МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ПУЛЮЯ

Александер М.Б., Балабан С.М.,
Карпінський М.П., Райба С.А., Чиж В.М.

ІНФОРМАЦІЙНА БЕЗПЕКА В СЕРЕДОВИЩІ БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖ

монографія

Тернопіль
2016

УДК 004.94
ББК 32.970
І-74

Автори:
Александер М.Б. докт. техн. наук, професор,
Балабан С.М., канд. техн. наук, доцент,
Карпінський М.П., докт. техн. наук, професор,
Райба С.А. докт. техн. наук, професор,
Чиж В.М., асистент.

Рекомендовано до друку вченою радою
Тернопільського національного технічного університету імені Івана Пулюя
протокол № 9 від 27 жовтня 2016 р.

Рецензенти:
Юдін О.К., докт. техн. наук, професор;
Смірнов О.А., докт. техн. наук, професор.

І-74 Інформаційна безпека в середовищі безпроводових сенсорних мереж : монографія / Александер М.Б., Балабан С.М., Карпінський М.П., Райба С.А., Чиж В.М. – Тернопіль : Вид-во ТНТУ імені Івана Пулюя, 2016. – 160 с.

ISBN 978-966-305-054-6

Для підвищення надійності автоматизованих систем з використанням безпроводових сенсорних мереж (БСМ), необхідна швидка ідентифікація пошкоджених інформаційних вузлів та їх графічне представлення. Існуючі засоби ідентифікації в переважній більшості стосуються пошуку одиничних пошкоджених елементів мережі. Відомі методи не дають можливості забезпечити надійність роботи БСМ при швидкому збільшенні кількості вузлів мережі та при «атаці» на групу сенсорів. У монографії здійснено аналіз загроз інформаційним ресурсам які обробляються в системах з використанням безпроводових сенсорних мережах. Описано прості та ефективні методи контролю та візуалізації параметрів, що характеризують роботу сенсорної мережі. Здійснено організацію контролю та візуалізації параметрів сигналів інформаційних вузлів, які являються складовими частинами мережі, створюють і використовують засоби моделювання безпроводових сенсорних мереж. Обґрунтовано доцільність використання кластерної моделі зі симплексним покриттям його поля для візуалізації областей трансформації сенсорів, сигнали яких зазнали атак. Реалізовано аналітичний метод дослідження зміни параметрів сигналів з використанням геометричних моделей в основі побудови яких використано чотириточкові симплекси. Доведено доцільність використання аналітичного методу для дослідження зміни сили сигналів інформаційних вузлів. Запропоновані методи моделювання допоможуть суттєво зменшувати час і фінансові затрати на розроблення апаратного і програмного забезпечення мереж порівняно з використанням реальних пристроїв. Отримані результати досліджень дають можливість забезпечити більш гнучкий моніторинг, виявлення пошкоджених елементів сенсорної мережі, отримання якісних і кількісних результатів. Монографія актуальна як для наукових працівників і дисертантів, так і для спеціалістів в галузі захисту інформації.

УДК 004.94
ББК 32.970

ISBN 978-966-305-054-6

Зміст

Передмова

Бурхливий розвиток інформаційних технологій сприяє створенню досконалих засобів зібрання та опрацювання великої кількості різноманітної інформації. Серед таких засобів особливе місце займають безпроводові сенсорні мережі (БСМ). В загальному випадку під безпроводовими сенсорними мережами (Wireless Sensor Network) розуміють мережі, що складаються із множини безпроводових інформаційних вузлів (ІВ), розміщених у просторі і призначених для моніторингу параметрів навколишнього середовища або об'єктів, що в ньому знаходяться.

БСМ являються одним із сучасних напрямків розвитку відказостійких та розподілених систем, які здатні до самоорганізації. Почали досліджувати і використовувати в середині 90-х років минулого століття, а найбільш успішним дослідником в цій галузі вважають професора Університету штату Каліфорнія Крістофеля Пістера. До теперішнього часу питанням створення та розгортання БСМ присвячено велику кількість наукових робіт, а дослідження в даній галузі проводяться практично у всьому світі. На даному етапі розвитку напівпровідникових технологій з'являються нові задачі пов'язані зі застосуванням БСМ, вважається, що технологія БСМ настільки універсальна, що її можна використовувати практично у всіх сферах діяльності людини, а можливість передавати інформацію від одного інформаційного вузла до іншого дозволяє розгортати БСМ на практично необмежених площах. Зі зменшенням вартості ІВ, дуже низьке енергоспоживання, а також використання безліцензійних діапазонів частот ISM (Industrial, Scientific, Medical) призводить до масового використання елементів сенсорних мереж в будь-які сфері людської діяльності.

До основних особливостей та переваг БСМ дослідники відносять:

- низьку вартість та малі габарити інформаційних вузлів;
- легкість та швидкість розгортання автоматизованих систем (АС) на базі БСМ;
- високу енергетичну ефективність – термін експлуатації може сягати декількох років;
- великі масштаби мереж (від одиниць до тисяч пристроїв) з щільним розміщенням інформаційних вузлів у просторі;
- масштабованість, та модернізація АС;

- високу надійність і відмовостійкість системи, яка досягається комунікаційною надлишковістю – наявністю альтернативних маршрутів транспортування даних;
- стійкість до зміни топології мережі;
- характеристик середовища розповсюдження радіохвиль;
- самоналаштування і самовідновлення мережі;
- здатність інформаційних вузлів самостійно опрацьовувати одержану інформацію і приймати рішення на базі розподілених алгоритмів;
- обмежені комунікаційні та енергетичні ресурси інформаційного вузла.

Розвиток і розширення сфер використання БСМ вимагають постійного підвищення їх надійності, довговічності, швидкодії і рівня захищеності інформації. Вирішувати дані проблеми важко без використання належних засобів для моделювання БСМ. З іншої сторони системи моделювання БСМ дозволяють розробляти апаратне і програмне забезпечення мереж із значно меншими затратами ніж у випадку використання реальних пристроїв.

Особливе місце серед засобів моделювання БСМ займає геометричне моделювання. Таке моделювання дозволяє використовувати методи обчислювальної геометрії, зокрема геометрії відстаней, яка дозволяє із факту існування співвідношень між вимірюваним відстанями досліджувати внутрішні властивості геометричних фігур.

На особливу увагу геометричне моделювання БСМ заслуговує під час відслідковування зміни сили сигналів інформаційних вузлів, оскільки за величиною зміни сили сигналів можна визначати енергетичний запас інформаційного вузла і спробу атаки направленої на руйнування сигналу. Дана монографія присвячена вивченню згаданих проблем.

Основою монографії є наукові дослідження авторів, де розглянуто особливості геометричного моделювання БСМ з використанням кластерних структур і запропоновано методи візуалізації величин змін сили сигналів інформаційних вузлів БСМ. Об’єктивний аналіз їх дозволить оцінити переваги і недоліки геометричного моделювання БСМ. Інформація, приведена у монографії буде корисною для розробки і удосконалення апаратно-програмного рішення пов’язаних з підвищенням рівня захищеності інформації у БСМ, а також у лекційних курсах, які читають у вищих навчальних закладах, для студентів, аспірантів та наукових працівників, що займаються питаннями захисту інформації.

Розділ 1. Аналіз структури та особливості поширення інформації в безпроводових сенсорних мереж

1.1. БСМ, їх будова і класифікація

Дослідники розвитку інформаційних технологій вказують, що в міру зростання необхідності зібрання , опрацювання і розповсюдження інформації необхідність у засобах більш складного опрацювання інформації зростає ще швидше [1]. Це приводить до необхідності об'єднувати відомі засоби зібрання, опрацювання і передачі інформації у структури, які називають мережами. Таким чином мережі це об'єднання необхідної кількості окремих інформаційних вузлів (ІВ) у єдину систему. При цьому для встановлення зв'язків між ІВ використовують проводовий зв'язок, волокнисту оптику, електромагнітні хвилі і супутниковий зв'язок. Крім організації зв'язку між ІВ мережі відрізняються між собою розмірами і принципами побудови. Так Е. Таненбаум пропонує за розмірами поділяти мережі на персональні (**PAN** - Personal Area Network), локальні(**LAN** - Local Area Network), глобальні та планетарні (**WAN** - Wide Area Network). Види зв'язків між ІВ і розміри мереж являються дуже важливими факторами класифікації, оскільки вони в основному впливають на технічні засоби, що використовуються для організації даних мереж.

Аналіз і дослідження, представлені в даній роботі, присвячені мережам, що організовані на основі радіохвильового зв'язку (БСМ) і підпадають під категорії персональних, локальних і муніципальних мереж. Відстань між ІВ в таких мережах може знаходитися в границях від 1 м до 10 км. Сама мережа може обмежуватися розмірами однієї кімнати, населеного пункту або адміністративно-територіальної одиниці. Персональні і локальні мережі називають приватними, оскільки вони розміщуються, як правило, в одному приміщені або на території організації чи підприємства і покривають площу до декількох квадратних кілометрів. Прикладом таких мереж можуть бути системи пожежної та охоронної сигналізації. Муніципальні мережі (MAN) об'єднують ІВ, які можуть бути розміщені на території адміністративно - територіальних одиниць і покривають площу від кількох десятків до тисяч квадратних кілометрів. Прикладом таких мереж можуть бути системи контролю за параметрами навколишнього середовища, станом здоров'я певної категорії хворих, обліку комунальних послуг.

Розширення сфер використання БСМ, зростання обсягу інформації, яку вони опрацьовують, підвищення умов надійності та конфіденційності приводить до ускладнення будови і програмного забезпечення БСМ, що у свою чергу сприяє виникненню великої кількості їх різновидностей. Відомі БСМ відрізняють за призначенням, будовою та організацією роботи. Тому питання їх класифікації займає особливе місце під час досліджень, виконання проектувальних робіт і розробки нових методів контролю і аналізу роботи [2, 3].

Оскільки для класифікації БСМ існує багато критеріїв, а самі мережі розвиваються надзвичайно швидко, відомі системи класифікації, як правило, в неповній мірі задовольняють вимоги дослідників. Отже, системи класифікації БСМ доцільно постійно доповнювати і змінювати. Для розробки і вибору методів геометричного моделювання БСМ запропоновано схему класифікації приведену у таблиці 1.

За середовищем передачі інформації БСМ поділяють на інфрачервоні (ІЧ) і радіочастотні (РЧ). Мережі з системами зв’язку, які працюють у інфрачервоному діапазоні використовують електромагнітні хвилі довжиною 0,74-2 мкм. Системи зв’язку складаються із випромінювача у вигляді інфрачервоного світлодіоду та приймача у вигляді фотодіода. Якщо у мережі використовують протоколи гарантованої передачі інформації, то передавачем і приймачем обладнують кожну зі сторін зв’язку. Інфрачервоні канали зв’язку можуть працювати в умовах прямої видимості та забезпечувати зв'язок на віддалі до декількох кілометрів. Використовують їх, як правило, для організації персональних мереж. Системи зв’язку, які працюють у інфрачервоному діапазоні, не чутливі до електромагнітних перешкод і не шкідливі для людського організму. До їх недоліків відносять недостатню захищеність інформації, відносно низьку швидкість передачі інформації, обмежену дальність дії, високу вартість приймачів і передавачів через необхідність організації перетворення електричних сигналів у інфрачервоні та навпаки.

Мережі зі системами зв’язку, які працюють у радіочастотному діапазоні використовують УВЧ і СВЧ. Кожен радіомодем комплектують антеною і передавачем для направленого передавання сигналів. Відомі системи суттєво відрізняються як за радіусом дії, так і за швидкістю передавання інформації. Системи зв’язку, які працюють у радіочастотному діапазоні, чуттєві до електромагнітних перешкод, не забезпечують достатньої захищеності і конфіденційності інформації.

За структурою (архітектурою) БСМ поділяють на однорівневі (гомогенні) і багаторівневі (гетерогенні) [4, 5]. БСМ до складу яких входять інформаційні вузли одного виду називають гомогенними (рис. 1.1).

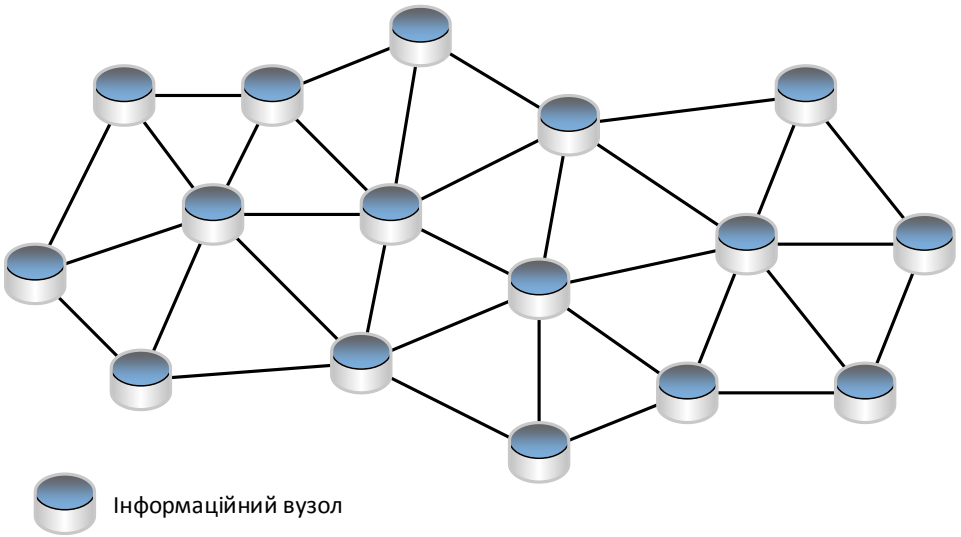


Рис. 1.1. Топологія гомогенної мережі

Таблиця 1.1.

Класифікація безпроводових сенсорних мереж (БСМ)

За радіусом дії				
	Персональні			
	Локальні			
	Муніципальні			
За середовищем передачі інформації				
	Інфрачервоні			
		Звичайні		
		Лазерні		
	Радіочастотні			
		СВЧ		
		УВЧ		
За структурою (архітектурою)				
	Однорівневі (гомогенні)			
	Багаторівневі (гетерогенні)			

За характером роботи				
	Постійної дії (асинхронні)			
	Періодичної дії (синхронні)			
	Комбіновані			
За джерелами живлення				
	Централізоване			
		Постійного струму		
		Змінного струму		
	Автономне			
		Батарейне		
		Акумуляторне		
За принципами розміщення				
	Хаотичне			
	Планове			
За характером використання				
	Стаціонарні			
	Мобільні			
За характером модуляції радіосигналів				
	Шумоподібні			
	З безпосередньою модуляцією частоти			
	З лінійною частотною модуляцією			
	З вузькосмуговою модуляцією			

В основу роботи гомогенних БСМ закладено принцип самоорганізації. В такій мережі всі вузли здатні ретранслювати пакети інформації в процесі їх передачі. Причому в конкретний момент часу роль головного вузла бере на себе довільний ІВ, топологічні та фізичні параметри якого відповідають встановленим вимогам.

БСМ до яких входять ІВ різних видів називають гетерогенними. Як правило, такі мережі складаються з координаторів (К), маршрутизаторів (М) та кінцевих ІВ (рис. 1.2). Координатор керує процесом створення мережі та задає параметри режимів роботи всіх інших вузлів. В мережі присутній тільки один

PAN – координатор. Маршрутизатор ретранслює пакети інформації, підтримує всі топології мережі і може виконувати функції координатора частини мережі, яку називають кластером. Кінцевий ІВ (просто ІВ) збирає необхідну інформацію на обмеженій території, виконує передачу її до маршрутизатора. При такій організації роботи маршрути передачі інформації зв'язані зі структурою мережі та можуть сильно відрізнятися від оптимальних. Крім того, гетерогенні мережі не стійкі до змін у топології.

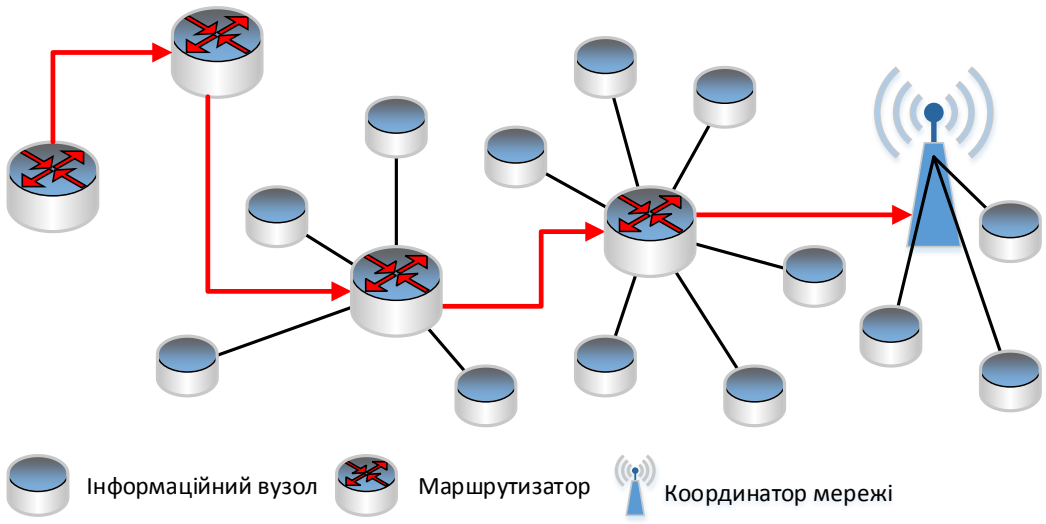


Рис. 1.2. Топологія гетерогенної мережі

За характером роботи БСМ поділяють на мережі постійної та періодичної дії [6, 7]. ІВ, які входять до складу постійно діючих (асинхронних) БСМ, постійно знаходять у робочому режимі. Тобто постійно відслідковують і передають інформацію. Така організація мереж оправдана під час виконання ними охоронних функцій, слідкування за технологічними процесами, моніторингу екологічних параметрів навколишнього середовища, вирішення низки завдань оборонного характеру. За висновками дослідників, ІВ використовують найбільше енергії на організацію зв'язку у мережі, який передбачає як передавання так і приймання інформації. Так для цього ІВ витрачають від 60% до 80% енергії джерел живлення, якими вони обладнані [8]. Таким чином робота ІВ у безперервному режимі приводить до значної втрати енергії та скорочення часу функціонування мережі.

БСМ, в яких ІВ працюють періодично, відносять до мереж періодичної (синхронної) дії. Використання БСМ у синхронному режимі дозволяє зменшити

енергетичні витрати, збільшити час функціонування мережі, зменшити негативний вплив електромагнітних хвиль на навколишнє середовище, підвищити надійність роботи і збільшити рівень захищеності інформації.

Відомо, що включення передавача займає долі секунди і для цього затрачається мала кількість енергії. Але при зменшені пакетів інформації, що передають ІВ, потужність запуску починає домінувати поміж статтями витрат енергії ІВ. В результаті збільшення частоти включень і виключень ІВ стає неефективним. Тому останнім часом значного розповсюдження набули так звані комбіновані режими роботи БСМ. В результаті реалізації такого режиму роботи основна кількість ІВ, об'єднаних у кластери, працюють у синхронному режимі, а одночасно окремі ІВ працюють у асинхронному режимі. При цьому у гомогенних мережах режим роботи ІВ можуть з часом змінюватися.

За видом джерел живлення БСМ поділяють на мережі з централізованим і автономним живленням ІВ. В мережах з централізованим живленням передбачено підключення ІВ до електричних мереж з постійним або перемінним струмом. При цьому централізоване живлення, як правило, використовують ІВ, що працюють в асинхронному режимі [5, 6]. В мережах, до вузлів яких обмежений доступ, використовують автономне живлення. Джерела автономного живлення поділяють на невідновлювальні та відновлювальні. До невідновлювальних джерел живлення відносять батареї. До відновлювальних джерел відносять акумулятори з можливою підзарядкою від сонячної енергії або термальних елементів.

За принципом розміщення ІВ БСМ поділяють на мережі з планово і хаотично розміщеними вузлами [8, 9]. Планове або упорядковане розміщення ІВ в БСМ використовують для моніторингу об'єктів, розташованих у просторі. При цьому заданими є точки цього об'єкту, в яких обов'язково повинні бути розміщені ІВ, які здійснюють збір необхідної інформації. Інформація, одержана цими вузлами, повинна бути передана з необхідним ступенем надійності і точності. Мережі з плановим розміщенням ІВ використовують для моніторингу інженерних систем, будівель і споруд (системи охоронні, пожежної сигналізації, контролю доступності, моніторингу цілісності будівель і мостів, обліку комунальних послуг, контролю кліматичних параметрів); промислового та екологічного моніторингу (системи виявлення, ідентифікації джерел забруднення повітря та води, контролю за поливанням, сейсмічною активністю та вулканічною діяльністю).

Хаотичне або випадкове розміщення ІВ в БСМ застосовують у випадках, коли не залишається іншої можливості створення мережі. Наприклад, для організації спостережень у розвідувальних цілях в районах бойових дій, зонах стихійних лих або аварійних ситуацій. Для налагоджування роботи таких мереж важливе значення має вибір моделі випадкового розподілу ІВ. Запропоновано три моделі такого розподілу: простий (двовимірний нормальний розподіл); Гаусовий розподіл, R – випадковий розподіл, в якому ІВ однорідно-розподілені відносно радіальних і кутових напрямів від базової станції [10].

За характером використання БСМ поділяють на стаціонарні і мобільні [2, 3]. Стаціонарними називають БСМ, у яких ІВ прив'язані до відповідної точки у просторі. Їх відносять до класу чарункових (Wireless Mesh Network) [11]. До стаціонарних відносять практично всі БСМ з планово розміщеними ІВ.

Мобільними або спеціальними називають БСМ, у яких ІВ вільно переміщуються у просторі. Такі мережі відносять до класу MANET (Mobile Ad hoc Network) [4, 12]. З поміж мобільних БСМ виділяють рухомі або блукаючі. В таких мережах ІВ можуть переміщуватися на відстані, що перевищують радіус дії однієї точки доступу або одного сегменту радіомережі. При цьому передбачено автоматичне перемикання від однієї точки доступу до іншої. Аналіз роботи стаціонарних і мобільних БСМ дозволяє зробити висновок, що мобільні ІВ з періодичною активністю здатні забезпечити підвищену живучість мережі за рахунок забезпечення більшої самоорганізації та масштабування [13].

За характером модуляції радіосигналів БСМ поділяють на шумоподібні, з лінійною частотою модуляції, з вузькосмуговою модуляцією. Мережі, в яких використовують шумоподібні системи модуляції радіосигналів, поділяють на системи із скачкоподібною переналадкою частот FHSS (Frequency-hopping) і системи з безпосередньою модуляцією DSSS (Direct Sequence Spread Spectrum).

Роботу БСМ забезпечують апаратна і програмна складові. Апаратна складова БСМ залежить від багатьох факторів пов'язаних з призначенням, умовами роботи і особливостями мережі. В загальному випадку БСМ складаються з вузлів трьох рівнів: функціональні ІВ, які здійснюють збір інформації в зоні їх розміщення; транспортні вузли (шлюзи), які виконують передачу інформації і керування маршрутами її поширення; базові станції, які здійснюють глобальну координацію, організацію і встановлення параметрів мережі [9]. Програмна складова БСМ агрегатує канальний, мережевий рівні і рівень додатків, що дозволяє забез-

печити передавання інформації від всіх вузлів мережі до базових станцій і сервера мережі [6]. Мережі будують на основі протоколів IEEE 802.15.4, Zig Bee, Digi Mesh.

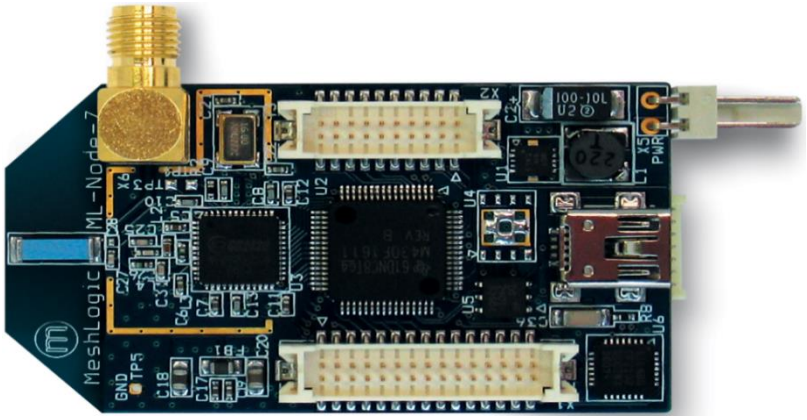
1.2. Будова функціональних ІВ першого рівня

У сучасних БСМ функціональні ІВ першого рівня виконують збір інформації, попереднє її опрацювання і передавання для подальшого опрацювання. У літературних джерелах такі вузли називають давачами, мотами або сенсорами [1, 3, 5, 7, 14]. За визначенням спеціалістів давачі здатні збирати строго визначену інформацію, наприклад, перетворювати конкретний параметр об'єкту, за яким ведеться спостереження, і передавати її до центральних вузлів для накопичення і опрацювання. Використання простих давачів у сучасних БСМ є не раціональним, а у багатьох випадках і не можливим, оскільки вони не мають можливості аналізувати одержану інформацію, відокремлювати її від шумів і в компактній формі передавати до ІВ вищого рівня. В такому випадку для одержання достовірної інформації необхідно використовувати велику кількість давачів і детально розробляти план їх розміщення у просторі, який необхідно контролювати. Відповідно для таких мереж характерним є мала перепускна спроможність інформації, висока енергоємність, низький рівень захищеності інформації та надійності.

Розвиток мікро-електроніки, безпроводового зв'язку та цифрової електроніки дозволили створити недорогі, малопотужні та багатофункціональні ІВ першого рівня, які називають мотами. Моти характеризуються невеликими геометричними розмірами і можливістю підтримувати зв'язок між собою. Це дозволяє використовувати велику кількість мотів, випадково розміщених близько до об'єкту, за яким ведеться спостереження. А мережеві протоколи та алгоритми роботи мотів дають можливість самоорганізації мережі. Кожен мот такої мережі виконує перетворення конкретної фізичної величини, попереднє опрацювання одержаної інформації та передачу її в ефір. Моти обладнані передавачами малої потужності, тому, як правило, для передачі інформації до ІВ вищого рівня використовують проміжні моти.

Подальший розвиток MEMS – технологій, безпровідного зв'язку та цифрової електроніки дозволив створити дешеві, енергоощадні та багатофункціональні ІВ першого рівня, які називають сенсорами (рис. 1.3).

а) б) в)



д)

Рис. 1.3. Зовнішній вигляд і компонування пристроїв сенсора: а) плата мудоля ML-Module-Z, б) безпроводовий шлюз системи моніторингу, в) безпроводові давачі температури та освітленності, д) компонування елементів ML-Module-Z

Сенсори складаються із чотирьох основних компонентів (рис. 1.4): блоку збору інформації, блоку опрацювання інформації, передавача і блоку живлення. Наявність додаткових модулів залежить від конкретного використання мережі. Наприклад, можна використовувати модулі визначення місця знаходження, силовий генератор і мобілізатор. Блок збору інформації, як правило, складається з двох частин: давача і аналого-цифрового перетворювача (АЦП). Аналоговий сигнал, який генерує давач на основі контрольованого параметру, АЦП перетворює у цифровий сигнал. Цифровий сигнал, у свою чергу, подається у блок опрацювання, до якого входять процесор і модуль пам'яті. Блок опрацювання керує процедурами, які дозволяють спільно з іншими сенсорами виконувати завдання, поставлені перед мережею. Передавач представляє собою радіочастотний прийомопередавач і з'єднує сенсор з іншими вузлами, що входять до складу мережі. Роботу ІВ забезпечує блок живлення.

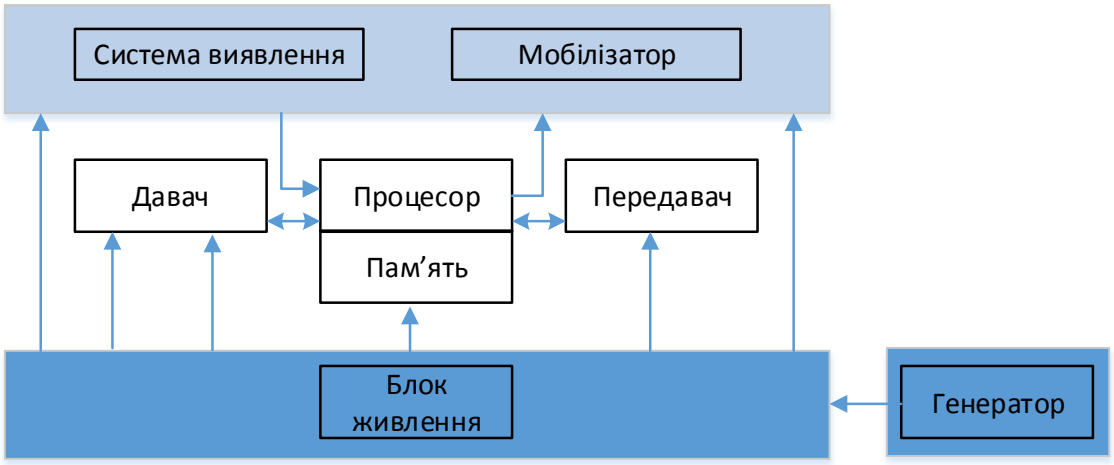


Рис. 1.4. Блок-схема сенсора

В загальному випадку ІВ першого рівня повинні відповідати наступним вимогам:

- споживати дуже мало енергії,
- працювати з великою кількістю вузлів на малих відстанях,
- мати низьку собівартість,
- бути автономними та працювати без нагляду,
- адаптуватися до навколишнього середовища.

Сьогодні існує велика кількість таких пристроїв різної конструкції. Серед них трапляються такі розміри, яких не перевищують кубічного сантиметра або настільки легкі, що зависають у повітрі.

1.3. Транзитні вузли

До транзитних вузлів БСМ відносять шлюзи і маршрутизатори [15]. Шлюзом називають електронний пристрій, що здатний агрегатувати інформацію одержану від ІВ мережі, конфігурувати мережеві параметри, під'єднувати мережеві елементи і функціонувати, як портал моніторингу мережевих характеристик. Шлюз координує зв'язок між функціональними ІВ і базовою станцією мережі. Для виконання вказаних функцій пристрій обладнаний вхідним вузлом з передавачем, який збирає інформацію від ІВ і порталом для гнучкого з'єднання з базовою станцією.

Працюючи без маршрутизатора шлюз NIWSN Ethernet може з'єднувати 8 ІВ. За рахунок використання у мережевій топології маршрутизаторів шлюз може з'єднувати 36 вузлів. На рис. 1.5 показано маршрутизатор Phy Net Router з

вбудованою двонапрямленою антеною на 2,4 ГГц. Розміри такого маршрутизатора 4,4 х 2,3 х 9,3 см, вага 718 г. Для його живлення від стаціонарної електричної мережі передбачено використання зовнішнього адаптера на 100-240 В АС на 50/60 Гц, який на виході забезпечує номінальну постійну напругу на 5 В.

Рис. 1.5. Маршрутизатори Phy Net Router

В сучасних БСМ маршрутизатори транслюють пакети інформації, здійснюють динамічну маршрутизацію, відновлюють маршрути, що зруйнувалися в результаті перевантаження мережі або виходу з ладу окремих ІВ. Маршрутизатори можуть працювати з базовою станцією, шлюзом, іншими маршрутизаторами та ІВ. Один маршрутизатор може контролювати одночасно 32 ІВ, які перебувають у режимі очікування.

Маршрутизатори дозволяють будувати великі масштабовані розгорнуті та розгалужені БСМ і керувати одночасно багатьма мережами з базової станції. Використання достатньої кількості маршрутизаторів дозволяє збільшити число підключених ІВ, зменшити затримання передачі інформації у зв’язку з її підготуванням, наприклад з розсиланням запитів, удосконалити маршрути трансляції інформації, що приведе до зменшення енергетичних витрат і збільшення строку служби БСМ.

1.4. Базові станції

Базові станції, які в літературних джерелах називають координаторами або серверами [15], організовують зв'язок, як з окремими інформаційними і транзитними вузлами, так і з сенсорними стільниковими mesh-мережами. Це дає змогу створити БСМ на великих територіях і відстанях, і контролювати їх централізовано. В загальному, базова станція формує мережу, виконує функції

центру керування мережею і центру довіри. Тобто встановлює політику безпеки, задає налаштування в процесі приєднання вузлів до мережі, володіє ключами безпеки мережі. Крім виконання функцій управління базова станція дозволяє організувати архівування інформації, її експортування, презентацію і аналіз.

Зокрема Phy Net Server забезпечує трансляцію інтерфейсів ІВ у веб-сервіси з SOAP/Rest/XM інтерфейсами, веб-консоль користувача для налаштування ІВ, візуалізацію стану розгортання БСМ на дисплеї у вигляді карти користувача або зображення, відкриває, реєструє, переміщує, конфігурує вузли, вмикає/вимикає ІВ, відображає батарейний статус, програмує гетерогенні вузли, дозволяє налаштувати маршрутизатори, графічно відображати статистику, налаштувати інтервали звітності, пороги і попередження.

До складу Phy Net Server (рис. 1.6) входить: процесор 1,6 ГГц, пам'ять 512 Мбайт, жорсткий диск 60 Гбайт, порти вводу/виводу RJ 45 10/1000 Ethernet, USB, Wi-Fi. Тобто для керування БСМ підприємства достатньо пристрою, який функціонально подібний до малого ІІК, вміщується у корпус з розмірами 14,6х25х4,198 см. важить 1,36 кг. Роботу такої базової станції забезпечує зовнішній адаптер перемінної напруги 100-240 В. Робоча температура сервера від 0 до 40 ^{0}С.

Рис. 1.6. Базова станція Phy Net Server

1.5. Спеціалізоване програмне забезпечення БСМ

Під час розроблення програмного забезпечення, яке використовують для проектування, налагодження та організації роботи БСМ, дотримуються відпові-

дних правил і дій, які об'єднані у стандарти і мережеві протоколи. На сьогоднішній день існує декілька комплексів стандартів, які регламентують процеси проектування та розробки інформаційних систем. Зокрема стандарт IEEE 802.15.4 встановлює фізичні параметри для апаратної складової БСМ (фізичного рівня OSI моделі) (табл. 1.2).

Таблиця 1.2.

Основні параметри інформаційних вузлів

Вузол сенсорної мережі	**Безпроводовий стандарт**	**Тип ЦПУ**	**ОЗП**	**Мова програмування**	**Операційна система**
BTNode	Bluetooth (2,4 ГГц)	Atmel Atmega 128 L	64+180 kB	C	Btnut, TinyOS
Imote	Bluetooth (2,4 ГГц)	TI/Chipcon CC2430 SoC	64 kB	C	TinyOS
Mulle	Bluetooth (2,4 ГГц)	Renesas M16C/62P	31 kB	NesC, C	TinyOS
Iris	IEEE 802.15.4/ZigBee (2,4 ГГц)	Atmel ATmega1281	8 kB	NesC	TinyOS, MoteWorks
MTM-CM3300-MSP	IEEE 802.15.4 (2,4 ГГц)	TI MSP430F1611	10 kB	NesC, C	TinyOS v2.x
SenseNode	IEEE 802.15.4 (2,4 ГГц)	TI MSP430F1611	10 kB	NesC, C	TinyOS, GenOs
Ember	IEEE 802.15.4/ZigBee (2,4 ГГц)	Atmel ATmega128L	4 kB	C	EmberNet
SunSPOT	IEEE 802.15.4 (2,4 ГГц)	Atmel ARM920T	1 kB	Java	Squawk J2ME
ZigBit ZDM	IEEE 802.15.4/ZigBee (2,4 ГГц)	Atmel ATmega1281V	8 kB	C ZigBeeNet	ZigBit Development Kit

Під терміном «протокол» розуміють сукупність домовленостей відносно способу представлення інформації, який забезпечує її передавання у потрібному напрямку і правильну її інтерпретацію всіма учасниками процесу обміну інформацією [16]. Оскільки обмін інформацією являється багатофункціональним процесом, то протоколи поділяються на рівні. Так мережеві протоколи умовно поділяються на канальні, мережеві, транспортні, сеансові, прикладні. До кожного рівня відноситься група споріднених функцій.

Для забезпечення умов безперебійної взаємодії вузлів різних мереж їхня архітектура повинна бути відкритою. Такі умови забезпечує уніфікація і стандартизація мережевих протоколів, яку виконують ряд міжнародних організацій. Тому одночасно з існуванням великої різноманітності мереж існує багато різних протоколів. До найбільш розповсюджених відносять протоколи розроблені Інститутом інженерів з електротехніки та електроніки (IEEE) і протоколи відкритих систем Міжнародної організації (ISO - International Standard Organization). Протоколи ISO відомі як протоколи базової еталонної моделі взаємозв'язку відкритих систем.

Протоколи, які забезпечують роботу мережі, об'єднують у специфікації. Для організації і забезпечення роботи БСМ використовують протоколи Zig Bee. Дані специфікації орієнтовані на додатки, які потребують гарантованої безпечної передачі інформації при відносно невеликих швидкостях і довготривалої роботи ІВ.

Процес стандартизації постійно розвивається. Так розробники БСМ мають можливість користуватися специфікацією Wireless HART, яка являється частиною 7-ої версії стандарту HART. В процесі розроблення знаходиться стандарт ISASP 100.11a. Відомі також окремі рішення, наприклад: SMARTMESH компанії Dustnetwork, Mesh scape від Millennial net та Sensi Net від Sensicast. До таких рішень відносять російську розробку – платформу Mesh Logic [17].

Розроблені програмні засоби дозволяють не тільки в автономному режимі розгортати сенсорні мережі, але і перепрограмувати, дистанційно керувати режимами їхнього функціонування, зібрання та візуалізації інформації. Крім зазначеного вище стеку протоколів Zig Bee, який базується на стандарті IEEE 802.13.4, розробники програмного забезпечення використовують операційну систему реального часу Tiny OS. Дана операційна система функціонує на мікропроцесорах з розрядною сіткою від 8 до 32 біт та оперативною пам'яттю, що не перевищує 2 КБ. До складу операційної системи входить набір функцій APJ, які дозволяють організувати попереднє опрацювання інформації безпосередньо ІВ.

