані різні способи, зокрема усереднена адитивна інтегральна функція винагороди:

$$C_R = \frac{R_{t+1} + R_{t+2} + \cdots + R_{t+n}}{n} = \frac{1}{n}\sum_{i=1}^{n} R_{t+i}, \quad (4)$$

де R_{t+i} – значення функції винагороди на i-ому кроці; n – кількість кроків, на яких визначається інтегральна цільова функція винагороди.

Цільова функція винагороди визначає кількісно внесок приманки в підвищення захищеності комп'ютерної мережі та повинна враховувати такі чинники:

1) виявлення зловмисного трафіку та зупинка процесу призводить до збільшення функції винагороди;

2) виявлення хибно-позитивного зловмисного трафіку призводить до зменшення функції винагороди;

3) збільшення часу виявлення зловмисного трафіку призводить до зменшення функції винагороди.

Після виявлення аномалія o_i порівнюється з множиною заданих патернів P. Якщо аномалія збігається з патерном, цільова функція винагороди збільшується на число $k_r r$, де r – винагорода, k_r – коефіцієнт, який враховує час виявлення. Якщо аномалія не збігається з жодним патерном, то функція винагороди залишається незмінною, а дані аномалії зберігаються для подальшого аналізу адміністратором (в режимі адміністратора чи змішаному режимі) або самою приманкою з появою додаткової інформації. Такою додатковою інформацією є оновлення патернів атак. Якщо такий додатковий аналіз дозволяє підтвердити аномалію, то функція винагороди збільшується. Якщо аномалія визначається як нормальний трафік, то функція винагороди зменшується на число w. Таким чином, на кожному кроці цільова функція винагороди визначається як:

$$R_t = p_r \cdot k_r r - p_w \cdot w, \quad (5)$$

де p_r – ймовірність винагороди, p_w – ймовірність стягнення.

Архітектура приманки як інтелектуального агенту описує: дані; рішення, які приймає приманка; дії, які виконує приманка (рис. 4).

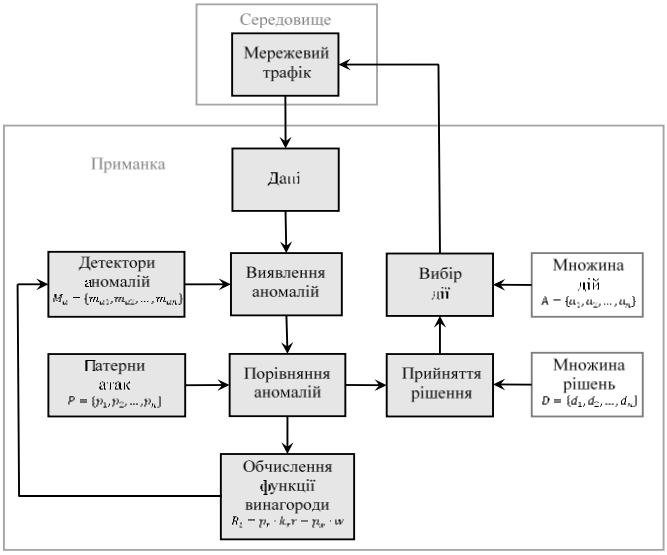

Рис. 4. Архітектура приманки як інтелектуального агенту

За наявності скінченого переліку трійок «стан середовища – рішення – дія» (рис. 4) приманка навчається оптимальній стратегії поведінки, яка приводить до зростання інтегральної функції винагороди. Але в умовах реального мережевого трафіку множина послідовностей станів S^* містить велику кількість послідовностей та є невизначеною, тому немає можливості отримати чітку відповідність $S^* \to D$. Крім того, для генерації оптимальних стратегій необхідні провести значні обсяги обчислень, що є ще одним суттєвим обмеженням в умовах онлайн режиму роботи приманки. Тому, для отримання функцій залежності $D(S^*)$ необхідно використовувати апроксимацію за допомогою моделей виявлення аномалій. Модель виявлення аномалій мережевого трафіка є моделлю, яка навчається з підкріпленням.

