Харківський національний університет імені В.Н. Каразіна

Факультет комп'ютерних наук

Безпека інформаційних систем і технологій

«Допущено до захисту»

Зав. кафедрою БІСТ

Сватовський І.І._____

« » червня 2023р.

Пояснювальна записка

до кваліфікаційної роботи бакалавра

спеціальність: 125 Кібербезпека

на тему: «Застосування теорії ігор захисту комп'ютерних систем»

оцінка « »

Керівник Нарєжній О.П.

(прізвище та ініціали/підпис)

Голова ЕК

Рецензент Осипчук А.В.

(прізвище та ініціали/підпис)

Лемешко О.В._____

Виконавець студентка групи КБ-41

Білюк А.О.

(прізвище та ініціали/підпис)

Харків – 2023

РЕФЕРАТ

Пояснювальна записка містить 69 сторінки, 11 рисунків, 18 джерел.

Метою дипломної роботи є дослідження вливу на застосування теорії ігор в захисті комп'ютерних систем, теоретичних методів ігрових застосувань в кібербезпеці, зокрема безпеці фізичного рівня, самоорганізованій безпеці мережі, виявленню та запобіганню вторгненням, збереженню конфіденційності та анонімності, економіці кібербезпеки та безпеці хмарних обчислень.

Об'єктом дослідження дипломної роботи є визначення гри та рівноваги Неша, зв'язок між теорією ігор та кібербезпекою, основні аспекти теорії ігор, включаючи визначення та типологію ігор.

Методи дослідження: аналіз теоретичних підходів до гри та рівноваги Неша, їх застосування в контексті кібербезпеки та виявлення можливого зв'язку між ними, розгляд основної концепції теорії ігор, їх визначення та принципи, дослідження типології ігор, що дозволяє класифікувати їх за різними критеріями, такими як кількість учасників, характер взаємодії та стратегічні елементи.

Результатами проведеної роботи є знаходження впливу теорії ігор у різних сферах життя, та приведення прикладів застосування, можливості поєднання теорії ігор і криптографії, а також майбутні напрямки досліджень у цій області.

Ключові слова: КІБЕРБЕЗПЕКА, ТЕОРІЯ ІГОР, РІВНОВАГА НЕША, БЕЗПЕКА ФІЗИЧНОГО РІВНЯ, САМООРГАНІЗОВАНА БЕЗПЕКА МЕРЕЖІ, ВИЯВЛЕННЯ ВТОРГНЕННЯ, КОНФІДЕНЦІЙНІСТЬ, АНОНІМНІСТЬ, ЕКОНОМІКА КІБЕРБЕЗПЕКИ, ХМАРНІ

ОБЧИСЛЕННЯ, КРИПТОГРАФІЯ, МАЙБУТНІ НАПРЯМКИ ДОСЛІДЖЕНЬ, ЗАСТОСУВАННЯ ТЕОРІЇ ІГОР У ЗАХИСТІ КОМП'ЮТЕРНИХ СИСТЕМ.

ABSTRACT

The explanatory note consists of 69 pages, 11 figures, and 18 sources.

The aim of this diploma thesis is to investigate the impact of game theory in the protection of computer systems, theoretical methods of game-based applications in cybersecurity, including physical security, self-organized network security, intrusion detection and prevention, confidentiality and anonymity preservation, cybersecurity economics, and cloud security.

The subject matter is the definition of game and Nash equilibrium, the connection between game theory and cybersecurity, the fundamental aspects of game theory, including the definition and typology of games.

The research methods include analyzing theoretical approaches to games and Nash equilibrium, their application in the context of cybersecurity and exploring the main concepts of game theory, their definitions, principles, and studying the typology of games that allows classifying them based on different criteria, such as the number of participants, interaction nature, and strategic elements.

The results of the conducted work include finding the influence of game theory in various spheres of life, providing examples of application, possibilities of combining game theory and cryptography, and future research directions in this field.

Keywords: CYBERSECURITY, GAME THEORY, NASH EQUILIBRIUM, PHYSICAL SECURITY, SELF-ORGANIZED NETWORK SECURITY, INTRUSION DETECTION, CONFIDENTIALITY, ANONYMITY, CYBERSECURITY ECONOMICS, CLOUD COMPUTING, CRYPTOGRAPHY,

FUTURE RESEARCH DIRECTIONS, APPLICATION OF GAME THEORY IN COMPUTER SYSTEMS PROTECTION.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, ТЕРМІНІВ

ІТС	-	Інформаційно-телекомунікаційні системи
APT	-	Advanced Persistent Threats
ККТ	-	Криптографічна ключова технологія
MANETs	-	Mobile ad hoc networks
IDS	-	Intrusion Detection System
IPS	-	Intrusion Prevention System
VPN	-	Virtual Private Network
IoT	-	Internet-of-Things
D2D	-	Device-to-Device

ВСТУП

Захист інформаційно-телекомунікаційних систем від кібератак постає як нагальна національна проблема, оскільки сучасні кіберзлочинці все частіше намагаються викрасти кошти та конфіденційну інформацію, а кібертерористи створюють загрозу безпеці громадян та країни в цілому. Отже, важливо мінімізувати ризики, пов'язані з різноманітними кібератаками.

Для прийняття рішень щодо безпеки інформаційно-комунікаційних систем широко використовуються ігрові методи, які дозволяють аналізувати операційний контент системи і ефективно вирішувати питання інвестицій у безпеку телекомунікаційних мереж. Використання теорії ігор дозволяє отримати набір засобів безпеки, які є паретооптимальними з точки зору кількісних параметрів кібер-ризику та витрат на інвестиції. Ці оптимальні засоби дозволяють службам захисту вибрати набір заходів, які найкраще знижують загальний кібер-ризик з урахуванням рівня інвестицій у систему безпеки. Таким чином, забезпечується рентабельність інвестицій у безпеку мережі.

Модель кібербезпеки, заснована на теорії ігор, дозволяє розглядати захист мережі з цілісного погляду - від розуміння мети функціонування ІТС до відбиття всіх можливих атак. Важливо враховувати реакцію порушника на захисні заходи, оскільки для кожної дії, спрямованої на поліпшення безпеки системи, порушник може вибрати найбільш доцільний наступний крок.

Необхідно підкреслити, що практична реалізація ідеї використання ігрових методів у кібербезпеці вимагає кількісної оцінки кіберризику в системі. Для цього необхідно збирати інформацію та формалізувати ризики, що пов'язані з інформаційною системою, та створити модель топології інформаційної системи та модель потенційних кіберзагроз.

Сучасні комунікаційні технології, як і інформація, стрімко прогресують з точки зору різноманітності та рівня своєї складності. Зростаючий зв'язок, поширеність і складність сучасних інформаційних систем створюють нові виклики безпеці, а кіберпростір стає ігровим майданчиком для людей з різними рівнями навичок і намірами – позитивними чи негативними. Таким чином, захист активів, ідентичності та інформації набуває все більшого значення, оскільки постійний зв'язок став невід'ємною частиною повсякденного життя людей. Крім того, соціальний добробут і економічний прогрес нації все більше залежать від кіберпростору. Збільшення взаємозв'язку, а також збільшення доступності обчислювальних ресурсів для зловмисників, пропонує їм можливість для складних, непередбачуваних і розподілених атак. Таким чином, зловмисники можуть спричинити збої в критичній інфраструктурі, включаючи фінансові мережі, телекомунікації, енергетичні трубопроводи, електроенергія, нафтопереробні заводи тощо. Останні події показують шкоду, яку кібератаки можуть завдати приватним підприємствам, урядам і громадськості в цілому з точки зору репутації, конфіденційності даних і грошей. Більше двадцяти років наукове співтовариство приділяє увагу сфері безпеки кіберпростору. Тим не менш, питання кібербезпеки досі не вирішено повністю. У цій роботі досліджено застосовність теоретико-ігрових методів у вирішенні проблем кібербезпеки.

Продовжуючи наші досягнення, ми досягли традиційних методів безпеки в захисті чітко визначених цілей, а саме. конфіденційність, цілісність і доступність. Криптографія є однією з таких сильних теоретичних основ безпеки, яка залежить від секретності криптографічного ключа. Але, як і в атаках соціальної інженерії або Advanced Persistent Threats (APT), де зловмисники викрадають цілі криптографічні ключі, припущення про конфіденційність ключів порушується, що призводить до проникнення в системи. Потрібна нова теоретична основа та інноваційна перспектива для

охоплення сценаріїв, коли зловмисники можуть повністю скомпрометувати системи, а захисники можуть захистити системи без фундаментального припущення секретності ключа.

Обмеженням звичайних рішень безпеки є відсутність кількісної системи прийняття рішень. Таким чином, багато дослідницьких груп почали заохочувати використання методів теорії ігор. Оскільки теорія ігор вирішує проблеми, коли кілька гравців з протилежними цілями змагаються один з одним, вона може запропонувати математичну основу для моделювання та аналізу проблем безпеки мережі.

Моделі, засновані на теорії ігор, є природною структурою для охоплення захисної, а також змагальної взаємодії між гравцями. Теорія ігор може запропонувати кількісну міру якості безпеки, що забезпечується за допомогою концепції рівноваги Неша, де як захисник, так і нападник шукають оптимальні стратегії, і жоден не має стимулу для одностороннього відхилення від своєї стратегії рівноваги, незалежно від їхніх протилежних цілей безпеки. Ця концепція рівноваги додатково, кількісно, передбачає результат безпеки сценарію, який фіксується ігровою моделлю. Теорія ігор, таким чином, забезпечує контрольовану безпеку за допомогою кількісної міри безпеки, на відміну від якісної міри, яку забезпечує криптографічна безпека. Крім того, теоретико-ігровий підхід можна розширити до проектування механізмів, дозволяючи розробникам системи зміщувати рівновагу, а також прогнозований результат на користь захисника, використовуючи складний ігровий дизайн.

Інтерес до теорії ігор і прийняття рішень зріс протягом більш ніж десятиліття, і вона стала добре перевіреною, систематичною, сильною теоретичною основою сучасних досліджень безпеки. Теорія ігор підтримує окрему та економічну перспективу безпеки, яка не така ж, як стандартне визначення, тобто безпека — це не відсутність загроз, а етап, на якому атака

на систему коштує дорожче, ніж неатака. Таким чином, починаючи з теоретико-ігрової основи, ми досягаємо найскладнішого самодостатнього захисту, оцінюючи та генеруючи стимули для заохочення чесної поведінки замість перешкоджання зловмисності. Водночас економічний підхід до безпеки також є важливим, оскільки він аналогічний прогресу зловмисників у наш час. Кіберзлочинність перетворилася на повнофункціональну економіку з підтримкою ланцюгів поставок, чорним маркетингом і здебільшого нагадує незаконний аналог ринку легального програмного забезпечення. Хоча звичайна безпека формує значну основу для вирішення проблеми знизу, теорія ігор забезпечує підхід зверху вниз шляхом прийняття стратегічних та економічних перспектив зловмисників, а також доповнює технологічні методи безпеки. Ідеальна стадія досягається, коли два обрані маршрути сходяться до середини, і це є метою теорії ігор.

Опитування, проведене в рамках цього дослідження, виявило зв’язок між різними типами ігор і різними проблемами безпеки. Приклади включають динамічні ігри для адаптивного захисту безпеки мережі, багаторівневі ігри та ігри Stackelberg для проактивного захисту, дослідження методів розподілу ресурсів з використанням теорії проектування механізмів для економіки безпеки мережі, ігри -теоретичне дослідження концепцій криптографії – автентифікація та конфіденційність, забезпечення та проектування мережі, кількісне управління ризиками безпеки та мережеві ігри для кібер-фізичного захисту інформації забезпечення та безпека критичної інфраструктури.

З точки зору кібербезпеки, новітні застосування теорії ігор до різноманітних тем, що розвиваються, включають безпеку критичної інфраструктури, управління кіберризиками, захист рухомої цілі, інсайдерську загрозу, міжрівневої кіберфізичної безпеки, змагального машинного навчання та кіберобману.

1 ОСНОВИ КІБЕРБЕЗПЕКИ

Перш ніж давати визначення кібербезпеці, необхідно визначити кіберпростір. Згідно з Законом України про основні засади забезпечення кібербезпеки України, «кіберпростір — середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних». Соціальний добробут та економічний розвиток нації тепер залежать від кіберпростору.

Крім того, термін «кібер» також пов'язаний з різними іншими жанрами, наприклад, кібергот асоціюється з музикою; кіберпанк — різновид роману, заснованого на фантастиці; кіберзлочинність включає злочини, скоєні з використанням комп'ютерів, а кібербулінг – це залякування будь-кого в соціальних мережах чи Інтернеті.

Кібербезпека визначена як «захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі». На практиці це означає, що наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів, розглядаються як кіберзагроза. Маніпулювання фізичними активами також вважається загрозою кібербезпеці. Тим не менш, межа між

інформаційною безпекою та кібербезпекою дуже тонка, оскільки проблеми кібербезпеки можуть бути трансформовані в питання інформаційної безпеки в кількох випадках і навпаки. Деякі публічні джерела навіть розглядають обидва терміни як синоніми. Однак кібербезпека передбачає людський фактор - люди як об'єкти кібератак, на відміну від інформаційної безпеки.

Закон України розглядає кібербезпеку як збірний термін різних сфер, які включають захист конституційних прав і свобод людини і громадянина; захист суспільства, сталого розвитку інформаційного суспільства та цифрового комунікативного середовища; захист держави, її конституційного ладу, суверенітету, територіальної цілісності і недоторканності; захист національних інтересів в усіх сферах життєдіяльності особи, суспільства та держави; захист об'єктів критичної інфраструктури.