Програмне забезпечення для БСМ разом зі засобами контролю та управління її роботою розділяють на три рівні [18] (рис.1.7): рівень ІВ, серверний рівень, рівень користувача. Кожному рівню відповідають його програмні засоби.

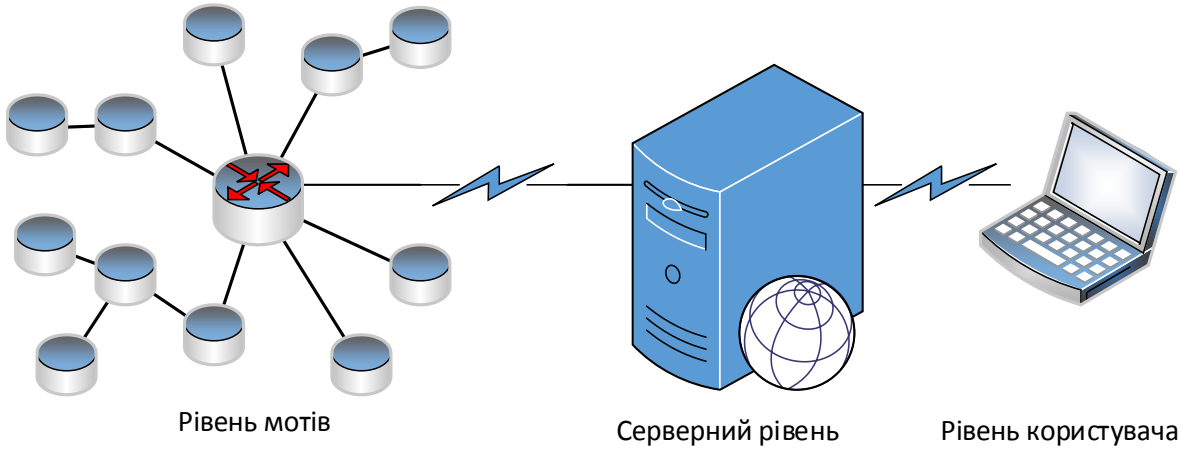


Рис. 1.7. Схема рівнів програмного забезпечення БСМ

Як приклад успішної роботи у напрямку розроблення програмного забезпечення для БСМ можна виділити компанії Sentilla та Crossbow. Зокрема компанія Sentilla здійснює перехід до нового покоління пристроїв і планує використовувати для програмного забезпечення не діалект мови С, а Java.

Компанія Crossbow використовує нові, більш ефективні апаратні засоби та програмне забезпечення орієнтуючись на мови С і С#. Програмні продукти цієї компанії підтримують, як коміркову топологію БСМ, так і топологію зірки. Програмне забезпечення Crossbow, розроблене для конфігурації мережі приведеної на рис. 1.7, називають Mote Works. Відповідно три його основні частини називають: XMesh – для рівня ІВ, XServe – для серверного рівня, Mote View –для рівня користувача. Крім цього до складу Mote Works входять ще декілька утиліт та оболонок, які використовують для розробки, розгортання та експлуатації БСМ.

Програмний засіб XMesh, який працює під керівництвом операційної системи Tiny OS, встановлений на кожен ІВ мережі. Таке програмне забезпечення в автоматичному режимі формує мережу та організовує транспортування інформації від ІВ до шлюзу. XMesh – це стек протоколів, який забезпечує передачу інформації по довільному ланцюжку від одного ІВ до іншого, що значно розширює загальний діапазон передачі радіосигналів і зменшує необхідну для передачі інформації енергетичну потужність. Залежно від потужності джерел живлення XMesh може організувати роботу мережі у трьох режимах: HP – високої потужності, LP – низької потужності, ELP – розширеної низької потужності.

Програмний засіб XServe встановлюють для організації взаємодії між мережею ІВ і додатками, які використовують їх інформацію. XServe забезпечує сервіси маршрутизації інформації від і до сенсорної мережі разом зі сервісами більш

високого рівня з аналізу, перетворення та опрацювання інформації. В сервісах більш високого рівня використовують керовані користувачами конфігураційні форми, які базуються на XML і завантажуються plugin – модулями. Для зберігання інформації XServe використовує реляційну СУБД Postgre SQL, а для запису журналів файли формату CSV. Важливо, що робота з Postgre SQL підтримується багатьма мовами в тому числі C, C++, Java, Perl і PHP. Для передавання інформації від сенсорної мережі до звичайної IP-мережі використовують стандартний стек протоколів TCP/IP.

Програмний засіб XServe надає декілька варіантів взаємодії зовнішніх додатків з XServe або з допомогою термінальних додатків, одержуючи при цьому безпосередній доступ до ІВ мережі, або через потужний командний інтерфейс, який базується на XML і служить для віддаленого виклику процедур.

Програмний засіб Mote View дозволяє відображати інформацію, яку генерує сенсорна мережа, у вигідній для розробників і користувачів формі. MoteView використовуєWindows подібний інтерфейс, а також графічні схеми і текстовий формат для представлення інформації. З допомогою Mote View можна аналізувати інформацію, яка зберігається у базі даних і лог-файлах XServe та відноситься до роботи мережі за певний період часу. Також Mote View може генерувати повідомлення електронної пошти на PDA або на мобільний телефон у випадку виникнення певних подій, наприклад реконфігурації сенсорної мережі або досягнення показниками, які зчитуються з ІВ, порогового значення. Програмний засіб Mote View дає можливість оптимізувати структуру мережі і змінювати її конфігурацію, фізично не змінюючи позицій ІВ. У складі Mote View є засоби дистанційного конфігурування кожного ІВ мережі. Наприклад, можна змінювати періодичність зчитування інформацій з ІВ не використовуючи засобів програмування. До складу Mote View входить вбудована бібліотека, яка підтримує роботу з усіма ІВ, які виробляє компанія Crossbow. Цю бібліотеку можна розшифрувати, тобто включати до її складу нові ІВ, які вироблені іншими компаніями.

У сучасних БСМ програмне забезпечення серверного рівня і рівня користувача може бути розміщено на одному персональному комп’ютері, який виконує у даному випадку роль хосту.

Розділ 2. Теоретичні основи геометричного моделювання БСМ

2.1. Фізичні основи моделювання сигналів ІВ

Однією з головних функцій апаратної складової кожної мережі є передавання інформації. Для цього використовують різні фізичні носії, які ще називають середовищем розповсюдження інформації. Носії інформації поділяють на керовані і некеровані [1]. До керованих носіїв інформації відносять мідний провід і оптиковолоконний кабель. До некерованих носіїв інформації відносять радіозв'язок і передавання інформації з використанням лазерного променю без дроту. Таким чином, для організації зв'язку у БСМ використовують некеровані носії інформації. Зокрема, як зазначено вище, автори розглядають мережі, що організовані на основі радіохвильового зв'язку. Радіохвилями умовно називають – електромагнітні хвилі строго встановлених параметрів [20].

Сучасна фізика електромагнітні хвилі представляє як електромагнітне поле, яке після утворення в деякій ділянці простору не локалізується в цій ділянці, а з певною швидкістю поширюється у навколишньому просторі [19]. Електромагнітні хвилі характеризуються довжиною λ, частотою f і швидкістю поширення c. Під довжиною електромагнітної хвилі розуміють відстань між двома послідовними максимумами або мінімумами. Частотою називають кількість електромагнітних коливань в секунду. На швидкість поширення електромагнітних хвиль впливає діелектрична проникність середовища, в якому вони поширюються ξ і магнітна проникність середовища μ. Загальну формулу для розрахунку швидкості поширення електромагнітних хвиль одержують із аналізу рівнянь Даламбера, якими описують електромагнітне поле.

Швидкість поширення електромагнітних хвиль обернено пропорційна показнику заломлення середовища та рівна:

$$c = \frac{1}{\sqrt{\xi_0 \mu_0 \xi\ \mu}} \tag{2.1}$$

де $\xi_0 = 8{,}85 \cdot 10^{-12}$ - електрична постійна$(ф/м)$;

$\mu_0 = 4\pi \cdot 10^{-7}$ - магнітна постійна$(Гн/м)$;

ξ - діелектрична проникність середовища$(ф/м)$;

μ - магнітна проникність середовища$(Гн/м)$.

Оскільки вакуум не піддається діелектричній поляризації, то у вакуумі діелектрична проникність $\xi = 1$. У вакуумі відсутні атоми будь-якої речовини, тому магнітна проникність в такому середовищі $\mu = 1$. Отже, швидкість поширення електромагнітних хвиль у вакуумі дорівнює:

$$c_0 = \frac{1}{\sqrt{\xi_0 \mu_0}} \approx 3 \cdot 10^8 \ м/с \tag{2.2}$$

Швидкість поширення електромагнітних хвиль у вакуумі називають швидкістю світла і вважають верхньою межею швидкості світла [1]. Якщо λ вимірюють в метрах, а f в мегагерцах, то f, λ і c зв'язані фундаментальними співвідношенням:

$$\lambda f = c \approx 300$$

Тобто електромагнітній хвилі довжиною $\lambda = 10^{-1}$ *м (10 см)* відповідає частота $f = 3 \cdot 10^3$ *МГц (3 ГГц)*.

Відповідно до вимог, які передбачені вище згаданим стандартом IEEE 802.154 і протоколом Zig Bee, для організації зв'язку у сучасних БСМ використовують радіохвилі сантиметрової довжини частотою 2-2,4 ГГц . Для моделювання і організації роботи БСМ важливо врахувати вплив навколишнього середовища на роботу функціональних базових вузлів, що входять до складу мережі. Особливої уваги заслуговує врахування впливу тропосфери на поширення радіохвиль сантиметрового діапазону, які використовують ІВ для передавання і транспортування інформації. Досвід експлуатації ліній радіозв'язку, приведений у літературних джерелах [20], переконливо показує, що радіохвилі довжиною менше 10 см при поширенні у тропосфері зазнають значного поглинання. При цьому, за деяких обставин поглинання може бути настільки сильним, що приводить до порушення радіозв'язку. Слід зазначити, що зі зменшенням довжини радіохвиль, поглинання їх тропосферою зростає. Така обставина набуває особливого значення оскільки ряд дослідників вважають, що стрімке зростання кількості БСМ приведе до необхідності використовувати для зв'язку в середині мережі радіохвилі довжиною меншою сантиметрового діапазону. Поглинання хвиль у тропосфері розділяють на: поглинання в крапельних утвореннях, тобто дощем, туманом, градом, снігом; молекулярне поглинання; розсіювання на молекулах і агрегатах молекул в умовах задимлення; поглинання твердими частинами в умовах запилення. Вказані обставини доцільно розглядати під час дослідження і моделювання сили сигналів ІВ у БСМ.

Виходячи із вище сказаного для геометричного моделювання БСМ запропоновано ІВ у конфігураційному просторі двох вимірів геометрично представляти сигнальними точками (СТ). При тому, відстані між СТ представляють як сили їх сигналів [21]. Якщо сили сигналів відповідних ІВ дорівнюють Ω_i та Ω_j, то відстань між ними представляють, як:

$$l_{ij} = l(\Omega_i, \Omega_j) \tag{2.3}$$

При такому представлені істинні відстані між ІВ в реальному просторі не мають значення, оскільки в середовищі, де зазвичай працюють БСМ, сигнал поширюється зі швидкістю близькою до швидкості світла. Для створення відповідності між ІВ і СТ у двовимірному евклідовому конфігураційному просторі (ЕКП) враховують і «шумові сигнали» ω, якими наповнений простір розташування реальних ІВ. Тому як відповідність шумовому сигналу ω, у моделі представляють відрізок $l_0 = l(\omega)$, а сигналом двох однотипних ІВ $\Omega_1 = \Omega_2$ відрізки однакової довжини $l_j = l(\Omega_1) = l(\Omega_2)$. Отриманий таким чином відрізок довжиною $l_{12} = 2l_j + l_0$ є функціональним зв'язком (ФЗ), який визначає у ЕКП відстань між СТ 1 і 2 (рис. 2.1). Таким чином ФЗ представляє два однотипні ІВ в ЕКП:

- кінці l_{12} є СТ, які представляють ІВ в ЕКП;
- довжина відрізка l_{12} є ФЗ, який характеризує роботу ІВ.

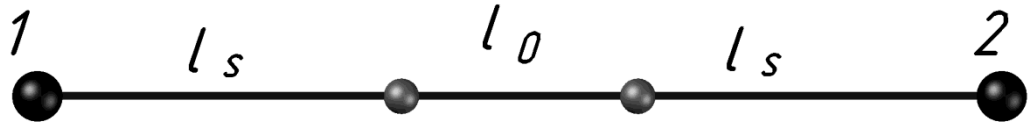


Рис. 2.1. Функціональний зв'язок (ФК) між двома сигнальними точками (СТ)

ФЗ між двома СТ, які представляють не однотипні ІВ визначають відрізком

$$l_{12} = l_1' + l_2 + l_0 \tag{2.4}$$

де l_1' і l_2- характеризують параметри сигналів ІВ Ω_1 і Ω_2 з врахуванням того, що $\Omega_1 \neq \Omega_2$.

Якщо ІВ у реальній БСМ зв'язаний з більшою кількістю ІВ, то в ЕКП моделі його представляє СТ з цією ж кількістю ФЗ відповідної довжини (рис. 2.2), які формуються аналогічно. Наприклад, ФЗ між СТ 1 і 3 рівний

$$l_{13} = l_1 + l_3 + l_0 \tag{2.5}$$

де $l_3 = l(\Omega_3)$

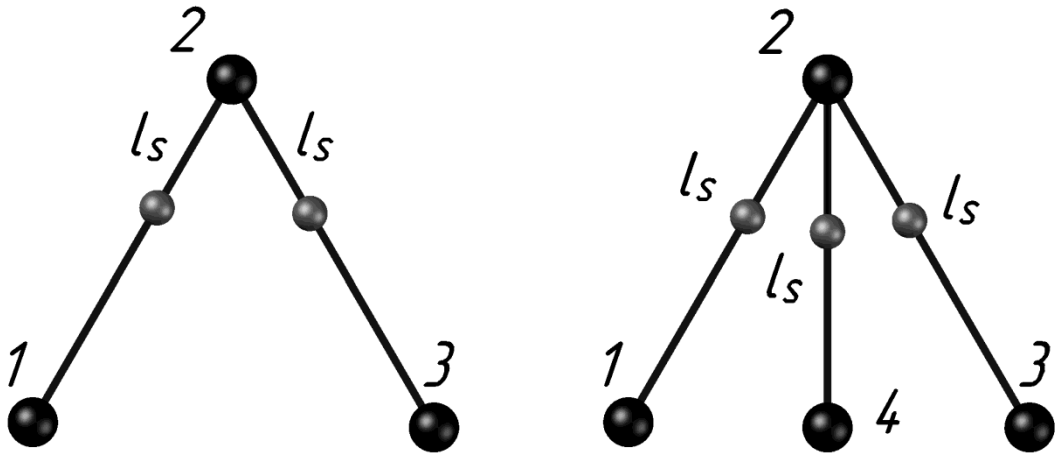


Рис. 2.2. Функціональні зв'язки сигнальної точки з двома і трьома сусідніми сигнальними точками

2.2. Математичні основи моделювання БСМ

Для моделювання БСМ, зокрема для розподіленого оцінювання топологічного стану мереж, запропоновано теоретико-графовий підхід [21]. При цьому графи адаптовані для представлення обмеженої поточної інформації в мережі, в якій дуги між вузлами відповідають спільно використовуваній інформації.

Топологію БСМ запропоновано описати орієнтованим графом $G(V,E,w)$, який визначається набором вузлів $V=\{1,...n\}$ і дуг $e \in E$, пов'язаних з набором вузлів декартовим добутком, тобто $E \subset V \times V$, причому w – ваговий коефіцієнт дуги графа (рис. 2.3). Кількість вузлів графа G – це його порядок, а загальна кількість дуг – розмір. Нехай набір вузлів і дуг графа G іменуються $V(G)$та $E(G)$, відповідно. Якщо застосовується символ $|\ |$ для позначення кардинального числа (кількості елементів множини), тоді порядок графа – це $|V(G)|$, а його розмір $|E(G)|$ – це кількість його дуг [142, 143].

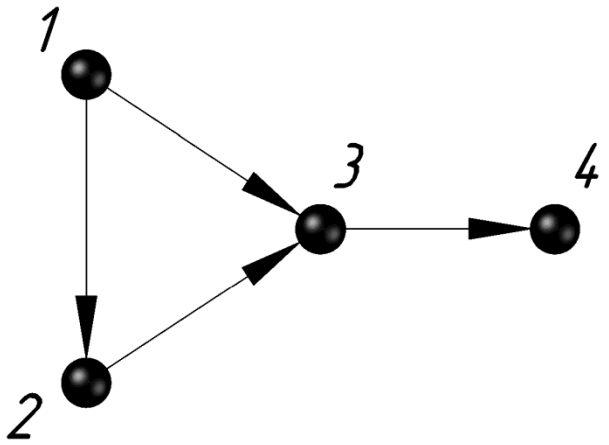


Рис. 2.3. Орієнтований граф на вузлах $V=\{1, 2, 3, 4\}$ з набором дуг $E=\{(1, 2), (1, 3), (2, 3),(3, 4)\}$

Для розгляду моделі БСМ на підставі графів, співставляють граф взаємодії, в якому вузли відповідають ІВ, а дуги – доступним каналам зв'язку між ІВ, з наявним інформаційним потоком. Такі графи взаємодії являються відповідними представниками основної мережевої топології, викликаної обмеженістю інформації та локалізованою взаємодією.

Вводять математичне поняття площі мережі [21]:

$$S_{i|i=\overline{1,n}} = \beta_i \sum_{j=1}^{n_i} w_{ij} \left(x_i(t) - x_j(t) \right) \Delta t_{ij} \tag{2.6}$$

де $x_i(t) \in \Re^n$ – вектор стану сенсора ϑ_i в момент часу t, що характеризує його положення, виражене у відстані;

β_i, w_{ij} – вагові коефіцієнти, що визначаються для конкретної БСМ;

n_i – набір сусідів сенсора ϑ_i, наприклад, комплект сенсорів ϑ_j, які взаємодіють з сенсором ϑ_i,

Δt_{ij} – середній час обміну даними між сусідніми сенсорами.

Застосовують правило найближчих сусідів для оцінки відстані між ІВ:

$$x_i(t) = \frac{S_{i|i=\overline{1,n}}}{\Delta t_{ij}}; \quad \Delta t_{ij} = const. \tag{2.7}$$

Для визначення швидкості передачі даних від групи сусідніх ІВ до визначеного вузла використовують математичну модель (2.7). Для цього розділяють

значення відстані між вузлами на час передачі інформації та отримують залежність швидкості передачі даних від часу та відстані між ІВ:

$$v_*\left(\Delta t_{ij},\Delta x_{ij}\right)=\frac{\beta_i\sum_{j\in n} w_{ij}\left(x_i(t)-x_j(t)\right)}{\Delta t_{ij}v_{nom}} \qquad (2.8)$$

де $v_*\left(\Delta t_{ij},\Delta x_{ij}\right)$ – швидкість передачі даних у відносних одиницях, причому $\Delta x_{ij}=\left(x_i(t)-x_j(t)\right)$.

Результати чисельного експерименту наведені рис. 2.4. Дослідження показали, що із збільшенням відстані між вузлами, необхідно збільшувати швидкість передачі даних за законом v_*. За такої умови забезпечується стабільна робота мережі, оскільки час передачі з довільного вузла буде однаковий.

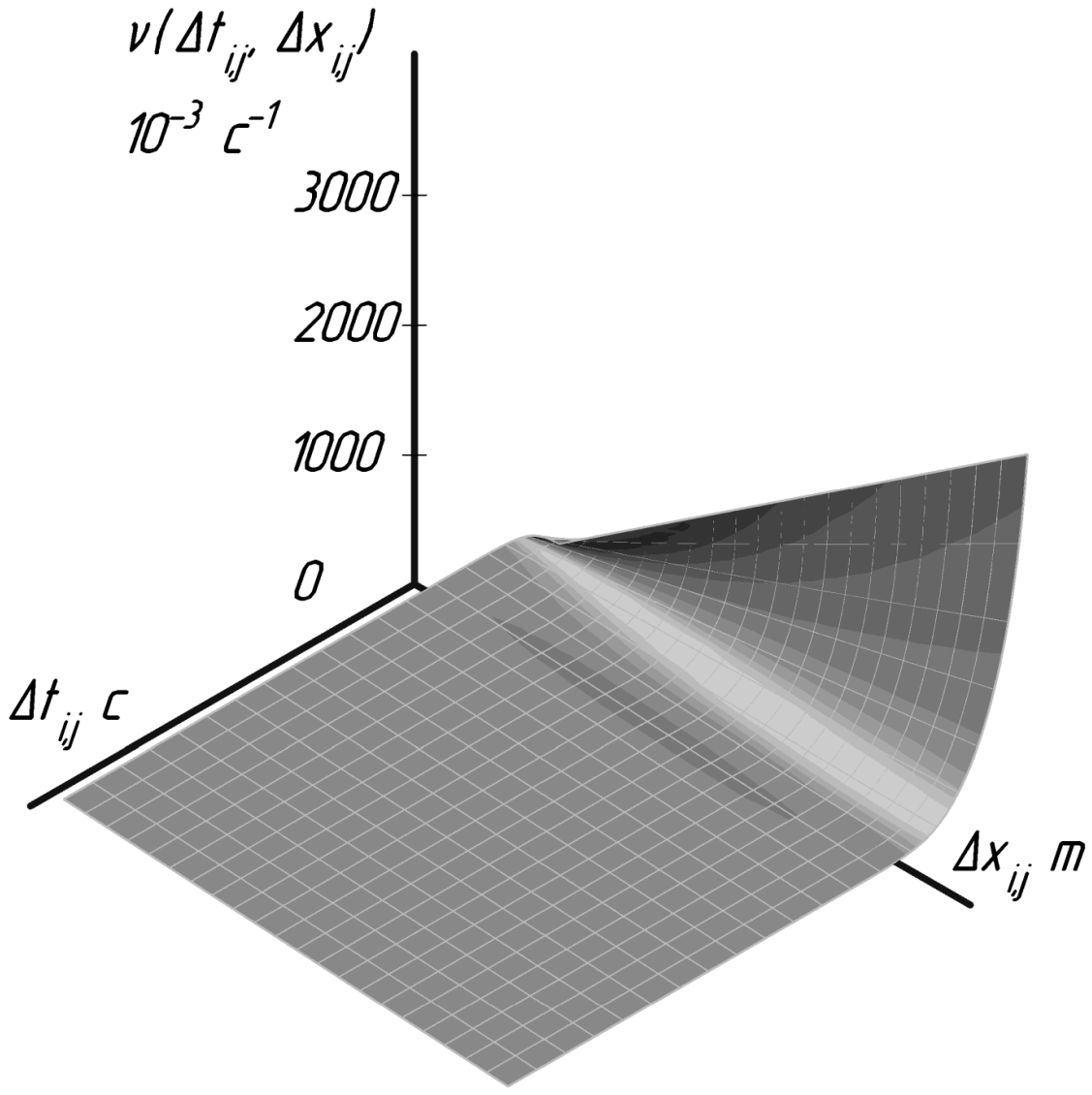


Рис. 2.4. Залежність швидкості передачі даних від часу та відстані між вузлами

Особливе значення для подальших досліджень відіграють графи з R_p - кругом суміжності (рис. 2.5) [38,21,144]. У графі з R_p - кругом суміжності дуги встановлені між вузлами ϑ_i та ϑ_j, якщо та лише якщо ІВ знаходяться на відстані R_p один від одного, тобто, коли $\left|x_i - x_j\right| \le R_p$.

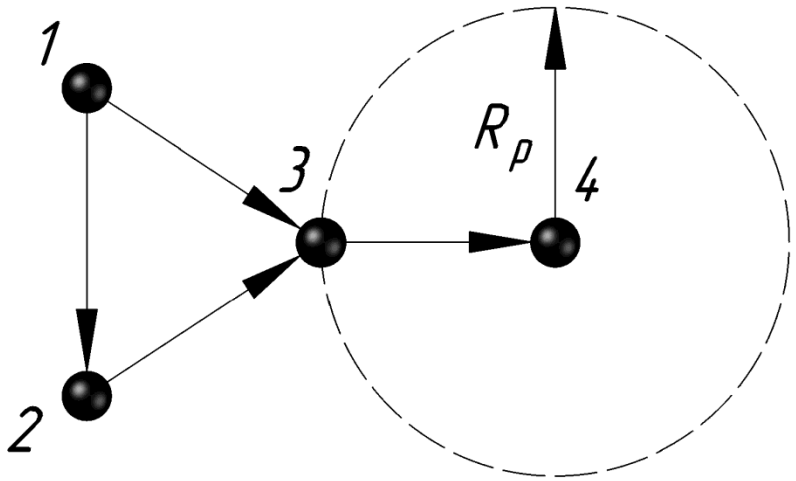


Рис. 2.5. Граф з R_p - кругом суміжності для $V = \{1,2,3,4\}$

Такі графи носять динамічний характер, зокрема можуть з'явитися чи зникнути в цих ребрах в якості ІВ або переміститися поза відстань сприйняття чи комунікації один з одним. Крім цього, можна припустити, що ІВ приєднуються або видаляються, в результаті чого не тільки набір дуг, але й комплект вузлів створює динамічну структуру.

Для оцінювання топологічного стану мереж на підставі графів розглядають БСМ з n ІВ, базовий граф $G_s = (V_s, E_s, w_s)$, вершини якого містять давачі, а дугами є канали зв'язку між парами вершин, нехай $u_i \in \Re$ – вихідний радіосигнал давача вузла (вершини) ϑ_i, $i = \{1,...,n\}$. Потім за $x \in \Re^n$ приймають стан розподіленого оцінювача та за x_i – радіосигнал суміжного компонента, пов'язаного з вершиною ϑ_i. Слід зауважити, що x_i відрізняються формою від дійсного радіосигналу сприйняття u_i, причому x_i визначають на підставі алгоритму розподіленої оцінки. Ці дані x_i, а не u_i, передають по каналах зв'язку та над ними здійснюють обчислення за допомогою процесорів, вбудованих в ІВ БСМ. Іншими словами, кожній вершині притаманні три функції: перша – давача, який моніторить зна-

чення рівня радіосигналу u_i; друга – компонента оброблення системи розподілених обчислень, який оновлює своє значення x_i при обробці інформації, отриманої з її каналів зв'язку; третя – трансивера, що обмінюється інформацією про стан зі своїми сусідами $\left(x_j, j \in n(i)\right)$.

Необхідний алгоритм оцінювання топологічного стану БСМ описують наступним чином [21]. В початковий момент відліку часу вузол (вершина) ϑ_i записує значення перетвореної або виміряної (сприйнятої чи зчитаної) ним величини u_i та використовує його початковим значенням для x_i. Потім вузол оновлює власний стан, ґрунтуючись на локальній інформації, тобто на усіх станах суміжних вузлів і своєму стані. Алгоритм приймає вигляд:

$$\frac{dx_i}{dt} = \beta_i \sum_{j \in n(i)} w_{ij}(x)\, f\left(x_j(t) - x_i(t)\right), \;\; x_i(0) = u_i, \;\; i = 1,...,n, \tag{2.9}$$

де $w_{ij}(x) = f\left(J_0(jau_i), J_n(jau_i)\right)$, причому

$$J_0(jae_i) = \frac{\left(j\frac{ae_i}{2}\right)^2}{1!^2} - \frac{\left(j\frac{ae_i}{2}\right)^4}{2!^2} + \frac{\left(j\frac{ae_i}{2}\right)^6}{3!^2} - ..., \tag{2.10}$$

$$J_n(jae_i) = \frac{\left(j\frac{ae_i}{2}\right)^n}{0!n!} - \frac{\left(j\frac{ae_i}{2}\right)^{n+2}}{1!(n+1)!} + \frac{\left(j\frac{ae_i}{2}\right)^{n+4}}{2!(n+2)!} - ... \tag{2.11}$$

є функціями Бесселя з уявним аргументом нульового та вищих порядків.

На основі цього удосконаленого підходу центральні вузли здійснюють вибірку даних спостереження

$$y(t) = \varphi\left(x(t)\right), \;\; y(t) \in \Re^q, \;\; q << n, \tag{2.12}$$

де q – наявна кількість центральних вузлів, причому

$$x(t) = \left[x_1(t),...,x_n(t)\right]^T \tag{2.13}$$

Задача в подальшому зводиться до однозначного визначення $u = \left[u_1,...,u_n\right]^T$ із $y(t)$.

З врахуванням правила найближчого суміжного вузла для $f(j)$ залежність (2.9) приймає вигляд:

$$\frac{dx_i}{dt} = \beta_i \sum_{j \in n\,(i)} \beta_{ij}\left(x_j - x_i\right), i = 1,...,n \tag{2.14}$$

Використовуючи умовне позначення керування на основі графа, вираз (2.14) записують у вигляді:

$$\begin{cases} \dot{x} = -L\left(G_s\right)x, \;\; x\left(0\right) = u, \\ y = Mx, \end{cases} \tag{2.15}$$

де $L\left(G_s\right)$ – лапласівська матриця графу, що відповідає БСМ,

$M \in \Re^{q \times n}$ – матриця даних моніторингу.

Оскільки граф вважається статичним, то надалі використовують L_s для $L\left(G_s\right)$, щоб це не викликало жодної плутанини. Ґрунтуючись на доведенні (Ji M, 2007), можна констатувати, що система (2.15) стійка та $x_i\left(t\right)$ збігається до $\sum_1^n u_1 / n$ для всіх $i \in \left\{1,n\right\}$ та $w_{ij} = const$. Тим не менш, з теорії керування відомо: якщо система $\left(-L_s, M\right)$ є спостережуваною, то можна повністю відновити первісний її стан $x\left(0\right)$ на підставі даних моніторингу $y\left(t\right)$. Слід відзначити, що для випадку декількох центральних вершин, кожний центральний вузол збирає "сирі" неопрацьовані відомості з підмножини ІВ та накопичує їх разом, – ця дія рівнозначна множенню y на кожен рядок M. Потім сумарні результати повідомляються на одну супервершину для остаточного оброблення інформації та прийняття рішення.

Також обмежено M до (0, 1)-матриці, а це означає, що всі канали однаково зважені. Якщо M містить ненульовий елемент у стовпці j, рядок i, то це означає, що є комунікація між давачем j та центральним вузлом i.

Інший алгоритм моніторингу на основі (2.15) та нескладний спосіб відновлення інформації, виходячи з наявних статичних параметрів або параметрів, що змінюються дуже повільно, полягає у розв'язанні системи [27]:

$$y\left(t\right) = M\, exp\left(-tL_s\right)x\left(0\right), \;\; t \geq 0 \tag{2.16}$$

або в дискретному часовому поданні

$$\begin{bmatrix} y(0) \\ y(1) \\ \vdots \\ y(T-1) \end{bmatrix} = \underbrace{\begin{bmatrix} M \\ -ML_s \\ \vdots \\ M\left(-L_s\right)^{T-1} \end{bmatrix}}_{O_T} x(0), \tag{2.17}$$

де O_T стає матрицею моніторингу (спостереження), якщо $T = n$.

Запропонований підхід до оцінювання топологічного стану БСМ ґрунтується на одному важливому припущенні: система $(-L_s, M)$ моніториться. В подальшому переглянуто теорему спостереження з точки зору теорії керування. Для цього записують лінійну стаціонарну в часі систему у вигляді:

$$\begin{cases} \dot{x} = Ax, \ \ x(0) = x_0, \\ y = Mx, \end{cases} \tag{2.18}$$

де A – матриця суміжності графа, причому ранг rk визначають згідно з виразом:

$$rk = \begin{bmatrix} A - \lambda I_n \\ C \end{bmatrix}, \tag{2.19}$$

в якому I_n – одинична матриця, λ – власне значення матриці$(\forall i, \lambda_i \geq 0, \lambda_0 = 0)$.

Подана лема гласить, що для цієї системи справджується наступне:

• система (2.18) спостерігається;

• ранг матриці спостереження $(O(n))$ є n;

• ранг rk дорівнює n для кожного власного значення λ в A.

Завжди можна перевірити стан рангу для здійснення моніторингу мережі. Однак, цього не можна здійснити, якщо кількість вершин (вузлів) є дуже великою. Потрібно забезпечити можливість спостережуваності під час будови мережі та, задля цього, доцільно дослідити вплив топології мережі на здатність спостереження. Результати дослідження спостережуваності БСМ тісно пов’язані з іншими розв’язками із-за аналізу між задачами спостереження та керування. Надалі використовуються деякі позначення, пов'язані з нетривіальним об’єктивним розділенням (НОР). При цьому очевидний тривіальний розклад зводиться до n - розділів, тобто $p = \{\{1\},\{2\},...,\{n\}\}$.

Розглядаючи БСМ, припускають, що її основному сенсорному графу притаманний НОР p_s з $p_s = r$ та C_{ps} – характеристична матриця НОР p_s. Нехай в

подальшому $\overline{C_{ps}} = \left(C_{ps}^{T}\, C_{ps}\right)^{-0,5} C_{ps}$ буде нормалізованою характеристичною матрицею для C_{ps} та H_{ps}, які вибирають таким чином, що формується ортогональна матриця $T = \left[\overline{C_{ps} \middle| H_{ps}}\right]$.

Спочатку розглядають випадок єдиного центрального вузла, позначивши цей вузол C_{n+1}. В цей же час, M є вектор-рядок і y представляє собою скаляр, що дорівнює сумі станів вершин, приєднаних до центрального вузла. Оскільки M є (0, 1) - матрицею, вона не може належати до ортогонального доповнення C. Якщо це станеться, то отримаємо характерний вектор нетривіальних сотів, деякі стани не будуть спостережуваними [27].

Згідно з теоремою, система (2.18) не є цілком спостережуваною, якщо центральний вузол комунікується зі всіма вершинами (вузлами) в одній або декількох сотах (комірках), тобто:

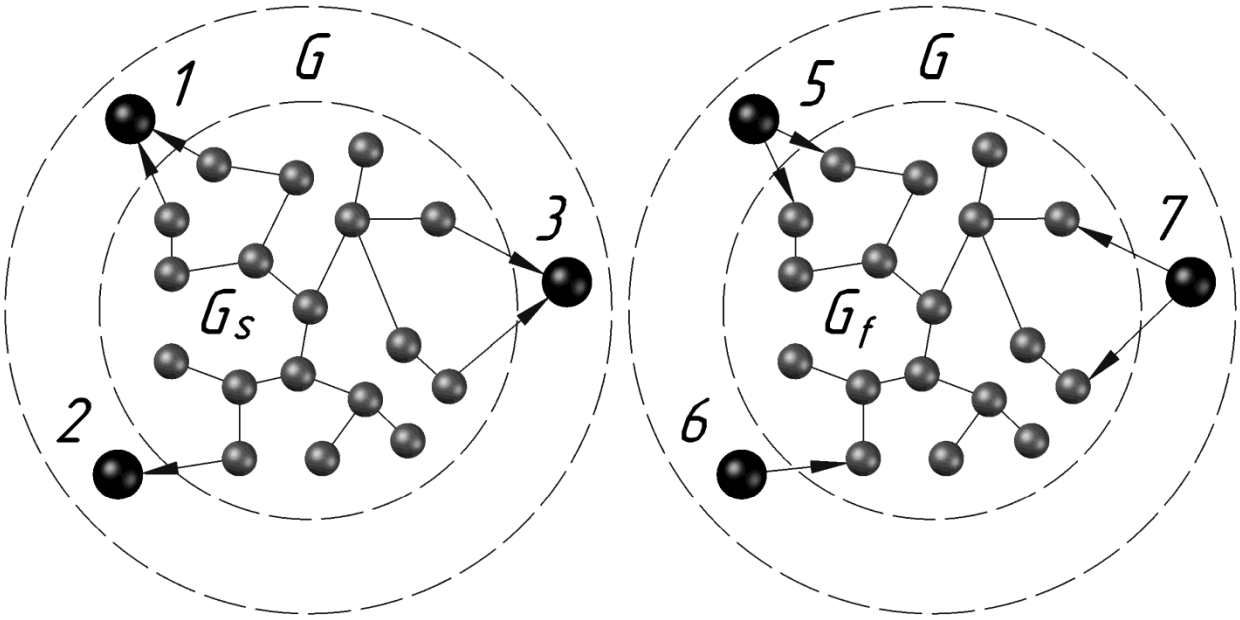
$$n(n+1) = \left\{\cup_{l=1}^{k} M_{ij}\right\}, k, i_l \in \{1,...,r\} \tag{2.20}$$

При цьому G – граф, покладений в основу БСМ, та p є тільки одним НОР над G_s. Звідси випливає наступний наслідок:

- для основного графа БСМ G_s та якщо (2.20) справджується для всіх НОР над G_s і $w_{ij} = const$, система (2.15) не є повністю спостережуваною.
- для випадку декількох центральних вузлів, безпосереднє застосування вищезазначеної леми, що описується (2.20), до кожного лідера не приводить до правильного висновку. З дуалізму відомо, що система (2.18) спостерігається, якщо і тільки якщо $\left(A^T,\ M^T\right)$ піддається контролю.

Беручи до уваги БСМ, розцінюють центральні вузли лідерами в структурі лідер-послідовник та позначають результуючий граф розширеним графом ІВ G. При цьому G – це ніщо інше, як доповнення графа ІВ G_s центральними вершинами та доданням в G_s дуг, які представляють собою потоки інформації від ІВ до центрального вузла. Граф ІВ G_s відіграє роль, аналогічну до повторюваного графа G_f в топології лідер-послідовник (рис. 2.6). Відмінність полягає в тому, що в БСМ інформаційні потоки спрямовані від ІВ до центрального вузла, тоді як у лідер-повторюваній топології інформаційні потоки напрямлені від лідерів до

послідовників. Завдяки такій архітектурі мережі будуються кластери, що дозволяє зменшити обсяг наданої інформації, а це в свою чергу збільшує швидкодію, надійність та покращує інші техніко-економічні показники функціонування БСМ.