Висновки

Розроблено механізм колективної поведінки в мультиагентній системі приманок, що дає змогу створювати динамічні сценарії реагування на загрози. Запроваджено систему моніторингу мережевого трафіку, яка дозволяє аналізувати кількість запитів, відкритих з'єднань, спроби несанкціонованого доступу, об'єм переданих пакетів та інші критичні параметри мережевої активності. Всі ці дані використовуються для оперативного виявлення аномальної активності та своєчасного блокування загроз. Крім того, забезпечено розроблення та впровадження розподіленого середовища функціонування приманок, яке дозволяє масштабувати систему відповідно до потреб корпоративної мережі. Для цього створено спеціалізовану систему підтримки та організації функціонування приманок, що включає механізми самонавчання та адаптації до змін в інфраструктурі мережі.

Напрямами подальших досліджень є розроблення архітектури мультикомп'ютерних систем, їх позиціонування в корпоративних мережах та зв'язок з інтелектуальними приманками та пастками.

Література

1. Nicheporuk, A., Savenko, O., A. Nicheporuk, and Y. Nicheporuk. 2020. An android malware detection method based on CNN mixed-data model. *CEUR Workshop Proceedings* Kharkiv, Ukraine. 2732:198–213.

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. 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

4. 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

5. 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

6. Mehresh, R., Upadhyaya, S.J. (2016). Deception-Based Survivability. In: Chang, CH., Potkonjak, M. (eds) Secure System Design and Trustable Computing. Springer, Cham. https://doi.org/10.1007/978-3-319-14971-4_17

7. Baykara, Muhammet & Das, Resul. (2019). SoftSwitch: a centralized honeypot-based security approach usingsoftware-defined switching for secure management of VLAN networks. TURKISH JOURNAL OF ELECTRICAL ENGINEERING & COMPUTER SCIENCES. 27. 3309-3325. 10.3906/elk-1812-86.

8. Khoa, N.H., Do Hoang, H., Ngo-Khanh, K., Duy, P.T., Pham, VH. (2023). SDN-Based Cyber Deception Deployment for Proactive Defense Strategy Using Honey of Things and Cyber Threat Intelligence. In: Dao, NN., Thinh, T.N., Nguyen, N.T. (eds) Intelligence of Things: Technologies and Applications. ICIT 2023. Lecture Notes on Data Engineering and Communications Technologies, vol 188. Springer, Cham. https://doi.org/10.1007/978-3-031-46749-3_26

9. C. Gao, Y. Wang, X. Xiong and W. Zhao, "MTDCD: an MTD Enhanced Cyber Deception Defense System," 2021 IEEE 4th Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), Chongqing, China, 2021, pp. 1412-1417, doi: 10.1109/IMCEC51613.2021.9482133.

10. Fan, Wenjun & Fernández, David & Du, Zhihui. (2015). Adaptive and Flexible Virtual Honeynet. 10.1007/978-3-319-25744-0_1.

11. D. Sever and T. Kišasondi, "Efficiency and security of docker based honeypot systems," 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 2018, pp. 1167-1173, doi: 10.23919/MIPRO.2018.8400212.

12. Ravi, Akash & Sharma, Bhavye & Mukherjee, Avigyan. (2023). A Cloud-Native Honeynet Automation and Orchestration Framework. 10.31219/osf.io/xkqzr.

13. M. M. Islam and E. Al-Shaer, "Active Deception Framework: An Extensible Development Environment for Adaptive Cyber Deception," 2020 IEEE Secure Development (SecDev), Atlanta, GA, USA, 2020, pp. 41-48, doi: 10.1109/SecDev45635.2020.00023.

14. Chiang, C.J., Gottlieb, Y.M., Sugrim, S., Chadha, R., Serban, C., Poylisher, A., Marvel, L.M., & Santos, J. (2016). ACyDS: An adaptive cyber deception system. MILCOM 2016 - 2016 IEEE Military Communications Conference, pp. 800-805. doi: 10.1109/MILCOM.2016.7795427.

15. Underbrink, A.J. (2016). Effective Cyber Deception. In: Jajodia, S., Subrahmanian, V., Swarup, V., Wang, C. (eds) Cyber Deception. Springer, Cham. https://doi.org/10.1007/978-3-319-32699-3_6

16. Xingyuan Yang & Jie Yuan & Hao Yang & Ya Kong & Hao Zhang & Jinyu Zhao, 2023. "A Highly Interactive Honeypot-Based Approach to Network Threat Management," Future Internet, MDPI, vol. 15(4), pages 1-31, March. https://doi.org/10.3390/fi15040127

17. William Steingartner, Darko Galinec, Andrija Kozina. Threat Defense: Cyber Deception Approach and Education for Resilience in Hybrid Threats Model. Symmetry 2021, 13(4), 597; https://doi.org/10.3390/sym13040597

18. Beltrán, Pedro & Pérez, Manuel & Nespoli, Pantaleone. (2024). Cyber Deception: State of the art, Trends and Open challenges. 10.48550/arXiv.2409.07194.