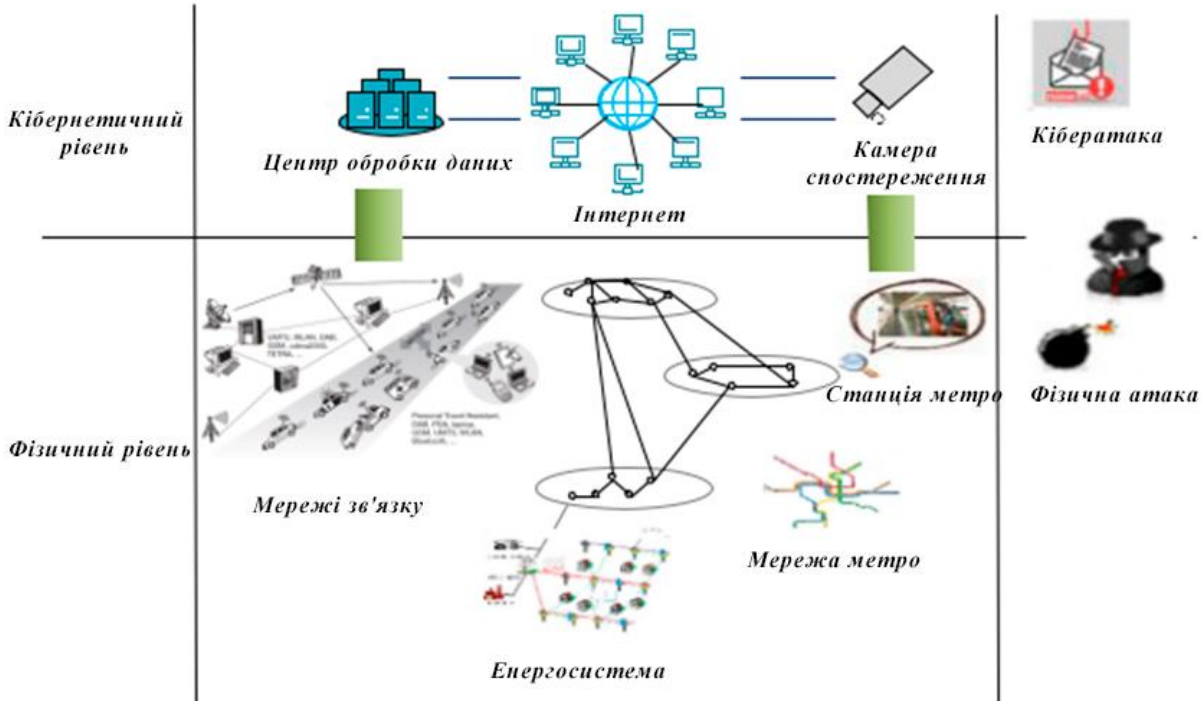

Рисунок 1.1 - Взаємозалежність кібермережі та фізичних систем

На рисунку 1.1 показано, як кібермережі взаємопов'язані з фізичними системами, які складаються з ключових інфраструктур, таких як мережа

зв’язку, метро та електромережі. Фізичні компоненти системи, такі як станції метро, можуть функціонувати належним чином, лише якщо міжрівневі вузли (наприклад, камери спостереження та електропідстанції) та інші станції метро працюють правильно. Цей взаємозалежний характер кіберфізичної інфраструктури прокладає шлях для скоординованої експлуатації атак, використовуючи сприйнятливість кібермереж і фізичних систем і збільшуючи ймовірність атаки, а також рівень відмов інфраструктури. Наприклад, кібератаки можуть бути використані терористами для зламу камер спостереження в урядовій будівлі, громадському місці чи аеропорту та непомітного встановлення бомби без фізичного відчуття. Фізичні втрати, завдані системам інфраструктури, також можуть допомогти зловмисникам проникнути в кіберсистеми, такі як диспетчерські та центри обробки даних. Таким чином, як фізичні, так і кіберінфраструктурні збої можуть призвести до шкідливих наслідків. Крім того, фізичний, логічний і кіберзв’язок установок призводить до взаємозалежностей і залежностей між компонентами та вузлами всередині і між інфраструктурами. Отже, відмова елемента може спричинити каскадні відмови в кількох схемах. Для пом’якшення цих кіберфізичних загроз розробка ефективних механізмів проектування має важливе значення для посилення фізичної та кібербезпеки на вузлах інфраструктури, щоб захистити їх від збоїв.

Разом із розвитком кіберінфраструктури кіберризики зростають швидкими темпами. Традиційні технології кібербезпеки зосереджені на поширених загрозах, але не призначені для інфраструктур з інтенсивним трафіком. Теорія ігор пропонує кращий підхід до вирішення проблем кібербезпеки, ніж традиційні рішення безпеки.

1.1 Визначення гри

Застосування математичного аналізу кооперативної та/або індивідуальної поведінки між гравцями, які вибирають конкретну

дію/стратегію для задоволення своїх власних інтересів, можна розуміти як теорію ігор.

Основні параметри гри:

1) Гра визначається як стратегічна взаємодія між взаємодіючими або протилежними інтересами, враховуючи виграш за дії, вжиті гравцями, і обмеження, не розкриваючи нічого про фактично здійснені кроки.

2) Гравець — це фундаментальна ігрова сутність, яка бере участь у грі зі скінченним набором гравців (позначених N), які виконують логічні дії (позначені A_i) для кожного гравця i. Гравець може бути машиною, групою людей або окремою особою в грі.

3) Виплата/корисність – це негативна або позитивна винагорода, яка надається гравцям за їхні дії в грі. Це позначається так $u_i: A \rightarrow \mathbb{R}$, що вимірює результат для гравця i на основі дій інших гравців $A = \times_{i \in N} A_i$, де $\mathbb{R}$ – набір дійсних чисел, а $\times$ – декартів добуток.

4) Стратегія передбачає план дій, який може прийняти гравець у грі, який може бути представлений у стратегічній/розширеній формі як:

$$\text{Гра} = \langle N, (A), (u_i) \rangle \qquad (1.1)$$

Теорія ігор — це опис сценарію прийняття рішення кількома особами як гри, де кожен гравець обирає дію, яка приведе до найкращої винагороди для нього самого, очікуючи логічних дій від решти гравців. У застосуванні до теорії ігор типова гра характеризується чотирма основними ознаками, а саме:

а) Два або більше гравців

б) Конкуруючий характер

c) Правила кожної гри

d) Виплати для кожного гравця

1.2 Рівновага Неша

Важливою концепцією теорії ігор є рівновага Неша, яка визначається як точка перетину найкращих відповідей, тобто кожен гравець грає свою

найкращу відповідь проти дій решти гравців. Загалом, рівновага Неша є інтелектуальним рішенням соціальних проблем, які стали сприятливою концепцією безпеки бездротових сенсорних мереж.

Рівновага Неша — це концепція рішення, що описує умову стаціонарної гри; жоден гравець не захоче змінювати свою стратегію, оскільки це може зменшити їхні виграші за умови, що решта гравців дотримуються визначеної політики.

Однак ця концепція рішення вказує на стійкий стан у грі, не вказуючи, як досягти такого стану. Хоча різні інші концепції рішення використовуються час від часу, рівновага Неша є найбільш помітною. Ця інформація повинна використовуватися для визначення ігор, які мають відповідні характеристики для представлення питань безпеки мережі.

Припустімо, що профіль стратегії для N гравців:

$$a_1, a_2, a_3, \dots \dots \dots \ a_N^* \tag{1.2}$$

де a_N^* позначає рівновагу Неша, якщо кожен гравець і має значення виграшу u_i, потім

$$u_i(a_i^*, a_{-i}^*) \geq u_i(a_i, a_{-i}^*) \tag{1.3}$$

Має бути дійсним для кожного гравця і з a_i^* позначення профілю дій гравця і та a_{-i}^* , що вказує на рівноважну дію решти гравців.

Для кожного гравця існують дві важливі концепції, а саме загальновідомість і раціональність. Загальні знання включають якнайшвидше розуміння результатів, так і взаємне знання кожного гравця про результати. Раціональність, з іншого боку, визначає послідовність у рішеннях без урахування симпатій/антипатій гравців у грі.

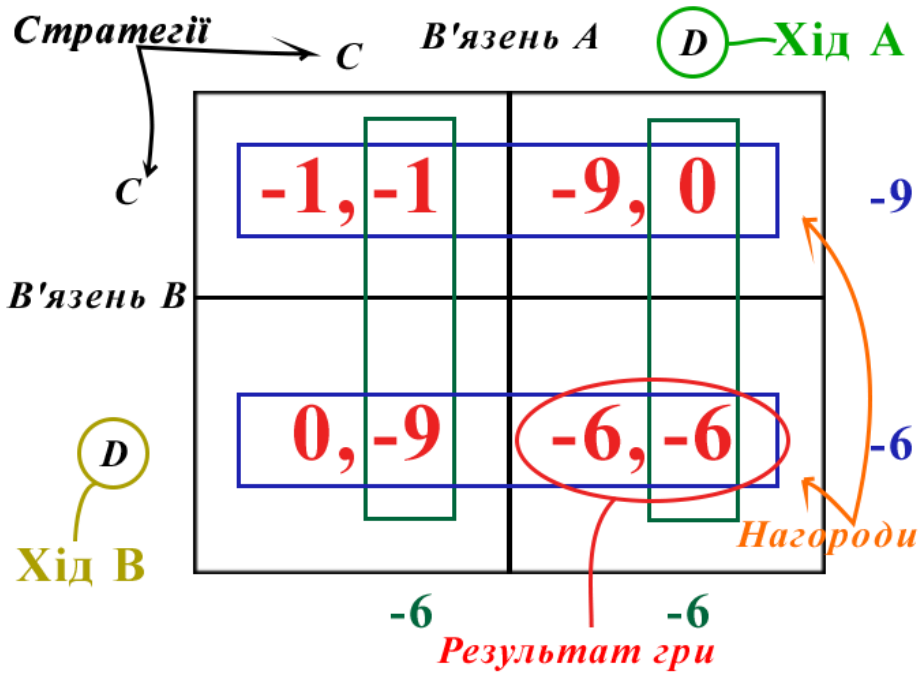

Рисунок 1.2 - Матричне представлення гри

Візьмемо до уваги просту гру – Дилема в’язня, в якій беруть участь лише два гравці. Матричне представлення гри подано на рисунку 1.2.

Поліція затримала двох осіб, яких звинувачують у зберіганні зброї. Їх підозрюють у скоєнні злочину; обох посадять за ґрати на 6 років, якщо жоден із них не зізнається. Але якщо тільки один з них зізнається, він буде звільнений, а інший буде ув'язнений на дев'ять років. Тепер, якщо обоє зізнаються у скоєному, то кожного з них посадять на рік. У такій грі рівновага Неша буде досягнута, коли обидва вони відмовляються від злочину, оскільки жоден не має попередніх знань про дії свого партнера. Результат цієї гри зображено на рисунку 1.2 як (-6, -6).

1.3 Теорія ігор та кібербезпека

Нещодавнє поширення кібератак, а також крадіжки особистих даних перетворили Інтернет на жахливе місце. Кібератаки створили глобальну загрозу як для глобальних, так і для локальних мереж. Вони також загрожують суспільству, оскільки комунікація, а економічна інфраструктура в основному покладається на інформаційні технології та комп’ютерні мережі.

Тому більш ефективні стратегії захисту є обов'язковими для протидії загрозам, спричиненим зростанням проблем кібербезпеки. У кібербезпеці теорія ігор може допомогти дізнатися про реакцію захисника на атакуючого і навпаки. Гру з двома гравцями можна використати, щоб відобразити стратегічну взаємодію між нападником і захисником, у якій обидва гравці намагаються максимізувати свої інтереси. Стратегія нападника визначається діями захисника і навпаки. Таким чином, можна сказати, що захисний механізм діє на основі стратегічної поведінки нападника та захисника. Тактичний аналіз можна виконати, використовуючи теорію ігор для дослідження атак з кількох вузлів або одного вузла. Як наслідок, теорія ігор має важливе значення для вивчення сценаріїв прийняття стратегічних рішень захисниками та аналізу стимулів атакуючих.

Існує декілька аспектів, у яких теоретико-ігрові методи кращі за традиційні підходи до кібербезпеки та конфіденційності, які обговорюються нижче:

1) Своєчасна дія: через відсутність стимулів для учасників традиційні рішення безпеки застосовуються досить повільно. Однак методи теорії ігор підтримують захисників шляхом використання фундаментальних механізмів стимулювання для розподілу обмежених ресурсів для вирівнювання сприйнятих ризиків.

2) Перевірена математика: більшість традиційних підходів до безпеки, які реалізуються в реактивних пристроях, таких як антивірусні програми або профілактичні засоби, такі як брандмауери, залежать лише від евристики. Тим не менш, підходи до теорії ігор методично аналізують рішення щодо безпеки за допомогою перевіреної математики.

3) Розподілене рішення: прийняття рішень у звичайних рішеннях безпеки є централізованим, а не розподіленим (або індивідуальним) за своєю природою. Через відсутність координаторів в автономних системах

централізований процес прийняття рішень практично неможливий в іграх безпеки мережі. Таким чином, рішення безпеки можуть бути реалізовані розподіленим способом за допомогою теорії ігор.

4) Надійний захист: дослідники можуть розробляти стратегії захисту для міцних і надійних систем кібербезпеки від атак (або егоїстичної поведінки) на основі аналітичних результатів, отриманих з теорії ігор.

Усі ці причини, згадані вище, роблять теорію ігор відповідним рішенням проблем кібербезпеки. Тим не менш, при використанні теоретико-ігрових методів для реалізації в кіберсистемах необхідно мати на увазі наступні моменти:

a) Багаторівневий захист: у розглянутих попередніх роботах помічено, що захисник націлений на певний захисний механізм і намагається максимізувати його корисність шляхом налаштування відповідних параметрів. Тим не менш, присутність кількох рівнів захисників, що забезпечують захист від атак, що часто реалізується в сучасних кіберсистемах, не помічається. Таким чином, необхідний відповідний теоретико-ігровий підхід, щоб визначити, як багаторівневі захисники можуть забезпечувати безпеку від атак при одночасному застосуванні захисних рівнів і як інші рівні можна покращити.

b) Раціональність: більшість теоретико-ігрових методів, що використовуються в кібербезпеці, наголошують на стратегіях рівноваги в профілях дій атакуючих і захисників. Але зловмиснику чи захиснику непросто забезпечити найкращі дії у відповідь через обмежену раціональність (з точки зору обмежених ресурсів чи інформації) у реальних кіберсистемах. Таким чином, відповідні моделі, такі як Рівновага квантової реакції і Теорія перспектив, необхідні для прогнозування поведінки гравців. Крім того, у сценаріях із кількома рівноважними ситуаціями неясно, що гравці мають вибрати, чи погоджуються вони взагалі вибрати один.

c) Реалізація: коли захисники та зловмисники приймають рішення в реальних кіберсистемах, вони беруть до уваги декілька факторів, які є реальними, але невизначеними, як-от співвідношення сигнал/шум, трафік, створений у типовій мережі, та/або потужність вузла в бездротові мережі. Тим не менш, захисники можуть не сприймати всю інформацію точно в реалістичних ситуаціях. Отже, вони повинні вміти вивчати навколишнє середовище і розуміти його. Крім того, існує кілька теоретико-ігрових методів, які моделюють ігри безпеки як ігри для двох гравців з кількома захисниками або нападниками, які розглядаються як єдине ціле. Ігри для двох гравців є реалістичними моделями, якщо кілька захисників або нападників мають однакові виграші та стратегії, але можуть бути недоцільними в реальній системі через різноманітність виграшів і стратегій захисників і нападників.

Таким чином, теорія ігор відіграє невід'ємну роль у розробці стратегії рівноваги для виживання від непередбачених перерв і атак через взаємодію між користувачами в кіберкомунікації. Крім того, у зв'язку з кіберконфіденційністю теорія ігор також знаходить застосування в обміні інформацією, анонімності, конфіденційності та криптографії.

2 ОСНОВИ ТЕОРІЇ ІГОР

2.1 Основні аспекти теорії ігор

Сьогодні дослідницьке співтовариство докладає всіх зусиль, щоб запропонувати організаціям ефективні рішення безпеки мережі; і одним із таких рішень є використання теорій, придатних для ситуацій реального життя, для розробки методів пом'якшення. Теорія ігор належить до категорії одного з таких підходів, який досліджують дослідники. Протягом багатьох років дослідники досліджували застосовність методів теорії ігор для боротьби з кібербезпекою; і багато з цих методів були успішними. Теорія ігор допомагає зрозуміти сценарії, де певним чином існує взаємодія між особами, які приймають рішення. У звичайному розумінні гру можна розглядати як змагальну діяльність, у якій гравці змагаються один з одним на основі чіткого набору правил або ходів, які вже були закладені.