а) б)

Рис. 2.6. Графи БСМ: а) асоційований з БСМ граф G_s та доповнений граф G; б) граф взаємодії G топології лідер-послідовник з ідентичною до БСМ архітектурою а): 1, 2, 3 – центральні вузли; 5, 6, 7 – вузли-лідери

Слід зазначити, що наведений на рис. 2.6 повторюваний граф G_f аналогічний до графа G_s, однак інформаційні потоки спрямовані від лідера до послідовника.

За такої побудови справджується наступна теорема.

Для БСМ з графом комунікації G_s і розширеним графом G система (2.15) не є повністю спостережуваною, якщо існують НОР на G і G_s, іншими словами такі p та p_s, що всі нетривіальні соти НОР p містяться в *НОР* p_s, тобто такі p та p_s, що $|C_i| = 1,\ \forall C_i \in \pi \setminus \pi_s$. Більше того, $T_s = \left[\overline{P_s} \middle| \overline{Q_s}\right]$ є перетворенням подібності, що дає декомпозицію моніторованості системи.

Нехай C_s – характеристична матриця, яка відноситься до НОР p_s в графі G_s. Беручи до уваги, що

$$L_s \sim \overline{L_s} = \begin{bmatrix} L_{sC} & 0 \\ 0 & L_{sH} \end{bmatrix} \tag{2.21}$$

є результатом перетворення подібності T_s, показано, що таке ж перетворення на M може дати необхідну структуру блоку. Іншими словами, слід довести, що

$$MT_s = \overline{M} = [M_0, 0]. \tag{2.22}$$

Відомо, що G_s має нульову суму по стовпцях, а стовпці можуть містити ненульові елементи тільки в рядках, що відповідають нетривіальним сотам. З іншого боку, рядок i в M позначає, яким чином ІВ комунікуються з центральним вузлом i, причому матимемо 1 (один) в j-му елементі, якщо присутнє ребро між центральним вузлом i та ІВ j. Звідси, нижче p всі нетривіальні соти містяться в G_s і всі центральні вершини є звичайним чи тривіальним розгалуженням, тобто кожен лідер зв'язаний чи ні зі всіма вузлами в M_i для деяких $i \in 1,2,...,r_i$. Таким чином, стовпці M^T знаходяться в зоні стовпців G_s. Отже, отримується $M\overline{H_s} = 0$ і перетворену систему можна подати у вигляді:

$$\begin{cases} \dot{z}^o = -\overline{L_s}\ z,\ z(0) = T_s^T p, \\ y = \overline{M}\ z \end{cases} \tag{2.23}$$

де $z = T_s^T p$ – перетворений вектор стану.

Крім цього, можна ствердити, що:

$$\begin{cases} \dot{z}^o = -L_{sC} z^o, \\ \dot{z}^{uo} = -L_{sH} z^o, \\ y = M_0\, z^o \end{cases} \tag{2.24}$$

де $z^o = \overline{C_s^T} x$ – спостережувана складова перетвореного стану, тоді як $z^{uo} = \overline{H_s^T} x$ – немоніторений компонент перетвореного стану.

Зауваження. Якщо прийняти, що $x^p = C_s^+ x$, де $C_s^+ = (C_s^T C_s)^{-1} C_s^T$ є псевдоінверсією C_s, та помножити обидві сторони другого рівняння в системі (2.19) на $\left(C_s^T C_s\right)^{-0.5}$, то отримується $x^p = C_s^+ L_s C_s C_s^+ y = \hat{L}_s C_s^+ y = \hat{L}_s x^p$,причому L_s – лапсасіан частки (G_s / p).

Таким чином, сформульована достатня умова для не повністю керованої БСМ. Зворотне твердження цієї леми забезпечує необхідні умови для цілком моніторованої БСМ. Стверджують це наступним наслідком: маючи в наявності ІВ комунікації G_s та його доповнений граф G, необхідна умова для системи (L_s, M) щодо спостережуваності полягає в тому, що не існує жоден НОР p та p_s над G та G_s, так що p та p_s спільно використовують всі нетривіальні соти.

Одержані результати удосконалюють оцінювання техніко-економічної ефективності функціонування існуючої розподіленої БСМ та дозволяють розв'язати задачу забезпечення зв'язності в цій мережі під час експлуатації. Згідно з цією концепцією кожен ІВ вільно переміщується за зближувально-подібною схемою в локальній інформаційній системі, а також центральні вузли оцінюють первинну дійсну інформацію шляхом спостереження невеликої групи ІВ. Висвітлено одне з найважливіших питань запропонованого модифікованого підходу – спостережуваність та отримано низку необхідних умов. Запропонований нелінійний зважений підхід розв'язує задачу забезпечення зв'язності. Ґрунтуючись на цьому, можна аналізувати не лише базову наперед відому топологію БСМ, а й застосувати розроблений підхід для інших мережевих задач і не лише під час експлуатації БСМ. Зокрема шляхом перебору можливих форматів можна синтезувати, вибрати, сформувати та запропонувати необхідну топологію БСМ також на стадії проектування. Подано теоретичну інтерпретацію із застосуванням графів для задач керованості та спостережуваності.

Перевагу запропонованого модифікованого методу становлять три складові.

По-перше, вимагається мінімальний обсяг інформації обміну між ІВ та центральним вузлом. Відповідно до ретрансляційної концепції з лише одним центральним вузлом БСМ по суті представляє граф зірки з центральною вершиною в його центрі. В цьому випадку кількість пакетів даних N, кожен з яких містить отриману із ІВ інформацію, надходить до центрального вузла безпосередньо або шляхом маршрутизації. Тоді як в покращеному методі кількість отриманих центральним вузлом пакетів визначається лише кількістю під'єднаних до нього ІВ. Якщо мережа коректно побудована, то потрібно зчитувати дані тільки з одного вузла для відновлення всього сценарію, – дана мережа є спостережуваною з цим вузлом.

По-друге, обсяг інформації обміну між ІВ не змінюється в залежності від відстані до центрального вузла. В n - ретрансляційному маршруті наявні $\sum_1^{n+1} i$ пакетів передаються з вихідного вузла до центрального вузла. До того ж, за однакової кількості центральних вузлів зростає розмірність n відносно масштабу зони (пропорційно до квадрату в 2-D та до куба в 3-D вимірі). У запропонованій же концепції для реалізації кожного зв'язку необхідно лише 2 пакети інформації, тому за однакової кількості елементів або відстані n передається тільки $(2n+1)$ пакетів. Центральні вузли приймають лише один пакет від кожного комунікованого з ним давача. При цьому, завдяки зменшеному обсягу передавань інформації притаманні деякі особливості. Зокрема, кожен вузол має за завдання узагальнити інформацію свого сусіда та центральний вузол повинен передбачити чи інтерполювати область параметрів при розв'язанні системи лінійних рівнянь. Тим не менш, по відношенню до згаданих обчислень це суттєво дешевше та супроводжується споживанням набагато меншої енергії, ніж процес передавання інформації, тому удосконалений метод все-таки володіє суттєвою перевагою у порівнянні з ретрансляційною концепцією. В науковій літературі наводяться аргументи, що комунікація в 2000 разів дорожча, ніж обчислення характеристик процесу для такої самої кількості інформації [145]. Незважаючи на те, що мобільному центральному вузлу необхідно збирати тільки N пакетів у всій зоні покриття, порівнюючи $(2M+m)$ за удосконаленим методом, причому M – наявна кількість каналів комунікації, яка загалом більша від N, то цей метод характеризується набагато вищою швидкодією у великому просторі.

По-третє, запропонований модифікований метод менш складний порівняно із ретрансляційною концепцією чи принципом мобільного центрального вузла. Кожен ІВ нескладно обчислює середнє значення свого та сусідніх положень, навіть не знаючи ідентифікаційних ознак своїх сусідів. Він не повинен займатися задачею маршрутизації – найважливішою частиною в системах із застосуванням ретрансляторів чи багатократним відбиттям радіохвиль. З точки зору центральних вузлів, необхідно пройти через зону для зібрання даних, так що їм не доведеться турбуватися про задачу покриття чи планування руху.

Оскільки, центральні вузли мають широкий діапазон комунікаційних можливостей, то вони можуть спільно використовувати чи сумісно розподілити ін-

формацію та зберегти копію для кожного з них. Таким чином, кожен центральний вузол може відігравати роль засобу прийняття рішення. А подальше розширення може бути таким, що кожен вузол виступає центральним вузлом, використовує хронологію (передісторію) свого власного стану, та робить логічний висновок про стан інших. Беручи до уваги, що ця схема є витонченою та стійкою в сенсі толерантності до помилок, вбачається перспективним займатися цим напрямом.

2.3. Геометричні основи моделювання БСМ

Для розроблення оптимальних енергозберігаючих маршрутів передачі інформації і механізмів контролю за силою сигналів ІВ використовують геометричне моделювання для графічного представлення БСМ у двовимірному евклідовому конфігураційному просторі [22, 23]. Зокрема, для моделювання мереж до складу яких входять ІВ одного типу конфігураційний простір представляють СТ, які знаходяться у вершинах квадратів, а ФЗ між ними представлені, як сторони цих квадратів (рис. 2.7).

Дослідники вказують, що квадратна модель БСМ проста і зручна у використанні. Одночасно таку модель характеризують ряд недоліків. Зокрема, для розроблення маршрутів передачі інформації така модель не є оптимальною, оскільки передбачає використання ФЗ тільки у вертикальному і горизонтальному напрямках. В результаті цього значно збільшується довжина шляху переміщення інформації в середині мережі і кількість циклів приймання та передавання інформації ІВ першого рівня, що приводить до зростання енергетичних затрат на функціонування БСМ в цілому.

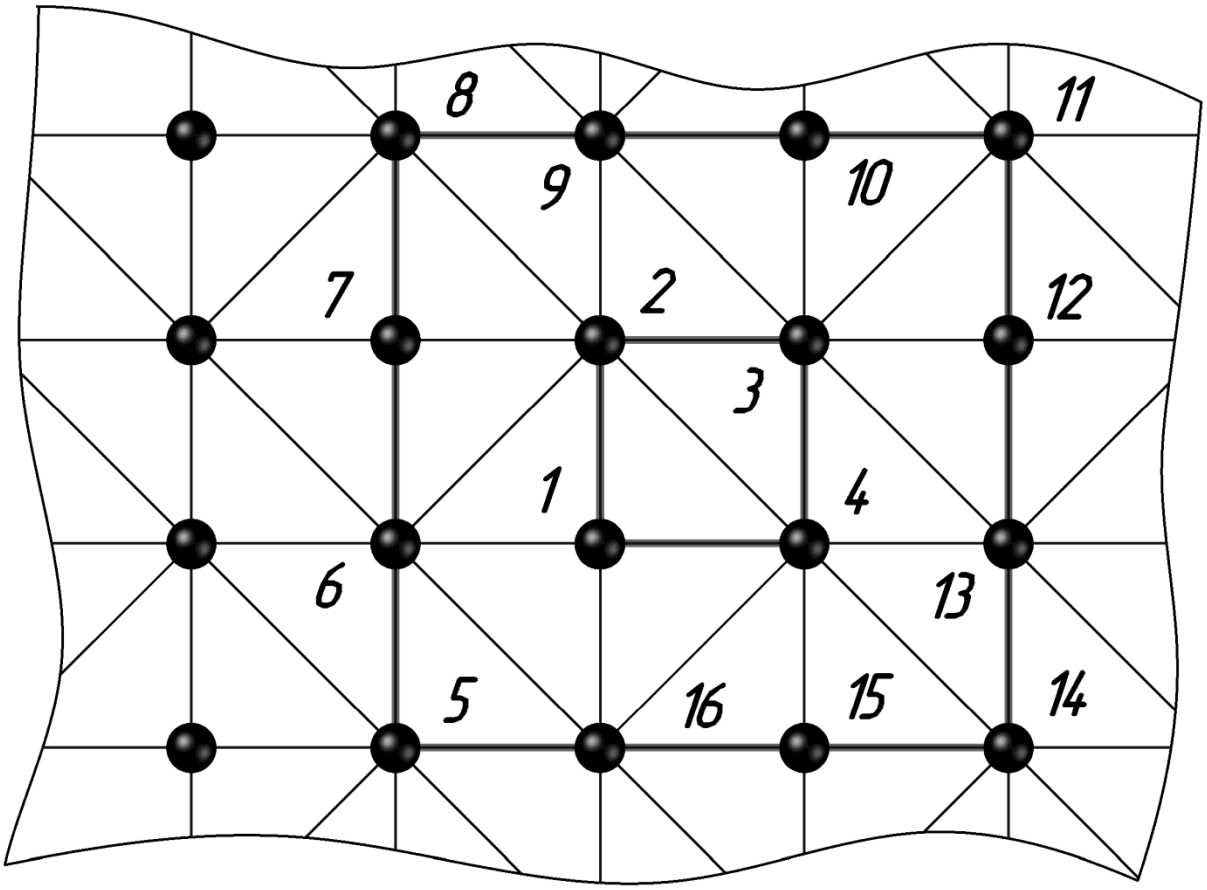


Рис. 2.7. Квадратна модель БСМ

Використання моделі БСМ у вигляді гексагональної сітки ІВ дозволяє планувати переміщення інформації у трьох напрямках (рис. 2.8), але передбачає збільшення числа ІВ на одиниці площі, порівняно з квадратною сіткою. Як стверджують літературні джерела – це збільшує вартість мережі майже на 10 % [8].

Згадані геометричні моделі БСМ не дозволяють аналізувати зміни параметрів сигналів ІВ, що не сприяє підвищенню надійності роботи БСМ і не забезпечує належного рівня захищеності інформації. Для дослідження параметрів сигналів ІВ, зокрема сили сигналів, пропонуються геометричні моделі для створення яких використовують методи обчислювальної геометрії [24, 25, 26, 27, 28], яка дозволяє із факту існування співвідношень між вимірюваними відстанями досліджувати внутрішні властивості геометричних фігур. При цьому зручними, з точки зору оптимальної кількості ФЗ, є планарні графи, всі внутрішні області яких – трикутники.

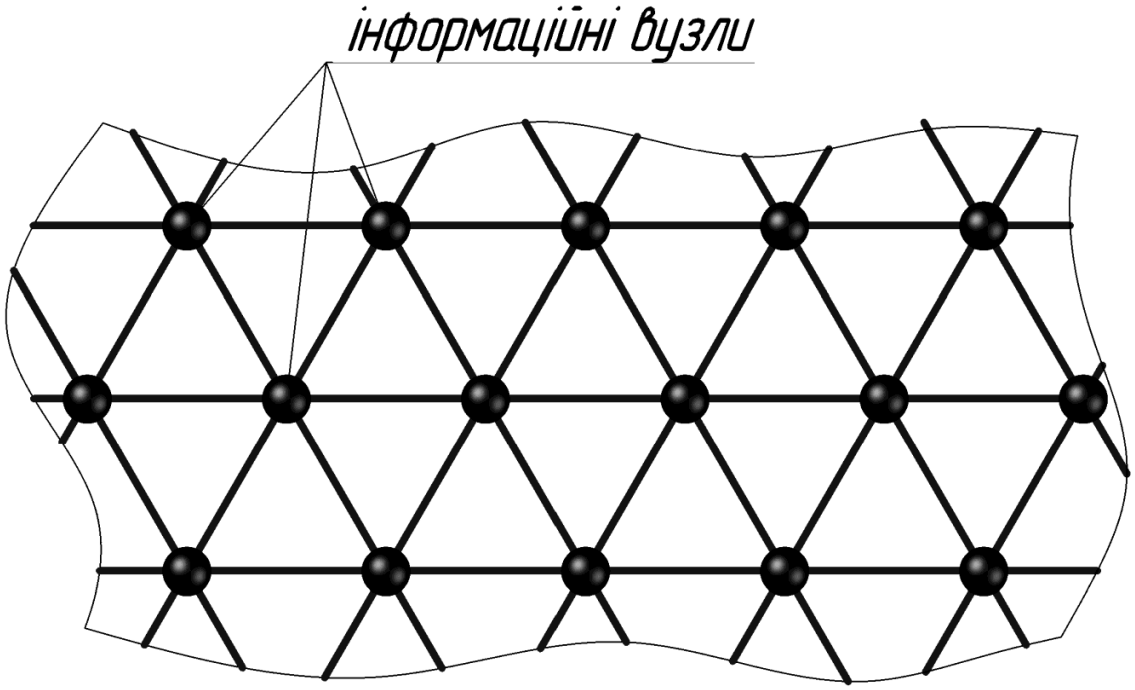


Рис. 2.8. Гексагональна модель БСМ

Використання трикутників для геометричного моделювання фізичних процесів називається тріангуляцією. Серед тріангуляцій особливе місце займає тріангуляція за методом Делоне [29], який полягає в тому, що виконується умова Делоне: всередину кола, описаного навколо будь-якого побудованого трикутника, не повинна попадати жодна інша точка, яка використовується при побудові (рис. 2.9).

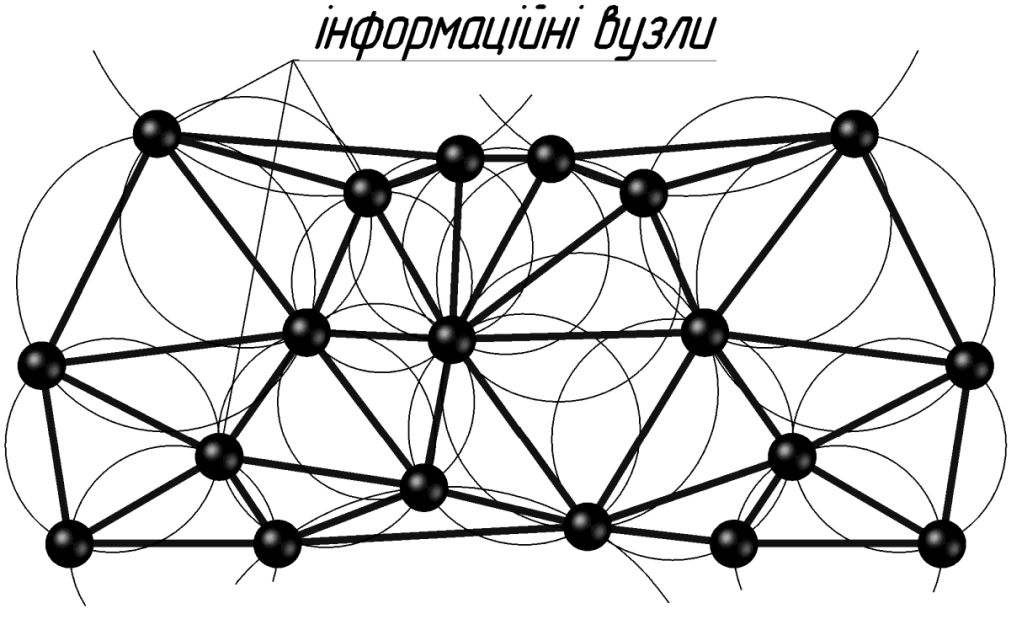
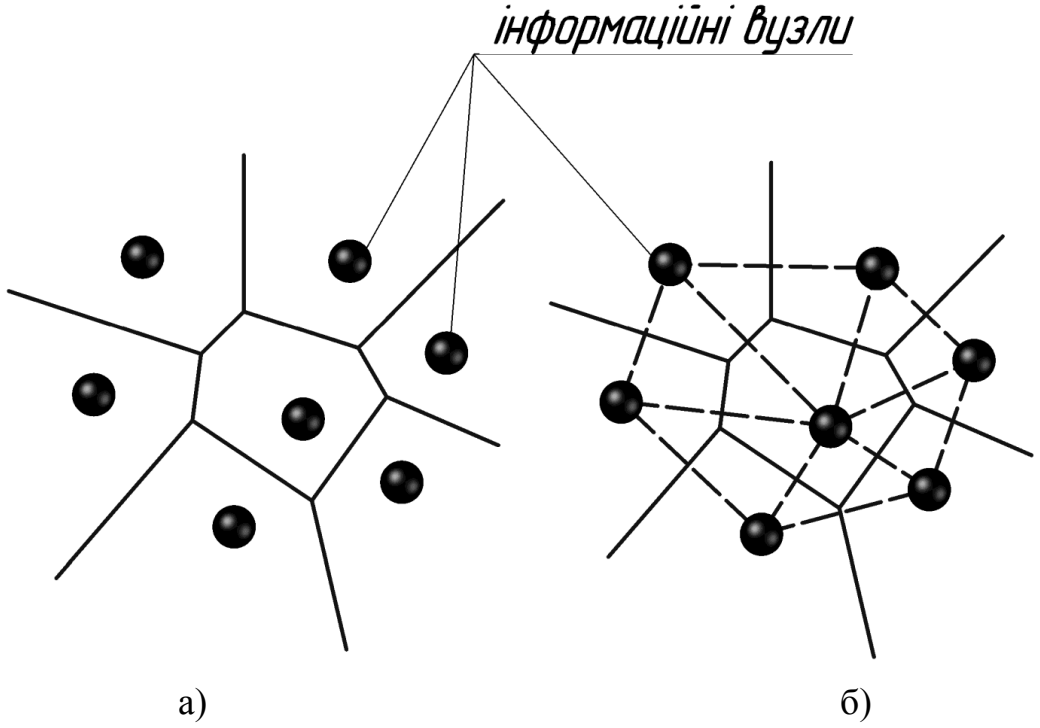


Рис. 2.9. Тріангуляція Делоне

Тріангуляцію Делоне розглядають як граф-двійник діаграмі Вороного – одній із базових структур обчислювальної геометрії. Діаграмою Вороного для множини точок $\{P_1,...P_n\}$ називають сукупність усіх многокутників Вороного цих точок. Для заданої точки $P_i \in \{P_1,...P_n\}$ на площині многокутником (коміркою) Вороного називають геометричне місце точок на площині, які знаходяться до P_i ближче, ніж до любої іншої заданої точки P_j, $j \neq i$ (рис. 2.9а) [31]. Діаграми Вороного називають розбиттям Тіссена або комірками Діріхле. Двійниковість діаграми Вороного і тріангуляції Делоне заключається в тому, що з'єднавши відрізками ті вихідні точки, чиї многокутники Вороного дотикаються хоча б кутами одержують тріангуляцію Делоне (рис. 2.9 б).



а) б)

Рис. 2.10. Діаграма Вороного: а – приклад діаграми;
б – двійникова діаграма тріангуляції Делоне

Умова Делоне є початковим визначенням двовимірного простору. Її можна використовувати для тривимірного простору, якщо використовувати описанні сфери замість описаних кіл [32].

Закономірності тріангуляції являються основою для реалізації методу локалізації, який запропоновано використовувати для визначення розміщення компонентів БСМ [61]. Характерна особливість локалізації систем полягає в здатності визначати місце розташування вузла та перевіряти його відстань від суміжних

вузлів. Кожен вузол може визначити своє положення шляхом обчислення відстані до своїх сусідів, використовуючи один з чотирьох методів тріангуляції, що ґрунтуються на вимірюваннях відстаней (lateration), рівнів радіосигналу (attenuation), різниць часу (propagation) та взаємних кутів (angulation) [69, 70, 71]. Місце знаходження вузла згідно з тріангуляцією обчислюється за допомогою тригонометричних теорем синусів і косинусів таким чином (рис. 2.10):

за теоремою синусів

$$\frac{\sin\alpha}{BC} = \frac{\sin\beta}{AC} = \frac{\sin\gamma}{AB}, \tag{2.25}$$

за теоремою косинусів

$$\begin{cases} BC^2 = AC^2 + AB^2 - 2AC \cdot AB\cos\alpha \\ AC^2 = BC^2 + AB^2 - 2BC \cdot AB\cos\beta \\ AB^2 = BC^2 + AC^2 - 2BC \cdot AC\cos\gamma \end{cases} \tag{2.26}$$

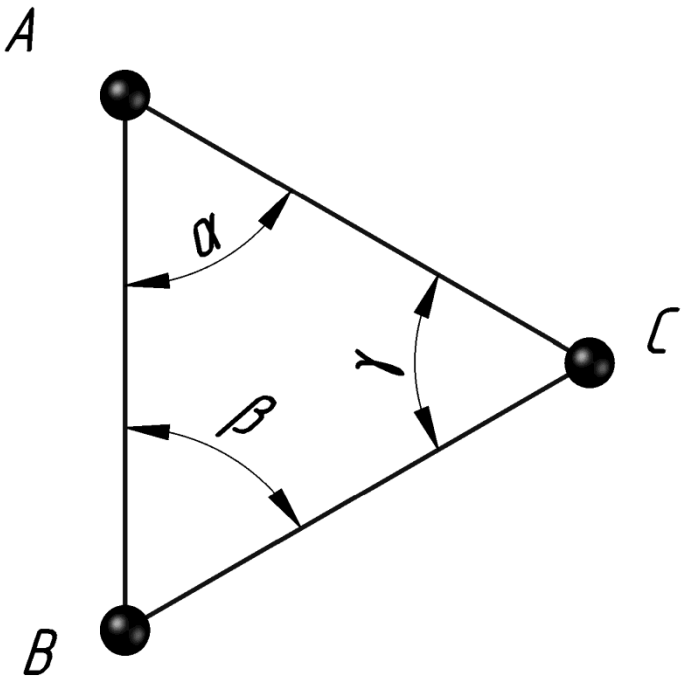


Рис. 2.11.Схема розміщення вузлів у вершинах трикутника

Тріангуляцію, що ґрунтується на вимірюваннях відстаней називають трилатерацією. Вона передбачає, що після розміщення вузли знають про своє місце завдяки процесу атомарної мультилатерації. Під час цього процесу вузол оцінює своє місце розташування, якщо він знаходиться в межах радіодіапазону трьох

інших вузлів. Коли базова станція передає маяк для формування топології мережі, вузли відповідають з їх положенням у мережі. Кожен вузол визначає своє положення шляхом розрахунку відстані від своїх сусідів, як показано нижче на рис. 2.11 та на якому параметром p є відстань d.

Для реалізації тріангуляції на підставі рівнів радіосигналу, використовують закономірність зменшення рівня радіосигналу s зі збільшенням відстані між двома вузлами (рис. 2.11). При цьому використовують припущення про щільну мережу, де вузли розміщені близько один до одного. В ієрархічній кластерній моделі вузли батьків знають про положення їх дочірніх вузлів.

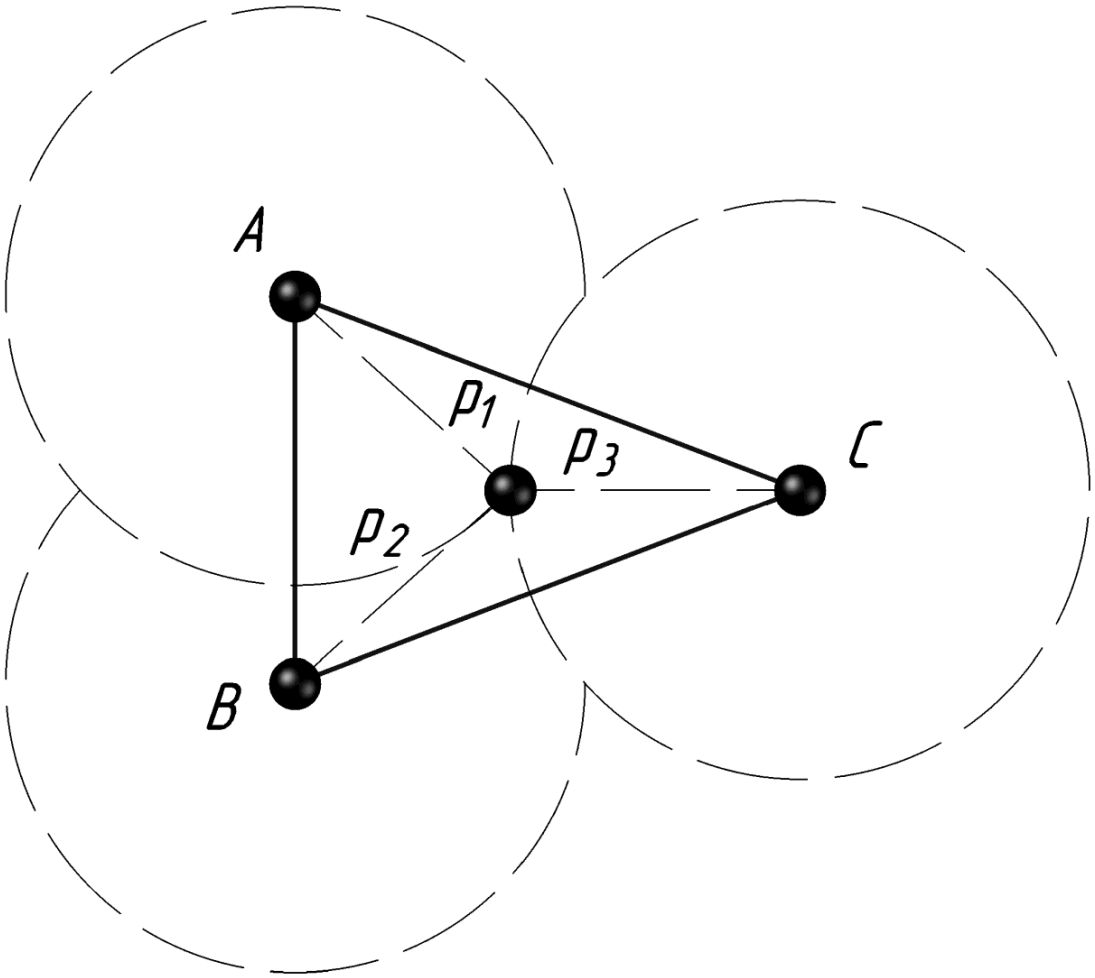


Рис. 2.12.Види тріангуляції: трилатерація – $\overline{\{p_1, p_3\}} = \overline{\{d_1, d_3\}}$,

рівнів радіосигналу – $\overline{\{p_1, p_3\}} = \overline{\{s_1, s_3\}}$, різниць часу – $\overline{\{p_1, p_3\}} = \overline{\{t_1, t_3\}}$

Під час реалізації тріангуляції на основі різниць часу вузол А посилає повідомлення до вузла В і вузол В обчислює різницю в часі t_2-t_1, за якою він в стані визначити своє розміщення (рис. 2.11).

Обертова тріангуляція чи визначення напряму передбачає використання під час обертання кутів для визначення відстані між вузлами при застосуванні напрямних антен (рис. 2.12). У 2-D розміщенні вимірюють два кути та відстань, а в 3-D положенні – два кути, одна довжина та один азимут.

Для визначення розміщення ІВ використовують метод тріангуляції на підставі рівнів радіосигналу, який на сьогоднішньому рівні розвитку апаратного забезпечення БСМ є найбільш економічно ефективним методом, оскільки для його реалізації не вимагається жодного додаткового обладнання на ІВ. Основним недоліком даного методу вважають неточність вимірювання відстаней. Так за даними дослідників [61] похибка визначення відстаней може коливатися від 5% до 40% в радіодіапазоні. Точність вимірювань дозволяють покращити створення точнішої технічної моделі розповсюдження радіосигналу та забезпечення стабільної різниці потужностей в різних точках.

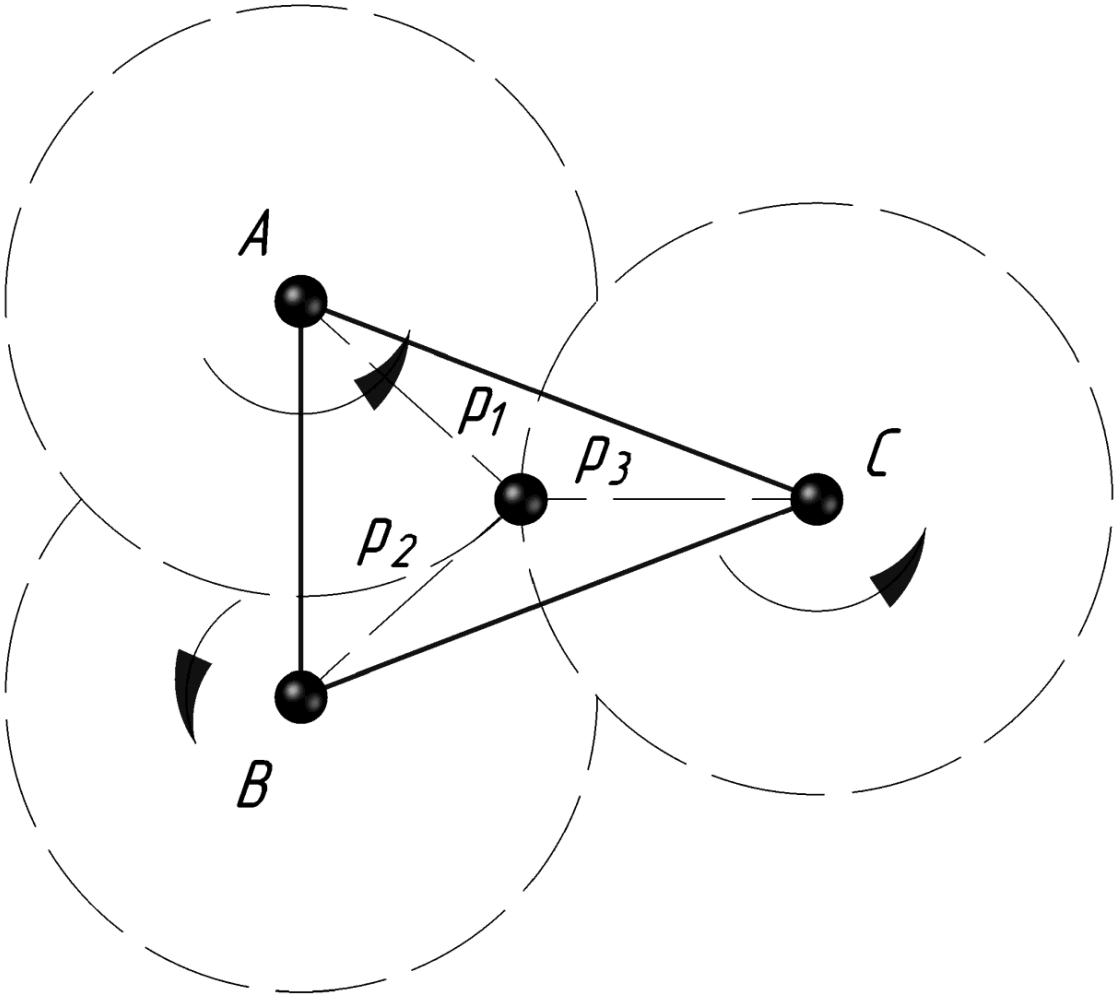


Рис. 2.13. Визначення напряму

Для подальшого згладжування реконструйованої топологічної поверхні БСМ використовують метод з комп'ютерною графікою, що ґрунтується на теорії дуального графу діаграми Вороного. При цьому спочатку здійснюють тріангуляцію Делоне над графом $G(<V>,<E>)$ (рис. 2.8). Завдяки цьому максимізується мінімальний кут $\{\alpha_i;\beta_i;\nu_i\}$ всіх трикутників: $max\{min\alpha_i;\beta_i;\nu_i\}$.

Результат методу 3Д тріангуляції Делоне використовують для вибору характерних ліній між відповідними парами вузлів. Обрана особливість ліній підвищує основну інформацію про поверхневу топологію БСМ.

В подальшому застосовують модифікований локально-стохастичний метод просторової інтерполяції, а саме проводять кригінг-інтерполяцію реконструйованої топологічної поверхні, що відповідно до прогнозних даних, наведених у літературних джерелах [107], повинен забезпечити хороші результати. Кригін названо на честь африканського інженера Д. Дж. Кріге.

До переваг методу кригінгу відносять можливість обґрунтовування радіусу околу розглянутої точки, який повинен враховуватися під час інтерполяції вигляду вагової функції, а також можливість оцінювання точності просторової інтерполяції. Загалом за допомогою методу кригінгу оптимізують процедуру побудови поверхні, ґрунтуючись на уявленнях про її статистичну природу [227, 109, 110, 111, 112, 113]. В методі кригінгу застосовують ідею врахування закономірностей статистичної структури просторового розподілу розглянутої змінної, що змінюється від місця до місця з деякою відомою безперервністю, але не може бути адекватно описана тільки одним математичним рівнянням. Завдяки цьому кригінг-інтерполяція має перевагу порівняно з локальними детермінованими методами, до яких належать методи кускової поліноміальної і сплайнової інтерполяції та ковзного осереднення [107]. Згідно з методом кригінгу обробляють вихідні дані, приймаючи, що поверхня складається з трьох незалежних компонент. Перша складова поверхні – це структурна компонента під назвою загального тренду, дрейфу чи структури, яка має постійне значення або тренд (детермінована складова) та характеризує загальну тенденцію зміни поверхні у визначених напрямках. Друга складова поверхні – це випадкова, але просторово корельована компонента, яка є місцевим відносно невеликим відхиленням змінної від тренду,

що, власне, і називається регіоналізованою змінною. Третя компонента, яку можна розглядати як випадкову похибку, – це просторово не корельований випадковий шум, що не пов'язаний із загальною тенденцією.

З кожною із трьох зазначених складових поверхні оперується окремо. Першу складову, тобто дрейф враховують із застосуванням математичної функції, яка визначає загальні зміни поверхні подібно до тренду. Слід зазначити, що найчастіше при цьому застосовують такі випадки: тренд відсутній взагалі, присутній лінійний тренд та наявний квадратичний тренд. Функція, за допомогою якої описується тренд, дозволяє обчислити значення дрейфу у вузлах сітки.

Другу складову поверхні оцінюють наступним чином. Спочатку будують варіограму, на якій по горизонтальній осі відкладають відстань між вихідними точками (так званий лаг), а по вертикальній –так звану напівдисперсію. Останню обчислюють як половину квадрату різниці величини поверхні між значеннями у вихідних точках. На варіограмі проводять криву найкращого наближення, яка дозволяє встановити критичне значення лага – граничний радіус просторової кореляції. За умови перевищення граничного радіусу значення згаданого квадрату різниці залишається постійним. Таким чином, визначають радіус, у межах якого вихідні точки мають суттєвий взаємний вплив. Потім визначають значення другої складової кожному вузлу сітки на підставі вихідних точок, які розміщені на відстані від вузла, що не перевищує радіуса граничної просторової кореляції. Ваговий коефіцієнт, який надають кожній вихідній точці для обчислення значення поверхні у вузлі сітки, є пропорційний до відстані від вихідної точки до розрахункового вузла сітки.