References

1. Nicheporuk, A., Savenko, O., A. Nicheporuk, and Y. Nicheporuk. 2020. An android malware detection method based on CNN mixed-data model. *CEUR Workshop Proceedings* Kharkiv, Ukraine. 2732:198–213.

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. 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

4. 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

5. 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

6. Mehresh, R., Upadhyaya, S.J. (2016). Deception-Based Survivability. In: Chang, CH., Potkonjak, M. (eds) Secure System Design and Trustable Computing. Springer, Cham. https://doi.org/10.1007/978-3-319-14971-4_17

7. Baykara, Muhammet & Das, Resul. (2019). SoftSwitch: a centralized honeypot-based security approach usingsoftware-defined switching for secure management of VLAN networks. TURKISH JOURNAL OF ELECTRICAL ENGINEERING & COMPUTER SCIENCES. 27. 3309-3325. 10.3906/elk-1812-86.

8. Khoa, N.H., Do Hoang, H., Ngo-Khanh, K., Duy, P.T., Pham, VH. (2023). SDN-Based Cyber Deception Deployment for Proactive Defense Strategy Using Honey of Things and Cyber Threat Intelligence. In: Dao, NN., Thinh, T.N., Nguyen, N.T. (eds) Intelligence of Things: Technologies and Applications. ICIT 2023. Lecture Notes on Data Engineering and Communications Technologies, vol 188. Springer, Cham. https://doi.org/10.1007/978-3-031-46749-3_26

9. C. Gao, Y. Wang, X. Xiong and W. Zhao, "MTDCD: an MTD Enhanced Cyber Deception Defense System," 2021 IEEE 4th Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), Chongqing, China, 2021, pp. 1412-1417, doi: 10.1109/IMCEC51613.2021.9482133.

10. Fan, Wenjun & Fernández, David & Du, Zhihui. (2015). Adaptive and Flexible Virtual Honeynet. 10.1007/978-3-319-25744-0_1.

11. D. Sever and T. Kišasondi, "Efficiency and security of docker based honeypot systems," 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 2018, pp. 1167-1173, doi: 10.23919/MIPRO.2018.8400212.

12. Ravi, Akash & Sharma, Bhavye & Mukherjee, Avigyan. (2023). A Cloud-Native Honeynet Automation and Orchestration Framework. 10.31219/osf.io/xkqzr.

13. M. M. Islam and E. Al-Shaer, "Active Deception Framework: An Extensible Development Environment for Adaptive Cyber Deception," 2020 IEEE Secure Development (SecDev), Atlanta, GA, USA, 2020, pp. 41-48, doi: 10.1109/SecDev45635.2020.00023.

14. Chiang, C.J., Gottlieb, Y.M., Sugrim, S., Chadha, R., Serban, C., Poylisher, A., Marvel, L.M., & Santos, J. (2016). ACyDS: An adaptive cyber deception system. MILCOM 2016 - 2016 IEEE Military Communications Conference, pp. 800-805. doi: 10.1109/MILCOM.2016.7795427.

15. Underbrink, A.J. (2016). Effective Cyber Deception. In: Jajodia, S., Subrahmanian, V., Swarup, V., Wang, C. (eds) Cyber Deception. Springer, Cham. https://doi.org/10.1007/978-3-319-32699-3_6

16. Xingyuan Yang & Jie Yuan & Hao Yang & Ya Kong & Hao Zhang & Jinyu Zhao, 2023. "A Highly Interactive Honeypot-Based Approach to Network Threat Management," Future Internet, MDPI, vol. 15(4), pages 1-31, March. https://doi.org/10.3390/fi15040127

17. William Steingartner, Darko Galinec, Andrija Kozina. Threat Defense: Cyber Deception Approach and Education for Resilience in Hybrid Threats Model. Symmetry 2021, 13(4), 597; https://doi.org/10.3390/sym13040597

18. Beltrán, Pedro & Pérez, Manuel & Nespoli, Pantaleone. (2024). Cyber Deception: State of the art, Trends and Open challenges. 10.48550/arXiv.2409.07194.