Зі зростанням розподілених систем без інфраструктури теорія ігор також знайшла застосування в безпеці децентралізованих систем зв'язку, а саме. бездротові сенсорні мережі. Такий сценарій безпеки, що передбачає взаємодію зловмисника та захисника, можна точно відобразити на гру між гравцями, де кожен гравець намагається зробити все можливе, щоб збільшити свій прибуток. Найважливіше те, що теорія ігор ідеально підходить для такої моделі безпеки, оскільки дії, вжиті зловмисником або захисником, залежать від поведінки протилежної сторони.

Останнім часом широке застосування теорії ігор у сфері безпеки класифікується як ігри безпеки. Окрім кібербезпеки, теорія ігор має застосування в багатьох інших сферах, таких як політика, наука, економіка, аукціон, фінанси тощо. У цій статті розглядається застосування теорії ігор у кібербезпеці.

2.2 Основні визначення

Історія теорії ігор починається з робіт вченого Джона фон Неймана та економіста Оскара Моргенштерна в 1940-х роках. Вони розвивали математичну теорію, що дозволяла досліджувати взаємодію різних суб'єктів у конфліктній ситуації, коли виграш одного гравця залежить від вибору іншого гравця.

Конфліктна ситуація - це ситуація, в якій два або більше гравців знаходяться в конфлікті між своїми інтересами і вибирають свої дії залежно від дій інших гравців.

Гравці - це учасники гри, які мають відмінні від інших гравців інтереси та можуть вибирати свої дії.

Стратегії - це плани дій, які гравці можуть обирати в конфліктній ситуації. Кожен гравець може мати декілька стратегій, але він обирає ту стратегію, яка дає йому найбільший виграш.

Рівноваги в іграх - це такі стратегії гравців, коли жоден з гравців не має можливості змінити свою стратегію, не зменшуючи свій виграш. Це означає, що в конкретній ситуації гравці не можуть досягти кращого результату, ніж у поточній ситуації.

Теорія ігор має багато застосувань в оптимізаційних задачах. Наприклад, при проектуванні аукціонів, розподілу ресурсів та інших задачах, що вимагають прийняття рішень в умовах конкуренції, теорія ігор може бути корисною для визначення оптимальних стратегій та досягнення більшого виграшу для всіх учасників. Також, теорія ігор застосовується в економіці, політиці, психології, біології та інших галузях, де необхідно вивчати поведінку суб'єктів у конфліктних ситуаціях.

Для того, щоб розв'язати задачі теорії ігор, необхідно визначити конфліктну ситуацію та її параметри, такі як гравці, їх можливі стратегії та виграші. Гравці можуть бути індивідуальними особами, компаніями, країнами

та іншими суб'єктами. Стратегії - це плани дій, які гравці можуть обирати в залежності від дій інших гравців. Рівновага в іграх - це такий набір стратегій гравців, при якому жоден з гравців не може збільшити свій виграш, змінивши свою стратегію, якщо інші гравці не змінюють свої стратегії.

Задачі теорії ігор мають важливе застосування в оптимізаційних задачах, так як вони дозволяють визначити найкращі рішення в умовах обмежень та конкуренції між різними варіантами дій. Наприклад, в економіці теорія ігор використовується для дослідження поведінки підприємств та ринків з метою визначення оптимальних стратегій для досягнення максимального виграшу. У політиці теорія ігор може допомогти вирішити конфліктні ситуації та досягнути компромісу між різними інтересами.

Отже, теорія ігор є важливим інструментом для аналізу конфліктних ситуацій та прийняття рішень в умовах нестійкості та невизначеності.

2.3 Типологія ігор

На основі перспективи ігри можна розділити на кілька класів. Різноманітні види ігор обговорювалися в цьому розділі нижче: Рисунок 2.1 представляє класифікацію різних моделей ігор, а також проблеми безпеки, які вирішує кожен клас ігор.

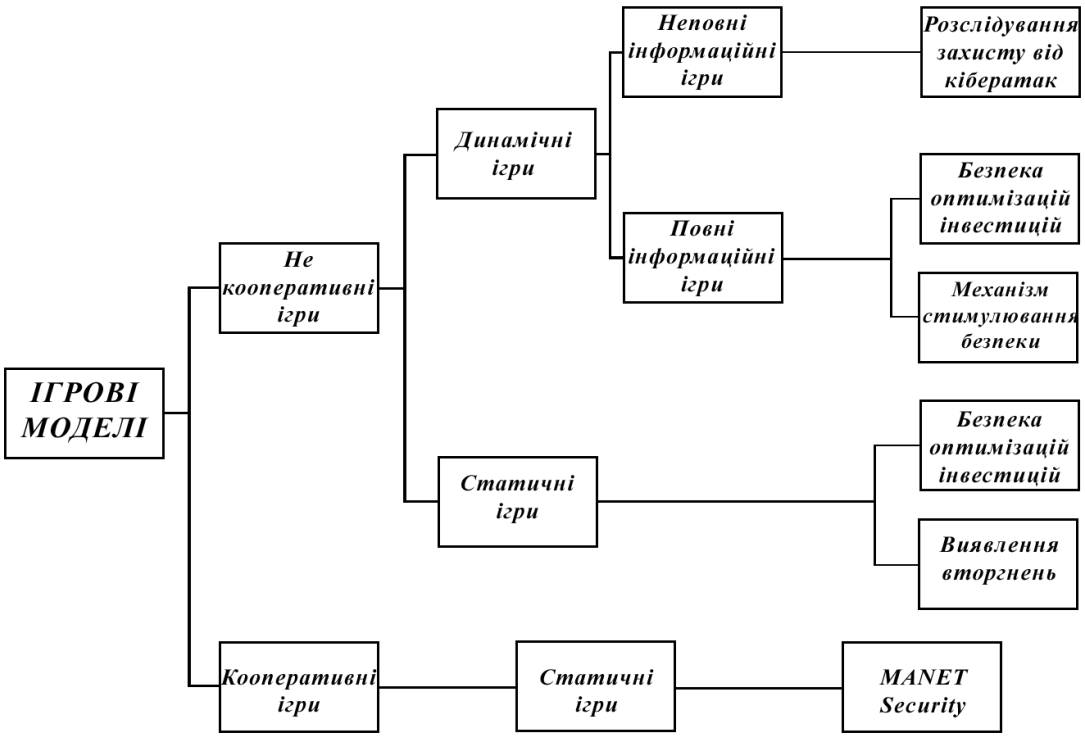

Рисунок 2.1 - Класифікація ігрових моделей

Ігри з повною інформацією - це такі ігри, у яких гравці знають всю інформацію про стан гри, включаючи можливі ходи, випадкові наслідки та винагороди. Прикладами ігор з повною інформацією є шахи, го, тетріс тощо.

Ігри з нульовою сумою - це ігри, у яких сума виграшів гравців дорівнює нулю, тобто виграш одного гравця призводить до втрати іншого гравця. Прикладами ігор з нульовою сумою є покер, камінь-ножиці-папір тощо.

$$\mathrm{E}_{\mathrm{i}=1}^{2}\mathrm{u}_{\mathrm{i}}(\mathrm{s}) = 0 \forall \mathrm{s} \in \mathrm{S} \qquad (2.1)$$

де $\mathrm{s} -$ стратегічний профіль

Багатокрокові ігри - це ігри, у яких гравці здійснюють послідовні ходи, залежно від результатів попередніх ходів. Прикладами багатокрокових ігор є шахи, го, стратегічні ігри тощо.

Байєсівські ігри - це ігри, у яких гравці мають неповну інформацію про стан гри та імовірності різних подій, і вони повинні використовувати свої знання про можливість цих подій, щоб вибрати оптимальну стратегію. Прикладами Байєсівських ігор є ігри на виживання, де гравці мають різні знання про харчовий ланцюг.

Кооперативні ігри - це ігри, у яких гравці працюють разом для досягнення спільної мети, не конкуруючи один з одним. Прикладами кооперативних ігор є гра в команді, де кожен гравець має свою роль в команді.

Некооперативні ігри - це ігри, у яких гравці змагаються один з одним та діють самостійно з метою отримання найкращого можливого результату. Прикладами некооперативних ігор є покер, де кожен гравець змагається за виграш з іншими гравцями, з використанням своїх індивідуальних стратегій.

Стохастичні ігри - це ігри, у яких випадкові події впливають на результат гри. Прикладами стохастичних ігор є ігри на казино, лотереї тощо, де випадковість може визначати виграш або програш гравця.

Важливо зазначити, що багато ігор мають елементи кількох категорій. Наприклад, багатокрокові ігри можуть бути іграми з повною інформацією або стохастичними іграми, а некооперативні ігри можуть бути іграми з нульовою сумою або байєсівськими іграми.

Гра з ненульовою сумою: у цей тип гри можуть грати кілька гравців, і сума виграшів гравців не залишається постійною протягом гри. Таким чином, усі гравці є або максимайзерами, або мінімізаторами, не маючи жодних обмежень щодо загального значення виграшу, як у випадку з іграми з нульовою сумою. Таким чином, усі гравці в грі можуть програти або виграти разом.

Повторювана гра: як уже визначено, повторювані ігри – це взаємодія двох гравців, які грають у гру неодноразово. Також відома як ітераційні ігри, ця гра складається з багатьох повторюваних етапів, і на кожному кроці

поточна дія визначає наступну дію гравців. Повторювані ігри можуть повторюватися як кінцево, так і нескінченно. У нескінченно повторюваних іграх існує фіксований і відомий період часу. Однак у нього є обмеження, яке змушує гравця поводитися егоїстично, і Рівновага Неша використовується для дорівнювання мінімальної виграші. Найпопулярнішим типом є нескінченно повторювана гра, в якій гра триває нескінченно.

Еволюційна гра: Еволюційні ігри в основному застосовуються до біологічних мереж, у яких чисті та змішані стратегії можуть бути об'єднані гравцями з логічною поведінкою для покращення характеристик популяції. Примітно, що еволюційні ігри використовувалися в минулому для моделювання різних додатків бездротової сенсорної мережі.

Гра Stackelberg: ігри Stackelberg використовуються для моделювання двох гравців, які змагаються, де один із гравців є ініціатором (або лідером) гри, який обирає дію з певного набору 1, а інший гравець слідує за діями лідера, щоб вибрати пізніше хід з іншого набору 2. Така ситуація є поширеною для захисту різноманітних бездротових сенсорних мереж, де зловмисник виступає як послідовник, а захисник відіграє роль лідера.

Особлива категорія ігор, які називаються іграми безпеки, аналізують взаємодію між захисниками та зловмисниками. Ці ігри, разом із їхніми рішеннями, формують базу розробки алгоритму та формального прийняття рішень, окрім прогнозування поведінки зловмисників. Крім того, ігри безпеки знаходять широке застосування для вирішення проблем безпеки, таких як виявлення вторгнень і конфіденційність у комп'ютерних, бездротових і автомобільних мережах.

3 ТЕОРЕТИЧНІ МЕТОДИ ІГРОВИХ ЗАСТОСУВАНЬ ДЛЯ КІБЕРБЕЗПЕКИ

3.1 Безпека фізичного рівня

3.1.1 Модель системи

Це сфера безпеки, що розвивається. Атаки підслуховування та глушіння є звичним явищем на каналах зв'язку мереж. Примітно, що ці атаки викликають більшу тривогу для бездротових мереж, ніж для дротових мереж.

Розглянемо мережу з джерелом, пунктом призначення, зловмисним вузлом-перехоплювачем і J-дружніми вузлами перешкод, як показано на малюнку I. Зловмисний вузол намагається підслухати передані дані, що надходять від вузла-джерела. Коли канал підслуховування від джерела до зловмисного вузла є погіршеною версією основного каналу джерело-приймач, джерело та адресат можуть обмінюватися абсолютно безпечними повідомленнями з ненульовою швидкістю. Передаючи повідомлення зі швидкістю, вищою за швидкість зловмисного вузла, зловмисний вузол майже нічого не може дізнатися про повідомлення зі своїх спостережень. Максимальний рівень секретності інформації від джерела до її призначення визначається терміном секретності.

Припустимо, джерело передає потужність P_0. Виграш каналу від джерела до пункту призначення та від джерела до шкідливого вузла становить G_{sd} and G_{sm} відповідно. Кожен дружній глушник $i, i = 1, \ldots, J$ передає з потужністю P_i і канал виграє від цього до пункту призначення та зловмисника

вузол, є G_{id} and G_{im} відповідно. Для зручності позначаємо J набір індексів $\{1, 2, 3 \ldots\ldots J\}$.

Якщо використовується модель втрат на шляху, посилення каналу визначається відстанню до негативного ступеня

коефіцієнт втрат на шляху. Тепловий шум для кожного каналу дорівнює σ^2, а смуга пропускання дорівнює W. Пропускна здатність каналу від джерела до місця призначення становить

$$C_1 = W \log_2\left(1 + \frac{P_0 G_{sd}}{\sigma^2 + \sum_{i \in J} P_i G_{id}}\right) \quad (3.1)$$

Пропускна здатність каналу від джерела до шкідливого вузла становить

$$C_2 = W \log_2\left(1 + \frac{P_0 G_{sm}}{\sigma^2 + \sum_{i \in J} P_i G_{im}}\right) \quad (3.2)$$

Скритність є

$$C_s = (C_1 - C_2)^+ \quad (3.3)$$

де $(\cdot)^+ = \max(\cdot, 0)$. І C_1, і C_2є спадними та опуклими функціями потужності перешкод P_i. Однак, $C_s = C_1 - C_2$ не є монотонною і опуклою функцією. Це пояснюється тим, що потужність перешкод C_1 може зменшуватися швидше, ніж C_2. У результаті C_s може збільшитися в деякій області значення P_i. Таким чином, питання полягають у тому, чи можна збільшити C_s і як контролювати потужність перешкод розподіленим чином. Спробуємо вирішити проблеми, використовуючи теоретичний підхід.

3.1.2 Гра для захисту фізичного рівня

По-перше, ми визначимо гру між джерелом і дружніми перешкодами. Далі ми оптимізуємо сторони джерела та джерела перешкод відповідно. Потім ми доведемо деякі властивості запропонованої гри. Крім того, побудовано порівняння з централізованою схемою. Нарешті, ми обговорюємо деякі проблеми впровадження.

А Визначення

Джерело можна змоделювати як покупця, який хоче оптимізувати свою секретність за вирахуванням витрат, модифікувавши «сервіс» (потужність перешкод P_i) від дружніх перешкод, тобто

$$\text{Гра джерела: } \max U_s = (a \max(C_1 - C_2, 0) - M) \tag{3.4}$$

при тому, $P_i \leq P_{max}$, де a — посилення на одиницю потужності, P_{max} — максимальна потужність, яку може забезпечити перешкод, а M — вартість інших дружніх вузлів перешкод. Звідси

$$M = \sum_{i \in J} p_i P_i \tag{3.5}$$

де p_i — ціна за одиницю потужності для дружнього глушника, P_i — потужність дружнього глушника, а J — набір дружніх глушників. З (3.3) зауважимо, що джерело не братиме участі в грі, якщо $C_1 < C_2$, або, іншими словами, секретність дорівнює нулю. Для кожного джерела перешкод $U_i(p_i, P_i(p_i))$ є функцією корисності ціни та потужності, придбаної джерелом. Для корисності глушника (продавця) у цій статті ми визначаємо наступну корисність

$$U_i = p_i P_i^{c_i} \tag{3.6}$$

де $c_i \geq 1$ є константою для балансування від оплати p_i, P_i від джерела та вартості передачі P_i. Зауважте, що P_iтакож є функцією вектора цін $(p_i, \ldots p_N)$, оскільки потужність, яку придбає джерело, також залежить від ціни, яку запитують дружні перешкоди. Отже, для кожного дружнього глушника існує проблема оптимізації

$$\text{Гра дружнього глушника: } \max_{p_i} U_i \tag{3.7}$$

Проаналізуємо оптимальні стратегії для вихідних і дружніх глушників для максимізації власних корисностей.