Врахування третьої складової поверхні перетворює метод кригінгу в апроксимаційний чи наближений метод. Тоді обчислене та дійсне значення поверхні у вихідних точках не будуть співпадати точно, однак розрахункова поверхня буде загалом більш плавна.

Доцільно детальніше розглянути особливості застосування модифікованого локально – стохастичного методу просторової інтерполяції до згладжування реконструйованої топологічної поверхні БСМ, а саме нормального чи ординарного кригінгу, який базується на положенні про те, що постійне середнє значення невідоме [101]. Застосування цього методу має більше сенсу у порівнянні з іншими, тому що за його допомогою обробляють дані не за напрямками, а за площею [114]. При цьому приймають до уваги рекомендації провідної американської

компанії з розробки спеціального програмного забезпечення для просторової інтерполяції Golden Software[115], а також друкованих [107] та інтернетних джерел [116] щодо вибору оптимального методу просторової інтерполяції:

- за наявності менше 250 точок рекомендується кригінг із лінійною варіограмною моделлю;
- оброблення набору із 250 - 1000 точок з оптимальною швидкістю забезпечує тріангуляція з лінійною інтерполяцією, кригінг і радіальні базисні функції;
- швидке оцінювання даних для набору, що налічує більше 1000 точок, може бути здійснено із застосуванням методів мінімальної кривизни і тріангуляції з лінійною інтерполяцією. Точно, але порівняно повільно проводиться опрацювання даних за допомогою методів кригінгу та радіальних базисних функцій.

Доцільно відзначити, що дуже великі набори даних не дають істотних розбіжностей у швидкості інтерполяції різними методами. Вибір методу залежить від вимог користувача і ресурсів системи. Для моделювання безперервної топологічної поверхні БСМ на основі дискретного масиву даних застосовують процедуру локальної інтерполяції, базовану на локальному кригінгу та описану моделлю [101]:

$$f(x) = \sum_{i-1}^{n} w_i f(x_i) \tag{2.27}$$

де $x \in \{x_1, x_2, \ldots x_n, \}$ – задана множина точок евклідового простору $\Re^m$ (комірок растру) будь-якого виміру, в яких розміщені ІВ БСМ, $f(x) \in \{f_1 \equiv f(x_i), f_2 \equiv f(x_2) \ldots, f_n \equiv f(x_n)\}$ – відомі значення деякої функції $f(\cdot)$ в точках $x_1, x_2, \ldots x_n$, що отримані на основі вимірювань або спостережень, причому сама функція $f(\cdot)$ невідома, w_i - вагові коефіцієнти для кожної з цих точок.

В такому випадку постає задача побудувати інтерполяційну функцію $f^*(\cdot)$, яка була б оптимальною оцінкою невідомої функції $f(\cdot)$:

$$f^*(x) \approx f(x) \forall\, x \in \Re^m \tag{2.28}$$

Застосовуючи оцінку дисперсії, можна записати:

$$\sigma^2 \equiv D[f(x)] = E[(f(x) - \mu^2)] \tag{2.29}$$

де σ – стандартне відхилення величини $f(x)$ від її математичного сподівання μ,

$D[\cdot]$ – дисперсія дискретної випадкової величини $f(x)$,

$E[\cdot]$ – математичне сподівання випадкової величини, поданої у квадратних дужках.

В подальшому можна подати:

$$\sigma^2 = E[(f(x) - \mu^2)] = -\gamma(x,x) - \sum_{i=1}^{n}\sum_{j=1}^{n} w_i w_j \gamma(x_i, x_j) + 2\sum_{i=1}^{n} w_i \gamma(x_i, x) \qquad (2.30)$$

де $\gamma(\cdot)$– варіограма або структурна функція, що є першим кроком на шляху кількісного опису регіоналізованих змінних та надає корисну інформацію для інтерполяції, оптимізації мережі вимірювань (або пробовідбірну), а також визначення моделі просторового розподілу [144].

Надалі знаходять мінімум вище наведеної функції за додаткової умови:

$$\sum_{i=1}^{n} w_i = 1 \qquad (2.31)$$

Застосовуючи метод множників Лагранжа для розв'язання задачі умовного екстремуму [146], можна записати:

$$\begin{cases} \dfrac{\partial}{\partial w_i}(-\gamma(x,x) - \sum_{i=1}^{n}\sum_{j=1}^{n} w_i w_j \gamma(x_i, x_j) + \\ +2\sum_{j=1}^{n} w_i \gamma(x_i, x) + \lambda(\sum_{i=1}^{n} w_i - 1)) = 0, \\ \sum_{i=1}^{n} w_i = 1 \end{cases} \qquad (2.32)$$

де λ – множник Лагранжа.

Підставляючи

$$\mu = -0{,}5\lambda \qquad (2.33)$$

отримують систему лінійних рівнянь у вигляді [101]:

$$\begin{cases} \sum_{j=1}^{n} w_i \gamma(x_i, x) + \mu = \gamma(x_i, x) \;\; i = 1,\ldots n \\ \sum_{j=1}^{n} w_i = 1 \end{cases} \qquad (2.34)$$

розв'язанням якої є вагові коефіцієнти для окремих точок, в яких розміщені ІВ БСМ.

Форма варіограми абсолютно безумовно характеризує вигляд просторової варіації (тренда), що наявна в межах даної площі, і може допомогти прийняти рішення, як чинити в подальшому [107, 147]. Для опису варіограми застосовують одну з найпоширеніших на практиці варіограмних моделей з порогом (sill)– сферична, експоненціальна або гауссівська.

Якщо залишкова варіація – тобто дисперсія похибок вимірювань, а також тих просторових змін, які мають характерний розмір, набагато менший, ніж крок випробувань – суттєва, але не дуже велика, доцільно використати сферичну варіограмну модель (рис. 2.13):

$$\gamma(h) = C_0 + C_1\left(\frac{3h}{2r}\right) - 0{,}5\left(\frac{h}{r}\right)^3, \ для \quad 0 < h < r$$
$$\gamma(h) = C_0 + C_1, \qquad для \quad h > r \tag{2.35}$$

де h – крок,

C_0 – залишкова варіація,

C_1 – перевищення між пороговим значенням варіограми та залишковою варіацією,

r – радіус кореляції, інша назва радіус залучення або просто радіус (range), тобто значення кроку, при якому варіограма зростає до максимального значення.

Якщо мають місце виразно виражені залишкова дисперсія та поріг, а розмах є приблизним, для опису варіограми краще всього надається експоненціальна модель:

$$\gamma(h) = C_0 + C_1\left(1 - exp\left(-\frac{h}{r}\right)\right) \tag{2.36}$$

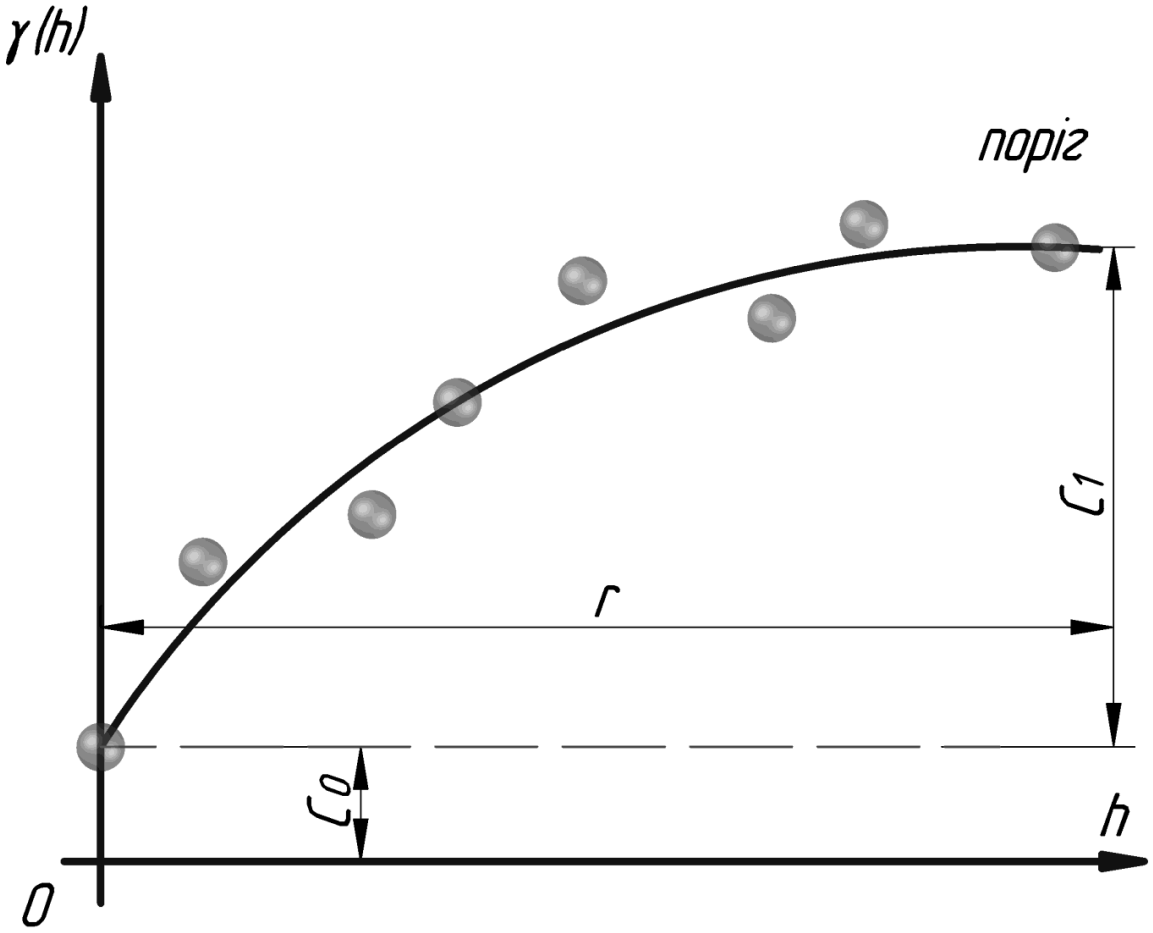


Рис. 2.14. Вибіркова варіограма

Не дивлячись на подібність графіків сферичної та експоненціальної моделей, останній притаманні декілька характерних рис. Термін “радіус” у ній не зовсім коректний. Варіограма досягає порогу асимптотично, залишаючи навіть для найдальших проб деякий малий взаємовплив. Однак на відстані радіуса візуально відрізнити її значення від порогу буває складно.

Модель задає зовсім іншу поведінку інтерполяційних алгоритмів на малих відстанях, “ослабляючи” міцність зв'язку поблизу нульового значення та знижуючи, таким чином, тут достовірність оцінки.

Для незначних змін варіограми та малої залишкової дисперсії порівняно з просторово залежною випадковою варіацією, варіограму можна оптимально представити гауссівською моделлю:

$$\gamma(h) = C_0 + C_1\left(1 - exp\left(-\left(\frac{h}{r}\right)^2\right)\right) \qquad (2.37)$$

Цій моделі притаманна дуже висока міцність взаємозв'язку в нулі, причому вона володіє порогом і радіусом, хоча порогу вона, як і експоненціальна модель, досягає не на значенні радіуса, а асимптотично. Особливості поведінки на малих відстанях дозволяють її застосувати замість процедур нелінійної статистики для об’єктів із значущим локальним трендом.

Можна застосувати і інші варіограмні моделі, стисла характеристика яких зведена в табл. 2.1.

Таблиця 2.1.

Моделі варіограми

№ з/п	Варіограмна модель	Варіограма $\gamma(h)$	Діапазон h
1	Бесселя [Pebesma E.J., 2001]	$1-\frac{h}{r}K_1\left(\frac{h}{r}\right)$, K_1 – модифікована функція Бесселя першого порядку	≥ 0
2	Квадратна [199]	$C\left(2h-h^2\right)$	<1
		C	≥ 1
3	Квадратна вимірна [199, Gressie N.A.C., 1991]	$C\left(\frac{h^2}{1+h^2}\right)$	≥ 0
4	Кубічна [199, Olea R.A., 1999]	$C\left(7h^2-8{,}5h^3+3{,}5h^5-0{,}75h^7\right)$	≥ 0
5	Лінійна [199]	Ch	≥ 0
6	Логарифмічна [Pebesma E.J., 2001]	0	0
		$log\left(h+r\right)$	>0
7	Пентасферична [Pebesma E.J., 2001]	$\frac{15h}{8r}-\frac{5}{4}\left(\frac{h}{r}\right)^3+\frac{3}{8}\left(\frac{h}{r}\right)^5$	$0\leq h\leq r$
8	Періодична [Pebesma E.J., 2001]	$1-cos\left(\frac{2\pi h}{r}\right)$	≥ 0
9	Степенева [Pebesma E.J., 2001]	h^n	≥ 0 $0<r\leq 2$
10	Хвильова [199, Gressie N.A.C., 1991]	$C\left(1-\frac{sin\ h}{h}\right)$	>0

Якщо переходити з декартової системи координат до циліндричні координати, то додатково можна скористатися з ординарного кригінгу в циліндричних координатах [148].

Потім проводять аналіз візуалізованої форми згладженої реконструйованої топологічної поверхні БСМ із застосуванням сітки трикутників з розміщеними у їх вершинах ІВ з координатами в евклідовому просторі та виявлення фальшивих з’єднань між сусідніми ІВ, зумовлених атакою червоточини (рис. 2.15) [61, 64].

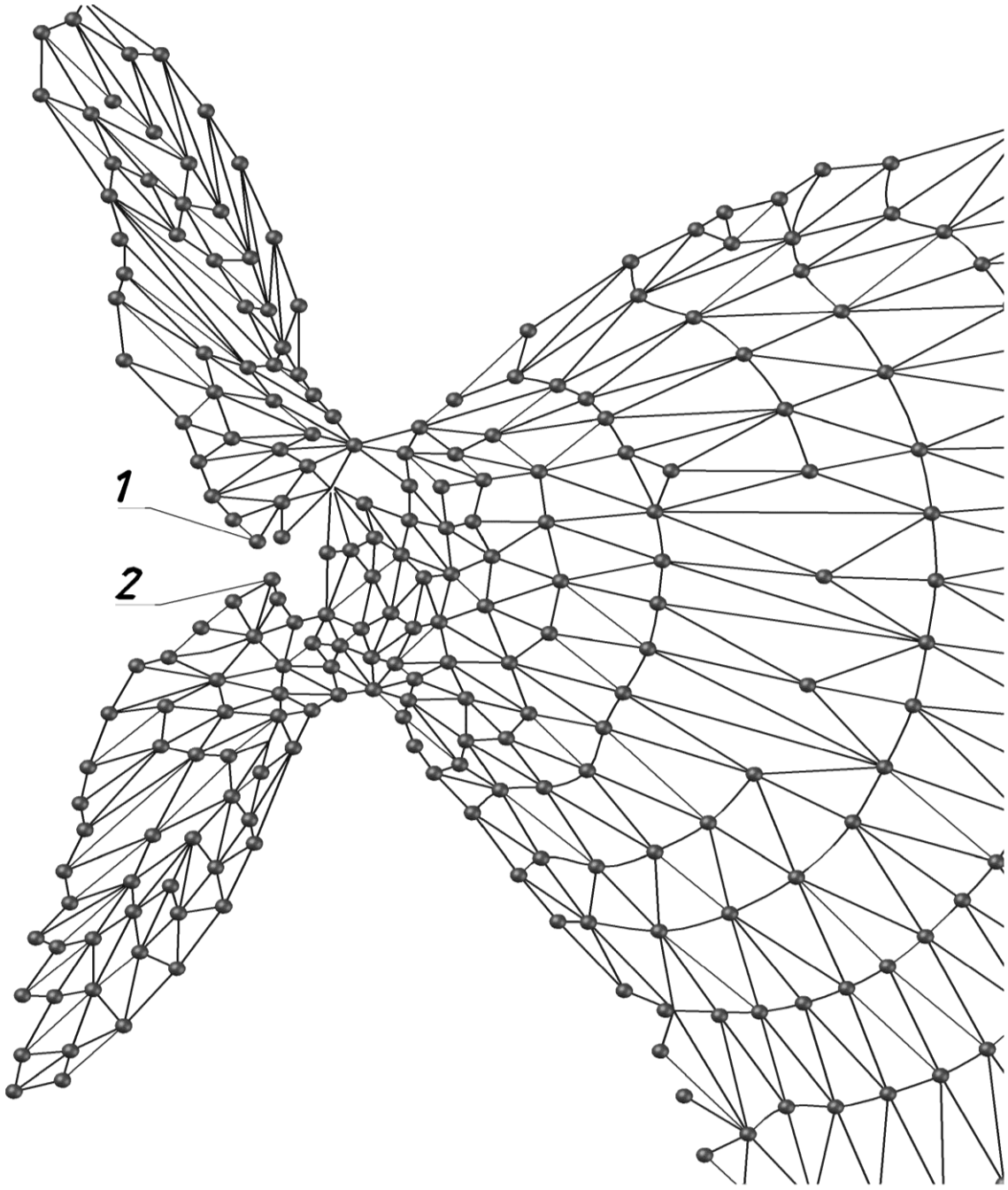


Рис. 2.15. Результати моделювання візуального виявлення атаки червоточини в БСМ на підставі кригінг-інтерполяції реконструйованої топологічної поверхні мережі та сітки трикутників з розміщеними у їх вершинах ІВ з координатами в евклідовому просторі: 1, 2 – вершини, у яких розміщені ІВ

Використовуючи запропоновану формалізовану ознаку ідентифікації зловмисного вузла в БСМ, можна автоматично виявити атаку. Це дає змогу оператору спростити процедуру виявлення зловмисного вузла та пришвидшити прийняття рішення щодо його подальшої локалізації на підставі відповідного списку ІВ, сформованого на підставі вищезгаданої ознаки.

На підставі результатів проведеного аналізу можна констатувати, що атака червоточини вигинає згладжену реконструйовану топологічну поверхню БСМ, притягуючи ІВ один до одного, та створює фальшиві з'єднання в точках 1 та 2 розміщення ІВ рис. 2.15 [100].

2.4. Програмне забезпечення геометричного моделювання БСМ

Для моделювання БСМ використовують операційну систему Tiny OS, яка дозволяє здійснювати керування ІВ першого рівня, організовувати передачу інформації в середині мережі та одержувати схеми розташування ІВ. Основним механізмом керування для операційної системи Tiny OS є подія. Подією називають отримання показників, спрацювання таймера, надходження пакетних даних, завершення обчислення параметрів ІВ та ін. Отже, для моделювання роботи ІВ у складі БСМ необхідно змоделювати апаратні події. Для моделювання подій БСМ, ІВ якої працюють під керуванням Tiny OS, використовують програмне забезпечення TOSSIM, яке в поєднанні з Tiny Viz дозволяє отримати графічне представлення БСМ (рис.2.15) [33].

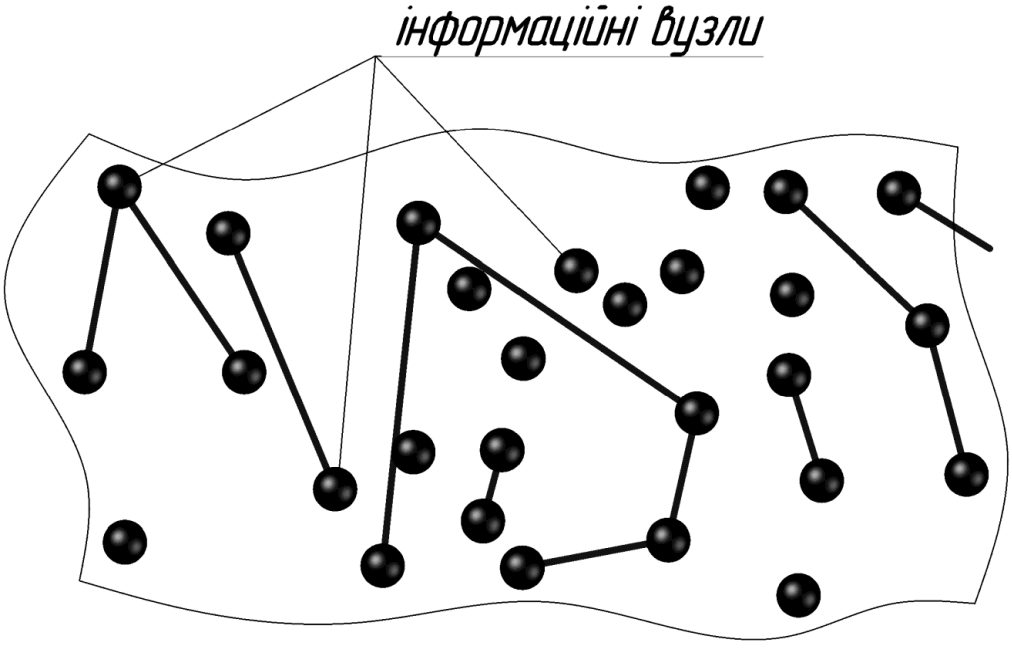


Рис. 2.16.Модель сенсорної мережі одержаної за допомогою Tiny Viz

Програму – емулятор TOSSIM (Tiny OSSI Mulator)встановлюють на звичайний ПК разом з набором інструментальних засобів, які необхідні для створення, компіляції, встановлення і налагодження додатків для БСМ [34]. Робота з цими інструментами здійснюється з допомогою командного інтерфейсу, характерного для OSUNIX. До загальних характеристик емулятора TOSSIM відносять:

- масштабованість – емулятор може моделювати роботу, як окремих ІВ, так і великих мереж, які складаються з кількох тисяч точок ІВ;
- повноту – емулятор здатен моделювати різні схеми взаємодії елементів БСМ, зокрема не тільки алгоритми і мережеві протоколи, але й структуру мережі ІВ, що змінюється;
- точність – емулятор може представляти поведінку мережі з необхідною точністю;
- достовірність – емулятор реалізує адекватний перехід від змодельованого до реального середовища використання додатку, надаючи розробнику можливість тестувати код, який призначається для реального обладнання.

До складу емулятора TOSSIM (рис. 2.16) входять наступні елементи:

- черга подій;
- набір програмних компонентів, які замінюють відповідні апаратні компоненти реальних ІВ;
- механізми опису моделей радіоканалів і аналогово-цифрових перетворювачів (АДС);
- засоби зв’язку, які дають можливість зовнішнім програмам взаємодіяти з емулятором.

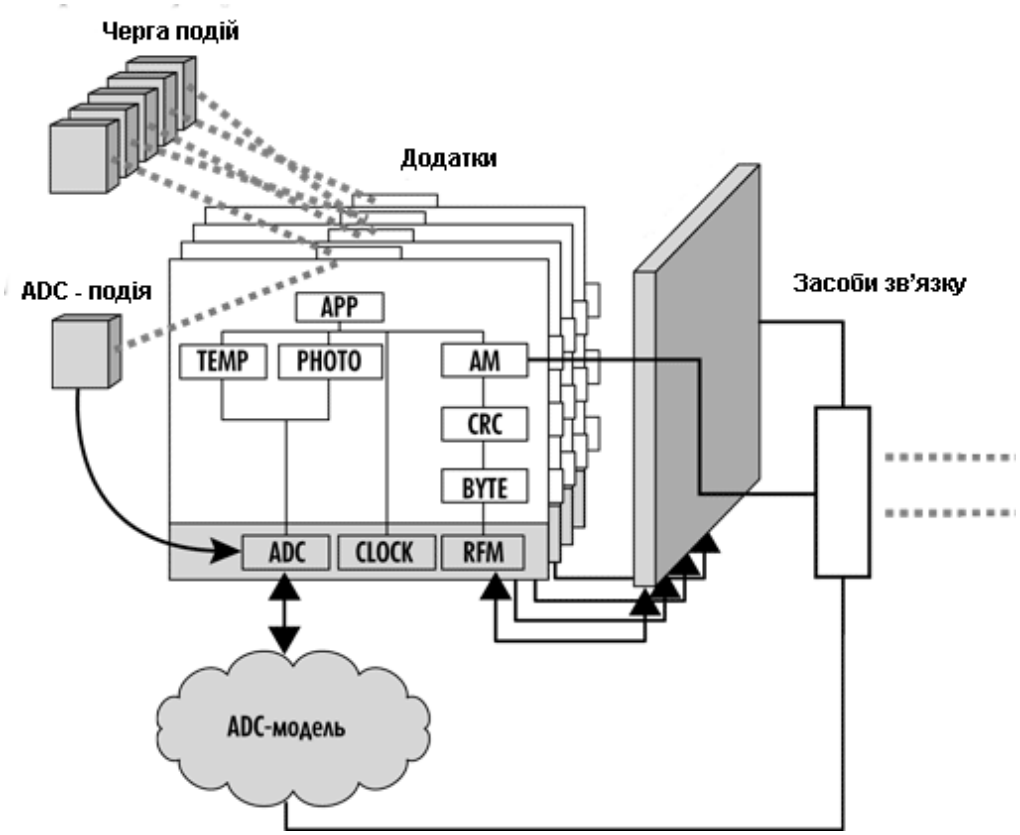


Рис. 2.17. Архітектура емулятора TOSSIM

Незважаючи на широкі можливості TOSSIM, може виникнути необхідність у зміні його функціональності. Для цього в ньому передбачені засоби зв’язку зі зовнішніми додатками, які дозволяють керувати процесом моделювання і спостерігати за моделлю. Зокрема, для графічного моделювання БСМ організовують зв'язок TOSSIM з Tiny Viz. Tiny Viz – це додаток, який реалізує написаний на мові програмуванняJava графічний інтерфейс і дозволяє полегшити роботу з емулятором. Tiny Viz представляє змодельовану мережу у графічному вигляді, а також дозволяє курувати процесом моделювання за допомогою меню. Tiny Viz надає розробникам можливість вводити свої механізми керування емулятором.

Розділ 3. Геометричне моделювання параметрів сигналів ІВ

3.1. Класифікація атак на БСМ

Успішність та надійність роботи БСМ залежить від досконалості прогнозування та ефективності методів боротьби з атаками на апаратне та програмне забезпечення мереж. Під час розробки та оцінювання ефективності методів боротьби з атаками на БСМ доцільно опиратися на систему класифікації атак, яка б врахувала сьогоднішній рівень знань і досвіду створення та експлуатації БСМ, а також прогнози щодо шляхів їх розвитку.

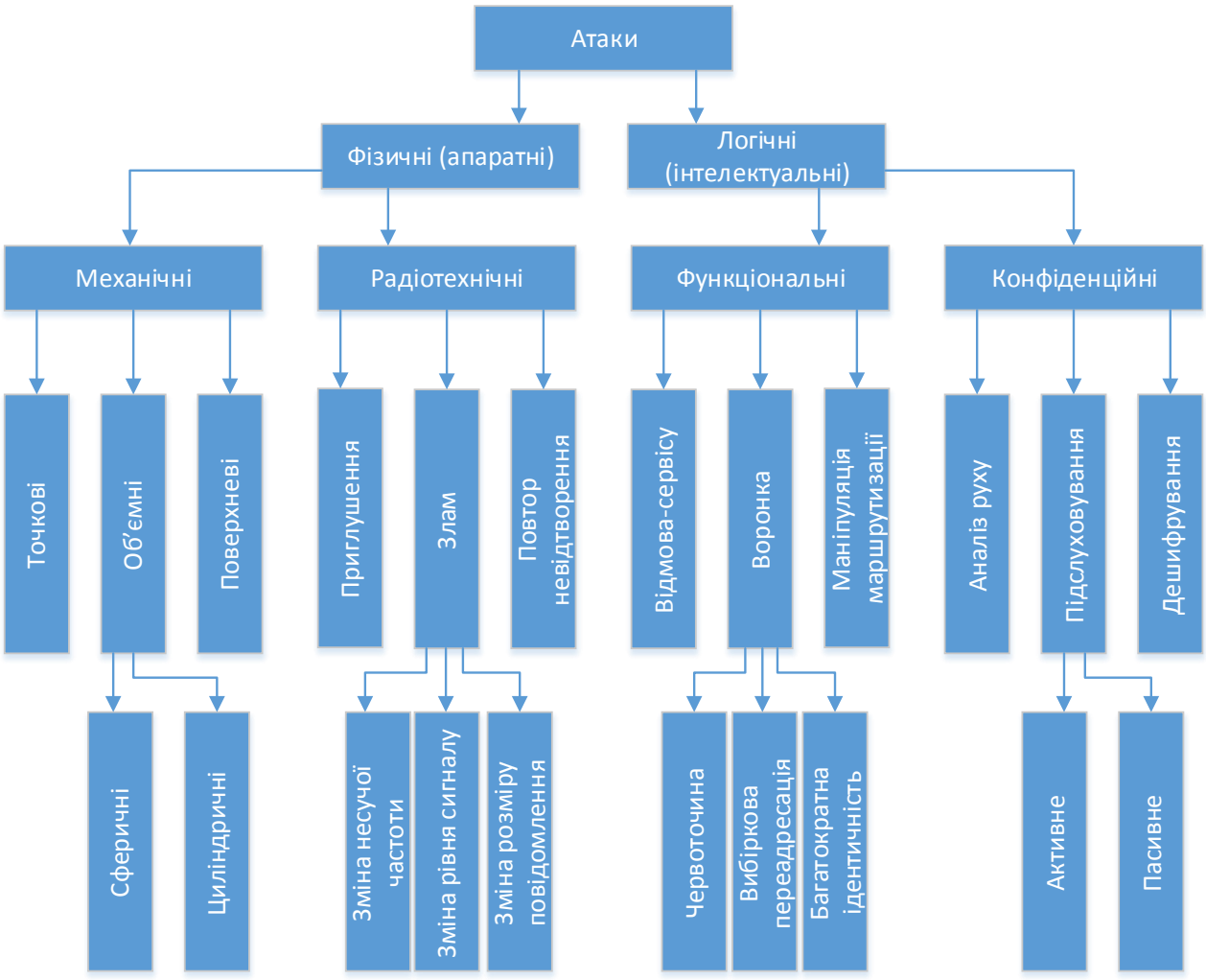


Рис. 3.1. Класифікація атак на БСМ

Атакам можуть піддаватися ІВ, сигнали, що транслюють у мережі та конфіденційність інформації. Тому атаки розділяють на фізичні та інтелектуальні (рис. 3.1). При цьому до фізичних атак відносять механічні і радіотехнічні. Механічні атаки передбачають пошкодження або виведення з ладу ІВ. Залежно від взаємного розташування пошкоджених ІВ атаки можуть бути точковими, поверхневим або об'ємними.

Об'ємні механічні атаки доцільно розділяти за геометричними особливостями зон виведення з ладу мережі на сферичні та циліндричні.

Запропонована класифікація механічних атак дозволяє полегшити вибір методу візуалізації зони розповсюдження атаки та параметрів її розрахунку. Так для візуалізації поверхневої атаки використовують два характерні лінійні розміри, які характеризують відповідну площину. При цьому третім просторовим напрямком нехтують. Для візуалізації сфероподібної атаки вважають, що зона атаки поширюється у трьох просторових напрямах, які є рівновеликими, тому її можна подати у вигляді сфери або множини сфер, які перетинаються. Для візуалізації циліндроподібних атак використовують три просторові напрямки їх поширення. При цьому два з них є практично незмінним, але достатньо великими, щоб ними нехтувати, а третій є визначальним і достатнім для характеристики напрямку розповсюдження атаки.

Радіотехнічні атаки передбачають руйнування електромагнітного сигналу. Такого руйнування досягають повним або частковим його приглушенням, зламом з подальшою повною або частковою зміною параметрів сигналу і трансляцією зміненого сигналу у мережі. Детальна класифікація атак, спрямованих на руйнування сигналу приведена у літературних джерелах [36]. Для візуалізації таких атак застосовують вимірювання рівня потужності прийнятого сигналу. При цьому зменшення потужності сигналу розглядають як результат збільшення відстаней між ІВ і відповідно збільшення площі БСМ.

Атаки, які супроводжуються зламом сигналу, доцільно розділяти на атаки зі зміною несучої частоти, атаки зі зміною рівня сигналу і атаки зі зміною розміру повідомлення. Як правило, успішне проведення більшості радіотехнічних атак вимагає втручання у структуру сигналу, тому вони науковцями розглядаються як функціональні атаки [37]. Візуалізацію атак, які супроводжуються зламом сигналу, виконують шляхом постійного аналізу структури сигналу і у випадку ви-

явлення відхилень вважають ІВ непрацюючим. Відповідно візуалізацію зон поширення таких атак доцільно проводити аналогічно візуалізації зон поширення механічних атак.

Атаки повторного відтворення передбачають несанкціоноване відтворення інформації. При цьому може використовуватися попередньо підслухана або випадково придумана інформація [38].Даний вид атаки потребує перебування вузла «шкідника» в одній локальній мережі, що і пошкоджуваний вузол. Вузол «шкідник» відносно просто може слідкувати за обміном інформації та блокувати її [39]. Такий вузол перехоплює пакети інформації та імітує роботу звичайного ІВ.

Інтелектуальні або логічні атаки розділяють на функціональні та конфіденційні. Під функціональністю БСМ розуміють коректну роботу всіх ІВ мережі, маршрутизацію та фізичний рівень. Під конфіденційністю розуміють гарантію того, що інформація доступна тільки повноваженим особам, які мають повні права доступу до неї та своєчасно і без спотворень її одержують у повному обсязі. Таким чином функціональні атаки направлені на руйнування функціональних параметрів БСМ. Конфіденційні атаки спрямовані на прослуховування, розшифрування, викрадення інформації. Детальна класифікація, опис таких атак наведені у літературних джерелах [36]. Особливе місце серед функціональних атак займає, так звана, група атак «воронка» [40, 41]. Такі атаки перешкоджають базовим ІВ одержувати повну і коректну інформацію від ІВ нижчого рівня. З допомогою атак «воронка» можна одержати необхідний доступ до інформації у зоні БСМ, яка цікавить зловмисника. Для проведення таких атак створюють шкідливий вузол, дія якого направлена на найближчі ІВ відповідно до маршрутизації. Вузол «шкідник» руйнує алгоритми маршрутизації. Результати таких атак можуть проявитися у спрямуванні руху інформації через конкретний вузол, блокуванні передавання пакетів інформації шляхом їх відбору для подальшої трансляції, наданні конкретному ІВ декількох ідентифікаторів(часто неіснуючих ІВ, причому цей конкретний ІВ може ідентифікуватися у багатьох місцях водночас). З поміж групи атак «воронка» виділяють такі впливи на БСМ як червоточина, вибіркова переадресація та багатократна ідентичність. Дія таких атак на алгоритми маршрутизації, які ґрунтуються на географічному положенні ІВ, може при-

вести до неправильної інтерпретації отриманої інформації та дозволити зловмиснику перехоплювати конфіденційні дані. Для візуалізації вказаних атак використовують відомі методи тріангуляції Делоне та діаграми Вороного [41].

Конфіденційні атаки розділяють на аналіз руху інформації, підслуховування і маніпуляцію маршрутизацією інформації. Як правило, в результаті таких атак зловмисник одержує можливість розшифрування інформації, визначення маршруту і частоти передачі інформації для подальшої організації функціональних атак на БСМ.

Для планування, проектування та розробки ефективних методів протидії логічним атакам на БСМ запропоновано більш детальні аналіз та класифікацію таких атак. Під час їх створення додатково використовують аналіз інтелектуальних та технічних можливостей зловмисників. Зокрема, в літературних джерелах [88] зазначено, що зловмисник може розгорнути в БСМ декілька шкідливих ІВ з аналогічними технічними характеристиками, вдаючи ІВ санкціонованими, які в подальшому можуть спільно здійснювати атаку на систему. Крім цього, в деяких випадках такі ІВ, беручи участь у змові, можуть мати високої якості канали радіозв'язку, доступні для координації своїх атак. ІВ давачі не можуть бути стійкі проти маніпуляції, а якщо зловмисник компрометує ІВ, то може отримати всі ключові матеріали, дані та код, що зберігаються на цьому ІВ.

Зловмисників БСМ зазвичай поділяють на дві групи: такі, які мають доступ до дуже обмежених технічних ресурсів, і на такі, які становлять значно більшу загрозу з огляду на свої можливості (лептоп, радіопередавач високої потужності, чутлива антена, тощо). Серед нападників можна виділити таких, які діють зсередини – інсайдерів, та ззовні мережі – аутсайдерів, причому інсайдери часто володіють набагато більшими можливостями атаки [149].

Дані та конфіденційна інформація не повинні бути виявлені несанкціонованими суб'єктами [150]. Шляхом спуфінгу (Spoofig), відповідної маніпуляції інформацією протоколу маршрутизації БСМ можна досягти петель в маршрутизації, спрямувати рух в конкретне місце, маніпулювати протяжністю конкретних трас. Застосовуючи вибіркову переадресацію (Selective Forwarding) інформації, зловмисний ІВ мережі міг би, наприклад, не передавати далі жодного отриманого пакету інформації, а це призвело б до появи чорної діри (Black Hole) в БСМ. Така агресивна поведінка може бути відповідно осмислена та інтерпретована мережею як спроба атаки, з приводу чого буде обраний інший маршрут передавання.

Для ускладнення процесу виявлення шкідливої роботи ІВ зловмисника останній може обережніше блокувати передавання пакетів інформації шляхом відповідного їх вибору для подальшої трансляції у мережу, тобто здійснювати вибіркове передавання пакетів інформації. Поряд з атаками, що полягають у вибірковій переадресації особливо небезпечними є, так звані, воронкові атаки (AttackSinkhole), тобто атаки що передбачають спрямування інформації через конкретний ІВ в БСМ. Для реалізації такої атаки вибраний зловмисникомІВ роблять привабливим у трактуванні алгоритму маршрутизації у БСМ. Заслуговує також на особливу увагу атака багатократної ідентичності (Sybil Attack), яка полягає в тому,що конкретний ІВ в БСМ може мати декілька ідентифікаторів (часто неіснуючих ІВ, причому цей конкретний вузол може ідентифікуватися в багатьох місцях водночас), тим самим порушуючи функціонування мережі. Внаслідок цього атаки на алгоритми маршрутизації, які ґрунтуються на інформації про географічне положення ІВ, можуть неправильно інтерпретувати отриману інформацію та дозволити зловмиснику перехопити конфіденційні дані. Заслуговує на увагу метод атаки HELLO на БСМ. У багатьох протоколах передбачено, що ІВ повинен оголошувати шляхом широкотрансльованих повідомлень HELLO свою присутність сусідам. За допомогою потужного передавача можна обманути багато ІВ, що певний ІВ є сусідом. Тоді виявиться, що маршрут створений за участю фіктивного ІВ, до того ж дуже привабливий, використовуватиметься часто, натомість пакети інформації, що передаються через ІВ, які знаходяться далеко від атакованого вузла, пропадатимуть [84, 149, 151].

Ґрунтуючись на вищенаведеному викладенні та на підставі результатів аналізу наукових літературних джерел [84-87] і з врахуванням особистого досвіду запропоновано ідентифікацію та класифікацію моделей атак в БСМ за критеріями різних рівнів моделі OSI (Open Systens Interconnection) і характером впливу (активні та пасивні), що зображено на рис. 3.2 [88].

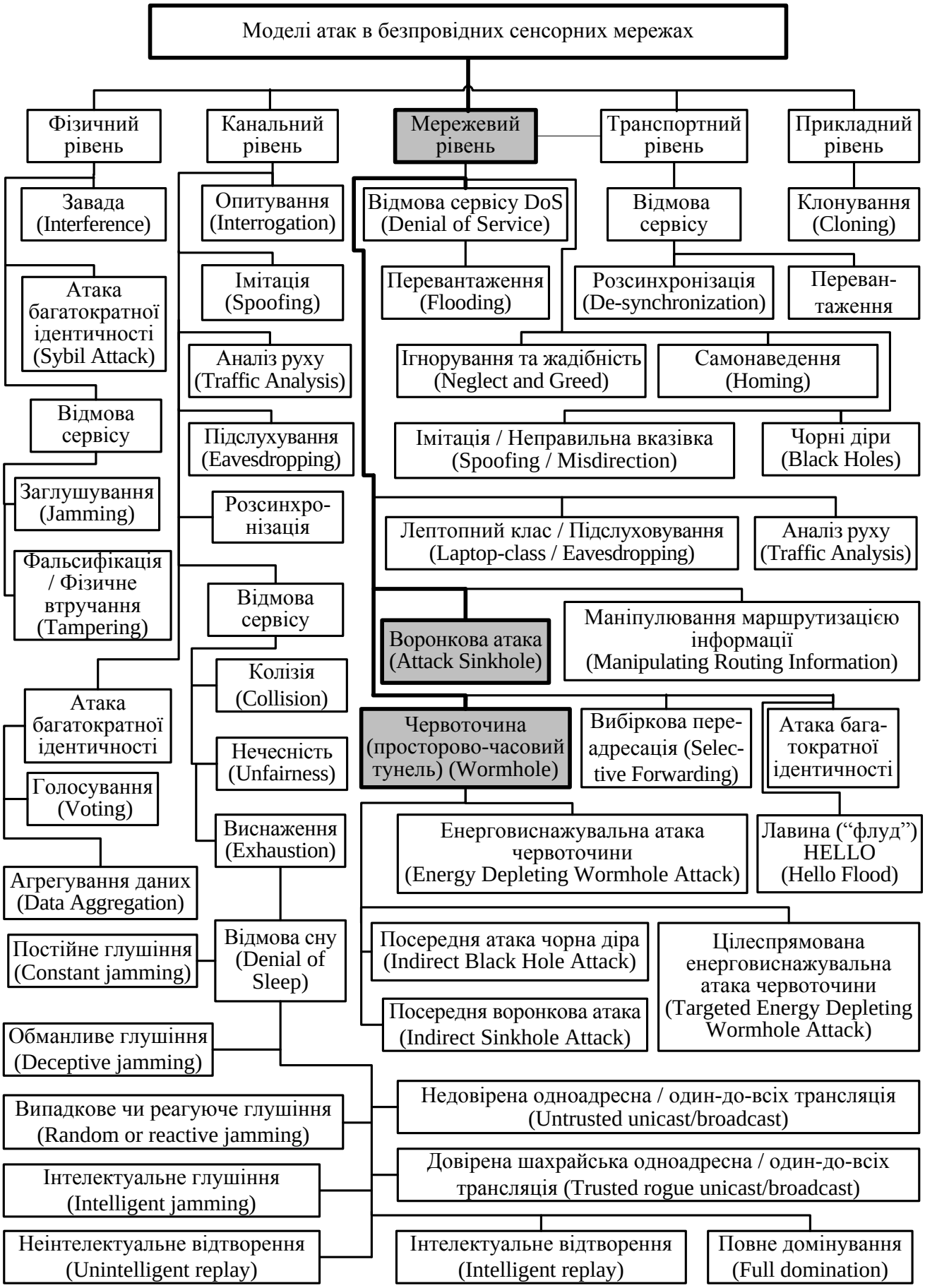


Рис. 3.2. Класифікація моделей інтелектуальних атак на БСМ

Зв’язок моделей атак на БСМ із рівнями OSI наведено в табл. 3.1.

Таблиця 3.1.

Зв’язок моделей атак на БСМ із рівнями OSI

Опис моделі атаки				Рівні OSI				
				Фізичний	Канальний	Мережевий	Транспортний	Прикладний
1				2	3	4	5	6
Завада				+				
Атака	багатократної ідентичності			+				
	Голосування				+			
	Агрегування даних				+			
Відмова сервісу	Заглушування			+				
	Фальсифікація / фізичне втручання			+				
	Колізія				+			
	Нечесність				+			
	Розсинхронізація				+		+	
	Перевантаження						+	
	Виснаження	Відмова сну	Обманливе глушіння		+			
			Постійне глушіння		+			
			Випадкове чи реагуюче глушіння		+			
			Інтелектуальне глушіння		+			
			Неінтелектуальне відтворення		+			
			Недовірена одноадресна / один-до-всіх трансляція		+			
			Довірена шахрайська одноадресна / один-до-всіх трансляція		+			
			Інтелектуальне відтворення		+			
			Повне домінування		+			

Продовження таблиці 3.1

1		2	3	4	5	6
Ігнорування та жадібність				+		
Самонаведення				+		
Імітація / Неправильна вказівка				+		
Чорні діри				+		
Лептопний клас / Підслуховування				+		
Аналіз руху			+	+		
Опитування						
Імітація						
Підслухування						
Воронкова атака				+		
Маніпулювання маршрутизацією інформації						
Черв точина (просторово-часовий тунель)	Енерговиснажувальна атака червоточини			+		
	Посередня атака чорна діра			+		
	Цілеспрямована енергоснажувальна атака червоточини			+		
	Посередня воронкова атака					
Лавина (“флуд”) HELLO				+		
Вибіркова переадресація						
Клонування						+

3.2. Моделювання режимів протидії атакам на БСМ

Сучасні БСМ є керованими та дозволяють виконувати їх моніторинг на довільному етапі роботи. Під час розподіленої координації мережі доцільно скористатися властивістю зв’язності, це дозволить на практиці ефективніше використовувати ресурс БСМ. Для розв’язку поставленої задачі доцільно скористатися моделлю інформаційної системи, яка володіє природнім паралелізмом та дозволяє продуктивно обробляти великі обсяги даних.

Робота БСМ в значній мірі залежить від топології, тому для успішного розв’язання задачі створення моделі протидії атакам на БСМ слід визначити місця розміщення ІВ, що входять до цієї мережі. Розглянемо гомогенні мережі, в яких використовують подібні ІВ, та гетерогенні БСМ, що об’єднують різнотипний ресурс.

Для моделювання режимів протидії атакам на БСМ використовують нечіткі відношення (fuzzy relation – *fR*), що дозволяє на практиці змоделювати їх динамічний стан. Таке відношення визначає індикаторна функція

$$I_{fR}(u_1,u_2,...,u_n)=\psi_{fR}(u_1,u_2,...,u_n):U_1\times U_2\times...\times U_n\to Z=\langle Z,\Omega_z\rangle, \quad (3.1)$$

де $(u_1,u_2,...,u_n)$ – вхідні радіосигнали для вузла ϑ_i;

Z – поле, яке описує радіосигнали БСМ;

Ω_z – сигнатура, що містить базові операції.

Тоді відношення між радіосигналами *fR*, заданими на декартовому добутку ресурсу мережі $U_1\times U_2\times...\times U_n$, визначатиме сукупність:

$$\left\{\begin{array}{c}\left(\left(u_1,u_2,...,u_n\right),I_{fR}\left(u_1,u_2,...,u_n\right)\right):I_{fR}\left(u_1,u_2,...,u_n\right)=\psi_{fR}\left(u_1,u_2,...,u_n\right),\\ \left(u_1,u_2,...,u_n\right)\in U_1\times U_2\times...\times U_n\end{array}\right\} \quad (3.2)$$

Визначена модель (3.2) дозволяє скористатися описом режимів роботи БСМ, включно з наявними загрозами та збурювальними чинниками, зумовленими проведенням атак, на основі використання нечіткого зваженого графа.

Слід зазначити, що нечіткому графу $fG(V,E,fV,fE)$ притаманна сукупність не порожньої множини ІВ сенсорної мережі *V*, множини *E* – радіосигналів вузла (ребер графа), *fV* (fuzzy vertex) – нечіткого ударного відношення (назва ресурсу мережі), *fE* (fuzzy edge) – нечіткого бінарного відношення.

Опис моделі топології БСМ виконують, беручи до уваги режим функціонування БСМ за умови дії зумовлених атаками збурювальних факторів, нечітким зваженим графом $fG(V,E,fV,fE)$ з множиною вершин $V=\{v_1,v_2,...,v_n\}$ мітки яких задають індикаторною функцією:

$$I_{fV}=\frac{v_2}{\sqrt{2}}+\frac{v_1}{\sqrt{2}}i. \quad (3.3)$$

Тоді ребра характеризуватиме такий декартів добуток: $E=(v_1\times v_2)$. Комплексно значимі мітки визначають функцією нечіткого відношення

$$I_{fE}=\frac{1}{2}(v_1,v_1)+\frac{1}{2}(v_1,v_2)+\frac{1}{2}(v_2,v_1)+\frac{1}{2}exp(i\phi)(v_2,v_2) \quad (3.4)$$

Для узагальнення опису моделі різних режимів функціонування БСМ, включно із врахуванням загроз та за наявності зумовлених атаками збурювальних чинників – особливо атаками маршрутизації, визначають кубіти. Базисні

стани першого кубіта визначають вершини $V = \{v_1, v_2\}$, причому $v_1 = |0_1\rangle$, $v_2 = |1_1\rangle$. Тоді хвильову функцію описують моделлю:

$$|\psi_1\rangle = \frac{i}{\sqrt{2}}|0_1\rangle + \frac{1}{\sqrt{2}}|1_1\rangle. \quad (3.5)$$

Беручи до уваги згадані викладки, стає зрозуміло, що $|\psi_1\rangle = I_{fV}$.

Розширюють модель вищезазначених режимів функціонування БСМ на базисні стани другого та третього кубітів, які є множиною ребер

$$E = \{(v_1, v_1), (v_2, v_1), (v_1, v_2), (v_2, v_2)\} \quad (3.6)$$

де $(v_1, v_1) = |00_{23}\rangle, (v_2, v_1) = |10_{23}\rangle, (v_1, v_2) = |01_{23}\rangle, (v_2, v_2) = |11_{23}\rangle$.

Тоді модель хвильової функції матиме вигляд:

$$|\psi_{23}\rangle = \frac{1}{2}|00_{23}\rangle + \frac{1}{2}|01_{23}\rangle + \frac{1}{2}|10_{23}\rangle + \frac{1}{2}exp(i\varphi)|11_{23}\rangle \quad (3.7)$$

причому комплексно значимі мітки ребер – це $|y_{23}\rangle = I_{fE}$

Представлені вище моделі нескладно розповсюджуються на орієнтовані графи, які вказують не лише на існування зв'язку, а враховують напрямок дії зв'язку, що дозволяє отримати покращені якісні та кількісні показники при детальному дослідженні БСМ з врахуванням наявних збурювальних чинників. Також завдяки таким моделям можна динамічно змінювати структурну та алгоритмічну організацію систем і методів моделювання БСМ в цих умовах, забезпечуючи їх подальше функціонування, особливо за наявності таких небезпечних атак маршрутизації, якими є вибране переадресування, воронкова атака, атаки Сибіли чи червоточини.

Поле діяльності в галузі засобів захисту та контролю доступу для безпечної комунікації у БСМ є досить широким, включаючи вибрані на ринку технології розробки консольної бібліотеки для обслуговування мікроконтролерів при застосуванні модулю USART (Universal Synchronous / Asynchronous Receiver / Transmitter – універсальний синхронний/асинхронний трансивер) з шифрувальною підпрограмою. Подібна система Kee Loq була запатентована фірмою Microchip і базується на динамічному (стрибкоподібному) коді (hopping code) [152]. Ця система використовується в багатьох галузях безпровідного зв'язку та належить до одного з найпоширеніших апаратних рішень із застосуванням регістра зсуву з нелінійною функцією. Згадана функція є стандартною складовою,

яку використовують в радіозв'язку та картах доступу, як найменш уразливу для криптоаналітичних атак в порівнянні зі стандартною лінійною функцією в поєднанні з регістром зсуву. Інші системи, в яких застосовуються нелінійні функції, це – Achterbahn, Grain, Trivium, VEST.

Одностороннім системам притаманні два істотні недоліки: код, який передається передавачем, загалом відомий та кількість комбінацій є відносно низькою. З цієї причини, ці пристрої можуть бути уразливі щодо несанкціонованого доступу [153]. Тому н**а**дійною буде система, в якій вищезгадані недоліки усунуті. До такого рішення належить змінно-кодова система Kee Loq, в якій передбачена велика кількість можливих комбінацій ключа [154, 155]. З метою забезпечення безпеки також повинна виконуватися друга умова – система не може вдруге реагувати на цей самий ключ [156]. Односторонній зв'язок в рамках технології Kee Loq був запропонований доктором наук Ф.Брувером з компанії Nanoteq Ltd., а система шифрування була розроблена професором Ґ. Куном. В подальшому вона була реалізована в мікросхемі доктором наук В. Смітом з компанії Nanoteq Ltd. Усередині 80-х років система Kee Loq набула стрімкого розвитку після покупки ліцензії на неї компанією Microchip Technology Inc. З того часу ця система набула великої популярност ізавдяки своїй надійності, а також низькій вартості таких мікросхем як NTQ105/106/115/125D/129D та HCS101/2XX/3XX/4XX/5XX. Їх застосовують в більшості безпровідних систем контролю доступу фірмами Chrysler, Daewoo, Fiat, GM, Honda, Toyota, Volvo, VW, Clifford, Shurlok, Jaguar. Однак, як показали аналізи літературних джерел і дослідження, згадана система вимагає доопрацювання та адаптації для успішного вирішення задач моделювання безпеки БСМ, що експлуатуються у багатьох галузях промисловості.

Один з підходів пришвидшення виявлення атак в БСМ та прийняття оператором своєчасного рішення по їх локалізації вбачається у підвищенні швидкодії оброблення сигналів із застосуванням швидкого перетворення Фур'є (ШПФ) [157]. У цьому випадку може бути використана система сигма-дельта (Σ-Δ) перетворення, де на заключному етапі є наявний модуль цифрової обробки сигналу DSP (Digital Signal Processing). Незамінним в цьому модулі є застосування ШПФ. Такі засоби можуть працювати в режимі реального часу, приміром, за умови використання 32-бітних мікроконтролерів DSP Texas Instruments, призначених для обслуговування засобів цифрової обробки сигналу та ШПФ. У безпровідних мережах, зокрема, для підтримки цифрової обробки сигналу спеціально десигнованим компонентом є згаданий раніше ІВ зі всіма системними функціями FFD.

Тому постає необхідність функціональної симуляції та верифікації моделей засобів ШПФ на сучасній мікроелектронній елементній базі, беручи до уваги її стрімкий розвиток та наявність алгоритмічно-структурних особливостей та технічних характеристик.

3.3. Моделі та методи запобігання загрозам на БСМ

Оскільки БСМ широко застосовують в різних середовищах та програмах, то забезпечення їхньої безпеки стало одним із головних пріоритетів. Серед численних характеристик, які підлягають захисту, унікальність та автентичність ідентичності ІВ повинні бути посилені для виконання основних операцій, таких як маршрутизація, розподіл ресурсів, і виявлення порушень поведінки ІВ. Наприклад, система виявлення вторгнень IDS (Intrusion Detection System) в БСМ виявляє атаки та ізолює шкідливі вузли [158], які відповідають моделям відомих вторгнень [159], або виявляє аномалії у функціонуванні БСМ [160, 161, 162]. Якщо зловмисники можуть внести засіб з таким самим підробленим ідентифікатором і втрутитись в мережеві операції, ефективність системи IDS буде істотно ослаблена. Таким чином, моделі та методи для запобігання та виявлення таких атак повинні бути належним чином розроблені.

Безпека в БСМ є надзвичайно важлива в практичному застосуванні. Зокрема, не передбачається впроваджувати компоненти БСМ в промисловості, особливо в системах енергоспоживання та інших об’єктах стратегічного призначення в електроенергетиці, якщо не будуть дотримані вимоги, що стосуються захисту мережі [149].

Беручи до уваги невпинність інтеграції та використання БСМ в повсякденних комп’ютерних пристроях, засобах автоматики та робототехніки, системах електроспоживання та обліку енергії, тощо [163, 164, 165], дослідження їх поведінки та аспектів моделювання з врахуванням безпеки цих мереж в реальних умовах стає головною вимогою. Враховуючи, що ІВ використовують радіоканал для передавання інформації, зкомпроментовані ІВ можуть підслуховувати та ретранслювати пакети, тунелювати їх в інше місце в мережі, залучаючи для цього додатково атаки дії завад та заглушування [70, 149]. Задачі з області мережевої безпеки, розв’язання яких методами моделювання та візуалізації для забезпечення додаткового рівня захисту щодо топології мережі і практичного застосування за межами традиційних механізмів безпеки, таких як шифрування і аутен-

тифікація, а також виявлення атак та ізолювання шкідливих ІВ шляхом зіставлення моделей відомих вторгнень або виявлення аномалій у функціонуванні мережі, відіграють суттєву роль в загальній важливій науково-практичній проблематиці [61]. В БСМ можуть виникати нештатні режими роботи, зумовлені різного типу зловмисними діями. Тому актуальною є розробка заходів протидії наявним атакам та моделювання їх ефективності [166].

Методи усунення впливу збурювальних чинників і протидії загрозам функціонуванню БСМ та підходи до їх безпеки на рівнях теоретичної моделі структури мережевої комунікації зводяться до наступного [80]:

1) прикладний рівень – на цьому рівні інформація зібрана та дані піддаються керуванню, тому важливо бути впевненим в достовірності відомостей. Тоді рекомендується використати стійкі схеми агрегації, запропоновані до кластерних мереж, в яких кластерний лідер функціонує агрегатором в БСМ [167]. Однак цей метод слід застосувати лише в тому випадку, якщо вузол агрегації перебуває в зоні дії усіх вихідних вузлів і відсутній інший проміжний агрегатор між ними. В підході ієрархічної кластеризації канал зв'язку між агрегатором і базовою станцією має потенційно обмежену перепускну здатність, тому що кластерний лідер, який представляється агрегатором, насправді є ІВ [167, 168]. Для забезпечення надійності агрегування, кластерним лідерам доцільно використовувати криптографічні методи, гарантуючи таким чином достовірність даних;

2) мережевий рівень – відповідає за маршрутизацію повідомлень від ІВ до ІВ, від ІВ до кластерного лідера, від кластерного лідера до кластерного лідера, від кластерного лідера до базової станції та навпаки.

Розрізняють два типи протоколів маршрутизації в БСМ:

протоколи на основі ідентифікації (ID), в яких пакети направляються до місця призначення на підставі зазначених у пакетах ідентифікаторів ID;

протоколи, орієнтовані на дані [169], в котрих пакети містять ознаки (атрибути), що визначають тип доставлених даних. Загрози функціонуванню БСМ, викликані наведеними в літературі [81] атаками маршрутизації, реалізуються в такій послідовності [170]:

а) пакети втрачаються повністю або вибірково;

б) мережа перевантажена (інакше floodding) глобальними широкотрансльованими повідомленнями.

Значна частка трафіка тунелюється з одного місця в БСМ до іншого більш віддаленого місця, позбавляючи доступу до даних інші сегменти мережі, які вони

отримали б за нормальних обставин. Іноді трафік заманюється на конкретний ІВ або до невеликої групи ІВ, знову ж позбавляючи інші сегменти БСМ трафіка, котрий вони зазвичай отримують.

Безпека протоколів маршрутизації полягає у локалізації ІВ і застосуванні алгоритмів шифрування [171, 172]. Оскільки всі ІВ в БСМ виконують функцію маршрутизаторів, то це зумовлює розробку протоколів маршрутизації дуже складною [173]. Вони повинні бути ефективними щодо споживаної електроенергії та обсягу пам'яті з водночас достатньою стійкістю проти помилок для протистояння загрозам на безпечне функціонування БСМ та збоям ІВ.

Розв’язання цих задач вбачається у застосуванні теорії графів, приміром, запропонованого в [21, 27, 166] підходу або поданих в [175] рекомендацій, чи ланцюгів пакетів [174], котрі додають додаткову інформацію до пакета для обмеження максимальної відстані, яку може подолати пакет за певний час. Для розв’язання задач маршрутизації в мережах, моделювання та синтезу їх топологій, тощо пропонується застосувати і інші теоретико-графові засади та моделі [41, 43, 46, 47, 48, 49, 176, 177, 178, 179].

3) канальний рівень – призначений для виявлення та виправлення помилок, а також шифрування даних. Цей рівень є уразливим для атак, які полягають у створенні завад (jamming) та відмові послуг (DoS – Denial of Service). Нижче наведені приклади атак для БСМ на канальному рівні [174]:

- спричинений конфлікт пакетів при передачі;
- розрядження батереї, котра живить вузол, під час повторення ретрансляції;
- створення безпорядку, використовуючи безпровідний канал поміж суміжними вузлами.

Протокол Tiny Sec вносить шифрування канального рівня, яке залежить від схеми керування ключами [181]. Однак зловмисний вузол з-зовні з кращою енергоефективністю все ще може здійснити успішну атаку. Деякі протоколи, зокрема LMAC мають кращі антизавадні властивості, котрі є ефективною протидією загрозам для БСМ на цьому рівні [182]. Для виявлення загроз функціонуванню БСМ на канальному рівні слід застосувати низку рішень, таких як методика виявлення конфліктів, зміна коду MAC (Message Authentication Code) для обмеження інтенсивності запитів і використання менших кадрів для кожного пакету [183].

4) фізичний рівень – узгоджує передавання носіями інформації між приймальними та передавальними ІВ, а також регламентує швидкість передавання даних, рівень і частоту радіосигналу. Створення завад для розповсюдження радіосигналу (jamming attack) належить до однієї із загальних атак на фізичному рівні. Глушення радіосигналу відбувається за наявності завад на радіочастотах функціонування БСМ. Зловмисник розміщує невелику кількість ІВ навколо мережі і руйнує всю радіокомунікацію. В ідеалі, в БСМ використовується швидка псевдовипадкова перебудова робочої частоти (FHSS – Frequency Hopping Spectrum Spreading). Подолати загрозу створення завад в БСМ пропонується за допомогою протоколу відображення (mapping protocol), який відповідним чином компонує зони перешкод для визначення пріоритетів доставки повідомлень в мережі [184].

В табл. 3.2 підсумовано загрози функціонуванню БСМ, які можуть призвести до аномальних режимів її роботи, а також рекомендовані підходи та засоби щодо зменшення чи усунення впливу збурювальних факторів відповідно до рівнів теоретичної моделі структури мережевої комунікації в БСМ [80].

Таблиця 3.2.

Розподіл атак на БСМ по рівнях і заходи протидії

№ п/п	Рівень	Атаки на БСМ	Заходи протидії атакам
1.	Фізичний	Атаки DoS та захоплення вузла (Node capture attack)	Адаптивні антени, розширений спектр (Spread Spectrum)
2.	Канальний	Заглушення каналу (Link Layer Jamming)	Шифрування канального рівня (Link Layer Encryption)
3.	Мережевий	Загрози, спричинені атаками типу: червоточини (Wormholes), воронкові (Sinkholes), Сивіли (Sybil), маршрутні петлі (Routing Loops)	Керування ключами (Key Management), захищена маршрутизація (Secure Routing)
4.	Прикладний	Повалені (Subversion) та шкідливі (Malicious) вузли	Виявлення шкідливого вузла та його ізоляція (Malicious Node Detection and Isolation)

До одного з критичних і надзвичайно важливих підходів до відповідності цілям безпеки щодо конфіденційності, цілісності та аутентифікації належить керування ключами, яке запобігає загрозам для БСМ і ґрунтується загалом на двох основних моделях побудови схем розподілу ключів: моделі типу «точка-точка» та моделі централізованого розподілу ключів. Внаслідок спеціального характеру та обмеженості ресурсів БСМ, забезпечення успішного керування ключами є складним завданням. Традиційні схеми керування ключами, засновані на довіреній третій стороні подібно до центру сертифікації (ЦС), недоцільні та непрактичні внаслідок невідомої апріорі застосованої топології. Довірчий ЦС зобов'язанийбути присутнім протягом всього часу для підтримки анулювання та оновлення відкритого ключа [185]. Довіра на єдиному ЦС для керування ключами також більш уразлива, оскільки при компрометації ЦС ставиться під загрозу безпека всієї БСМ.

На підставі аналізу результатів наведених у літературних джерелах [167, 186, 187, 188, 189, 190, 191, 192, 193, 194] підходів до застосування криптографічних ключів і ґрунтуючись на двох вище зазначених моделях побудови схем розподілу цих ключів, для усунення та обмеження загроз функціонуванню БСМ за допомогою розподілу ключів пропонується використовувати такі схеми [80]:

- базовий розподіл ключів (Basic Key Management);
- випадковий попередній розподіл ключів (Random Key Predistribution);
- випадкове присвоєння ключів (Random Key Assignment);
- створення парних ключів (Establishing Pairwise Keys);
- попередній розподіл парних ключів (Pairwise Key Pre-distribution);
- застосування знань (Deployment Knowledge);
- груповий розподіл ключів (Group Key Management);
- локально-базовані ключі (Location-Based Keys);
- безпечна схема потрійних ключів (Secure Triple Key Scheme).

Ґрунтуючись на схемах моделей розподілу ключів і на використанні існуючих методів тріангуляції запропонований метод безпечної локалізації вузлів в БСМ [145]. При цьому здійснено поділ на дві частини: визначення розміщення ІВ та захист розташування ІВ. Локалізація – процес, під час якого сенсорні ІВ визначають своє розташування. Виділяють три важливі показники, що пов'язані з локалізацією: енергетична ефективність (energy efficiency), точність (чи похибка – accuracy) безпека (чи захист або скритність – security) [145]. Хоча перші два

параметри в значній мірі досліджені, показник захисту привернув увагу дослідників лише недавно та недостатньо вивчений.

Характерна особливість локалізації систем полягає в здатності визначати місце розташування ІВ та перевіряти його відстань від суміжних ІВ [195]. У пропонованому методі безпечної локалізації кожен ІВ визначає своє положення шляхом обчислення відстані до своїх сусідів, використовуючи чотири методи тріангуляції: латерацію (lateration), затухання (attenuation), розповсюдження (propagation) та ангуляцію (angulation - точне вимірювання кутів). Місцезнаходження ІВ згідно з тріангуляцією обчислюється за допомогою тригонометричних теорем синусів і косинусів.

Попередній аналіз показав, що незначні додаткові витрати, зумовлені застосуванням схеми керування ключами, не ставлять під загрозу ефективність функціонування БСМ і дозволяють в поєднанні з методами тріангуляції стримати та усунути загрози захисту від присутності зловмисного ІВ в БСМ, що інакше спричинило б суттєві складнощі для надійної роботи БСМ. При цьому визначення локалізації ІВ здійснено на підставі застосування методів тріангуляції, що ґрунтуються на вимірюваннях відстані, рівнів радіосигналу, розбіжностей в часі та відносних кутів [80].

Результати імітаційного моделювання процесів виявлення та ізолювання негативних збурювальних чинників в БСМ, здійсненого на підставі методів протидії загрозам, систематизовано відповідно до різних рівнів моделі OSI, а саме [149]:

1) на фізичному рівні – а) перебудова каналу та занесення до чорного списку, б) фізичний захист пристроїв, зокрема екранування, в) захист і зміна ключа проти атак відповідно: завада та заглушування, багатократної ідентичності, втручання;

2) на канальному рівні – а) контроль за допомогою циклічного надлишкового коду та рознесення в часі, б) захист мережевого ID та іншої інформації, яка потрібна для з'єднання пристрою, в) використання різних маршрутів для повторного передавання повідомлення, г) регулярна зміна ключа, д) використання різних сусідів для синхронізації часу, е) передавання фіктивного пакету в певні години; регулярний моніторинг мережі БСМ, є) застосування захищеного ключа DLPDU проти атак відповідно: колізії, виснаження, імітації, багатократної ідентичності, розсинхронізації, аналізу руху, підслуховування;

3) на мережевому рівні – а) контроль польових пристроїв і регулярний моніторинг мережі, що використовує маршрутизацію від джерела. Система моніторингу може застосовувати технології: приписання пакету, Lite Worp, радіочастотного маркування, напрямлених антен, сигнальних ІВ, локальної суміжної інформації та інформації зв'язності, статистичного аналізу, б) регулярний мережевий контроль з використанням маршрутизації від джерела, застосування методу опорних векторів, в) захист мережевих специфічних даних подібно до даних мережевого ID і т.п. Фізичний захист та інспекція мережі, г) відновлення пристроїв і зміна ключів сесії, пряма та посередня валідації, д) передавання фіктивного пакету в певні години; регулярний моніторинг БСМ, е) застосування сесійних ключів NPDU, тощо проти атак відповідно а) червоточини, б) вибіркової переадресації, в) відмови сервісу, г) багатократної ідентичності, д) аналізу руху, е) підслуховування, тощо.

В цій частині увагу зосереджено на атаках маршрутизації, зокрема на атаках, що конкретно спрямовані на ідентичність ІВ в БСМ. В атаках маршрутизації один зловмисний ІВ відіграє роль декількох легітимних компонентів БСМ, імітуючи їхні тотожності або підробивши їхні ідентифікатори. Кожен зі зловмисників може претендувати на те, щоб перебувати в мережі в різних місцях одночасно, таким чином маніпулюючи результатами локалізованого голосування або агрегацією даних. Атака маршрутизації також дозволяє шкідливим ІВ взяти на себе контроль над всією мережею шляхом компрометації обмеженої кількості фізичних пристроїв і розбити заходи реплікації в розподілених системах [88, 196].

В існуючих підходах зазвичай, виявляють атаки маршрутизації, перевіривши чи пари ІВ мають різні ресурси, різні знання або несхожі позиції. Після перевірок, проведених локалізованим чином, такі методи особливо ефективні в середовищах з відносно стабільною топологією, таких, як БСМ, або якщо ІВ рухаються повільно. Однак, відповідно до сценарію, коли підроблені ідентифікатори динамічно переключаються між кількома зловмисниками, глобальна топологія мережі повинна моніторитися. Зі збільшенням розміру БСМ та продовженого терміну її життя різко зростатиме кількість інформації, тому потрібні потужніші методи, такі як наукова візуалізація для надання допомоги представлення даних і виявлення прихованих зв'язків між ними.

В подальшому представлений підхід до виявлення атак маршрутизації в БСМ, що об'єднує заходи безпеки та методи візуалізації [196]. Згідно з ним здійснюється моніторинг зв’язності сусідів між безпровідними ІВ та змін в топології БСМ, а також визначаються підозрілі ІВ через візуалізацію аномалій, викликаних підробленими ідентичностями. Універсальний інтерфейс візуалізації призначений для забезпечення можливості глобального огляду змін в топології БСМ так, щоб виявити зловмисників навіть тоді, коли вони динамічно перемикаються між кількома скомпрометованими фізичними пристроями.

Результати пропонованого підходу до забезпечення безпеки в БСМ зводяться до наступного [196]:

Беручи до уваги, що запропонований підхід базується на змінах глобальної топології БСМ, то забезпечується ефективний метод для виявлення атак маршрутизації, які не можуть бути визначені локалізованим чином.

Інтегрування методів візуалізації і захисту, що забезпечує зрозумілий і масштабований засіб відображення інформації та виявлення атак.

Оскільки запропонований підхід виявляє атаки маршрутизації ІВ винятково на основі зв’язків сусідів між безпровідними ІВ, то він може бути застосований в більш динамічному середовищі, такому як мобільні динамічні БСМ.

Приймають припущення, що зв'язки між безпровідними ІВ в БСМ є двонаправленими та два сусідні ІВ можуть завжди передавати пакети один до одного. Це припущення буде витримуватися за більшості умов, коли потужність вузлів ще не вичерпана [39]. Приймають, що два ІВ є сусідами, якщо відстань між ними менша, ніж r, де r визначається радіодіапазоном. Беруть до уваги, що існує спеціальний ІВ у БСМ, який називається “контролер”. Він буде інтегрувати, обробляти та візуалізувати інформацію про топологію, зібрану з безпровідних ІВ, а також виявляти атаки маршрутизації. При цьому контролер є фізично захищений та атака на нього не розглядається. Приймають, що контролер повинен зберігати та обчислювати ресурси, необхідні для запропонованого підходу. Наприклад, якщо топологія БСМ подається у вигляді графу, контролер може знайти його точки скорочення протягом короткого періоду часу [39, 88]. У експериментальних дослідженнях використовують комп'ютер з процесором, тактова частота якого становить 2 ГГц, в якості контролера, причому він може обробляти мережеву інформацію, що містить кілька сотень ІВ, у режимі реального часу. Для БСМ,

для яких характерна інфраструктура, контролер може бути обраний зі спеціальних ІВ. Наприклад, в багатоланковій БСМ стільникового зв'язку роль контролера може відігравати базова станція. У цих динамічних мережах підхід вибору лідера може бути прийнятий для визначення контролера, базованого на надійності мобільних ІВ та наявних ресурсів.

Для моніторингу та виявлення атак маршрутизації інтегровано моделі безпеки та методи візуалізації як зручний засіб моделювання виявлення атак маршрутизації в БСМ [93]. Система зосереджується на візуалізації та спостереженні важливих моделей інформації про топологію залежної від часу мережі. Впроваджені інтелектуальні алгоритми для виявлення потенційних аномальних подій і забезпечення додаткових методів перевірки. Як показано на рис. 3.3, спочатку збирають інформацію про топологію мережі, з метою її оброблення та візуалізації на контролері. Для спрощення взаємодії з користувачем у процесі візуалізації використовують статистичні дані про топологію, що надалі дає змогу визначити список підозрілих ІВ. Оператор може налаштувати список підозрілих ІВ і легко змінити параметри візуалізації для кращого виявлення кореляції подій. З метою забезпечення додаткової перевірки рішень оператора дві складові алгоритму призначені для автоматизованого виявлення прямих та непрямих атак маршрутизації, відповідно, на підставі виділених ознак, за якими їх можна відбирати.

Беручи до уваги, що згідно з запропонованим методом виявляються атаки маршрутизації шляхом моніторингу змін та аномалій у топології мережі, в подальшому описано, яким чином інформація повинна бути коректно і правильно зібрана та інтегрована контролером. В залежності від його обчислювальної потужності, накопичені статистичні дані можуть зберігатися не тільки короткочасно, а й протягом тривалого часу (дні, тижні), що дає змогу оператору з більшою ймовірністю виявити наявні атаки на БСМ.

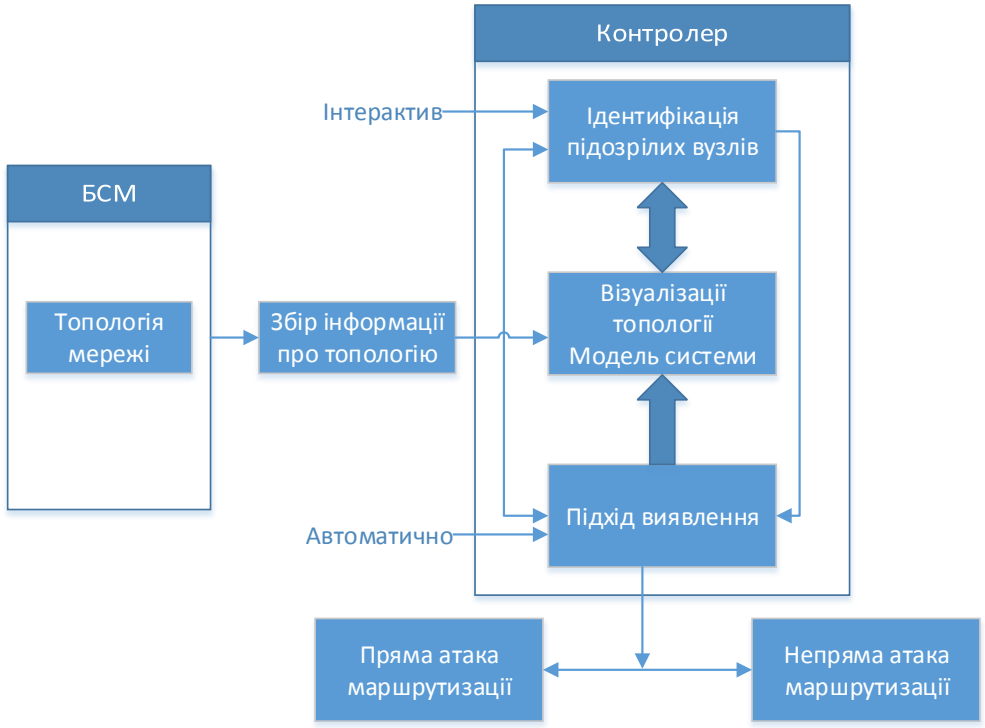


Рис. 3.3. Архітектура системи моделювання виявлення атаки маршрутизації в БСМ

Відомо, що зв'язки сусідів між безпровідними ІВ можуть змінюватися внаслідок різних причин, таких як переміщення ІВ, несправності пристрою, розряд акумулятора, ненадійне середовище передавання [97, 118]. Отже, ІВ повинен мати змогу динамічно виявити активних сусідів. Підхід передбачає періодично здійснювати ІВ широкотрансльовані повідомлення, що містить інформацію про його ідентичність (називається пакетом маяка) і сусідів, які отримали цей пакет та зможуть додати ІВ у свій список сусідів. У пропонованому підході кожен ІВ буде періодично транслювати список своїх сусідів до контролера. Для запобігання зміни списку протягом передавання його захищають за допомогою попарних ключів між контролером та ІВ. В той час як легітимний ІВ сумлінно розголошуватиме своїх сусідів, зловмисник буде контролювати та керувати списком для уникнення свого виявлення. Наприклад, шкідливий фізичний пристрій може претендувати на шлях до непрямого зловмисного ІВ, отже більше трафіку буде залучено до нього. Тим не менш, він не буде розголошувати зловмисного ІВ своїм сусідом до контролера. Для запобігання маніпуляції та його впливу на виявлення атаки маршрутизації, вимагають, щоб кожен список сусідів, який передається до контролера, був аутентифікований кодом MAC (Message Authentication Code) ІВ у списку. ІВ, які не знаходяться в списку, не будуть

прийняті сусідами для маршрутизації чи перебігу інших процесів активності у БСМ. Отже, зловмисний ІВ не може бути прихованим від контролера [196].