В Аналіз джерела (покупця)

Представимо $A = \frac{P_0 G_{sd}}{\sigma^2}, B = \frac{P_0 G_{sm}}{\sigma^2}, u_i = \frac{G_{id}}{\sigma^2}$, та $v_i = \frac{G_{im}}{\sigma^2}, i \in J$, маємо

$$U_s = aW\left(\left(\log(1+\frac{A}{1+\sum_{j\in J} u_j P_j})\right) - \log(1+\frac{B}{1+\sum_{j\in J} u_j P_j})\right)^+ - \sum_{j\in J} u_j P_j \quad (3.8)$$

Для зчитування розміру джерела (покупця) для початку проаналізуємо випадок де $C_1 > C_2$. З диференціювання (3.4), маємо

$$\frac{\partial U_s}{\partial P_i} = -\frac{\frac{aWAu_i}{\ln 2}}{(1+A+\sum_{j\in J} u_j P_j)(1+\sum_{j\in J} u_j P_j)} \frac{\frac{aWAv_i}{\ln 2}}{(1+A+\sum_{j\in J} v_j P_j)(1+\sum_{j\in J} v_j P_j)} \quad (3.9)$$

$$- p_i = 0$$

Переставляючи наведене вище рівняння, ми маємо

$$P_i^4 + F_{i,3}P_i^3 + F_{i,2}(p_i)P_i^2 + F_{i,1}(p_i)P_i + F_{i,0}(p_i) = 0 \quad (3.10)$$

Де

$$F_{i,3} = (2+2\alpha_i + A)^2 + (2+2\beta_i + B)^2 \quad (3.11)$$

$$F_{i,2}(p_i) = \frac{(2+2\alpha_i + A)(2+2\beta_i + B)}{u_i v_i} + \frac{L_i}{v_i^2} + \frac{K_i}{u_i^2} - \frac{aW}{p_i u_i v_i}\left(\frac{B}{v_i} - \frac{A}{u_i}\right) \quad (3.12)$$

$$F_{i,1}(p_i) = \frac{L_i C_i + K_i D_i}{u_i^2 v_i^2} + \frac{aW(AD_i - BC_i)}{p_i u_i^2 v_i^2} \quad (3.13)$$

$$F_{i,0}(p_i) = \frac{L_i K_i}{u_i^2 v_i^2} + \frac{aW(Au_i L_i - Bv_i K_i)}{p_i u_i^2 v_i^2} \quad (3.14)$$

та

$$\alpha_i = \sum_{j \neq i} G_{jd} P_j \tag{3.15}$$

$$\beta_i = \sum_{j \neq i} G_{jm} P_j \tag{3.16}$$

$$K_i = (1 + \alpha_i)(1 + \alpha_i + A) \tag{3.17}$$

$$L_i = (1 + \beta_i)(1 + \beta_i + B) \tag{3.18}$$

$$C_i = u_i(2 + 2\alpha_i + A) \tag{3.19}$$

$$D_i = v_i(2 + 2\beta_i + B) \tag{3.20}$$

Розв'язки квартичної функції можна виразити в закритій формі, але це не є основною метою. Важливо, що рішення задається наступною функцією

$$P_i^* = P_i^*\left(p_i, A, B\{u_j\}, \{v_j\}, \{P_j\}_{j \neq i}\right) \tag{3.21}$$

Зверніть увагу, що $0 \leq P_i \leq P_{max}$. Оскільки P_i задовольняє поліноміальну функцію, ми можемо мати оптимальну стратегію як

$$P_i^* = \min[\max(P_i, 0), P_{max}] \tag{3.22}$$

Через складність розв'язку рівняння четвертої частини в замкнутій формі в (3.22) ми також розглядаємо два спеціальні випадки: випадок нижчої інтерференції та випадок сильної інтерференції.

1) Перешкоди на місці призначення набагато менші за шум

Пам'ятаємо: $A = \frac{P_0 G_{sd}}{\sigma^2}$, $B = \frac{P_0 G_{sm}}{\sigma^2}$, $u_i = \frac{G_{id}}{\sigma^2}$, та $v_i = \frac{G_{im}}{\sigma^2}$.

Уявіть ситуацію, в якій усі перешкоди знаходяться поблизу шкідливого вузла та далеко від вузла призначення.

У цьому випадку перешкоди від джерел перешкод до місця призначення дуже малі порівняно з додатковим шумом, тому ми маємо:

$$U_s \approx aW\left(\log(1 + A) - \log\left(1 + \frac{B}{1 + \sum_{j \in J} v_j P_j}\right)\right)^+ - \sum_{j \in J} p_j P_j \tag{3.23}$$

Тоді:

$$\frac{\partial U_s}{\partial P_i} = \frac{aWBv_i/\ln 2}{\left(1 + B + \sum_{j\in J} v_j P_j\right)\left(1 + \sum_{j\in J} v_j P_j\right)} - p_i = 0 \tag{3.24}$$

Підставлячи, отримаємо:

$$P_i^2 + \frac{2 + 2\beta_i + B}{v_i} P_i + \frac{(1 + \beta_i)(1 + B + \beta_i)}{v_i^2} - \frac{aWB}{p_i v_i \ln 2} = 0 \tag{3.25}$$

Розв'язуючи наведене вище рівняння, ми отримуємо розв'язок замкнутої форми:

$$P_i^* = -\frac{2+2\beta_i+B}{2v_i} + \sqrt{\frac{(2+2\beta_i+B)^2}{4v_i^2} - \frac{(1+\beta_i)(1+B+\beta_i)}{v_i^2} + \frac{aWB}{p_i v_u \ln 2}} = q_i + \sqrt{w_i + \frac{z_i}{p_i}} \tag{3.26}$$

Нарешті, порівнюючи P_i^* з потужністю за граничних умов ($P_i = 0$, $P_i = P_{max}$ і $C_s = 0$), можна отримати оптимальне P_i^*в області низького відношення сигналу/шуму.

2) Один глушник із перешкодами, які набагато вищі за шум, але набагато менші за отриману потужність у пункті призначення та шкідливому вузлі

У цьому випадку перешкоди від перешкод значно вищі за додатковий шум, але набагато менші за потужність отриманого сигналу в пункті призначення та шкідливому вузлі. Іншими словами, це означає $1 \ll u_1 P_1 \ll A$ and $1 \ll v_1 P_1 \ll B$. Тому функція корисності джерела визначається як

$$\begin{aligned} U_s &\approx aW\left(\log\left(1 + \frac{A}{u_1 P_1}\right) - \log\left(1 + \frac{B}{v_1 P_1}\right)\right) - p_1 P_1 \\ &\approx \frac{aWA}{u_1 P_1} - \frac{aWB}{v_1 P_1} - p_1 P_1 \end{aligned} \tag{3.27}$$

Якщо $\frac{B}{v_1} - \frac{A}{u_1} \leq 0$, Us є спадною функцією P_1. У результаті P_s оптимізується, коли $P_1 = 0$, тобто глушник не бере участі в грі. З іншого боку, якщо $\frac{B}{v_1} - \frac{A}{u_1} > 0$,, щоб знайти максимальні потужності, ми повинні обчислити:

$$\frac{\partial U_s}{\partial P_i} = -\frac{aWA}{u_1 P_1^2} + \frac{aWB}{v_1 P_1^2} - p_1 = 0 \tag{3.28}$$

Отже

$$P_1^* = \sqrt{\frac{aW}{p_1}\left(\frac{B}{v_1} - \frac{A}{u_1}\right)} = \sqrt{\frac{D_1}{p_1}} \tag{3.29}$$

З цього рівняння ми отримуємо оптимальне рішення закритої форми P_i^* подібним чином, порівнюючи P_1^* потужністю за граничними умовами ($P1 = 0$, $P_1 = P_{max}$ і $C_s = 0$), ми можемо отримати оптимальне рішення для цей особливий випадок.

С Аналіз дружнього глушника (продавця)

Проаналізуємо як дружні перешкоди можуть встановити оптимальну ціну, щоб максимізувати свою корисність. Диференціюючи корисність у (3.6) і встановлюючи її на нуль, ми маємо

$$\frac{\partial U_i}{\partial p_i} = (P_i^*)^{c_i} + p_i c_i (P_i^*)^{c_i - 1} \frac{\partial P_i^*}{\partial p_i} = 0 \tag{3.30}$$

Це еквівалентно

$$(P_i^*)^{c_i - 1}\left(P_i^* + p_i c_i \cdot \frac{\partial P_i^*}{\partial p_i}\right) = 0 \tag{3.31}$$

Це відбувається або якщо $P_i^* = 0$ або якщо

$$P_i^* + p_i c_i \cdot \frac{\partial P_i^*}{\partial p_i} = 0 \tag{3.32}$$

Із замкнутого розв'язку P_i^* розв'язком p_i^*буде функція, задана як

$$p_i^* = p_i^*(\sigma^2, G_{sd}, G_{sm}, \{G_{id}\}, \{G_{im}\}) \tag{3.33}$$

Зверніть увагу, що p_i^* має бути додатним. Інакше дружній глушник не відтворювався б.

D Властивості

Доведемо деякі властивості запропонованої гри. По-перше, ми доведемо, що потужність є монотонною функцією ціни в двох крайніх випадках. Властивості можуть допомогти для доказу існування рівноваги в наступній частині цього підрозділу.

Властивість 1: у двох особливих випадках оптимальне споживання електроенергії P_i^* для дружнього глушителя і є монотонним із його ціною p_i, коли ціни інших дружніх глушників є фіксованими. Доказ випливає з (3.26) і (29).

Ми досліджуємо наступний аналіз співвідношення між ціною та потужністю. Ми з'ясовуємо, що дружня потужність перешкод P_i, куплена у джерела, опукла за власною ціною p_i за деяких умов. Щоб довести це, нам потрібно перевірити, чи друга похідна $\partial^2 P_i / \partial p_i^2 < 0$.

У першому окремому випадку, коли інтерференція мала

$$\frac{\partial P_i^*}{\partial p_i} = -\frac{z_i}{2p_i^2\sqrt{w_i + \frac{z_i}{p_i}}} \tag{3.34}$$

Та

$$\frac{\partial^2 P_i^*}{\partial p_i^2} = -\frac{z_i}{p_i^3\left(w_i + \frac{z_i}{p_i}\right)^{1/2}}\left(1 - \frac{1}{4\left(\frac{p_i w_i}{z_i} + 1\right)}\right) \tag{3.35}$$

Наведене вище рівняння більше нуля, коли p_i мало. Це означає, що коли перешкоди невеликі і ціна мала, потужність є опуклою як функція ціни.

У другому особливому випадку, коли втручання є серйозним

$$\frac{\partial P_i^*}{\partial p_i} = -\frac{1}{2}\sqrt{D_1}\,p_1^{-3/2} \tag{3.36}$$

та

$$\frac{\partial^2 P_i^*}{\partial p_i^2} = \frac{3}{4}\sqrt{D_1}\,p_1^{-5/2} > 0 \tag{3.37}$$

Це означає, що коли втручання серйозне, потужність є опуклою функцією ціни.

Далі ми досліджуємо рівновагу запропонованої гри. Іншими словами, жоден користувач не може покращити свою корисність, змінивши лише власну стратегію. Спочатку ми визначимо рівновагу Штакельберга таким чином:

Визначення 1: P_i^{SE} та p_i^{SE} є рівновагою Штакельберга запропонованої гри, коли p_i є фіксованим,

$$U_s\left(\{P_i^{SE}\}\right) = \sup 1_{P_{max} \geq \{P_i^{SE}\} \geq 0, \forall i} U_s(\{P_i\}), \forall i \in J \tag{3.38}$$

та коли P_i є фіксованим

$$U_i\left(p_i^{SE}\right) = \sup 1_{p_i} U_i(p_i), \forall i \in J \tag{3.39}$$

Нарешті, з аналізу ми можемо показати наступну властивість запропонованої гри.

Властивість 2: Пара $\{P_i^*\}_{i=1}^N$ у (22) та $\{p_i^*\}_{i=1}^N$ у (3.33) є рівновагою Штакельберга для запропонованої гри.

Зверніть увагу, що в (3.10) може бути кілька коренів, як наслідок, може бути кілька рівноваг Штакельберга. У результатах моделювання, наведених у наступному розділі, ми покажемо, що запропонована схема все ще може досягти рівноваги з кращими характеристиками, ніж у випадку без перешкод.

Е Розподілений алгоритм і конвергенція

Проаналізуємо, як розподілена гра може сходитися до рівноваги Штакельберга, визначеної у вищенаведеному підрозділі. Після перестановки (3.30) маємо

$$p_i = I_i(p) = -\frac{(P_i^*)}{c_i \frac{\partial P_i^*}{\partial p_i}} \tag{3.40}$$

де $p = [p_1, \ldots, p_N]^T$ and $I_i(p)$ є функцією оновлення ціни. Зауважте, що P_i^* є функцією p. Інформацію для оновлення можна отримати з вихідного вузла. Це схоже на розподілене керування потужністю. Оновлення цін дружніх глушників можна записати у векторній формі так

$$\text{Розподілений алгоритм: } p(t+1) = I\big(p(t)\big) \tag{3.41}$$

де $I = [I_1, \ldots, I_N]^T$ та ітерація триває від часу t до часу t + 1. Далі ми показуємо, що збіжність запропонованої схеми доведено, що функція оновлення ціни в (3.41) є стандартною функцією, визначеною як

Визначення 2: функція I(p) є стандартною, якщо для всіх $p \geq 0$ виконуються такі властивості

1) Позитивність: $p > 0$,
2) Монотонність: якщо $p \geq p'$, тоді $I(p) \geq I(p')$, or $I(p) \leq I(p')$,
3) Масштабованість: для всіх $\eta > 1$, $\eta I(p) \geq I(\eta p)$.

У було доведено, що ціна буде сходитися до фіксованої точки (тобто до рівноваги Штакельберга в нашому випадку) від будь-якого можливого початкового вектора ціни. Позитивність довести дуже легко. Якщо ціна p_i зросте, джерело буде купувати менше від і-го дружнього джерела перешкод. У результаті $\frac{\partial P_i^*}{\partial p_i}$ у (3.30) від'ємне, і ми доводимо позитивність $p_i = I_i(p) > 0$.

Для монотонності та масштабованості ми можемо показати лише два особливі випадки. Для випадку низьких перешкод з (3.26) очевидно, що

$$I_i(p) = -\frac{(P_i^*)}{c_i \frac{\partial P_i^*}{\partial p_i}} = \frac{2\sqrt{w_i p_i^2 + z_i p_i}\left(q_i p_i + \sqrt{w_i p_i^2 + z_i p_i}\right)}{c_i z_i} \tag{3.42}$$

яка монотонно зростає за p_i. Для масштабованості ми маємо

$$\frac{I_i(\eta p)}{\eta I_i(p)} = \frac{\sqrt{w_i p_i^2 + z_i p_i/\eta}\left(q_i p_i + \sqrt{w_i p_i^2 + z_i p_i/\eta}\right)}{\sqrt{w_i p_i^2 + z_i p_i}\left(q_i p_i + \sqrt{w_i p_i^2 + z_i p_i}\right)} < 1 \text{ since } \eta > 1 \quad (3.43)$$

Для випадку великої інтерференції з (3.29) маємо

$$I_i(p) = -\frac{(P_i^*)}{c_i \frac{\partial P_i^*}{\partial p_i}} = \frac{2p_i}{c_i} \quad (3.44)$$

який монотонно зростає в p_i і масштабується.

Для більш загальних випадків аналіз не можна виконати. Результати моделювання показують, що запропонована схема може збігатися та перевершувати випадок без перешкод.

F Централізована схема

Традиційно використовується централізована схема, припускаючи, що вся інформація про канал відома. Мета оптимізації секретності в умовах обмежень максимальної потужності перешкод

$$\max_{P_i} C_S = \max\left[W \log_2\left(\frac{1 + \frac{P_0 G_{sd}}{\sigma^2 + \sum_{i\in J} P_i G_{id}}}{1 + \frac{P_0 G_{sm}}{\sigma^2 + \sum_{i\in J} P_i G_{im}}}\right), 0\right] \quad (3.45)$$

при тому

$$0 \le P_i \le P_{max}, \forall i$$

Централізоване рішення знайдено лише шляхом максимізації секретності. Якщо ми не беремо до уваги обмеження, ми маємо

$$\frac{\partial C_s}{\partial P_i} = -\frac{AWu_i}{(1+\alpha_i+u_iP_i)(1+A+\alpha_i+u_iP_i)} + \frac{BWv_i}{(1+\beta_i+u_iP_i)(1+B+\beta_i+u_iP_i)} = 0 \quad (3.46)$$

Переставляючи ми отримуємо

$$P_i^2 + \frac{Au_i^2(2+B+2\beta_i) - Bv_i^2(2+A+2\alpha_i)}{Au_i^3 - Bv_i^3}P_i + \frac{Au_i(1+\beta_i)(1+B+\beta_i) - Bv_i(1+\alpha_i)(1+A+\alpha_i)}{Au_i^3 - Bv_i^3} = 0 \quad (3.47)$$

Використовуючи теорему про умову KKT, остаточне рішення буде отримано шляхом порівняння граничних умов (тобто Pi = 0, Pi = Pmax і Cs = 0).

Запропонований алгоритм є розподільним, у тому сенсі, що потрібно обмінюватися лише інформацією про ціни. У результатах моделювання порівнюється запропонований теоретичний підхід з цією централізованою схемою.

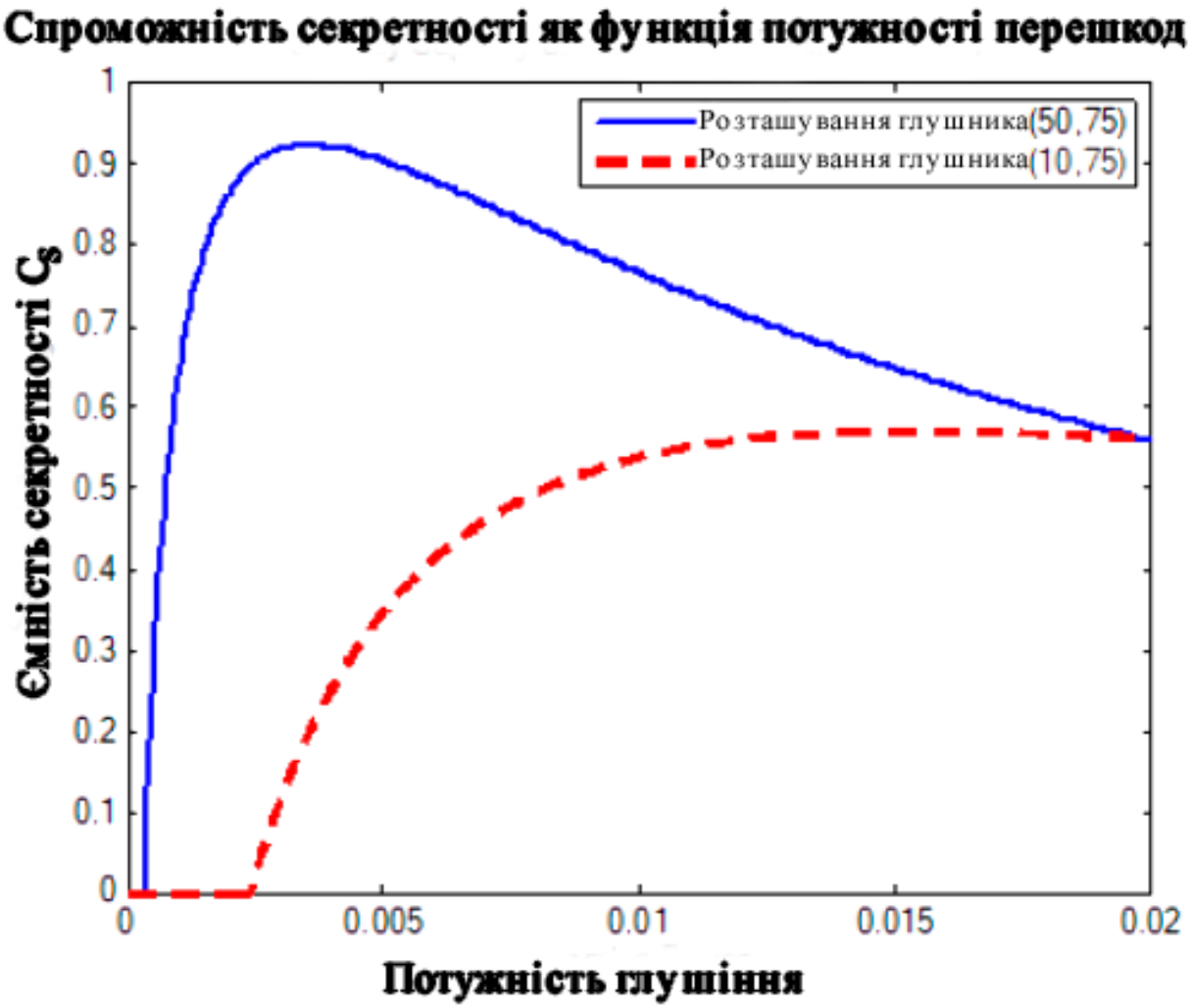

Рисунок 3.1 - Місткість секретності проти потужності глушіння

Нарешті, з результатів моделювання видно, що розподілене та централізоване рішення асимптотично однакові, якщо a достатньо велике (джерело піклується про секретність більше, ніж про оплату, тобто джерело є достатньо багатим).

3.1.3 Обговорення реалізації

Існує кілька проблем щодо впровадження запропонованої схеми. По-перше, інформація про канал від джерела до зловмисного перехоплювача

може бути невідомою або точно відомою. За цієї умови формулу секретності слід переписати з урахуванням невизначеності. Якщо напрямок прибуття відомий, можна використовувати багатоантенні методи. По-друге, запропонована схема потребує періодичного оновлення інформації про ціну та потужність. Виникає природне запитання, якщо розподілена схема має менше сигналізації, ніж централізована схема. Порівняння подібне до розподіленого та централізованого керування потужністю в літературі [15, 16]. Оскільки стан каналу постійно змінюється, розподіленому рішенню потрібно лише оновити різницю параметрів, таких як потужність і ціна, щоб бути адаптивним, тоді як централізована схема вимагає всієї інформації про канал за кожен період часу. Як наслідок, розподілене рішення має явну перевагу та домінує в поточному та майбутньому дизайні бездротової мережі. Наприклад, керування потужністю для стільникових мереж, керування потужністю відкритого циклу виконується лише один раз під час ініціалізації каналу, тоді як керування потужністю замкнутого циклу (розподілений розподіл потужності, такий як [15] виконується 1500 разів для UMTS і 800 разів для UMTS. CDMA2000. Нарешті, для випадку з кількома джерелами та декількома призначеннями є два можливі варіанти вирішення проблеми. По-перше, ми можемо використати метод кластеризації, щоб розділити мережу на підмережі, а потім застосувати пару «єдине джерело-одержувач» і рішення для кількох дружніх перешкод, запропоноване в цій статті. Або, якщо ми вважаємо, що потужність глушіння може бути корисною для кількох підслуховувачів, можна дослідити деякі методи, такі як подвійний аукціон. Детальне обговорення виходить за рамки цієї статті та буде розглянуто в наших майбутніх дослідженнях.

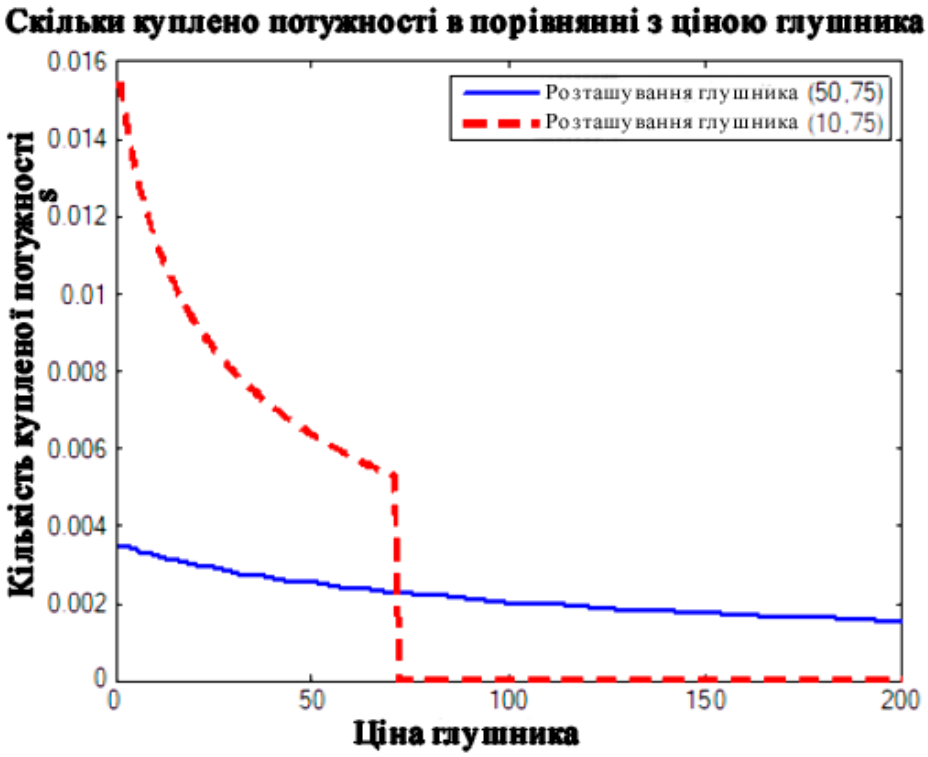

Рисунок 3.2 - Скільки електроенергії придбає джерело в порівнянні з ціною

3.1.4 Результати моделювання

Симуляція встановлюється наступним чином: джерело та дружній перешкод мають потужність 0,02, ширина смуги дорівнює 1, рівень шуму дорівнює 10^{-8}, коефіцієнт втрат при розповсюдженні дорівнює 3, передбачається канал AWGN. джерело, адресат і підслухувач розташовані в координатах (0,0), (100,0) і (50,50), відповідно. Тут a = 2 для зручної утиліти перешкод у (6).

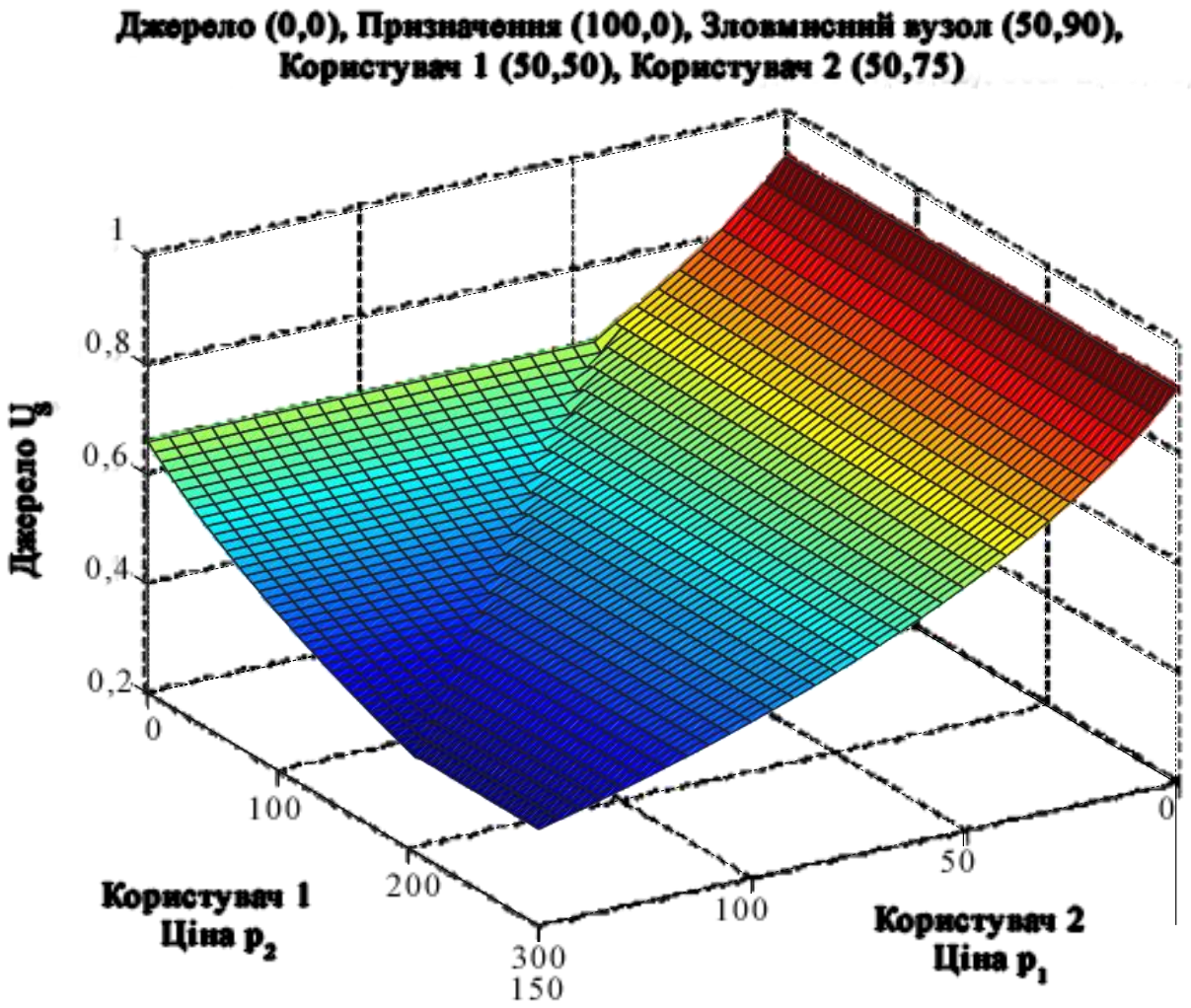

Рисунок 3.3 - U_s проти цін двох користувачів

Для одного випадку дружнього глушника ми показуємо симуляцію дружнього глушника в місці (50,75) і (10,75). На рисунку 3.1 показано ступінь секретності як функцію потужності перешкод.