Внаслідок зміни топології маршрути з ІВ до контролера повинні бути оновлені. У рамках пропонованого підходу контролер буде періодично передавати дані про викриття маршруту пакетів до ІВ в зоні радіодіапазону і позначить довжину шляху до себе як 0. ІВ, які отримали пакет, будуть збільшувати довжину шляху по одному і ретранслювати його. Оскільки кожен ІВ запам'ятовує попередній стрибок, збільшуючи довжину шляху на один, і ретранслює пакет, то будуть створені маршрути до контролера. Частота передавання даних про викриття маршруту пакетів може бути також визначена через радіодіапазон і моделі руху ІВ. Використовуючи отримані списки сусідів, контролер може регенерувати топологію мережі. Наприклад, може бути визначена матриця, що представляє під'єднання і найкоротші шляхи між безпровідними ІВ. Якщо кілька матриць сусіда сортуються за часом їх відбору, зміни в топології БСМ можна проілюструвати об'ємними даними. Оскільки обсяг інформації швидко збільшиться зі зростанням розміру БСМ та кількості знімків топології БСМ, застосовують методи візуалізації для представлення даних і надання допомоги при виявленні атак маршрутизації. Оскільки топологія БСМ є підставою для формування загальної інформації в багатьох мережевих програмах, зосереджують на створенні засобів візуалізації для цих даних, функціональність яких можна нескладно розширити для виявлення безлічі додаткових атак, причому не лише загроз маршрутизації.

Мережі передавання даних про топологію часто містять достатньо інформації для контролю і виявлення вторгнень. Тим не менш, важко уявити собі цю інформацію таким чином, щоб можна було користувачеві легко зрозуміти. Оскільки інформація про топологію БСМ, отримана з багатьох часових кроків, становить суттєві за обсягом поточні дані, спочатку використовують загальні 2D і 3D візуалізаційні підходи, щоб мати змогу побачити ці дані, в тому числі різні вирізані 2D вигляди, статистичні вигляди та прямі 3D об'ємні методи інтерпретації. Характерна особливість зводиться до того, що під час сортування послідовності ІВ у відповідності з визначеними критеріями можна побачити деякі закономірності, очевидні для 2D і 3D візуалізацій. Отже, основна ідея полягає в розробці підходу до виявлення важливих складових інформаційних моделей про топологію БСМ шляхом групування ІВ на основі подібності між їхніми топологічними особливостями, що дозволяє виявити зловмисні атаки. Масштабованість

належить до практичних аспектів візуалізації топології, передусім наданням розширення обмеженого розміром екрану та людським потенціалом сприйняття. Для збереження істотних особливостей топологічної інформації з різних точок зору, доцільно збільшити діапазон передбачуваних ситуацій і комунікацій. Одне з рішень полягає у призначенні взаємодій в залежності від загальної кількості сусідів кожного ІВ у вказаний період часу. В порівнянні з підходом загального зменшення функцій метод масштабування дозволяє зберегти значно більший обсяг інформації. Однак якщо користувач вручну налаштовує параметри ІВ, то в деяких випадках це буде довготривалим процесом. Звідси випливає, що доцільно інтегрувати автоматичний обчислювальний процес для сприяння у визначенні підозрілих ІВ і прискорення виявлення атак маршрутизації [196].

Надалі покажемо, що операції виявлення атаки маршрутизації зосереджуватимуться на відношеннях сусідів між безпровідними ІВ. Хоча інтенсивність цих операцій на кожному ІВ є невисокою в обчислювальному сенсі, приміром, визначення чи видалення ІВ від'єднуватиме БСМ, якщо мережа складається з сотень або навіть тисяч ІВ, контролер буде перевантажений процесами оброблення. Отже, досягти зменшення перевантаження контролера вбачається доцільним у застосуванні ефективного методу відфільтровування списку підозрілих ІВ.

Вивчаючи сценарії прямих і непрямих атак маршрутизації, можна зробити висновок, що точки з'єднання між зловмисними ІВ прикріплені до одного і того ж фізичного пристрою. Зокрема, для двох підроблених ідентичностей під час прямих атак маршрутизації, хоч вони і можуть вдавати, що не є сусідами, повинен існувати двопереприйомний шлях через легітимного сусіда. Аналогічно, для непрямих атак маршрутизації довжину шляху між підробленими ідентичностями визначають лише кількістю зловмисних ІВ і заявленою ними організаційною будовою. Звідси випливає, що можна ефективно розрахувати розподіл довжини шляху між кожною парою ІВ, ґрунтуючись на зібраній інформації про топологію БСМ, та визначити групу підозрілих ІВ [39, 88]. У прямій атаці маршрутизації ІВ багатократної ідентичності роблять вигляд, що вони не є сусідами та існує між ними двострибковий шлях. Зловмисний пристрій стверджує, що наявний трипереприйомний шлях між двома тотожностями для непрямої чи посередньої атаки маршрутизації. Аномалії можуть бути нескладно ідентифіковані [196].

Розглянемо знаходження місцеположення або локалізації прямої атаки маршрутизації на парі ІВ. Після того, як визначається група підозрілих ІВ, можуть бути проведені складніші обчислювальні операції виявлення атак маршрутизації.

У цій частині представлено виявлення прямої атаки маршрутизації на парі ІВ, базуючись на подібності їхніх сусідських зв'язків. При цьому приймають до уваги кілька підроблених ідентичностей, створених в результаті прямої атаки маршрутизації. Оскільки пакети викриття сусіда передаються тим самим фізичним пристроєм, група легітимних ІВ, які можуть отримувати пакети і вважатися сусідами, майже така сама. Навпаки, пара легітимних ІВ не буде мати ідентичності, якщо кожен з них переміщатиметься самостійно.

На підставі зібраної інформації про топологію мережі можна обчислити подібності зв'язків сусідів між двома підозрілими ІВ n_1 та n_2. Якщо набір сусідів ІВ n_1 в оновленій мережевій топології T представлений як R^{T}_{n1}, нормоване значення для опису ідентичності наборів сусідів $I_{n1,n2}$ для двох ІВ можна обчислити згідно із запропонованим виразом:

$$I_{n1,n2} = \frac{R^{T}_{n1} \cap R^{T}_{n2}}{R^{T}_{n1} \cup R^{T}_{n2}}, \quad 0 \le I_{n1,n2} \le 1 \tag{3.8}$$

Запропонована ознака ідентифікації зловмисного ІВ $I_{n1,n2}$ вказує на те, що для $I_{n1,n2} = 1$ має місце пряма атака, а при $I_{n1,n2} = 0$ атака відсутня. Зазначений вираз чітко визначає та дає аналітичну формульну складову, за допомогою якої можна виявити атаку на БСМ. Це дає підставу контролеру автоматично виявляти атаку. Контролер може оцінити схожість сусідніх зв'язків між двома ІВ в кожній відновленій мережевій топології. Оскільки, зловмисний ІВ може динамічно перемикати свій прикріплений фізичний пристрій, різноманітні пари ІВ можуть показувати подібність в різних періодах тривалості життя мережі [196].

Відобразимо локалізацію якірних ІВ для непрямої атаки маршрутизації. В цій атаці легітимні ІВ можуть бути притягнуті до ІВ з підробленими ідентифікаторами тільки через зловмисний ІВ. Отже, якщо мережева топологія розглядається графом, цей "якірний" ІВ є в ній вузлом границі розподілу: видалення цього ІВ та пов'язаних каналів призведе до від'єднання графа. Ґрунтуючись на цьому спостереженні, дослідимо частоту появи ІВ границі розподілу в топології. Оскільки, кілька підроблених ідентичностей можуть бути прикріплені до одного і того ж фізичного пристрою у непрямій атаці маршрутизації, повинен бути впроваджений спеціальний метод для пом'якшення впливу на точність виявлення,

якщо зловмисники почергово змінюють ідентичності “якірного” ІВ. Звідси випливає, що для випадку видалення якірного ІВ можна обчислити частоту, з якою ізолюється ІВ від мережевої більшості [196].

Для забезпечення надійності моніторингу та виявлення атаки маршрутизації розроблено метод виявлення та підхід візуалізації топології, як два важливих компоненти розглянутої системи безпеки. Об'єднання цих двох компонентів дає перевагу в багатьох аспектах. Основна ідея полягає у тому, щоб використовувати компоненти візуалізації для інтуїтивного розуміння мережевої топології та забезпечення її безпеки. Це також дозволяє користувачам налаштовувати та взаємодіяти з мережевою інформацією. Компонент безпеки використовується засобом для ідентифікації та перевірки наявності атаки, надаючи допомогу оператору прийняти остаточні рішення та дозволяючи зменшити відповідні додаткові витрати.

Для цього розміщено три паралельні вікна для візуалізації подій кореляції: 3D-перегляду, 2D-перегляду і вікно моделі організації взаємодії. 3D-перегляд головним чином призначений для відображення зв’язків між сусідами в залежності від часу. 2D-перегляд альтернативно ілюструє вирізані вигляди з об'ємних даних топології (взаємозв’язки сусідів в покроково в часі чи такті або сусідів ІВ в часовій послідовності) і статистичних матриць топології (з'єднання ІВ або подібності). Також додано вікно моделей організації взаємозв’язків з метою зберігання типових моделей аномалій і невирішених користувачами структур для порівняння. Ці три вікна дозволяють спостерігати інформацію про топології мережі та виявити кореляцію між даними [196].

Спочатку збирається та нагромаджується інформація про мережеву топологію та 2D-перегляд вказує на статистичні зв’язки між сусідами. Компонент безпеки обчислює список підозрілих ІВ і дає змогу оператору налаштувати 2D-зображення для виявлення аномальних структур. Ці структури порівнюються з типовими структурами прямих та непрямих атак маршрутизації та можуть здійснити ідентифікацію гібридної атаки. Список підозрілих ІВ передають до компонента безпеки, який призначений для підтвердження поведінки ІВ. Оператор може приймати остаточні рішення на базі даних візуалізації та результатів, виданих компонентом безпеки. Виявлені підроблені ІВ багатократної ідентичності будуть видалені з БСМ.

Пропонований підхід підтверджено результатами симуляції [196]. Експерименти проведено протягом двох етапів. На першому етапі використано запропоновану в [197] модель ns-2 для симуляції процедури викриття сусіда, а також розголошення топології до контролера. Під час другого етапу на підставі запропонованого удосконаленого методу здійснено спробу виявлення атаки маршрутизації і знаходження підроблених ідентичностей, а також проведено відповідне тестування. ІВ розміщені в площині з граничною довжиною 2000 метрів. Радіодіапазон *r* становить 50 метрів і будь-які 2 ІВ, які мають меншу за *r* відстань, можуть безпосередньо з'єднуватися один з одним. У симульованій області 500 ІВ розподілені випадково та рівномірно, маючи середній ступінь зв'язності 14,0. Контролером здійснено збирання інформації про топологію мережі через кожні 10 секунд, що є грубою оцінкою часу життя каналу, базованого на радіодіапазоні *r*. У кожній симуляції виконано нагромадження статистичних даних про топологію БСМ протягом 200 циклів.

Побудова моделей запобігання деяким атакам на БСМ і проведення їх симуляції вбачається у [166]застосуванні звичайного шифрування та автентифікації, використовуючи спільний ключ проти більшості зовнішніх атак на протоколи маршрутизації БСМ. До основних видів атак, які не враховуються при методах шифрування на канальному рівні та автентифікації, належать атаки черворочини (wormhole), що зводяться для створення просторово-часового тунелю, та атаки типу лавина чи "флуд" (HELLO Flood). Це викликано наступним: хоча зловмисник не може з'єднатись з мережею, однак ніщо не перешкоджає йому:

а) використовувати черворочину для тунелювання відправлених пакетів легальними ІВ в одній частині БСМ до легальних ІВ іншої ІВ, для переконання їх, що вони є сусідами;

б) збільшувати трансляцію підслуханого пакету широкотрансльованих повідомлень (Broadcast Packet) доти, поки кожен ІВ у БСМ його не отримає.

Методи захисту на канальному рівні, котрі використовують спільний ключ, загалом неефективні за наявності внутрішніх атак (атак інсайдерів) або компрометувальних ІВ. Інсайдери можуть атакувати мережу за допомогою імітації з'єднання або введенням в мережу фіктивної інформації маршрутизації, створення воронок (Sinkholes), вибіркової переадресації пакетів, використовуючи атаку типу багатократної ідентичності (Sybil Attack) чи транслюючи HELLO Flood повідомлення. Для змоги протистояння атакам типу черворочина (Wormhole, інакше просторово-часовий тунель) та атакам інсайдерів потрібні

складніші методи захисту. Особливо важливими є заходи протидії вищенаведеним атакам. Так для протидії атакам багатократної ідентичності (Sybil Attack) традиційно застосовують асиметричну криптографію, проте генерування та верифікація цифрових підписів знаходиться поза можливістю ІВ. При цьому слід врахувати, що неможливо запобігти інсайдерові користуватися мережею, але вона повинна бути здатною ідентифікувати скомпрометовані ІВ. Використання спільного ключа дозволяє інсайдерові маскуватися під будь-який, можливо навіть неіснуючий ІВ. Тому ідентичність ІВ повинна бути перевірена. Чи не єдиним виходом є поділ кожним ІВ унікального симетричного ключа з довіреною базовою станцією. Два ІВ можуть тоді застосовувати Needham-Schroeder подібний протокол для перевірки ідентичності один одного та встановити відкритий ключ. Пара сусідніх ІВ може використовувати результуючий ключ з метою автентифікованого та зашифрованого з'єднання між ними. Для запобігання інсайдерові переміщатися в стаціонарній мережі та встановлювати відкритий ключ з кожним ІВ в мережі базова станція може обмежити кількість сусідів ІВ, яким дозволено мати та надавати повідомлення про збій за умови перевищення цієї кількості. Тому, якщо ІВ поставлений під загрозу, зв'язок цього ІВ обмежується лише з перевіреними сусідами. Це не свідчить про те, що ІВ забороняється передавати повідомлення до базових станцій, проте вони обмежуються від використання будь-якого ІВ, окрім їхніх перевірених сусідів. Крім цього, нападник може все ще використовувати червоточину для створення штучного з'єднання між двома ІВ з метою переконати їх, що вони – сусіди, але порушник не зможе підслухати або змінити будь-які майбутні повідомлення між ними.

Для атак типу лавина HELLO застосовують перевірку двонаправленості зв'язку, що відноситься до найпростішого захисту. В подальшому на підставі отриманого за допомогою цього з'єднання повідомлення можна застосувати відчутніші заходи. Протоколу перевірки ідентичності достатньо для запобігання атакам типу лавини HELLO. При цьому не тільки перевіряють двонаправлене з'єднання між двома вузлами, але навіть за умови застосування супротивником високочутливого приймача або червоточини до багатьох локацій в мережі, довірена базова станція, яка обмежує кількість верифікованих сусідів для кожного ІВ, все ще запобігатиме атакам типу лавини HELLO на великих сегментах мережі, якщо під загрозу була поставлена мала кількість ІВ.

Для атак типів червоточина (Wormhole) та воронкова (Sinkhole) застосовують ретельне запроектування протоколів маршрутизації, в яких червоточинна та

воронкова атаки виявились би неефективними. Це обґрунтовується тим, що від червоточинної та воронкової атак дуже важко захиститись, особливо, якщо вони поєднуються. Червоточину важко виявити, тому що для її реалізації застосовують приватний поза смуговий канал, невидимий для основної сенсорної мережі. Захист від воронкових атак суттєво утруднений в протоколах, які використовують відкриту інформацію, наприклад, про енергію, що залишилася, або оцінку наскрізної (end-to-end) надійності для відтворення топології маршрутизації, тому що цю інформацію важко перевірити. Маршрути, що мінімізують кількість переприйомів до базової станції, простіше перевірити, проте ця кількість може бути повністю спотворена червоточиною. Якщо маршрути встановлюються, ґрунтуючись на звичайному прийманні пакету, наприклад, в сигналізуванні Tiny OS чи прямому поширенні, воронку легко створити, тому що відсутня будь-яка інформація, яку б захисник зміг перевірити. Певний підхід для виявлення атак червоточини поданий в [198], але це вимагає надзвичайно щільної синхронізації часу і тому є нездійсненним для більшості БСМ. Оскільки надзвичайно важко модифікувати існуючі протоколи із захистом проти цих атак і кращим рішенням вбачається розробка протоколів маршрутизації.

Для вибіркової переадресації (Selective Forwarding) використовують багатошляхову маршрутизацію, завдяки чому можна виявити ці види атак, зокрема беручи до уваги, що навіть в протоколах, повністю стійких до атак типу червоточина, воронкова, багатократної ідентичності, скомпрометований ІВ має значну ймовірність залучити себе до потоку даних для запуску атаки вибіркової переадресації, якщо він стратегічно розміщений біля джерела або базової станції. Повідомлення, передані маршрутами, в яких відсутній перетин вузлів, повністю захищені проти атак вибіркової переадресації. При цьому, навіть для скомпрометованих ІВ також можливий частковий захист. Проте шляхи, які зовсім не перетинаються, важко створити. Переплетені шляхи можуть бути притаманні ІВ загального використання, але в основному відсутні будь-які канали, тобто загалом немає жодних двох послідовних ІВ.

Застосування багатьох переплетених шляхів дозволяє забезпечити імовірнісний захист проти атаки вибіркової переадресації з використанням лише локалізованої інформації. Дозволяючи ІВ динамічно вибрати переприйом наступного пакету імовірнісним підходом з набору можливих кандидатів, можна надалі скоротити шанси зловмисника отримати повний контроль над управлінням потоком даних.

Автентифікацію широкотрансльованих повідомлень і перевантаження – обґрунтовують тим, що за наявності довірених базових станцій зловмисники не будуть здатні широкотранслювати повідомлення та перевантажити ними з будь-якої базової станції. Це вимагає деякого рівня асиметрії: з тих пір, як кожен ІВ в мережі може бути потенційно скомпрометований, ніякий ІВ не буде здатний підміняти повідомлення від базової станції, оскільки кожен ІВ буде здатним перевірити їх. Автентифікація широкотрансльованих повідомлень також корисна для локалізованих взаємодій ІВ. Багато протоколів вимагають, щоб ІВ передавали повідомлення HELLO до їхніх сусідів. Ці повідомлення повинні пройти перевірку автентичності, що запобігає неможливості їх спотворення. Пропозиції для автентифікації широкотрансльованих повідомлень призначаються для застосування в звичайних засобах, використовуючи цифрові підписи та/або заголовок пакету, що перевищує довжину типового пакету БСМ. TESLA – протокол для ефективної автентифікації широкотрансльованих повідомлень і перевантаження, використовує тільки криптографію симетричного ключа та вимагає мінімального заголовку пакету [199]. SPIN [200] і "плітко-алгоритми" (gossiping) [84, 201] є підставою методів для скорочення витрат на запит і колізії, які все ще досягають стійкого імовірнісного розповсюдження повідомлень до кожного ІВ в БСМ.

Метаданні (глобальні знання) використовують якщо розмір мережі обмежений або топологія збудована чи контрольована належним чином. Метадані знання можуть бути перевагою в підходах щодо захисту, враховуючи, що істотний виклик в забезпеченні захисту великих БСМ вносить їхня притаманна однорідна організація, децентралізована структура. Нехай наявна відносно незначна БСМ, яка містить приблизно 100 ІВ. Приймають , що ні один ІВ не компрометується протягом розгортання. Після сформування початкової топології кожен ІВ міг би надати інформацію, наприклад, про сусідні ІВ і своє географічне розташування, якщо воно відоме, назад до базової станції. Використовуючи цю інформацію, базова станція може відтворити топологію всієї БСМ. Для надання звіту про зміни топології в результаті радіозавади або збою ІВ, ІВ періодично оновлювали б базову станцію відповідною інформацією. Радикальні або підозрілі зміни в топології могли б вказати на компрометацію ІВ, завдяки чому була б ужита відповідна протидія. Відомо, чому географічна маршрутизація може бути відносно безпечною проти атак типу червоточина, воронкова, багатократної ідентичності, проте залишається нерозв'язаною основна задача щодо забезпечення достеменності розповсюджуваної інформації про розташування від сусідніх ІВ. Розголо-

шення скомпрометованим ІВ свого розташування в лінії між цільовим ІВ і базовою станцією гарантуватиме, що це пункт призначення для всіх переданих цим ІВ пакетів. Ймовірний вибір наступного переприйому з декількох прийнятих адресатів або багато шляхова маршрутизація до багатьох базових станцій може допомогти розв'язати цю задачу, проте це не є досконалим рішенням. Якщо ІВ повинен здійснювати маршрутизацію навколо "діри", зловмисник може "допомогти" в цьому, представляючись винятково коректним ІВ для передавання пакетів. Обмежуючи в достатній мірі структуру топології, можна усунути вимогу щодо поширення ІВ їхнього розташування, якщо всі локації ІВ відомі.

3.4. Використання тріангуляції Делоне для моделювання візуального виявлення атаки червоточин у БСМ

Наведені у літературних джерелах [41, 42] приклади візуалізації атаки червоточини зводяться до вимірювання відстаней між ІВ на підставі рівня потужності прийнятих сигналів, реконструювання топологічної поверхні БСМ шляхом багатовимірного шкалювання, обчислення віртуальної позиції кожного ІВ, згладжування реконструйованої топологічної поверхні БСМ, аналізу візуалізованої форми згладженої реконструйованої топологічної поверхні БСМ та виявлення фальшивих з'єднань сусідніх ІВ, зумовлених атакою червоточини.

Щоб зменшити похибки вимірювання відстаней між ІВ здійснюють моделювання похибки вимірювання відстаней між ІВ змішаним шумом, що описується функціями Бесселя з уявним аргументом нульового та вищого порядків [43]. Дійсне значення рівня радіосигналу U_{di} визначають за рівнянням

$$U_{di} = U_i \pm \Delta U_i, \tag{3.9}$$

де U_i – рівень потужності прийнятого радіосигналу;

ΔU_i – абсолютна похибка вимірювання радіосигналу, причому модель похибки має вигляд:

$$\Delta U_i = f(J_0(jdU_i),\ J_n(jdU_i)), \tag{3.10}$$

де $J_0(jdU),\ J_n(jdU_i)$ - функції Бесселя з уявним аргументом нульового та вищих порядків [44].

Зокрема запропоновано спосіб візуалізації атаки червоточини в БСМ [64]. Спосіб реалізують наступним чином. Вимірюють відстань між ІВ на підставі рі-

вня потужності прийнятого сигналу (рис. 3.4). Позиціями 1,2,3,4 на рисунку позначені ІВ БСМ. Потім здійснюють моделювання похибки вимірювання відстані між ІВ змішаним шумом, який описують функціями Бесселя з уявним аргументом нульового та вищих порядків та уточнюють значення виміряної відстані між ІВ на підставі рівня потужності прийнятого сигналу. Для цього запрограмовують модулі XBee з повним набором функцій. Модулі використовують запрограмований рівень стеку XBee.

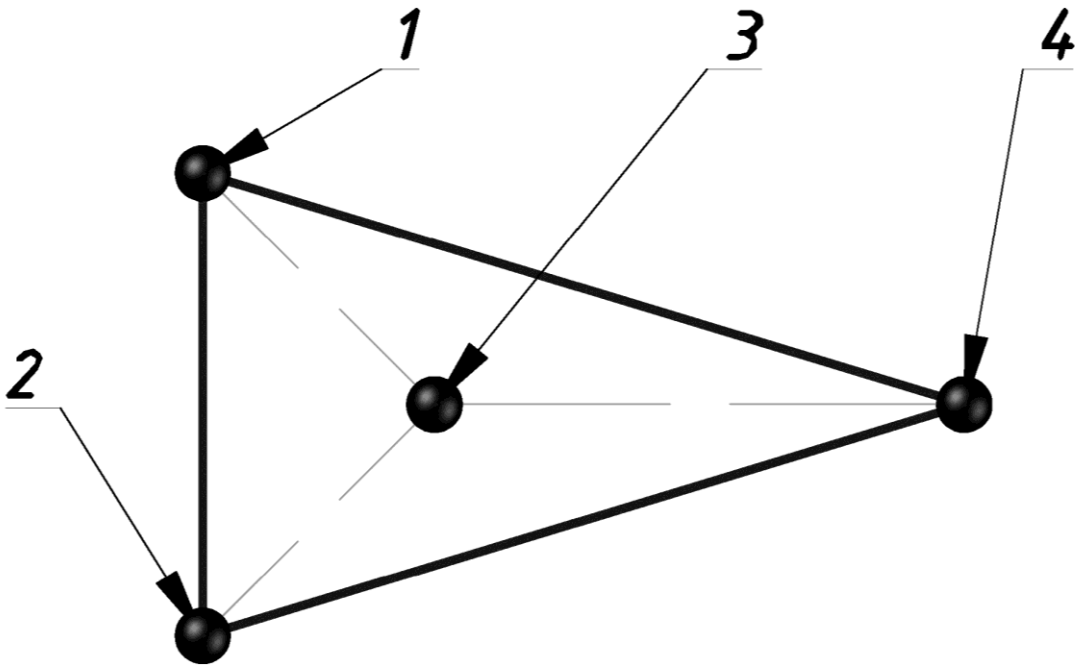


Рис. 3.4. Схема вимірювання відстані між ІВ на підставі рівня потужності рівня потужності прийнятого сигналу

Далі згладжують реконструйовану топологічну поверхню БСМ. При цьому спочатку здійснюють тріангуляцію Делоне (рис. 3.5), використовуючи сітки трикутників з розміщеними у їх вершинах ІВ з координатами в евклідовому просторі.

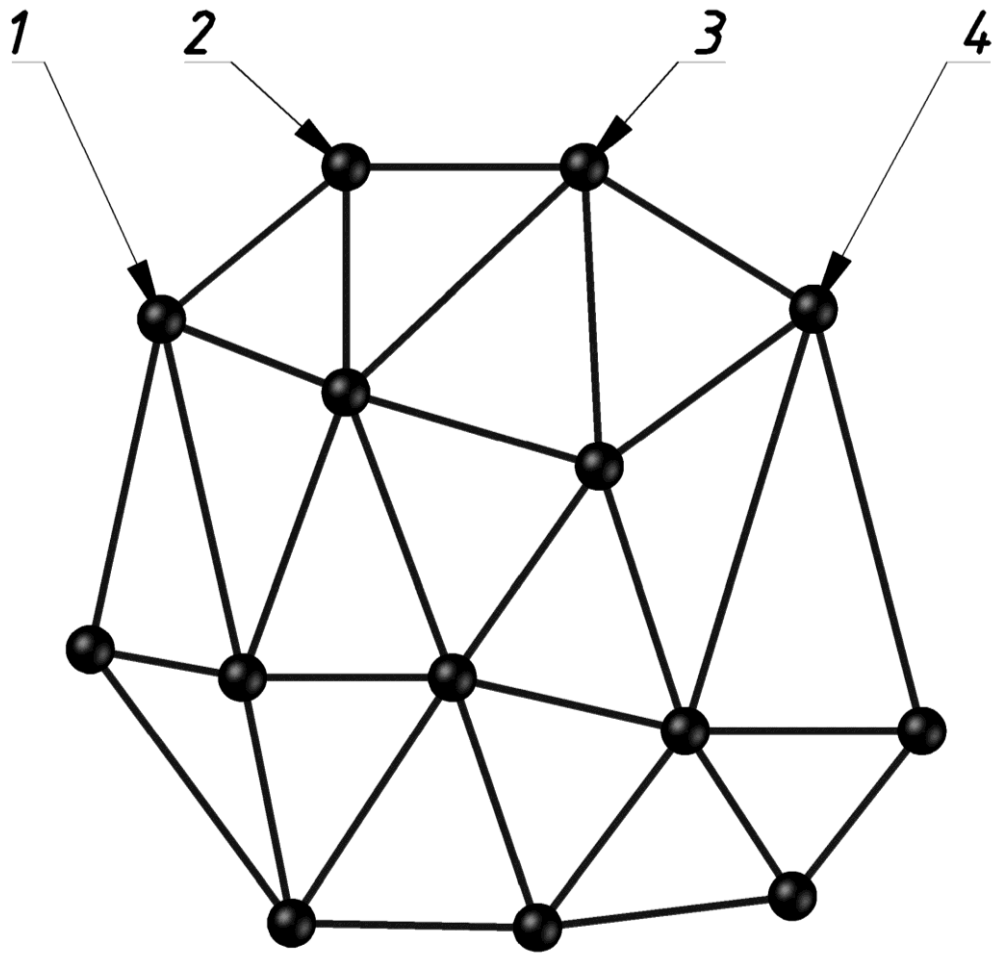


Рис. 3.5. Фрагмент згладженої реконструйованої топологічної поверхні БСМ з використанням тріангуляції Делоне

Після чого здійснюють кригінг – інтерполяцію реконструйованої топологічної поверхні та аналіз візуалізованої форми згладженої реконструйованої топологічної поверхні БСМ (рис. 3.6). Позиціями 1 і 2 на рисунку позначені ІВ розміщені по сусідству у БСМ. При цьому БСМ функціонує в нормальному режимі без наявності атаки червоточини.

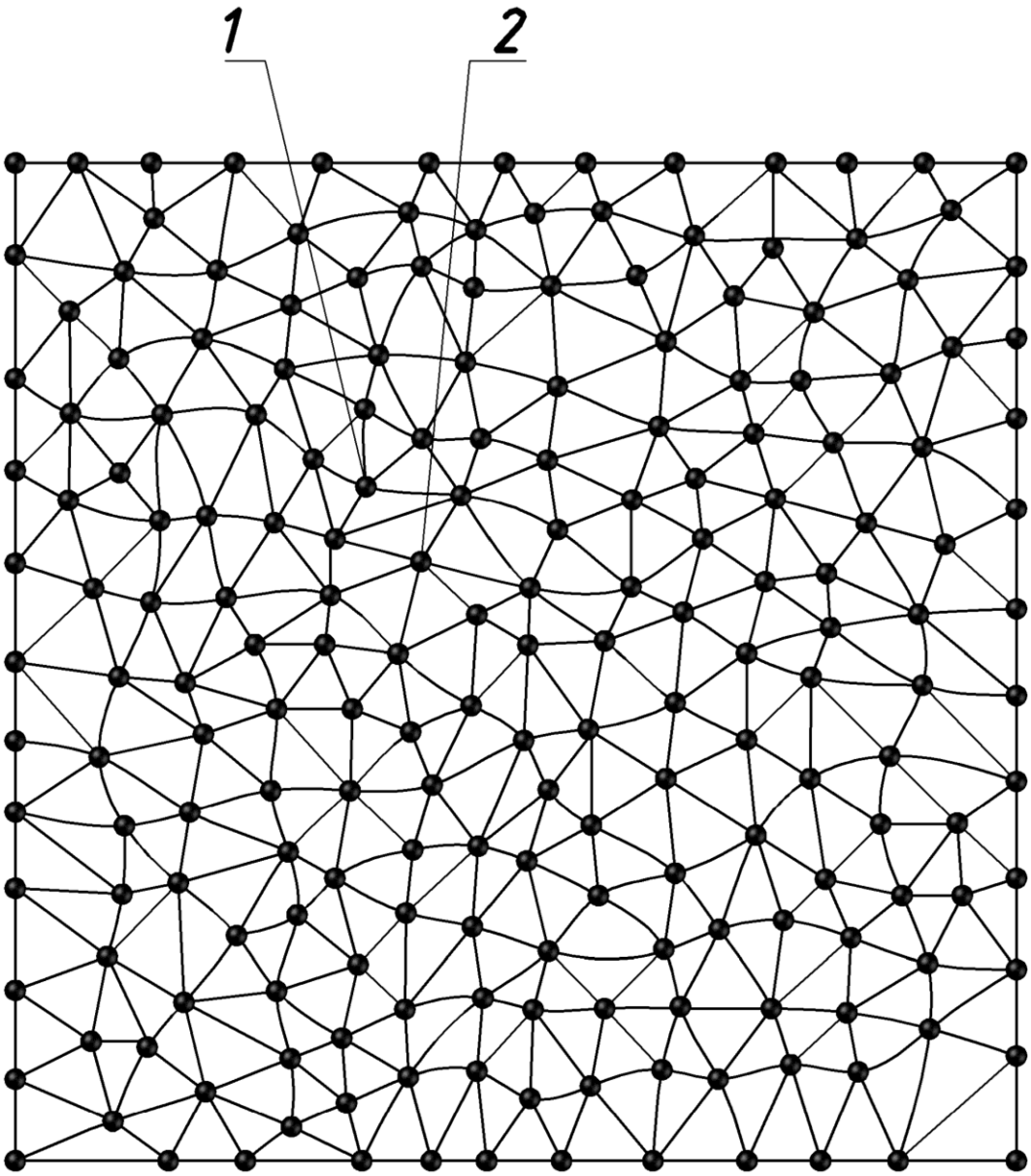


Рис. 3.6. Візуалізована форма згладженої топологічної поверхні БСМ, працюючої у нормальному режимі

В результаті організації атаки червоточини на ІВ піддослідної БСМ змінюється віддаль між ІВ, появляються фальшиві з’єднання між сусідніми ІВ, згладжена реконструйована топологічна поверхня збільшується і зазнає викривлення (рис. 3.7) [64]. Так відстань між сусідніми ІВ 1 і 2, яка під час роботи БСМ у нормальному режимі, без наявності атаки червоточини становила 67,6 м, в режимі організації атаки червоточини збільшилася до 192,9 м.

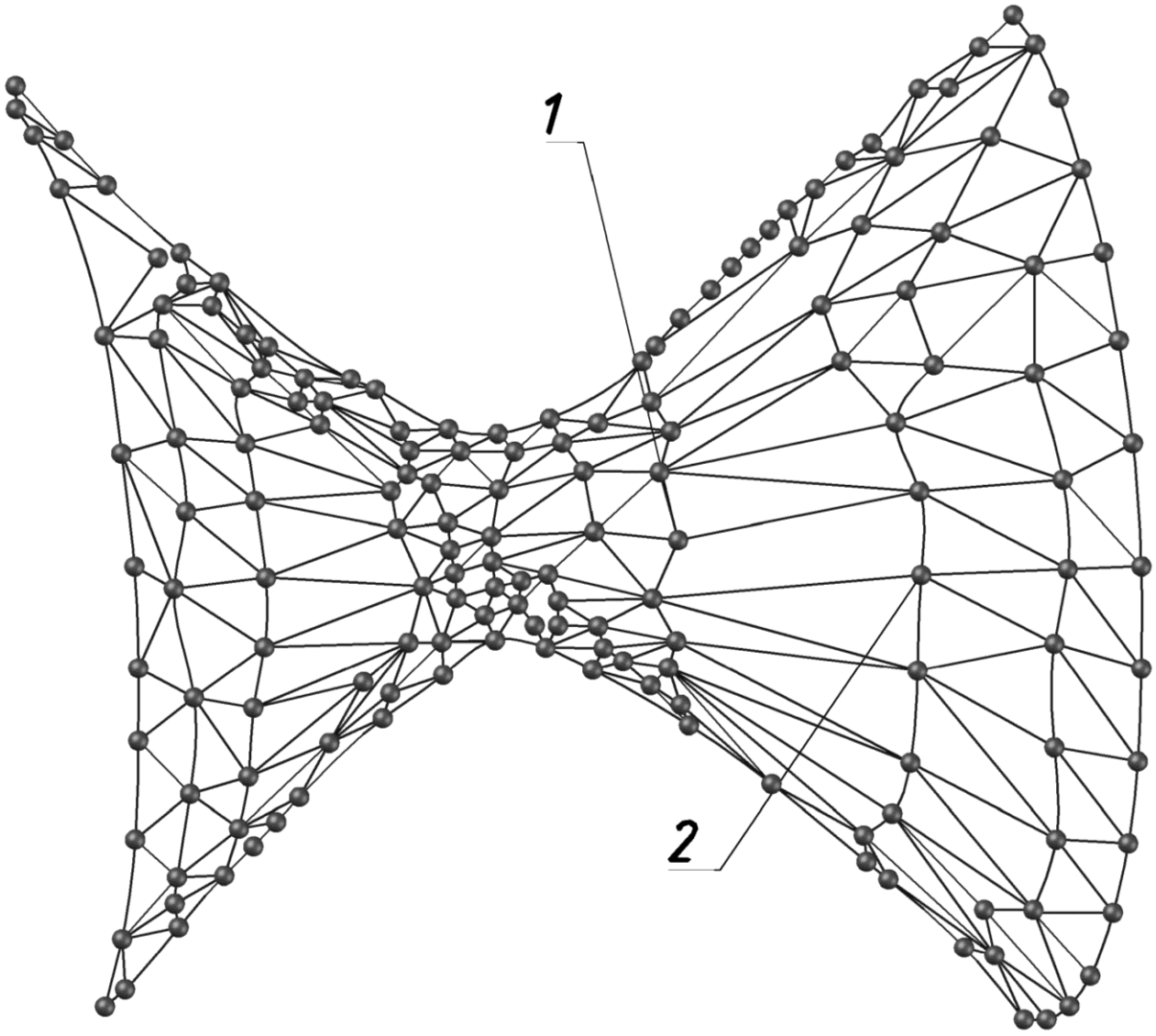


Рис. 3.7. Візуалізована форма згладженої топологічної поверхні БСМ за наявності атаки червоточини

Зміна віртуального положення ІВ 1,2,3,4, які займають крайні положення в БСМ показана на рис. 3.8 і рис. 3.9. При цьому імітація атаки червоточини зумовила зміну площі топологічної поверхні БСМ з 5,625 10^5м^2 до 6,631 10^5м^2.