Ми бачимо, що зі збільшенням потужності перешкод скритність спочатку зростає, а потім зменшується. Це пояснюється тим, що потужність перешкод має різний вплив на C_1 і C_2. Таким чином, є оптимальна точка для потужності перешкод. Крім того, оптимальна точка залежить від

розташування дружнього джерела перешкод, і дружнє джерело перешкод поблизу від перехоплювача є більш ефективним для підвищення секретності. Крім того, зауважте, що крива не опукла і не увігнута. На рисунку 3.2 видно, скільки потужності джерело купує від перешкод як функцію запитуваної ціни. Ми бачимо, що потужність знижується, якщо ціна зростає. У якийсь момент джерело перестане купувати електроенергію. Отже, існує компроміс для встановлення ціни, тобто якщо ціна надто висока, джерело буде купувати менше електроенергії або навіть не купуватиме нічого.

Для випадку двох користувачів ми налаштували наступне моделювання. Шкідливий вузол розташований у (50,90), дружній глушник один розташований у (50,50), а дружній глушник два розташований у (50,75). На рисунку 3.2, рисунку 3.3 та рисунку 3.4 видно корисність джерела U_s, корисність U_1 глушника один і корисність U_2 глушника два як функцію ціни обох користувачів відповідно. Ми бачимо, що джерело купує послугу лише в одного з дружніх глушників. Якщо дружній глушитель просить занадто низьку ціну, його корисність буде дуже низькою. З іншого боку, якщо джерело перешкод просить занадто високу ціну, це ризикує ситуацією, в якій джерело придбає послугу в іншого дружнього джерела перешкод. Існує оптимальна ціна для кожного доброзичливого глушника, і джерело завжди вибирає те, яке може забезпечити найкраще покращення продуктивності.

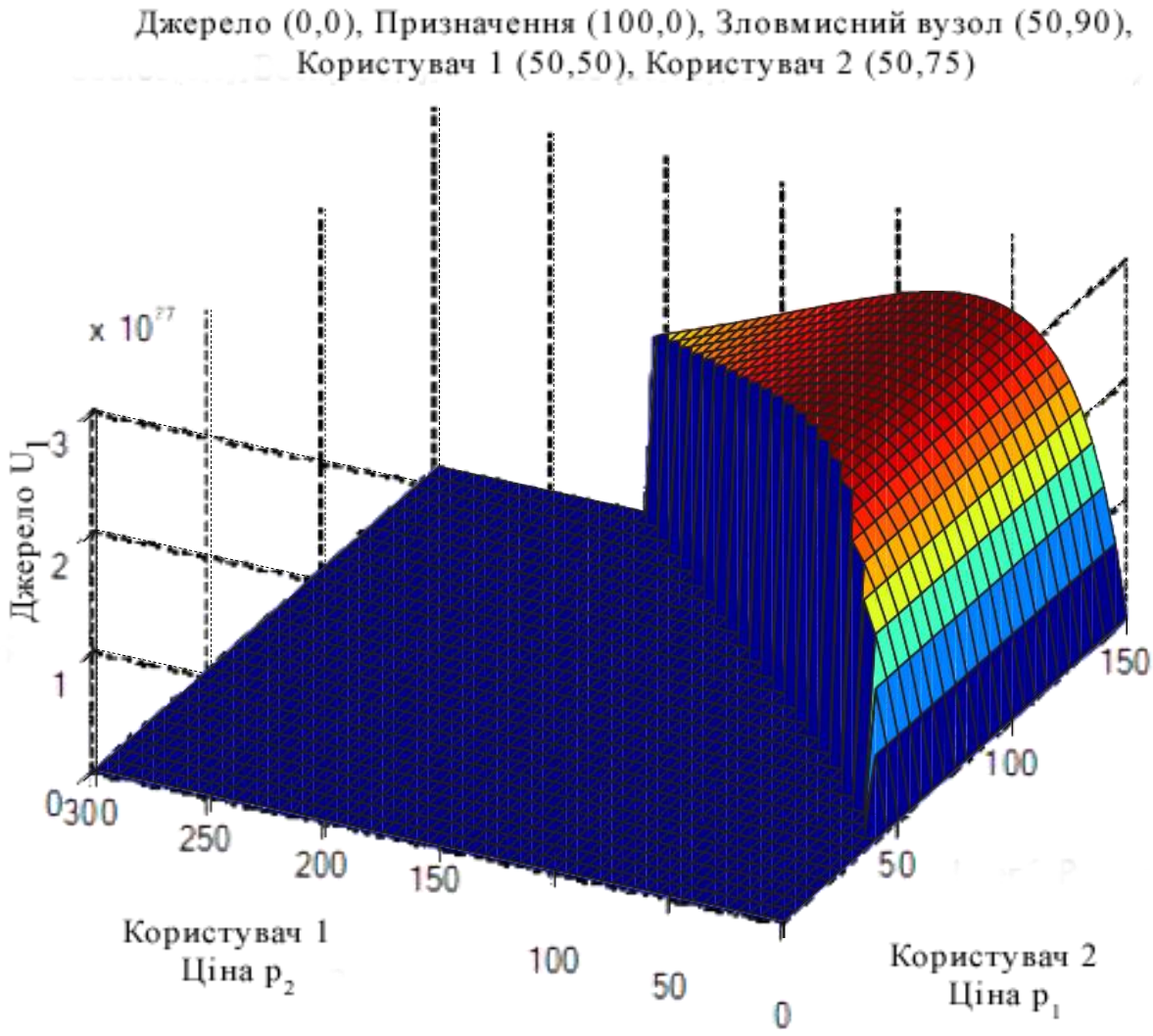

Рисунок 3.4 - U_1 проти цін двох користувачів

Далі ми встановлюємо симуляцію мобільності. Перший дружній глушитель фіксується на (50,50), а другий дружній глушитель змінюється від (-50,75) до (100,75). На рисунку 3.5 ми показуємо вихідні утиліти централізованої схеми та запропонованої гри. Ми бачимо, що централізована схема служить верхньою межею продуктивності. Результат гри знаходиться недалеко від верхньої межі, а рішення гри може бути реалізовано розподіленим способом. Ефективність гри тривіальна, коли дружній глушник

2 знаходиться близько до зловмисного перехоплювача від (20,75) до (70,75). На малюнку 3.5 видно потужність перешкод як функцію розташування перешкод 2. Ми бачимо, що залежно від розташування глушників джерело перемикається між двома глушителями для найкращої продуктивності. Крім того, джерело також купує оптимальну кількість потужності перешкод: коли пристрій перешкод знаходиться близько до зловмисного перехоплювача, джерело буде купувати менше енергії, оскільки пристрій перешкод є більш ефективним для підвищення секретності.

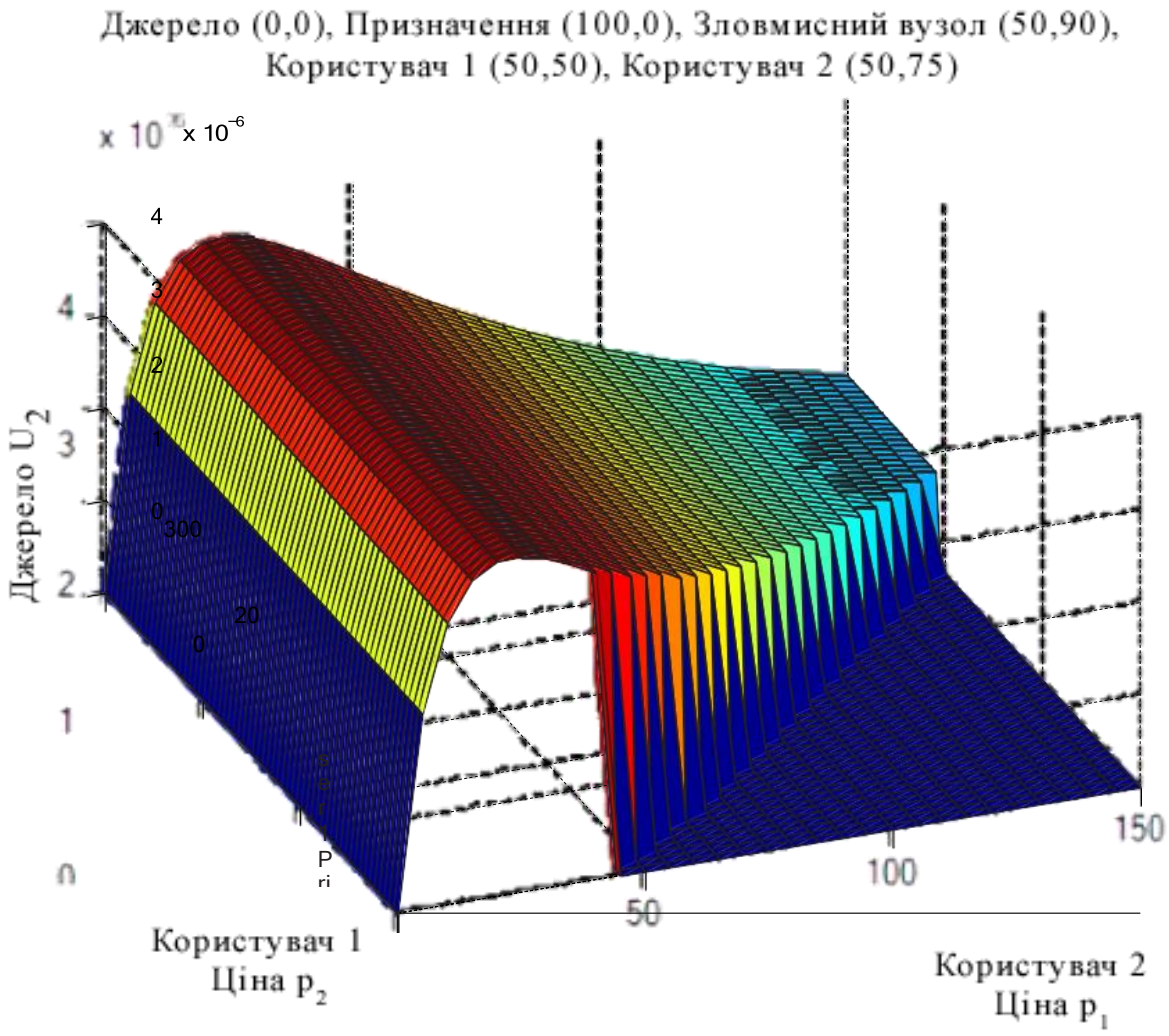

Рисунок 3.5 - U_2 проти цін двох користувачів

На малюнку 3.6 видно відповідні утиліти дружніх глушників запропонованої гри.

3.1.5 Висновки

Безпека на фізичному рівні – це нова техніка безпеки, яка є альтернативою традиційним криптографічним протоколам для досягнення ідеальної секретності, оскільки перехоплювачі не отримують інформації. У

літературі показано, що глушіння ефективно покращує секретність. У цій статті ми досліджуємо взаємодію між джерелом і дружніми перешкодами за допомогою теорії ігор, щоб отримати розподілене рішення. Джерело платить дружнім перешкодам за те, щоб вони перешкоджали зловмисному підслухувачу, щоб підвищити рівень секретності. Дружні глушники стягують з джерела плату за глушіння. Для аналізу результату гри ми досліджуємо гру Штакельбурга та будуємо розподілений алгоритм. Аналізуються такі властивості, як рівновага та конвергенція.

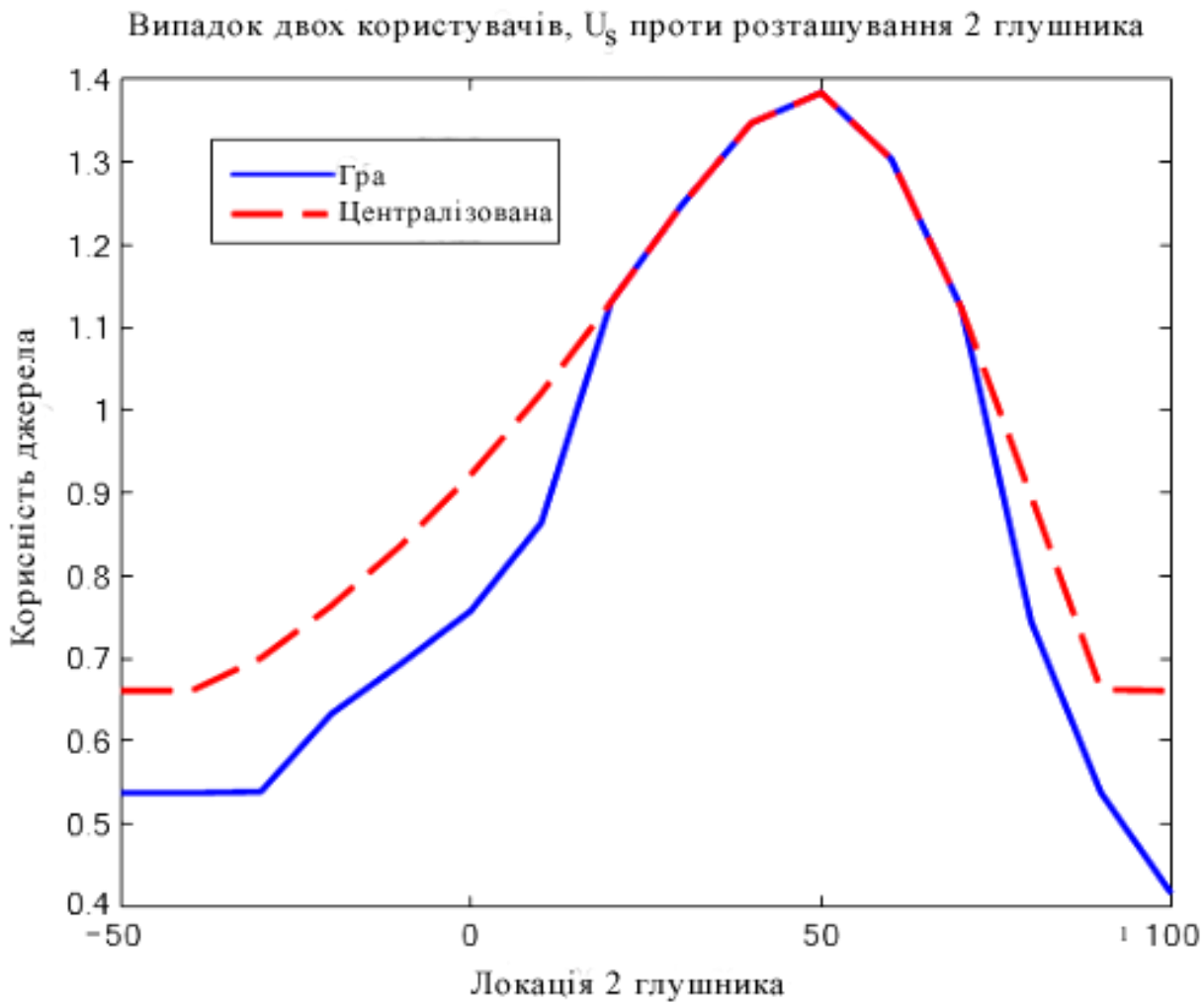

Рисунок 3.6 - U_s проти локації 2 глушника

Рисунок 3.7 - Потужність проти Локації 2 глушника

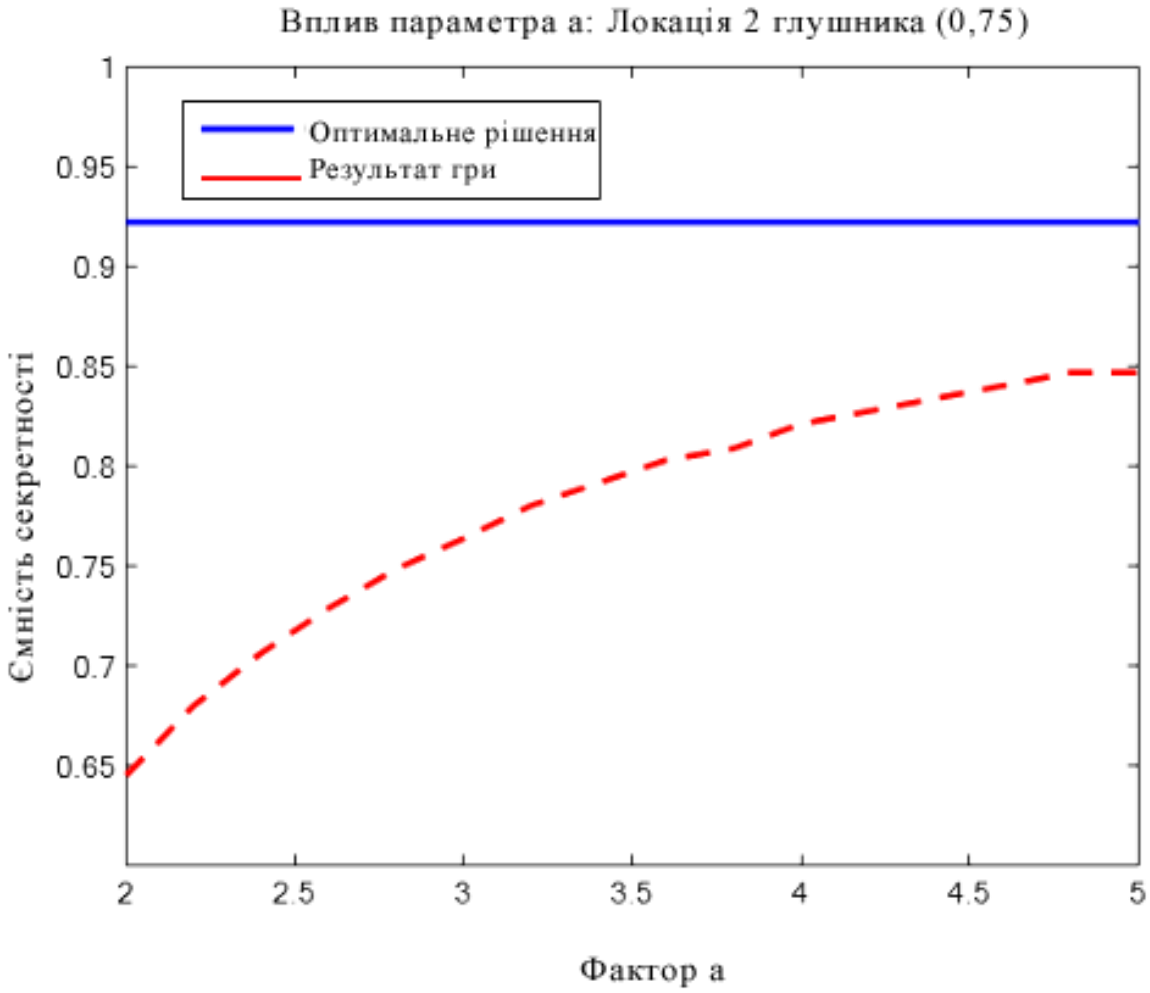

Рисунок 3.8 - Вплив параметра a на гру

3.2 Самоорганізована безпека мережі

Самоорганізована безпека мережі відноситься до підходу, в якому безпека мережі покладається на саму мережу та її складові елементи. Цей підхід передбачає, що мережеві компоненти повинні мати властивості та механізми, які дозволяють виявляти, уникати, відбивати або відновлюватися від можливих загроз безпеці.

Основні принципи самоорганізованої безпеки мережі включають:

1) Розподілена відповідальність: Кожен елемент мережі має бути відповідальним за свою безпеку та виявлення загроз у своєму окремому контексті. Це означає, що кожен вузол або компонент мережі повинен мати можливість виявляти та реагувати на потенційні загрози безпеці самостійно.

2) Автономне прийняття рішень: Елементи мережі повинні бути здатні самостійно приймати рішення про виявлення та реагування на загрози безпеці. Це означає, що вони мають мати вбудовану інтелектуальну здатність для аналізу та обробки інформації про стан мережі та виявлення загроз безпеці.

3) Зв'язок та співпраця: Елементи мережі повинні бути здатні спілкуватися та співпрацювати один з одним для обміну інформацією про стан безпеки та координації заходів для запобігання або відповіді на загрози.

4) Адаптивність: Мережа повинна мати здатність адаптуватися до нових загроз та змінюваних умов, виявляти нові шаблони загроз та застосовувати нові методи захисту для забезпечення безпеки.

5) Виявлення та відновлення: Мережа повинна мати механізми для виявлення атак та загроз безпеці, а також здатність до самовідновлення після атаки або відновлення нормального стану після інциденту.

Застосування самоорганізованої безпеки мережі може покращити стійкість мережі до атак та забезпечити швидку реакцію на нові загрози безпеці. Однак, варто пам'ятати, що це лише один з підходів до забезпечення безпеки мережі, і його застосування повинно бути доповнене іншими технологіями та практиками безпеки.

Конкретним застосуванням теорії ігор є розробка протоколів безпеки для самоорганізованих мереж, таких як мобільні adhoc мережі (MANETs), бездротові сенсорні мережі або автомобільні мережі. Завдяки відносно статичній конфігурації та однорідній архітектурі самоорганізованих мереж, поведінка мережі має тенденцію бути схожою на поведінку особи, яка приймає

розумні рішення, або логічної економічної людини, що робить її сумісною з вимогами теорії ігор.

3.3 Виявлення та запобігання вторгненням

Виявлення вторгнень вважається однією з найбільш широко застосовуваних областей дослідження безпеки з точки зору теорії ігор завдяки його характеристикам атаки та захисту. Вивчаючи ігрові моделі, можна оптимізувати розподілений дизайн, а також конфігурацію безпеки систем виявлення вторгнень. У зв'язку з цим були висунуті стратегії захисту, засновані на головоломках, проти флудових атак.

Виявлення та запобігання вторгненням можна розглядати з точки зору теорії ігор. Теорія ігор є математичним фреймворком для аналізу стратегічних взаємодій між різними учасниками, де кожен учасник приймає рішення, зокрема, стосовно безпеки та вторгнень.

У контексті виявлення та запобігання вторгненням, можна розглядати два основні типи гравців: атакуючий (хакер або зловмисник) та захисник (система безпеки мережі).

Атакуючий може використовувати різні стратегії, такі як проникнення через вразливості системи, злам паролів, соціальний інжиніринг тощо. Його метою може бути отримання незаконного доступу, крадіжка даних або завдання шкоди мережі.

Захисник також має свої стратегії для виявлення та запобігання вторгненням. Це може включати встановлення систем виявлення вторгнень (IDS) та систем запобігання вторгненням (IPS), налаштування мережевих правил та фільтрів, шифрування даних, аутентифікацію та авторизацію користувачів, оновлення програмного забезпечення для закриття вразливостей тощо.

Теорія ігор може допомогти уявити взаємодію між цими двома типами гравців та аналізувати їх рішення. Наприклад, атакуючий може аналізувати

систему безпеки, шукати її слабкі місця та використовувати їх. Захисник, з свого боку, може вдосконалювати систему безпеки, аналізувати попередні атаки та розробляти стратегії для запобігання подібним атакам у майбутньому.

У практиці виявлення та запобігання вторгненням використовуються різні методи та технології, такі як інтелектуальний аналіз даних, машинне навчання, аналіз журналів, аналіз трафіку, сигнатурні методи та евристичні алгоритми. Теорія ігор може допомогти виявити оптимальні стратегії для обох сторін у пошуку рішень, які найбільш ефективно забезпечують безпеку мережі.

3.4 Збереження конфіденційності та анонімності

Збереження конфіденційності та анонімності також можна розглядати з точки зору теорії ігор. У цьому контексті можна розглядати двох типів гравців: особу, яка хоче зберегти свою конфіденційність або анонімність (наприклад, користувача) і особу, яка намагається отримати інформацію про першу особу (наприклад, хакера або зловмисника).

Головною метою особи, яка хоче зберегти конфіденційність або анонімність, є уникнення розкриття своїх особистих даних або ідентифікації. Ця особа може використовувати різні стратегії, такі як шифрування комунікацій, використання анонімізаторів, використання віртуальних приватних мереж (VPN) або використання технологій анонімного перегляду.

З іншого боку, особа, яка намагається отримати інформацію про конфіденційну особу або розкрити її анонімність, може використовувати різні стратегії для отримання доступу до цієї інформації. Це може включати аналіз мережевого трафіку, використання методів перехоплення даних або спостереження за поведінкою користувача.

З точки зору теорії ігор, можна досліджувати стратегії обох типів гравців і аналізувати їх рішення в контексті збереження конфіденційності та анонімності. Головна мета полягає в тому, щоб особа, яка хоче зберегти

конфіденційність або анонімність, знаходила оптимальні стратегії, які максимально ускладнюють спроби отримати доступ до її інформації з боку особи, що намагається отримати цю інформацію.

Теорія ігор може також допомогти у визначенні оптимальних рішень та стратегій для третіх сторін, таких як органи правопорядку, які намагаються зберегти безпеку та захистити права людей у контексті конфіденційності та анонімності.

З точки зору теорії ігор, конфіденційність може бути оцінена користувачами, а різні стратегії можуть перевірятися на бажаний рівень конфіденційності. Теорія ігор може виявитися корисною для економічного аналізу збереження конфіденційності та пошуку найкращого компромісу між продуктивністю та конфіденційністю. Кілька ефективних служб на основі місцезнаходження забезпечують зручність для користувачів, але ціною конфіденційності користувачів. Ігри Штакельберга Байєса використовуються для моделювання взаємної оптимізації точності локалізації та конфіденційності розташування, і було доведено, що ця методологія показала кращі результати порівняно з механізмом прямої обфускації.

3.5 Економіка кібербезпеки

Оскільки теорія ігор спочатку була створена в теоретичних рамках економіки, вона може бути застосована головним чином до економіки кібербезпеки. Різноманітні стандартні економічні моделі та теорії знаходять застосування до економічної точки зору безпеки, як-от розробка політики безпеки, стимулювання безпеки та інвестиції в безпеку. Захист мережевої інфраструктури від атак є обов’язковим, оскільки атаки на високошвидкісні канали передачі даних можуть призвести до затримки або втрати великих даних.

Економіка кібербезпеки може бути розглянута з точки зору теорії ігор, яка досліджує стратегічні взаємодії між різними гравцями в умовах обмежених

ресурсів та конфліктів інтересів. Застосування теорії ігор до кібербезпеки допомагає розуміти динаміку між захисниками, атакуючими та іншими сторонами, що взаємодіють у кіберпросторі.

Основні аспекти економіки кібербезпеки, що можуть бути аналізовані з точки зору теорії ігор, включають:

a) Гра конфлікту між атакуючими та захисниками: Ця гра включає конфлікт інтересів між хакерами та захисниками. Атакуючі намагаються знайти вразливості в системах та отримати несанкціонований доступ, тоді як захисники намагаються запобігти таким атакам та зберегти безпеку мережі. Обидва боки можуть розробляти стратегії, аналізувати поведінку противника та використовувати різні тактики для досягнення своїх цілей.

b) Гра співробітництва між сторонами: У деяких випадках, захисники можуть співпрацювати між собою або з органами правопорядку для обміну інформацією про загрози та розробки захисних стратегій. Це може збільшити загальний рівень безпеки та покращити відповідь на загрози. Але тут виникає питання довіри та розподілу користі між учасниками.

c) Стратегії витрачання ресурсів: В економіці кібербезпеки, як і в багатьох інших сферах, існує обмеженість ресурсів. Захисники повинні приймати рішення про те, як виділити обмежені ресурси, такі як бюджет, персонал та технології, для запобігання атакам та забезпечення безпеки. В цьому контексті виникають стратегічні питання про оптимальні рішення, включаючи розподіл ресурсів, інвестування в нові технології та виявлення пріоритетів у витрачанні коштів.

Теорія ігор може допомогти в аналізі таких ситуацій, моделюванні стратегій та прийнятті рішень, які можуть покращити безпеку в кіберпросторі.

Вона може допомогти уявити різні сценарії взаємодії між учасниками та оцінити ризики та можливості в рамках економіки кібербезпеки.

3.6 Безпека хмарних обчислень

Хмарні обчислення – це процвітаюча галузь і добре відома концепція обробки інформації. Проте проблема безпеки є складною через використання різноманітних елементів інфраструктури в кожній моделі сервісу. Звичайні механізми безпеки не підходять для хмарних обчислень, оскільки нові хмарні концепції, такі як аутсорсинг, спільне використання ресурсів і багатокористування, є проблемою для спільноти дослідників безпеки. Але теорія ігор може змінити це питання.

Різні користувачі публічної хмари мають спільну платформу, таку як гіпервізор. Ця універсальна платформа посилює добре відому проблему взаємозалежності кібербезпеки, і користувач, який не інвестує в кібербезпеку, нав'язує іншим негативні зовнішні ефекти. Це одна з причин того, що багато великих організацій з конфіденційною інформацією не бажають приєднуватися до публічної хмари.

Безпека хмарних обчислень може бути розглянута з точки зору теорії ігор, яка вивчає стратегічні взаємодії між різними гравцями в умовах обмежених ресурсів та конфліктів інтересів. Застосування теорії ігор до безпеки хмарних обчислень може допомогти розуміти динаміку взаємодії між користувачами, хмарними провайдерами та потенційними зловмисниками.

Основні аспекти безпеки хмарних обчислень, які можна аналізувати з точки зору теорії ігор, включають:

1) Вибір хмарного провайдера: Користувачі мають вибирати хмарних провайдерів для своїх обчислювальних потреб. Ця гра включає конфлікт інтересів між користувачами, які хочуть максимальну безпеку та конфіденційність своїх даних, і провайдерами, які намагаються забезпечити послуги з високою доступністю та ефективністю.

Користувачі мають оцінювати рівень безпеки, надійності та довіри до провайдера перед вибором.