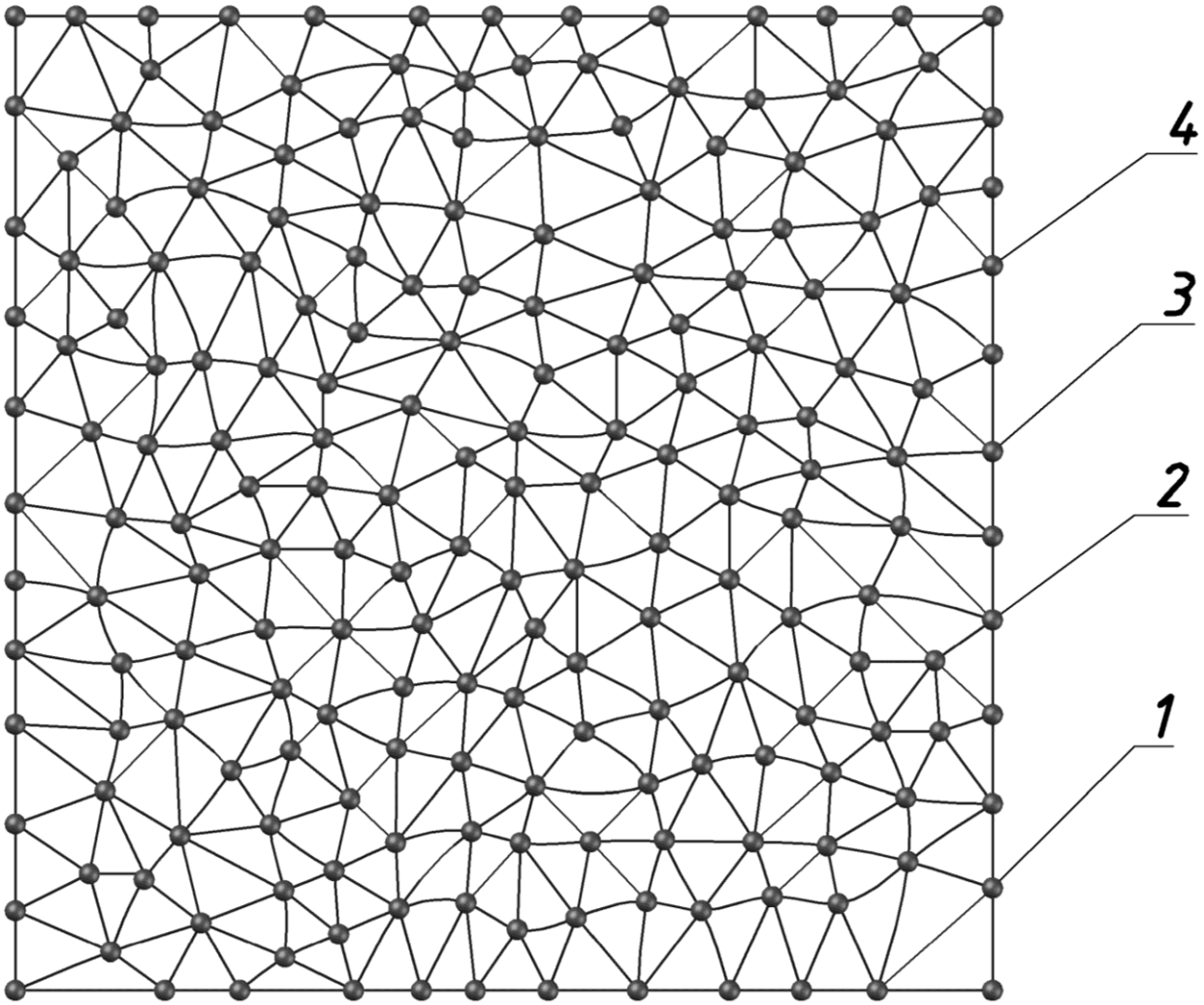


Рис. 3.8. Візуалізована форма згладженої топологічної поверхні БСМ, яка працює у нормальному режимі

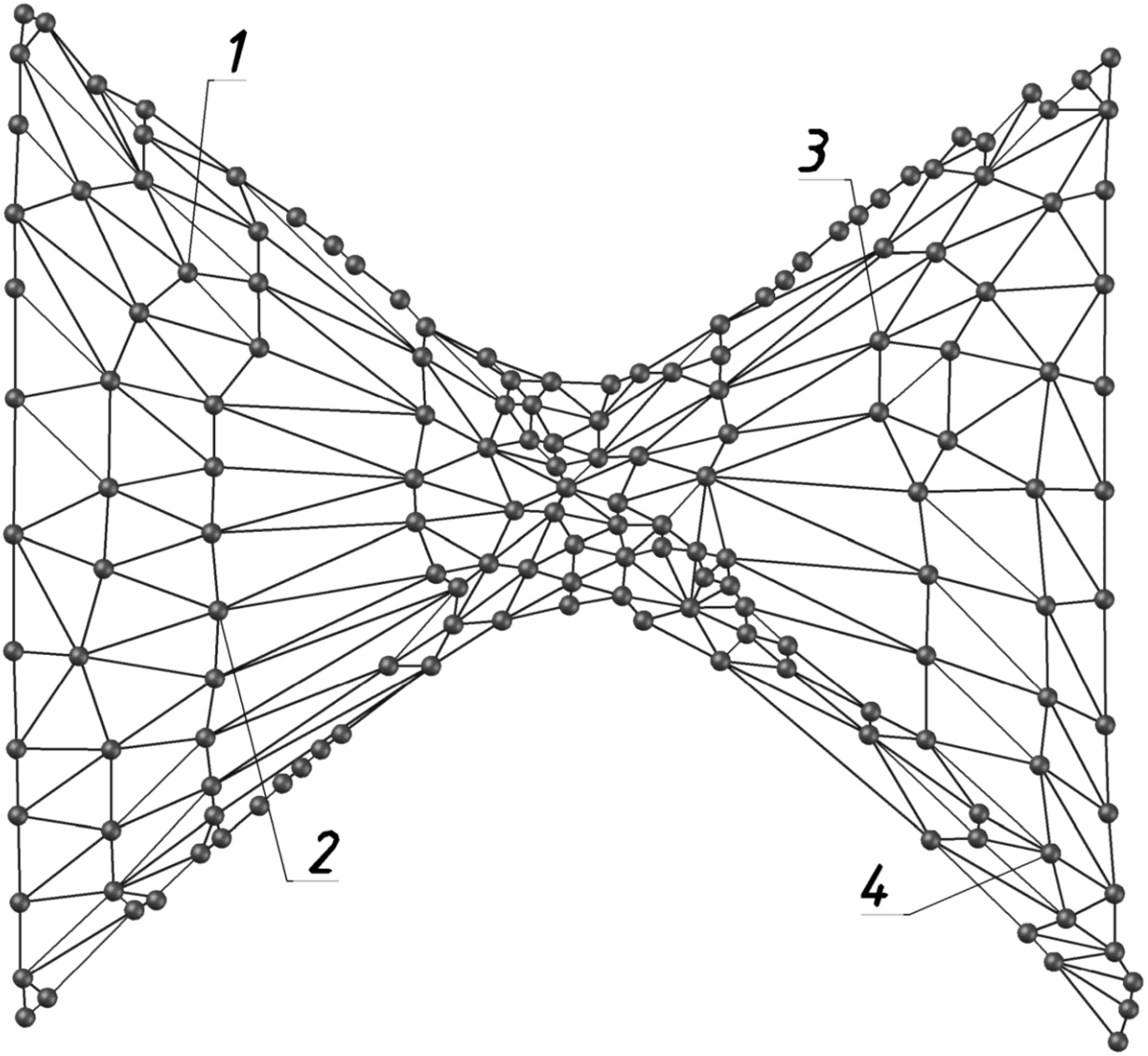


Рис. 3.9. Візуалізована форма згладженої топологічної поверхні БСМ за наявності атаки червоточини

3.5. Використання симплексів-ромбів для геометричного моделювання БСМ

Як зазначалось вище, до основних характеристик БСМ відносять довговічність, надійність та захищеність інформації. В значній мірі дані показники залежать від сили сигналів ІВ. В свою чергу сила сигналів ІВ, які працюють на автономних джерелах живлення, залежить від залишкової енергії джерел живлення ІВ.

ІВ одного виду, які працюють у складі гетерогенних БСМ, виконують однаковий об'єм роботи. Отже, залишкова енергія їхніх джерел живлення зменшується однаково. В основу роботи гомогенних БСМ закладено принцип самоорганізації. Тобто, в конкретний момент часу роль головного вузла бере на себе довільний ІВ, топологічні та фізичні параметри, якого відповідають встановленим вимогам. В таких мережах залишкова енергія джерел живлення ІВ зменшується нерівномірно, що приводить до різкого зменшення тривалості роботи і надійності БСМ [61, 62]. Для усунення вказаних недоліків запропоновано організувати безперервний контроль рівня залишкової енергії джерел живлення ІВ.

В літературних джерелах залишкову енергію джерел живлення ІВ пропонують представляти, як функцію сили сигналу даного вузла. В свою чергу силу сигналу представляють, як функцію відстані між сусідніми ІВ. Однак, в основі запропонованих вище геометричних моделей візуалізації параметрів сигналів ІВ є плоскі фігури (трикутники, квадрати, шестикутники), які при збільшені розмірів їх елементів не можуть трансформуватися в об'ємні геометричні фігури, отже не придатні для візуалізації окремих ІВ параметри сигналів яких змінюються.

Для візуалізації зміни параметрів сигналу окремого ІВ, або обмеженої кількості ІВ розміщених у різних місцях БСМ запропоновано використовувати симплекси – ромби [63]. Під час моделювання БСМ, до складу якої входять ІВ з однаковими параметрами, в основу побудови множини СТ конфігураційного простору використовують рівносторонній трикутник зі стороною l. У вершинах такого трикутника розміщують три СТ *(i, j,k)* і одержують ${}_i\Delta_k^j$, який визначається ФЗ $,l_{i,j},l_{jk}$ і l_{ki} між даними СТ. Якщо до складу БСМ входять ІВ з різними параметрами, в основу побудови беруть звичайний трикутник дотримуючись принципу його нерівності (сума двох сторін трикутника більша за довжину третьої сторони). Таким чином СТ, які представляють ІВ мережі у конфігураційному просторі, розміщують у вершинах трикутників (рис. 3.11).

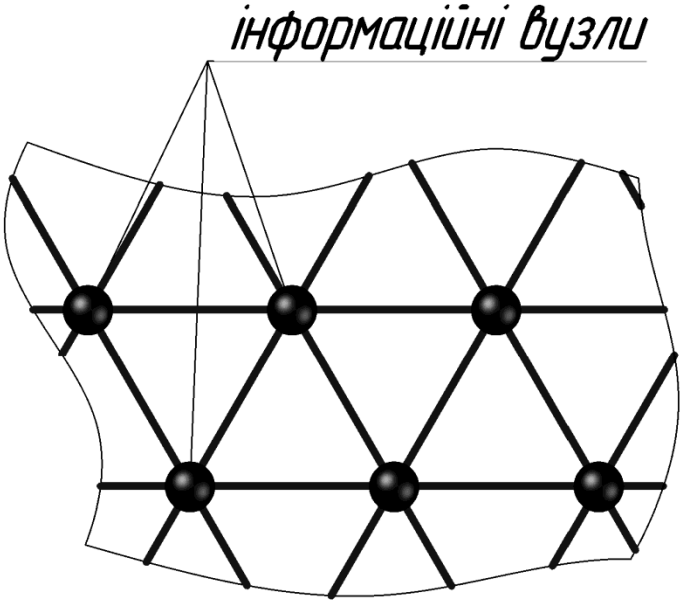


Рис. 3.10. Фрагмент геометричної моделі БСМ з трикутними комірками

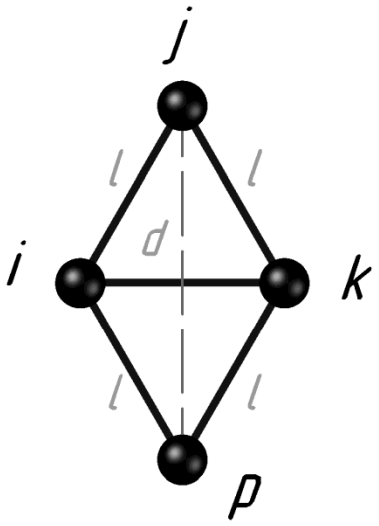


Рис. 3.11. Схема симплекса-ромба ${}^{i}_{j}[C]^{k}_{p}$ зі сигнальними точками (i,j,k,p) у вершинах

Оскільки, трикутники мало придатні для здійснення комп'ютерної візуалізації змін параметрів сигналів ІВ кожні два сусідні трикутники геометричної моделі БСМ об'єднують у чотириточкові симплекси з вершинами (i,j,k,p) (рис. 3.12). Такі симплекси значно зручніші для подальших досліджень оскільки, при переміщені СТ, що розміщені у їх вершинах симплекси можуть трансформуватися у відрізки прямої лінії, чотирикутники ${}^{i}_{j}[C]^{k}_{p}$ або трикутні піраміди.

Об'єднання двох рівносторонніх трикутників зі спільною стороною утворює чотирикутний симплекс-ромб, вершини якого з'єднані за допомогою п'яти ФЗ. Не з'єднаними залишаються дві вершини, які знаходяться на великій діагоналі ромба. З'єднавши ці вершини відрізком та визначивши його довжину із геометричних властивостей ЕКП, отримуємо симплекс-ромб ${}^{i}_{j}[C]^{k}_{p}$, в якому чотири вершини з'єднані п'ятьма ФЗ довжиною l (чотири сторони і мала діагональ) та одним геометричним зв'язком (ГЗ) довжиною $d = \sqrt{3}l$ (велика діагональ). Довжини ФЗ визначаються характером роботи ІВ і тому їхні довжини визначають положення СТ у симплексі. ГЗ не може змінювати форму симплекса. Він вказує лише відстань між двома його протилежними вершинами, причому цю відстань вимірюють у площині симплекса. ГЗ на рисунку позначений штриховою лінією.

При стабільній роботі ІВ у симплексі фіксується двовимірний евклідовий простір із ФЗ довжиною l. ФЗ визначаються характером роботи ІВ, які формують симплекс і визначають положення СТ, які представляють ці ІВ. Зміни в роботі ІВ приводять до зміни довжини ФЗ у симплексі. В залежності від того, яким чином встановлюють залежність між ФЗ і СТ у симплексі існують два види візуалізації сили сигналів ІВ.

Перший вид візуалізації ґрунтується на тому, що первинне положення СТ фіксують у кластері. СТ таким чином, залишаються нерухомими і при зміні сили сигналів ІВ. Такий вид візуалізації називають методом стаціонарних сигнальних точок (ССТ).

Другий вид візуалізації ґрунтується на можливості переміщення СТ в залежності від довжини ФЗ, які визначають СТ. В результаті реалізації такого виду візуалізації геометрія симплекса змінюється внаслідок зміни сили сигналу одного або декількох ІВ оскільки ФЗ, які характеризують роботу ІВ змінюють свою довжину.

3.6. Метод стаціонарних сигнальних точок

Зміна сили сигналу ІВ або групи ІВ спричиняє зміну відповідних ФЗ, які здійснюють викривлення простору навколо тих нерухомих СТ, які визначають ІВ сигнали яких аналізують. Змінені у довжині ФЗ стають дугами кіл, які відділяються від кіл хордами довжиною l. Дуги мають своїм початком зафіксовані СТ, які представляють ІВ сигнали, яких аналізують. Кінці дуг фіксують у СТ, які визначають ФЗ в початковому створені симплекса. Таким чином, навколо СТ сигнал ІВ, якої аналізують, відбувається викривлення простору. Такий вид візуалізації доцільно використовувати у випадках, коли одночасно змінюється сила сигналів великої кількості ІВ, зокрема для оцінювання енергетичного запасу ІВ з автономним живленням.

Під час реалізації методу стаціонарних сигнальних точок (ССТ) визначення ГЗ потрібне лише при вирішенні конкретних задач, які можуть виникати. Область повної трансформації симплекса ${}_j^i\left[C\right]_p^k$ складається із пари взаємозв'язаних трикутників ${}_i\Delta_p^j$ і ${}_i\Delta_k^p$ (рис. 3.11) дві сторони кожного з яких перетворюються на дуги, які з'єднують СТ із точкою-представником ІВ сигнал, якого аналізують.

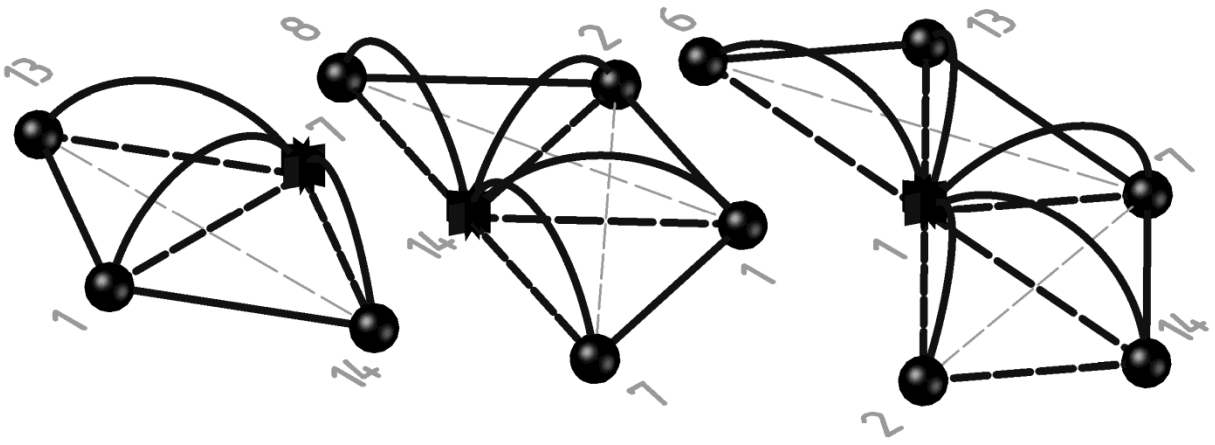


Рис. 3.12. Візуальне зображення області повної трансформації симплекса за методом ССТ

Розглянемо процес контролю за рівнем залишкової енергії ІВ мережі з автономним живленням. В процесі роботи ІВ запас енергії їхніх джерел живлення зменшується. Відповідно сила сигналів зменшується. Отже, сили сигналів ІВ представляють, як функцію залишкової енергії їхніх джерел живлення. Таким чином візуалізація сили сигналів дозволяє отримати інформацію про рівень залишкової енергії джерел живлення ІВ. Така візуалізація сили сигналу *i*-того ІВ, причиною зменшення, якої є зниження енергетичного запасу джерел живлення, відбувається за схемою приведеною на рис. 3.13.

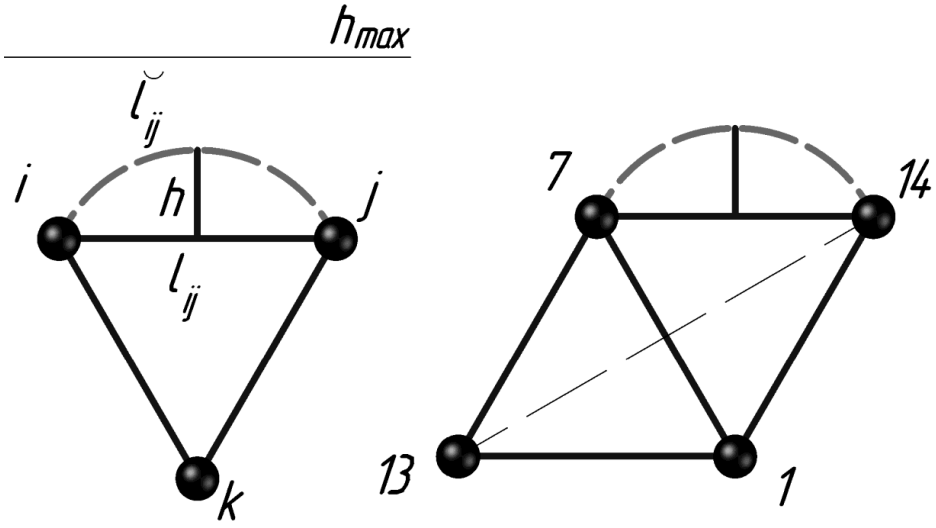


Рис. 3.13. Схема візуалізації зміни сили сигналу ІВ за методом ССТ.

i, j – номери досліджуваних СТ віртуальної мережі; $l_{i,j}$ – довжина ФЗ між СТ i, j на початку досліджень; $\breve{l}_{i,j}$ – змінена довжина ФЗ між СТ i, j в процесі досліджень; h – показник трансформації симплекса

Відповідно запропонованому методу візуалізації зменшення сили сигналу між СТ i, j приводить до збільшення довжини дуги $\breve{l}_{i,j}$ при незмінній довжині хорди $l_{i,j}$. Отже, збільшується h – величина найбільшого перевищення дуги $\breve{l}_{i,j}$ над хордою $l_{i,j}$, яку називають показником трансформації. При досягненні сили сигналу мінімально критичного значення експлуатація ІВ стає недоцільною, а показник трансформації набуває максимального значення h_{max}. Таким чином, встановивши на основі фізичних характеристик ІВ та умов експлуатації БСМ h_{max} і залежить між $l_{i,j}$; $\breve{l}_{i,j}$ і h одержують можливість аналізу надійності роботи окремих ІВ і БСМ в цілому.

Для встановлення залежності між вказаними геометричними параметрами представляють довжину дуги $\breve{l}_{i,j}$ у вигляді формули Гюйгенса:

$$\breve{l}_{i,j} \approx 2l + \frac{1}{3}(2l - l_{ij}) \tag{3.11}$$

Відповідно:

$$l \approx \frac{3\breve{l}_{ij} + l_{ij}}{8} \tag{3.12}$$

Як катет прямокутного трикутника:

$$h = \sqrt{l^2 - \frac{(l_{ij})^2}{4}} \tag{3.13}$$

Підставивши l з (3.12) в (3.13) одержуємо:

$$h = \frac{\sqrt{3}}{8}\sqrt{3(\breve{l}_{ij})^2 + 2\breve{l}_{ij}l_{ij} - 5(l_{ij})^2} \tag{3.14}$$

Приведені графічні та аналітичні дослідження підтверджують можливість відслідковувати силу сигналів всіх ІВ мережі та оцінювати їхню роботу.

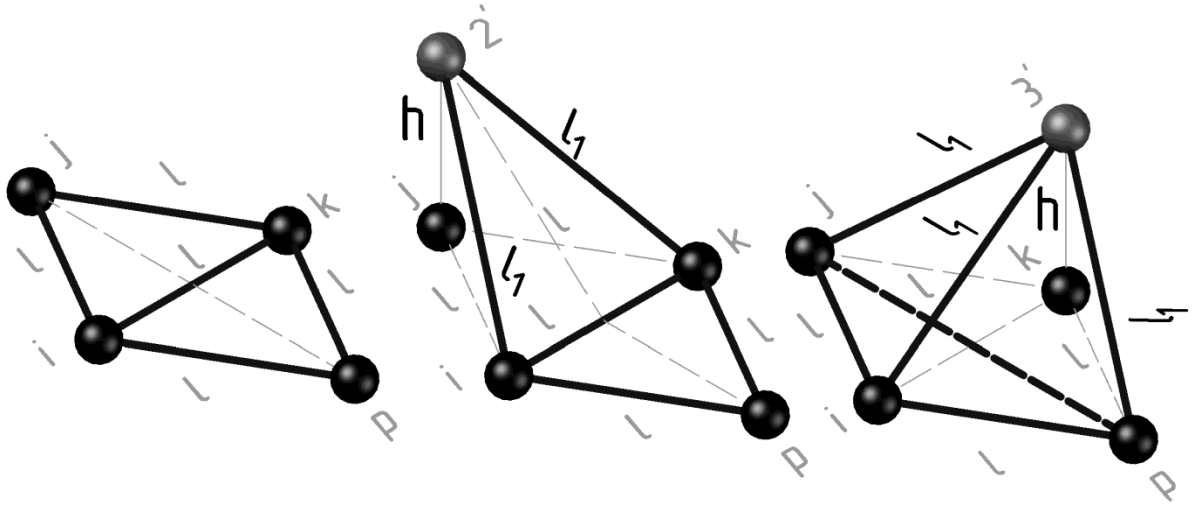
3.7. Метод рухомих сигнальних точок

За умов реалізації другого виду візуалізації сили сигналів ІВ геометрія симплекса змінюється в результаті зміни сили сигналу одного або декількох ІВ внаслідок того, що ФЗ, які характеризують роботу ІВ змінюють свою довжину. Зміна довжини ФЗ приводить до переміщення відповідних СТ. Таким чином, відбувається трансформація простору симплекса навколо СТ, які візуально визначають в конфігураційному просторі комп'ютера ІВ сила сигналів яких зазнала змін. Зміна сили сигналу на величину ε приведе до зміни структури симплекса. ФЗ, визначаючи характер роботи ІВ, змінять свою довжину на величину $l_\varepsilon = l(\varepsilon)$ і здійснять переміщення СТ, яка визначається даними ФЗ. Таким чином у моделі мережі утворяться три типи симплексів (рис. 3.14), [64,65]:

$[C]$ з відсутньою трансформацією (ОТр). Це будуть симплекси, які знаходяться поза областю трансформаційних процесів. Такі симплекси не мають видовження ФЗ (рис. 3.14а).

$[C]$ з частковою трансформацією (ЧТр), яка визначається двома ФЗ із видовженням $l_\varepsilon = l(\varepsilon)$ (рис. 3.14б). В таких симплексах один трикутник знаходиться в області трансформації, а інший поза нею. Трансформація такого симплекса приводить до утворення тривимірного геометричного об'єкту, який складається із двох трикутників зігнутих вздовж спільної основи – функціонального зв'язку, який не змінюється і залишає нерухомими кінці відрізка (СТ).

$[C]$ з повною трансформацією (ПТр), яка визначається трьома ФЗ із видовженням $l_\varepsilon = l(\varepsilon)$ (рис. 3.14в). Такі симплекси не можуть бути реалізовані у двовимірному просторі кластера. Вони утворять тривимірні геометричні об'єкти у вигляді трикутної піраміди. В основі такої піраміди знаходяться три нерухомі сигнальні точки, з'єднані двома функціональними зв'язками довжиною l і геометричним зв'язком довжиною $d = \sqrt{3}l$. Висота такої піраміди може бути використана для здійснення оцінки ступеня атаки на ІВ.



а) б) в)

Рис. 3.14. Типи трансформації симплекса: ОТр (а), ЧТр(б), ПТр(в)

Об’єм трансформованого симплекса представляють, як функцію видовження ФЗ

$$\Delta l : V_{ijkp} = V(\Delta\, l) \tag{3.15}$$

Об’єм тетраедра$V(\Delta\, l)$ представляють використовуючи відому залежність:

$$V(\Delta\, l) = \frac{1}{3} S_{ijk} \cdot H \tag{3.16}$$

Де H – висота тетраедра (м); S_{ijk} - площа основи тетраедра (в нашому випадку рівностороннього трикутника довжина сторони рівна $l_{i,j}$ (м). Для визначення площі основи тетраедра використовують узагальнену формулу Герона:

$$S_{ijk}^2 = \frac{(-1)^2}{2^2(2!)^2} \begin{pmatrix} 0 & 1 & 1 & 1 \\ -1 & 0 & l_{ij}^2 & l_{ik}^2 \\ -1 & l_{ij}^2 & 0 & l_{jk}^2 \\ -1 & l_{ik}^2 & l_{jk}^2 & 0 \end{pmatrix} \tag{3.17}$$

Для визначення об’єму тетраедра V_{ijkp} використовують формулу Ніколо Тартальї:

$$V^2_{ijkp} = \frac{(-1)^3}{2^3(3!)^2}\begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ -1 & 0 & l^2_{ij} & l^2_{ik} & l^2_{ip} \\ -1 & l^2_{ij} & 0 & l^2_{jk} & l^2_{jp} \\ -1 & l^2_{ik} & l^2_{jk} & 0 & l^2_{kp} \\ -1 & l^2_{ip} & l^2_{jp} & l^2_{kp} & 0 \end{pmatrix} \quad (3.18)$$

Таким чином залежність (3.10) представляє величину трансформації БСМ у двомірному евклідовому просторі. В загальному вигляді її можна представити, як:

$$V^2_{i\ldots n+1} = \frac{1}{2^2(n!)^2}\cdot(-1)^{n-1}\cdot\begin{pmatrix} 0 & 1 & 1 & \ldots & 1 \\ -1 & 0 & l^2_{ij} & \ldots & l^2_{i\ldots n+1} \\ -1 & l^2_{ij} & 0 & \ldots & l^2_{j\ldots n+1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ -1 & l^2_{i\ldots n+1} & l^2_{j..n+1} & \ldots & 0 \end{pmatrix} \quad (3.19)$$

Де n – вимірність модельованої БСМ; $\frac{1}{2^n(n!)^2}$ – коефіцієнт;

$(-1)^{n-1}\cdot\begin{pmatrix} 0 & 1 & 1 & \ldots & 1 \\ -1 & 0 & l^2_{ij} & \ldots & l^2_{i\ldots n+1} \\ -1 & l^2_{ij} & 0 & \ldots & l^2_{j\ldots n+1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ -1 & l^2_{i\ldots n+1} & l^2_{j..n+1} & \ldots & 0 \end{pmatrix}$ – діагональний визначник Келі-Менгера.

Для візуалізації трансформації об’ємних БСМ залежність (3.11) приймає вигляд:

$$V^2_{i\ldots n+1} = \frac{(-1)^4}{2^4(4!)^2}\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ -1 & 0 & l^2_{ij} & l^2_{ik} & l^2_{ip} & l^2_{ij} \\ -1 & l^2_{ij} & 0 & l^2_{jk} & l^2_{jp} & l^2_{ji} \\ -1 & l^2_{ik} & l^2_{jk} & 0 & l^2_{kp} & l^2_{kj} \\ -1 & l^2_{ip} & l^2_{jp} & l^2_{kp} & 0 & l^2_{pj} \\ -1 & l^2_{ij} & l^2_{ji} & l^2_{pj} & l^2_{kj} & 0 \end{pmatrix} \quad (3.20)$$

Для візуалізації трансформації двомірних БСМ відкалібрують всі ребра симплексів по відношенню до прийнятої відповідності, що шумовому сигналу ω відповідає відрізок $l_0 = l(\omega)$. Нехай $l_j = \alpha l_0$, а довжина, яка відповідає сигналу $\varepsilon - l_\varepsilon = \beta l_0$. Тоді зміну довжини ФЗ між двома СТ представляють довжиною

$$l = (2\alpha + 1)l_0 \tag{3.21}$$

А ГЗ – довжиною

$$d = \sqrt{3}l = (2\alpha + 1)l_0\sqrt{3};\ (d^2 = 3l^2) \tag{3.22}$$

Після зміни сили сигналу ІВ отримують наступні видовження:

$$-l_1 = \sqrt{k}l \tag{3.23}$$

$$k = (1 + \delta)^2 \tag{3.24}$$

$$\delta = \frac{l_\varepsilon}{l} = \frac{\beta}{2\alpha + 1} \tag{3.25}$$

де δ – коефіцієнт, який визначає відносне видовження ФЗ внаслідок зміни сили сигналу ІВ.

ГЗ після видовження описують залежністю:

$$d_1 = \frac{\sqrt{3} + \sqrt{4k - 1}}{2} l \tag{3.26}$$

або $$d_1^2 = (k + \gamma)l^2 \tag{3.27}$$

де $$\gamma = \frac{1 + \sqrt{12k - 3}}{2} \tag{3.28}$$

Таким чином, після зміни сили сигналу три типи симплексів із вершинами в точках i, j, k, p (рис. 3.14) будуть мати наступні довжини ребер:

$4C$ без видовження ФЗ: $l_{ij} = l_{ip} = l_{kp} = l_{ik} = l, \quad l_{jk} = d$;

$4C$ із двома видовженими ФЗ: $l_{ij} = l_{ip} = l_{jp} = l, \quad l_{ik} = l_{pk} = l_1 \quad l_{jk} = d_1$;

$4C$ із трьома видовженими ФЗ: $l_{ij} = l_{ik} = l, \quad l_{ip} = l_{jp} = l_{kp} = l_1 \quad l_{jk} = d$.

Із визначника Келі-Менгера приведеного в залежності (3.10) отримуємо три визначники: $\Delta(4C), \quad \Delta_2(4C), \quad \Delta_3(4C)$ (нижній індекс вказує на кількість ФЗ, які видовжуються), які після введення параметрів

$$K_1=\begin{cases}1, & \Delta(4C)=\Delta_0(4C);\\ 1, & \Delta(4C)=\Delta_2(4C);\\ k, & \Delta(4C)=\Delta_3(4C);\end{cases} \qquad K_2=\begin{cases}1, & \Delta(4C)=\Delta_0(4C);\\ k, & \Delta(4C)=\Delta_2(4C);\\ 1, & \Delta(4C)=\Delta_3(4C);\end{cases}$$

$$K_3=\begin{cases}3, & \Delta(4C)=\Delta_0(4C);\\ k+\gamma, & \Delta(4C)=\Delta_2(4C);\\ 3, & \Delta(4C)=\Delta_3(4C);\end{cases} \qquad K_4=\begin{cases}1, & \Delta(4C)=\Delta_0(4C);\\ k, & \Delta(4C)=\Delta_2(4C);\\ k, & \Delta(4C)=\Delta_3(4C);\end{cases} \tag{3.29}$$

записують одним визначником $\Delta(4C)$ 5-го порядку:

$$\Delta(4C)=\begin{vmatrix}0 & 1 & 1 & 1 & 1\\ -1 & 0 & l^2 & k_1l^2 & k_2l^2\\ -1 & l^2 & 0 & k_1l^2 & k_3l^2\\ -1 & k_1l^2 & k_1l^2 & 0 & k_4l^2\\ -1 & k_2l^2 & k_3l^2 & k_4l^2 & 0\end{vmatrix}, \tag{3.30}$$

Використовуючи властивості визначників визначник (3.30) зводимо до симетричного визначника третього порядку:

$$\Delta(4C)=l^6\begin{vmatrix}-2 & -1 & k_3-k_2-1\\ -1 & -2k_1 & k_4-k_2-k_1\\ k_3-k_2-1 & k_4-k_2-k_1 & -2k_2\end{vmatrix}, \tag{3.31}$$

Для $(4C)$ без видовження ФЗ: $k_1=k_2=k_4=1$і $k_3=3$. Об'єми таких симплексів дорівнюють нулю, внаслідок того, що

$$\Delta(4C)=\Delta_0(4C)=l^6\begin{vmatrix}-2 & -1 & 1\\ -1 & -2 & -1\\ 1 & -1 & -2\end{vmatrix}=0, \tag{3.32}$$

Визначник $\Delta_2(4C)$ для симплексів із двома функціональними зв'язками визначається параметрами: $k_1=1,\ k_2=k_4=k,\ k_3=k+\gamma$, і також дорівнює нулю тому що:

$$\Delta(4C)=\Delta_2(4C)=l^6\begin{vmatrix}-2 & -1 & \gamma-1\\ -1 & -2 & -1\\ \gamma-1 & -1 & -2k\end{vmatrix}=-l^6(\gamma^2-\gamma+1-3k) \tag{3.33}$$

Оскільки,

$$\gamma^2 = \left(\frac{1+\sqrt{12k-3}}{2} \right)^2 = \frac{\sqrt{12k-3}+12k-3}{4} = 3k + \frac{\sqrt{12k-3}-1}{2} = 3k+\gamma-1, \quad (3.34)$$

отримуємо $\Delta_2(4C) = -2l^6(3k+\gamma-1-\gamma+1-3k) = 0,$ (3.35)

Рівність нулю визначника вказує на те, що об'єми симплексів із двома зміненими ФЗ також дорівнюють нулю, тобто трансформовані таким чином симплекси залишаються плоскими геометричними об'єктами і не здійснюють структурних змін конфігураційного простору.

Для симплексів із трьома зміненими функціональними зв'язками визначник $\Delta(4C) = \Delta_3(4C)$ із параметрами $k_1 = k_4 = k,\ k_2 = 1,\ k_3 = 3$ буде дорівнювати:

$$\Delta_3(4C) = l^6 \begin{vmatrix} -2 & 1 & -1 \\ -1 & 2k & 1 \\ -1 & 1 & 2 \end{vmatrix} = 6l^6(k-1), \quad (3.36)$$

де $k = (1+\delta)^2$ і $\delta = \frac{l_\varepsilon}{l} = \frac{\beta}{2d+1}$.

Відмінність від нуля визначника ,а, отже, і об'єму симплекса, вказує, що трансформація$(4C)$ із трьома ФЗ, які змінюються приводить до утворення тримірного геометричного об'єкта – трикутної піраміди. Простір змодельованої БСМ отримає локальне викривлення з епіцентром в СТ, яка є представником у конфігураційному просторі ІВ, сила сигналу якого зазнала змін.