2) Захист даних та конфіденційність: Користувачі, що використовують хмарні обчислення, мають бути упевнені в безпеці своїх даних та конфіденційності. Це вимагає використання стратегій шифрування даних, контролю доступу та захисту від зловмисних атак. З точки зору теорії ігор, можна аналізувати взаємодію між користувачами та провайдерами щодо забезпечення безпеки даних та уникнення можливих загроз.
3) Атаки та відповідь на них: Зловмисники можуть намагатися зламати хмарні системи, отримати несанкціонований доступ до даних користувачів або провести інші атаки. З точки зору теорії ігор, можна досліджувати стратегії захисників та атакуючих сторін, їх рішення та вплив на безпеку хмарних обчислень. Це може допомогти розробити ефективні алгоритми виявлення та запобігання атакам.
4) Співпраця між учасниками: Деякі аспекти безпеки хмарних обчислень можуть потребувати співпраці між користувачами, провайдерами та іншими сторонами, такими як органи правопорядку. Співпраця може включати обмін інформацією про загрози, спільні стратегії захисту та спільні зусилля для забезпечення безпеки хмарних обчислень.

Теорія ігор може допомогти аналізувати стратегії та рішення учасників екосистеми хмарних обчислень, моделювати їх взаємодію та оцінювати ризики та можливості в рамках безпеки хмарних обчислень.

Гра FlipIt для хмарної безпеки, яка надає деталі про те, коли пристрої повинні довіряти командам хмарного гіпервізора. Це спілкування моделюється як гра з пристроєм, нападником і захисником як гравцями. Теоретико-ігрова модель оцінки ризиків безпеки була запропонована для хмарних обчислень, яка є масштабованою таким чином, що оцінюється, чи

системні ризики повинні бути виправлені орендарем або хмарним постачальником.

4 ПОЄДНАННЯ ТЕОРІЇ ІГР І КРИПТОГРАФІЇ

І теорія ігор, і криптографічні протоколи мають справу з аналізом взаємодії між взаємно підозрілими сторонами. Історично склалося так, що обидві галузі розвивалися незалежно одна від одної в різних дослідницьких спільнотах і, отже, ймовірно, матимуть різні смаки. Тим не менш, зростає інтерес до об'єднання підходів і технік цих галузей, які були натхненні бажанням розробки більш прагматичних протоколів і моделей такої взаємодії. Нинішнє дослідження зв'язку криптографії та теорії ігор можна розділити на дві категорії: застосування теоретико-ігрових моделей до розробки криптографічних протоколів і застосування криптографічних протоколів до проблем, заснованих на теорії ігор.

Традиційно протоколи в криптографії розробляються, припускаючи, що кілька учасників є автентичними та сумлінно дотримуються протоколів, тоді як інші учасники є зловмисними та діють хаотично. Проте теоретико-ігрова думка полягає в тому, що кожен учасник є раціональним і діє відповідно до своїх інтересів. Така перспектива відрізняється від криптографічної, згідно з якою протокол не повинен запобігати ірраціональній поведінці, хоча нікому не можна довіряти дотримання протоколу, якщо він не діє в найкращих інтересах учасника.

Загалом, криптографія зосереджена на гарантії того, що сторони продовжуватимуть використовувати авторизовану службу, і теоретико-ігровий підхід має ту саму мету. Теоретико-ігрові методи використовуються для розробки механізмів стимулювання, спрямованих на запобігання відволіканню. Важливим мотивом застосування теоретико-ігрового методу в криптографії є моделювання зловмисної поведінки користувача. Обґрунтування цього полягає в тому, що зловмисні дії не тільки важче

контролювати, ніж раціональні дії, але також більш поширеним і практичним для деяких сторін є нечесне дотримання криптографічного протоколу. Для підвищення безпеки та ефективності криптографічних протоколів дослідники запропонували багато нових термінів і підходів. Наприклад, соціально-раціональний обмін секретами, використання ідеальної байєсівської рівноваги (PBE) або використання каналів «точка-точка», а не надійних посередників. Крім того, у стеганографії використовувалися теоретико-ігрові методи, які виявилися ідеальними для того, щоб дозволити дослідникам оцінювати кілька варіантів дизайну, наприклад розподіл корисного навантаження в пакетній стеганографії або функції спотворення в адаптивній стеганографії. Усі ці підходи демонструють величезну користь, яку приносить поєднання криптографії та теорії ігор у розробці механізмів захисту.

5 МАЙБУТНІ НАПРЯМКИ ДОСЛІДЖЕНЬ

Можливі майбутні напрямки дослідження теоретико-ігрових підходів до кібербезпеки та конфіденційності можуть складатися з кількох нових областей, а саме:

5.1 Соціальні медіа

Останнім часом соціальні медіа, наприклад, Twitter, Facebook, Telegram, Instagram, стали чудовими способами спілкування. Ці платформи можуть використовуватися зловмисниками як нові засоби масової інформації для проведення підступних атак. У зв'язку з масивними централізованими даними користувачів необхідно приділяти підвищену увагу захисту конфіденційності. Застосування теорії ігор до соціальних мереж може допомогти нам визначити цілі користувачів соціальних мереж і те, як вони працюють для їх досягнення. На основі формалізованих утиліт політик безпеки та правил безпеки вибір політик безпеки в доступі до контенту описується як гра між постачальником контенту та запитувачем контенту.

5.2 Хмарні обчислення

Безперечно, хмарні обчислення вважаються одним із важливих технологічних зрушень останнім часом. Тим не менш, під час переміщення даних у хмари виникають різні проблеми з безпекою та конфіденційністю. Теорія ігор є потенційною математичною основою для аналізу наслідків і причин проблем конфіденційності та цілісності для хмарних обчислень.

5.3 Bitcoin

Bitcoin — це електронна децентралізована фіатна валюта, яка реалізується за допомогою однорангової технології та криптографії. Розробка безпечних і ефективних методів майнінгу є однією з проблем, з якою

стикаються біткойни. Minigas, гру, можна моделювати серед усіх користувачів за допомогою теорії ігор.

5.4 Вбудована безпека

В одній точці можуть статися атаки зловмисного програмного забезпечення на апаратне забезпечення. Це найвигідніша сутність, яка надає можливість маніпулювати обчислювальною системою. Зловмисники таємно й навмисно модифікують електронні пристрої, як-от схеми цілісності, для створення апаратних троянів. Теорія ігор — це математична обробка конфліктів, тому її можна використовувати для стратегічного керування тестуванням мікросхем, щоб збалансувати ризики, пов’язані з апаратними троянами.

5.5 Кібер-страхування

Методи управління ризиками для покращення кібербезпеки є перспективними рішеннями з економічною вигодою для постачальників програмного забезпечення безпеки, користувачів і політиків. Теоретико-ігрові підходи використовувалися в різних дослідницьких роботах з кіберстрахування для моделювання взаємодії між гравцями кіберринкового страхування, де роздрібна торгівля кіберстрахуванням розглядається як механізм захисту. Хоча теорія ігор може допомогти в розробці механізмів стимулювання страховиків, потрібні додаткові методи для відповіді на запитання, які ставить кіберстрахування для покращення кібербезпеки та конфіденційності.

5.6 Internet-of-Things

IoT забезпечує зв’язок між численними інтелектуальними пристроями, інтегрованими в мережі, для надання послуг у кожному аспекті людського життя. Будучи сприйнятливою до різноманітних атак, дослідницьке співтовариство має наголошувати на конфіденційності, а також на безпеці додатків IoT. У зв’язку зі швидким розвитком технологій, що утворюють IoT,

кілька нових ключових проблем і серйозні питання безпеки в IoT будуть потенційними темами для теоретико-ігрових методів.

5.7 Зв'язок між пристроями(D2D)

D2D стає новою тенденцією в промислових, а також академічних спільнотах через економічне споживання енергії та високу пропускну здатність. Очікується, що це буде ключова функція, підтримувана стільниковими мережами нового покоління. D2D може розширити покриття стільникового зв’язку, дозволяючи користувачам спілкуватися, коли телекомунікаційна інфраструктура сильно перевантажена або відсутня. Різноманітні потенційні теми, пов’язані з D2D-комунікаціями, такі як безпечна передача, покращена якість обслуговування та енергоефективність, можна розглядати з використанням ігрових структур максимізації функції корисності.

ВИСНОВОК

Теорія ігор відіграє життєво важливу роль у численних ситуаціях безпеки та широко застосована в кібербезпеці. Останні проведені дослідження показують ефективне використання теорії ігор у веб-безпеці, мережевій безпеці тощо. Теорія ігор дозволяє захиснику кількісно оцінити безпеку та передбачити результат безпеки, а також запропонувати інструмент розробки механізму для забезпечення безпеки за допомогою проектування та повернення переваги нападника. Ігри можна аналізувати та проектувати; Оптимальні рухи гравців можна використовувати для визначення того, наскільки ефективно можна підійти до безпеки в кіберсвіті. Однак важливою проблемою теорії ігор є здатність знайти можливе математичне рішення проблеми гри. Рекомендуються більш системні рішення, які вирішують проблему кібербезпеки з використанням теорії ігор, які передбачають практичні математичні рішення. Одним із таких підходів, який зараз вивчається дослідницьким співтовариством, є використання лінійного програмування. Крім того, можна заглибитися в цілочисельне програмування, щоб запропонувати більш прагматичне рішення для розподілених атак на відмову в обслуговуванні в кіберсвіті.

У цій дипломній роботі було досліджено застосування теорії ігор для захисту комп'ютерних систем. Головною метою було визначити, як теорія ігор може бути використана для забезпечення кібербезпеки і покращення захисту комп'ютерних систем.

У першому розділі роботи були розглянуті основні поняття та визначення теорії ігор, а також концепція рівноваги Неша. Це дало нам загальне розуміння того, як гравці взаємодіють у кіберпросторі і як їхні рішення впливають на безпеку комп'ютерних систем.

У другому розділі було розглянуто основні аспекти теорії ігор, такі як стратегії, граничні рішення, платежі, кооперація та конкуренція. Це дозволило нам розглянути різні сценарії взаємодії між гравцями в кіберпросторі та аналізувати їхні можливі наслідки для безпеки комп'ютерних систем.

Третій розділ роботи був присвячений теоретичним методам ігрових застосувань для кібербезпеки. Ми розглянули різні аспекти, такі як безпека фізичного рівня, самоорганізована безпека мережі, виявлення та запобігання вторгненням, збереження конфіденційності та анонімності, економіка кібербезпеки та безпека хмарних обчислень. Було виявлено, що застосування ігрових методів може забезпечити ефективний захист комп'ютерних систем у різних сферах.

У четвертому розділі було досліджено поєднання теорії ігор і криптографії. Ми встановили, що ці дві області можуть взаємодоповнюватися та сприяти створенню більш ефективних заходів безпеки для комп'ютерних систем.

В п'ятому розділі ми розглянули майбутні напрямки досліджень у галузі застосування теорії ігор для захисту комп'ютерних систем. Ми обговорили такі аспекти, як соціальні медіа, хмарні обчислення, Bitcoin, вбудована безпека, кібер-страхування, Internet-of-Things та зв'язок між пристроями (D2D). Ці напрямки досліджень відкривають нові можливості для покращення кібербезпеки та забезпечення безпеки комп'ютерних систем.

Загальним висновком дослідження є те, що застосування теорії ігор може бути важливим інструментом для покращення кібербезпеки і захисту комп'ютерних систем. Вона дозволяє аналізувати взаємодію між гравцями в кіберпросторі, враховувати їхні рішення та стратегії, і визначати оптимальні заходи для забезпечення безпеки.

Однак, необхідно продовжувати дослідження в цій галузі, зокрема розширюючи її застосування на нові сфери, які стають дедалі більш

важливими в контексті кібербезпеки. Такі напрямки, як соціальні медіа, хмарні обчислення, криптовалюти та Internet-of-Things, вимагають подальшого дослідження та розробки нових методів та стратегій для забезпечення їхньої безпеки.

Загалом, ця дипломна робота підтверджує важливість використання теорії ігор для захисту комп'ютерних систем і надає підґрунтя для подальших досліджень та розвитку в цій галузі. Це важливий крок у напрямку покращення кібербезпеки та захисту наших цифрових ресурсів.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Wang Y., Liu J., . Huang Z., and Xie P. A survey of game theoretic methods for cyber security, IEEE First International Conference on Data Science in Cyberspace (DSC), June 2016.
2. Li Z., Trappe W., Yates R. Secret communication via multi-antenna transmission, Proc. of 41st Conference on Information Sciences and Systems, Baltimore, MD, March 2007.
3. Liang Y., Poor H. V., Shamai (Shitz) S., Secure communication over fading channels, IEEE Transactions on Information Theory, June 2008, p.p. 2470-2492.
4. Zhu Q., Rass S., Game Theory Meets Network Security: A Tutorial, in CCS '18: 2018 ACM SIGSAC Conference on Computer & Communications Security. Toronto, October 2018.
5. Про основні засади забезпечення кібербезпеки України (Відомості Верховної Ради (ВВР), 2017, № 45, ст.403). URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 19.05.2023).
6. Fighting Cyber Attacks With Game Theory. *The first stop for security news: Threatpost.* URL: https://cutt.ly/m1YYRNF (дата звернення: 15.05.2023).
7. Cano-Berlanga S., Giménez-Gómez J-M., Vilella C. Enjoying cooperative games: The R package Game Theory, URL: https://www.sciencedirect.com/science/article/abs/pii/S0096300317301145?via%3Dihub (дата звернення: 21.05.2023).

8. Musman S., Turner A. A game theoretic approach to cyber security risk management. *Journal of Defense Modeling and Simulation: Applications, Methodology*. 2018, p.p. 127–146.
9. Губанов Д. А., Калашников А. О., Новиков Д. А. Теоретико-игровые модели информационногопротивоборства в социальных сетях, *Управление большими системами. Выпуск 31.* 2017, p.p. 192-204.
10. Alpcan T., Baar T. Network Security: A Decision and Game-Theoretic Approach, *Cambridge University Press40 W. 20*. St. New York, 2010.
11. Zhu H., Ninoslav M., Debbah M., Hjorungnes A.. Physical Layer Security Game: Interaction between Source, Eavesdropper and Friendly Jammer. EURASIP Journal on Wireless Communications and Networking, SpringerOpen, 2009, 21 p.
12. Bonneau N., Debbah M., Altman E., Hjørungnes A. Non-atomic games for multi-user systems, IEEE Journal on Selected Areas in Communications, *issue "Game Theory in Communication Systems"*, vol.26, no.7, p.p.1047-1058, September 2008.
13. Chung K., Kamhoua C. A., Kwiat K. A., Kalbarczyk Z. T., Iyer R. K. Game Theory with Learning for Cyber Security Monitoring, Proceedings of the 2016 IEEE 17th International Symposium on High Assurance Systems Engineering (HASE), IEEE, 2016, p.p. 1–8.
14. Han Z., Liu K. J. R. Resource Allocation for Wireless Networks: Basics, Techniques, and Applications, Cambridge University Press, UK, April, 2008.
15. Yates R. A framework for uplink power control in cellular radio systems, IEEE Journals on Selected Areas on Communications, vol.13, no.7, September 1995, p.p.1341-1348,.
16. Han Z., Liu K. J. R. Resource Allocation for Wireless Networks: Basics, Techniques, and Applications, *Cambridge University Press*. UK, April, 2008.

17. Negi R., Goelm S. Secret communication using artificial noise, in Proc. of IEEE Vehicular Technology Conference, vol. 3, September 2005, p.p. 1906-1910.
18. Musman S., Turner A. A game theoretic approach to cybersecurity risk management, *Journal of Defense Modeling and Simulation: Applications, Methodology*, Technology 2018.