Відповідно запропонованому методу візуалізації зменшення сили сигналу ІВ приводить до збільшення об'єму трансформованого у тригранну піраміду симплекса. За умови незмінності площі основи піраміди при цьому збільшується висота піраміди H. Таким чином H називають показником трансформації. При досягненні сили сигналу мінімально критичного значення експлуатація ІВ стає недоцільною, а показник трансформації набуває максимального значення H_{max}. Таким чином, встановивши на основі фізичних характеристик ІВ та умов експлуатації БСМ H_{max} і залежність між V_{ijkp}, S_{ijk} і H одержують можливість аналізу надійності роботи окремих ІВ і БСМ в цілому. Для встановлення вказаної залежності використовують рівняння (3.8). оскільки за умовою основа піраміди – рівносторонній трикутник зі стороною l_{ij}, рівняння (3.9) приймає вигляд:

$$S_{ijk} = \frac{\sqrt{3}}{4} l_{ij}^2 \tag{3.37}$$

Тоді (3.8) представляють у вигляді:

$$V(\Delta\, l) = \frac{\sqrt{3}}{12} l_{ij}^2 \cdot H \tag{3.38}$$

Звідси одержують:

$$H = \frac{12}{\sqrt{3}} \cdot \frac{V(\Delta l)}{l_{ij}^2} \tag{3.39}$$

Одержані залежності дозволяють аналогічно приведеному вище методу ССТ, встановивши на основі фізичних характеристик ІВ та умов експлуатації БСМ, H_{max} аналізувати надійність роботи окремих ІВ і БСМ в цілому.

Таким чином використання чотириточкових симплексів для геометричного моделювання БСМ дає можливість проводити аналіз трансформації процесів організувавши візуальні спостереження за відповідними параметрами ІВ у просторі комп'ютера.

Запропонована модель при відповідному виборі узгоджувальної функціональної залежності визначає геометричні утворення в евклідовому конфігураційному просторі і дає можливість побудувати ієрархічну структуру із СТ. Створення структури ґрунтується на принципі самоподібності, який є основою побудови різного виду геометричних структур у фрактальній геометрії [67,68,69]. Ієрархічна структура дозволяє швидко, опускаючись по «ієрархічній драбині», відшукати первинний геометричний об'єкт конфігураційного простору, складений із невеликої кількості СТ, в якому відбулися структурні зміни внаслідок зміни параметрів сигналу одного із ІВ.

Але, як показано вище, чотириточковий симплекс трансформується у тетраедр тільки у тому випадку, коли змін зазнає сила сигналу ІВ, СТ якого зв'язана у симплексі трьома ФЗ з іншими СТ (розміщена на кінцях малої діагоналі ромба). Якщо змін зазнає сила сигналу ІВ, СТ якого розміщена на кінці великої діагоналі ромба або змін зазнали одночасно сигнали кількох ІВ, СТ яких належать одному симплексу, візуалізація трансформації симплекса ускладняється або стає неможливою. Для вирішення даної проблеми запропоновано використання симплексно-кластерного моделювання.

Розділ 4. Симплексно-кластерне моделювання БСМ

4.1. Алгоритм побудови та дослідження структури шестикутного кластера

Побудова кластерної моделі комп'ютерної візуалізації групи однотипних ІВ ґрунтується на використанні принципів побудови фрактальних структур типу «сніжинка Коха» [68], виходячи із формуючого (основного) елементу конфігураційного простору – ФЗ між двома СТ. Така модель передбачає побудову на першому етапі за допомогою базового елементу геометричного об'єкту – основи для створення складніших геометричних структур.

В основу побудови множин СТ конфігураційного простору, які здійснюють візуалізацію мережі ІВ із однаковими параметрами, покладено правильний шестикутник зі стороною l [67]. У вершинах такого шестикутника розміщують шість СТ. Наступним кроком побудови є окантування шестикутника правильними трикутниками зі сторонами такої ж довжини, у вершинах яких також розміщують СТ.

Утворений таким чином кластер $K(18;36)$ має шестикутну структуру і повністю знаходиться у двомірному евклідовому конфігураційному просторі комп'ютера. Кластер складається з 18 СТ, з'єднаних за допомогою 36 однакових відрізків – ФЗ (довжиною l) (рис. 4.1). ФЗ а, отже, і розміщення СТ визначаються характеристиками ІВ, а не властивостями евклідового конфігураційного простору.

Таким чином, СТ є представниками ІВ у конфігураційному просторі комп'ютера, а ФЗ характеризують роботу ІВ у «польових умовах».

Побудова дає можливість утворити ще одну СТ, яку можна помістити у центр внутрішнього шестикутника, з'єднавши її шістьма ФЗ з вершинами шестикутника. Але це робити недоцільно внаслідок того, що при збільшені СТ на одиницю кількості ФЗ збільшується на шість.

У представленому кластері множину функціональних зв'язків $L=\{l_{1,7}; l_{1,13}; l_{1,14}; l_{1,2}; l_{1,6}; l_{2,14}; l_{2,8}; l_{2,15}; l_{2,3}; l_{3,15}; l_{3,9}; l_{3,16}; l_{3,4}; l_{4,16}; l_{4,10}; l_{4,17}; l_{4,5}; l_{5,17}; l_{5,11}; l_{5,18}; l_{5,6}; l_{6,18}; l_{6,12}; l_{6,13}; l_{7,13}; l_{7,14}; l_{8,14}; l_{8,15}; l_{9,15}; l_{9,16}; l_{10,16}; l_{10,17}; l_{11,17}; l_{11,18}; l_{12,18}; l_{12,13}\}$ розділяють на три класи – $L = L_1 \cup L_2 \cup L_3$.

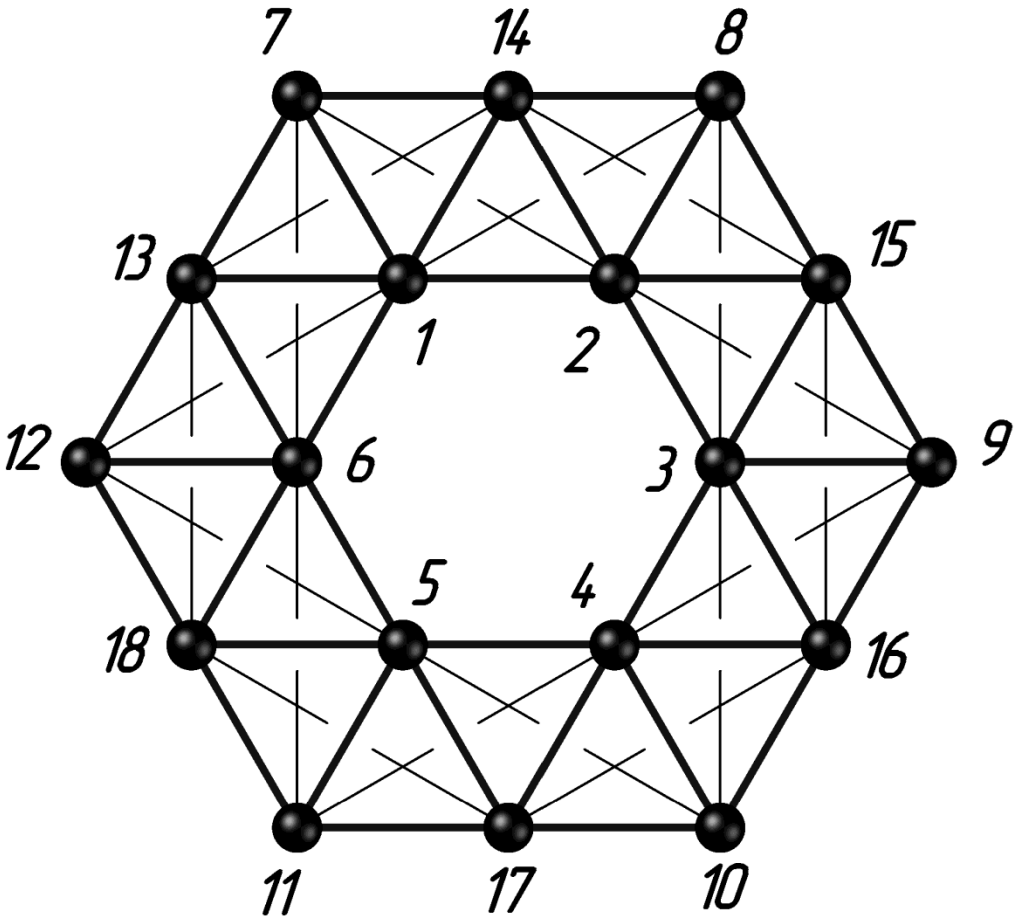


Рис. 4.1. Кластерна модель із СТ в евклідовому конфігураційному просторі Множину 12-ти ФЗ, які утворюють сторони зовнішнього обвідного шестикутника $L1=\{ l_{7,13}; l_{7,14}; l_{8,14}; l_{8,15}; l_{9,15}; l_{9,16}; l_{10,16}; l_{10,17}; l_{11,17}; l_{11,18}; l_{12,18}; l_{12,13} \}$.

1. Множину 6-ти ФЗ, які є сторонами внутрішнього шестикутника: $L_2 = \{ l_{1,2}; l_{2,3}; l_{3,4}; l_{4,5}; l_{5,6}; l_{6,1} \}$.

2. Множину 18-ти ФЗ, які з'єднують вершини внутрішнього шестикутника із вершинами і серединами сторін зовнішнього шестикутника: $L_3 = \{ l_{1,7}; l_{1,13}; l_{1,14}; l_{2,14}; l_{2,8}; l_{2,15}; l_{3,15}; l_{3,9}; l_{3,16}; l_{4,16}; l_{4,10}; l_{4,17}; l_{5,17}; l_{5,11}; l_{5,18}; l_{6,18}; l_{6,12}; l_{6,13} \}$.

ФЗ, як утворюючі елементи кластера $K(18;36)$, в перетині визначають множину $C18$ - ти СТ кластера:

$$C = \{ C_1; C_2; C_3; C_4; C_5; C_6; C_7; C_8; C_9; C_{10}; C_{12}; C_{13}; C_{14}; C_{15}; C_{16}; C_{17}; C_{18} \}$$

В залежності від того, перетином скількох ФЗ визначається СТ, усю множину СТ розбивають на три класи - $C = C_1 \cup C_2 \cup C_3$:

Вершини зовнішнього обвідного шестикутника C_1. Цей клас СТ визначають перетином двох сусідніх ФЗ із класу L_1 та один ФЗ із класу $L_3 : C_1 = \{ C_7; C_8; C_9; C_{10}; C_{11}; C_{12} \}$

Таблиця 4.1.

СТ утворені трьома ФЗ

Сигнальні точки	Перетин функціональних зв'язків
C_7	$l_{1,7} \cap l_{7,13} \cap l_{7,14}$
C_8	$l_{2,8} \cap l_{8,14} \cap l_{8,15}$
C_9	$l_{3,9} \cap l_{9,15} \cap l_{9,16}$
C_{10}	$l_{4,10} \cap l_{10,16} \cap l_{10,17}$
C_{11}	$l_{5,11} \cap l_{11,17} \cap l_{11,18}$
C_{12}	$l_{6,12} \cap l_{12,18} \cap l_{12,13}$

Кожна СТ класу C_1 має три ФЗ з іншими СТ. Вона функціонально з'єднана із однією вершиною внутрішнього шестикутника і двома СТ, які є серединами сторін зовнішнього обвідного шестикутника.

Середини сторін зовнішнього обвідного шестикутника C_2. Цей клас СТ визначають перетином двох сусідніх ФЗ із складу L_1 та двох відповідних ФЗ із класу $L_3 : \ C_2 = \{ C_{13}; C_{14}; C_{15}; C_{16}; \ C_{17}; C_{18} \}$.

Таблиця 4.2.

СТ утворені чотирма ФЗ

Сигнальні точки	Перетин функціональних зв'язків
C_{13}	$l_{7,13} \cap l_{12,13} \cap l_{1,13} \cap l_{6,13}$
C_{14}	$l_{7,14} \cap l_{8,14} \cap l_{1,14} \cap l_{2,14}$
C_{15}	$l_{8,15} \cap l_{9,15} \cap l_{2,15} \cap l_{3,15}$
C_{16}	$l_{9,16} \cap l_{10,16} \cap l_{3,16} \cap l_{4,16}$
C_{17}	$l_{10,17} \cap l_{11,17} \cap l_{4,17} \cap l_{5,17}$
C_{18}	$l_{11,18} \cap l_{12,18} \cap l_{5,18} \cap l_{6,18}$

Кожна СТ класу C_2 має по чотири ФЗ з іншими СТ. вона функціонально з'єднана із двома сусідніми вершинами зовнішнього обвідного шестикутника та двома вершинами внутрішнього шестикутника.

Вершини внутрішнього шестикутника C_3. Цей клас СТ визначають перетином трьох відповідних ФЗ із класу L_3 та двох сусідніх ФЗ із класу $L_2 : C_3 = \{C_1;\ C_2;\ C_3;\ C_4;\ C_5;\ C_6\}$.Кожна СТ класу C_3 має по п'ять ФЗ з іншими СТ. Вона функціонально з'єднана із двома сусідніми вершинами внутрішнього шестикутника, однією вершиною зовнішнього обвідного шестикутника та двома СТ, які є серединами сторін зовнішнього обвідного шестикутника.

Таблиця 4.3.

СТ утворені п'ятьма ФЗ

Сигнальні точки	Перетин функціональних зв'язків
C_1	$l_{1,2} \cap l_{1,6} \cap l_{1,7} \cap l_{1,13} \cap l_{1,14}$
C_2	$l_{1,2} \cap l_{2,3} \cap l_{2,8} \cap l_{2,14} \cap l_{2,15}$
C_3	$l_{2,3} \cap l_{3,4} \cap l_{3,9} \cap l_{3,15} \cap l_{3,16}$
C_4	$l_{3,4} \cap l_{4,5} \cap l_{4,10} \cap l_{4,16} \cap l_{4,17}$
C_5	$l_{4,5} \cap l_{5,6} \cap l_{5,11} \cap l_{5,17} \cap l_{5,19}$
C_6	$l_{5,6} \cap l_{1,6} \cap l_{6,12} \cap l_{6,18} \cap l_{6,13}$

Множини ФЗ L і СТ **с** дозволяють здійснювати покриття двовимірного евклідового комп'ютерного простору кластера $K\ (18,36)$ множиною трикутників, яка налічує 18 елементів:

$$T = \{ {}_1\Delta\,{}^{7}_{14};\ {}_1\Delta\,{}^{14}_{2};\ {}_2\Delta\,{}^{14}_{8};\ {}_2\Delta\,{}^{8}_{15};\ {}_2\Delta\,{}^{15}_{3};\ {}_3\Delta\,{}^{15}_{9};\ {}_3\Delta\,{}^{9}_{16};\ {}_3\Delta\,{}^{16}_{4};\ {}_4\Delta\,{}^{16}_{10};\ {}_4\Delta\,{}^{10}_{17};\ {}_4\Delta\,{}^{17}_{5};\ {}_5\Delta\,{}^{17}_{11};$$
$${}_5\Delta\,{}^{11}_{18};\ {}_5\Delta\,{}^{18}_{6};\ {}_6\Delta\,{}^{18}_{12};\ {}_6\Delta\,{}^{12}_{13};\ {}_6\Delta\,{}^{13}_{1};\ {}_1\Delta\,{}^{13}_{7}\ \};$$

Множину трикутників розділяють на дві групи $T = T_1 \cup T_2$:

1. $T_1 = \{ {}_1\Delta\,{}^{14}_{2};\ {}_2\Delta\,{}^{15}_{3};\ {}_3\Delta\,{}^{16}_{4};\ {}_4\Delta\,{}^{17}_{5};\ {}_5\Delta\,{}^{18}_{6};\ {}_6\Delta\,{}^{13}_{1}\ \}$ - множина трикутників, в основі яких наявний ФЗ між двома СТ внутрішнього шестикутника;
2. $T_2 = \{ {}_1\Delta\,{}^{13}_{7};\ {}_1\Delta\,{}^{7}_{14};\ {}_2\Delta\,{}^{14}_{8};\ {}_2\Delta\,{}^{8}_{15};\ {}_3\Delta\,{}^{15}_{9};\ {}_3\Delta\,{}^{9}_{16};\ {}_4\Delta\,{}^{16}_{10};\ {}_4\Delta\,{}^{10}_{17};\ {}_5\Delta\,{}^{17}_{11};\ {}_5\Delta\,{}^{11}_{18};\ {}_6\Delta\,{}^{18}_{12};\ {}_6\Delta\,{}^{12}_{13}\ \}$ – множина трикутників, вершини яких є СТ із різних класів СТ.

Контур внутрішнього шестикутника вважають представленим 18 ${}^{i}_{j}[4C]^{k}_{p}$, які при побудові мають початкову геометричну форму ромба $R_i\ (i \in N_{18})$.

В табл. 4.4 приведені усі утворенні ромби R_i $(i \in N_{18})$, які є представниками симплексів ${}^{i}_{j}[4C]^{k}_{p}$, при нормальній роботі ІВ у кластері.

При такому розбитті обвідки внутрішнього шестикутника на 18 симплексів в кожному симплексі дві протилежні СТ визначають трьома ФЗ, при чому один ФЗ визначає відстань між цими СТ. Дві інші протилежні СТ визначають двома ФЗ і одним ГЗ, який визначає відстань між цими СТ.

Таблиця 4.4.

Симплекси-ромби кластера при нормальній роботі ІВ.

Ромби	Симплекси	Ромби	Симплекси	Ромби	Симплекси
R1	${}^{7}_{13}[C]^{14}_{1}$	R7	${}^{13}_{6}[C]^{7}_{1}$	R13	${}^{7}_{1}[C]^{14}_{2}$
R2	${}^{14}_{2}[C]^{8}_{15}$	R8	${}^{14}_{1}[C]^{8}_{2}$	R14	${}^{8}_{2}[C]^{15}_{3}$
R3	${}^{15}_{3}[C]^{9}_{16}$	R9	${}^{15}_{2}[C]^{9}_{3}$	R15	${}^{9}_{3}[C]^{16}_{4}$
R4	${}^{16}_{4}[C]^{10}_{17}$	R10	${}^{16}_{3}[C]^{10}_{4}$	R16	${}^{10}_{4}[C]^{17}_{5}$
R5	${}^{17}_{5}[C]^{11}_{18}$	R11	${}^{17}_{4}[C]^{11}_{5}$	R17	${}^{11}_{5}[C]^{18}_{6}$
R6	${}^{18}_{6}[C]^{12}_{13}$	R12	${}^{18}_{5}[C]^{12}_{6}$	R18	${}^{12}_{6}[C]^{13}_{1}$

У кластері СТ можуть одночасно належати одному, двом або трьом симплексам. За цими ознаками СТ поділяють на три групи:

СТ групи C_1 є вершинами для трьох ${}^{i}_{j}[C]^{k}_{p}$;

СТ групи C_2 є вершинами для чотирьох ${}^{i}_{j}[C]^{k}_{p}$;

СТ групи C_3 є вершинами для п’яти ${}^{i}_{j}[C]^{k}_{p}$.

Покриття простору кластера симплексами дає можливість означити покриття кластера трикутниками шляхом перетину симплексів, оскільки кожний трикутник є результатом перетину двох симплексів.

$${}_{1}\Delta^{14}_{2} = {}^{7}_{1}[C]^{14}_{2} \cap^{14}_{1} [C]^{8}_{2}; \quad {}_{2}\Delta^{15}_{3} = {}^{8}_{2}[C]^{15}_{3} \cap^{15}_{2} [C]^{9}_{3}; \quad {}_{3}\Delta^{16}_{4} = {}^{9}_{3}[C]^{16}_{4} \cap^{16}_{3} [C]^{10}_{4};$$
$${}_{4}\Delta^{17}_{5} = {}^{10}_{4}[C]^{17}_{5} \cap^{17}_{4} [C]^{11}_{5}; \quad {}_{5}\Delta^{18}_{6} = {}^{11}_{5}[C]^{18}_{6} \cap^{18}_{5} [C]^{12}_{6}; \quad {}_{6}\Delta^{13}_{1} = {}^{12}_{6}[C]^{13}_{1} \cap^{13}_{6} [C]^{7}_{1};$$
$${}_{1}\Delta^{13}_{7} = {}^{7}_{13}[C]^{14}_{1} \cap^{13}_{6} [C]^{7}_{1}; \quad {}_{1}\Delta^{7}_{14} = {}^{7}_{13}[C]^{14}_{1} \cap^{7}_{1} [C]^{14}_{2}; \quad {}_{2}\Delta^{14}_{8} = {}^{14}_{1}[C]^{8}_{2} \cap^{14}_{2} [C]^{8}_{15};$$
$${}_{2}\Delta^{8}_{15} = {}^{14}_{2}[C]^{8}_{15} \cap^{8}_{2} [C]^{15}_{3}; \quad {}_{3}\Delta^{15}_{9} = {}^{15}_{2}[C]^{9}_{3} \cap^{15}_{3} [C]^{9}_{16}; \quad {}_{3}\Delta^{9}_{16} = {}^{9}_{3}[C]^{16}_{4} \cap^{15}_{3} [C]^{9}_{16};$$
$${}_{4}\Delta^{16}_{10} = {}^{16}_{3}[C]^{10}_{4} \cap^{16}_{3} [C]^{10}_{4}; \quad {}_{4}\Delta^{10}_{17} = {}^{10}_{4}[C]^{17}_{5} \cap^{16}_{4} [C]^{10}_{17}; \quad {}_{5}\Delta^{17}_{11} = {}^{17}_{4}[C]^{11}_{5} \cap^{17}_{5} [C]^{11}_{18};$$
$${}_{5}\Delta^{11}_{18} = {}^{11}_{5}[C]^{18}_{6} \cap^{17}_{5} [C]^{11}_{18}; \quad {}_{6}\Delta^{18}_{12} = {}^{18}_{5}[C]^{12}_{6} \cap^{18}_{6} [C]^{12}_{13}; \quad {}_{6}\Delta^{12}_{13} = {}^{13}_{6}[C]^{7}_{1} \cap^{18}_{6} [C]^{12}_{13}.$$

Приведені вище методи візуального та аналітичного спостереження за роботою ІВ можна використовувати для спостереження за роботою ІВ, які представлені у кластері сигнальними точками, якщо зміни параметрів зазнають сигнали

одного або кількох ІВ, але таким чином, що процеси, які при цьому виникають у кластері не перетинаються і не здійснюють впливу один на одного.

4.2. Метод чотириточкових симплексів (метод *[C]*)

Зміна параметрів сигналу ІВ або групи ІВ приведе до зміни структури кластера. Внаслідок цього у кластері утвориться область трансформації, яка буде складатися із групи симплексів, ребрами яких є трансформовані і нетрансформовані ФЗ. Таким чином у кластері утворяться три типи симплексів: *[C]* з відсутньою трансформацією *(ОТр)*, *[C]* з частковою трансформацією *(ЧТр)*, *[C]* з повною трансформацією *(ПТр)*.

В залежності від того, параметри сигналу якого ІВ зазнали змін отримують різні області трансформації кластера (рис. 4.2).

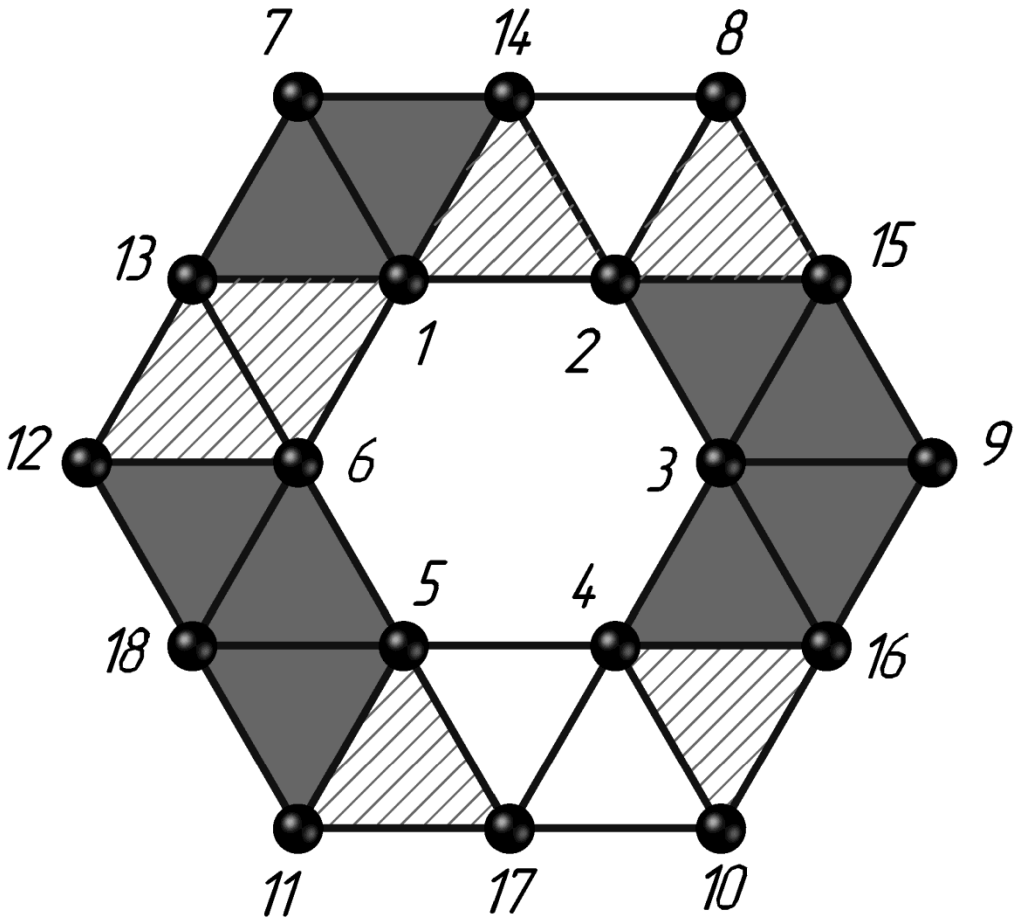


Рис. 4.2. Області трансформації при зміні параметрів сигналів ІВ, які представлені СТ різних класів

Якщо зазнав зміни параметр сигналу ІВ, який представлений СТ класу C_1, то в область трансформації кожної точки входять три симплекси. При цьому

один симплекс отримує *(ПТр)*, а два інші, які в перетині з цим симплексом мають його складові, отримують *(ЧТр)*. Усі інші 15 симплексів залишають у вигляді первинних ромбів двомірного простору кластера. В табл. 4.5 приведені усі симплекси, які можуть зазнати при цьому трансформацій.

Нехай зміни параметрів зазнав сигнал ІВ, який у кластері представлений СТ C_7. Область трансформації складається із множини СТ $C_{tr} = \{C_1; C_2; C_6; C_7; C_{13}; C_{14}\}$ і множини симплексів $S_{tr} = \{ {}^{13}_{6}[C]^{7}_{1}; {}^{7}_{13}[C]^{14}_{1}; {}^{7}_{1}[C]^{14}_{2} \}$

Область повної трансформації на рисунку зображена однотонно і складається із одного симплекса ${}^{7}_{13}[C]^{14}_{1}$. Він трансформується у трикутну піраміду типу а (рис. 4.3 а), вершиною якої є дана СТ. Основою піраміди буде трикутник, визначений трьома СТ C_1, C_{13}, C_{14}, які не задіяні в трансформаційному процесі. Бічні грані піраміди трикутники ${}_1\Delta^{13}_{7}$ і ${}_1\Delta^{7}_{14}$ - є трансформованими частинами двох бічних симплексів ${}^{13}_{6}[C]^{7}_{1}$ і ${}^{7}_{1}[C]^{14}_{2}$ з частковою трансформацією (рис. 4.3б). На рисунку не трансформовані частини цих симплексів заштриховано.

Таблиця 4.5.

Трансформація симплексів у яких зміни параметрів сигналів зазнали ІВ представлені СТ класу C_1

	C_7	C_8	C_9	C_{10}	C_{11}	C_{12}
ЧТр	${}^{13}_{6}[C]^{7}_{1}$	${}^{14}_{1}[C]^{8}_{2}$	${}^{15}_{2}[4C]^{9}_{3}$	${}^{16}_{3}[C]^{10}_{4}$	${}^{17}_{4}[C]^{11}_{5}$	${}^{18}_{5}[C]^{12}_{6}$
	${}^{7}_{1}[C]^{14}_{2}$	${}^{8}_{2}[C]^{15}_{3}$	${}^{9}_{3}[C]^{16}_{4}$	${}^{10}_{4}[C]^{17}_{5}$	${}^{11}_{5}[C]^{18}_{6}$	${}^{12}_{6}[C]^{13}_{1}$
ПТр	${}^{7}_{13}[C]^{14}_{1}$	${}^{14}_{2}[C]^{8}_{15}$	${}^{15}_{3}[C]^{9}_{16}$	${}^{7}_{13}[C]^{14}_{1}$	${}^{17}_{5}[C]^{11}_{18}$	${}^{18}_{6}[C]^{12}_{13}$

Якщо зазнав змін параметр сигналу ІВ, який представлений СТ класу C_2, то в область трансформації попадають чотири симплекси. При цьому два симплекси отримають *(ПТр)*, а два інші, які в перетині із цими симплексами мають спільні складові, отримують *(ЧТр)*. Інші 14 симплексів, які не входять в область трансформації залишаються у вигляді первинних ромбів двовимірного простору кластера. В табл. 4.6 приведені усі симплекси, які можуть зазнати при цьому трансформацій.

Таблиця 4.6.

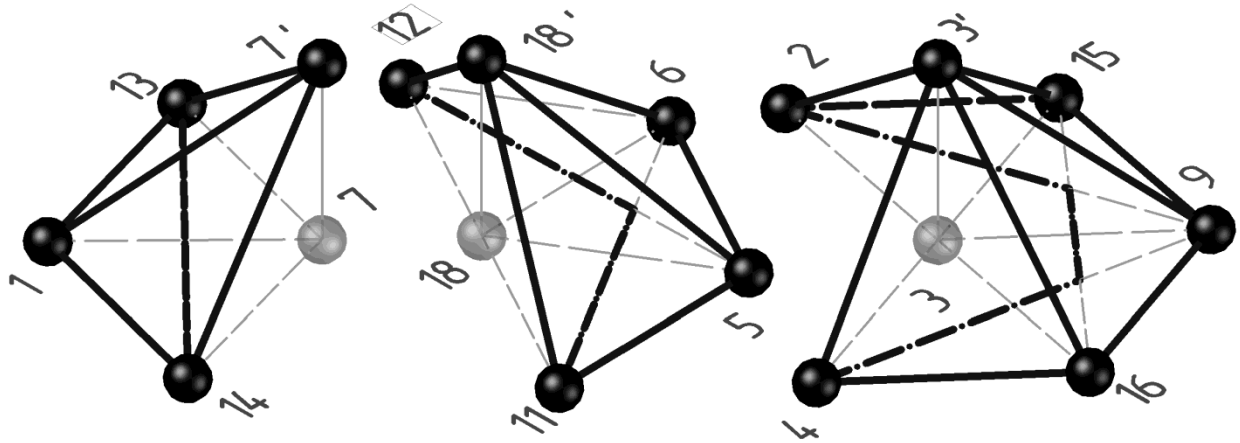
Трансформації симплексів, у яких зміни параметрів сигналів зазнали ІВ представлені СТ класу C_2

	C_{13}	C_{14}	C_{15}	C_{16}	C_{17}	C_{18}
ЧТр	${}^{7}_{13}[C]^{14}_{1}$	${}^{14}_{2}[C]^{8}_{15}$	${}^{15}_{3}[C]^{9}_{16}$	${}^{16}_{4}[C]^{10}_{17}$	${}^{17}_{5}[C]^{11}_{18}$	${}^{18}_{6}[C]^{12}_{13}$
	${}^{18}_{6}[C]^{12}_{13}$	${}^{7}_{13}[C]^{14}_{1}$	${}^{14}_{2}[C]^{8}_{15}$	${}^{15}_{3}[C]^{9}_{16}$	${}^{16}_{4}[C]^{10}_{17}$	${}^{17}_{5}[C]^{11}_{18}$
ПТр	${}^{13}_{6}[C]^{7}_{1}$	${}^{14}_{1}[C]^{8}_{2}$	${}^{15}_{2}[C]^{9}_{3}$	${}^{16}_{3}[C]^{10}_{4}$	${}^{17}_{4}[C]^{11}_{5}$	${}^{18}_{5}[C]^{12}_{6}$
	${}^{18}_{5}[C]^{12}_{6}$	${}^{7}_{1}[C]^{14}_{2}$	${}^{8}_{2}[C]^{15}_{3}$	${}^{9}_{3}[C]^{16}_{4}$	${}^{10}_{4}[C]^{17}_{5}$	${}^{11}_{5}[C]^{18}_{6}$

Нехай зміни параметрів зазнав сигнал ІВ, який у кластері представлений СТ C_{18}. Область трансформації складається із:

- множини СТ $C_{tr} = \{C_5;\ C_6;\ C_{11};\ C_{12};\ C_{13};\ C_{17};\ C_{18}\}$
- множини симплексів $S_{tr} = \{{}^{18}_{6}[C]^{12}_{13}; {}^{17}_{5}[C]^{11}_{18}; {}^{18}_{5}[C]^{12}_{6}; {}^{11}_{5}[C]^{18}_{6}\}$

Два симплекси ${}^{18}_{5}[C]^{12}_{6}$ і ${}^{11}_{5}[C]^{18}_{6}$ із повною трансформацією утворюють тривимірний геометричний об'єкт (рис.4.3 б), утворений перетином двох трикутних пірамід таким чином, що спільна вершина є зазначеною сигнальною точкою. В основі такого об'єкту знаходиться плоска геометрична фігура, яка на рисунку вказана перетином двох трикутників із вершинами в СТ C_{12}, C_6, C_5, C_{11}. Як і у попередньому випадку дві бічні грані є частинами двох бокових симплексів із частковою трансформацією.



а) б) в)

Рис. 4.3. Візуальне зображення областей повної трансформації за методом *[4C]*

Якщо зазнав змін параметр сигналу ІВ, який представлений СТ класу C_3, то в область трансформації попадуть п'ять симплексів(рис. 4.3 в). При цьому три симплекси отримують *(ПТр)*, а два, які в перетині з цими симплексами мають спільні геометричні складові отримують *(ЧТр)*. Інші 13 симплексів, які не входять в область трансформації, залишаються у вигляді первинних ромбів двовимірного простору кластера. В табл. 4.7 приведені усі симплекси, які можуть зазнати при цьому трансформацій.

Таблиця 4.7.

Трансформації кластерів, у яких зміни параметрів сигналів зазнали ІВ представлені СТ класу C_3.

	C_1	C_2	C_3	C_4	C_5	C_6
ЧТр	${}^{14}_{1}[C]^{8}_{2}$	${}^{15}_{2}[C]^{9}_{3}$	${}^{16}_{3}[C]^{10}_{4}$	${}^{17}_{4}[C]^{11}_{5}$	${}^{18}_{5}[C]^{12}_{6}$	${}^{18}_{6}[C]^{12}_{13}$
	${}^{12}_{6}[C]^{13}_{1}$	${}^{7}_{1}[C]^{14}_{2}$	${}^{8}_{2}[C]^{15}_{3}$	${}^{9}_{3}[C]^{16}_{4}$	${}^{10}_{4}[C]^{17}_{5}$	${}^{11}_{5}[C]^{18}_{6}$
ПТр	${}^{7}_{13}[C]^{14}_{1}$	${}^{14}_{2}[C]^{8}_{15}$	${}^{15}_{3}[C]^{9}_{16}$	${}^{16}_{4}[C]^{10}_{17}$	${}^{17}_{5}[C]^{11}_{18}$	${}^{18}_{6}[C]^{12}_{13}$
	${}^{13}_{6}[C]^{7}_{1}$	${}^{14}_{1}[C]^{8}_{2}$	${}^{15}_{2}[C]^{9}_{3}$	${}^{16}_{3}[C]^{10}_{4}$	${}^{17}_{4}[C]^{11}_{5}$	${}^{18}_{5}[C]^{12}_{6}$
	${}^{7}_{1}[C]^{14}_{2}$	${}^{8}_{2}[4C]^{15}_{3}$	${}^{9}_{3}[C]^{16}_{4}$	${}^{10}_{4}[4C]^{17}_{5}$	${}^{11}_{5}[C]^{18}_{6}$	${}^{12}_{6}[C]^{13}_{1}$

Нехай зміни параметрів зазнав сигнал ІВ, який у кластері представлений СТ C_3. Область трансформації складається із:

- множини СТ $C_{tr} = \{C_2;\ C_3;\ C_4;\ C_8;\ C_9;\ C_{10};\ C_{15};\ C_{16}\}$
- множини симплексів $S_{tr} = \{{}^{16}_{3}[C]^{10}_{4};\ {}^{8}_{2}[C]^{15}_{3};\ {}^{15}_{3}[C]^{9}_{16};\ {}^{15}_{2}[C]^{9}_{3};\ {}^{9}_{3}[C]^{16}_{4}\}$

Три симплекси ${}^{15}_{3}[C]^{9}_{16}$, ${}^{15}_{2}[C]^{9}_{3}$ і ${}^{9}_{3}[C]^{16}_{4}$ із повною трансформацією утворюють тривимірний геометричний об'єкт типу В (рис. 4.3 в), утворений перетином трьох трикутних пірамід таким чином, що спільна величина є зазначеною СТ C_3. В основі такого об'єкту знаходиться плоска геометрична фігура, яка на рисунку вказана перетином трьох трикутників із вершинами в сигнальних точках $C_2, C_{15}, C_9, C_{16}, C_4$. Фігура обмежена трьома геометричними зв'язками, які визначають відстані між СТ C_2 і C_9, C_{15} і C_{16}, C_9 і C_4. Два симплекси ${}^{3}_{16}[C]^{10}_{4}$ і ${}^{3}_{11}[C]^{8}_{2}$ частково трансформовані. В них деформованими є лише по одному трикутнику. Ці трикутники стають гранями повністю трансформованої геометричної тривимірної фігури із вершиною в СТ C_3.

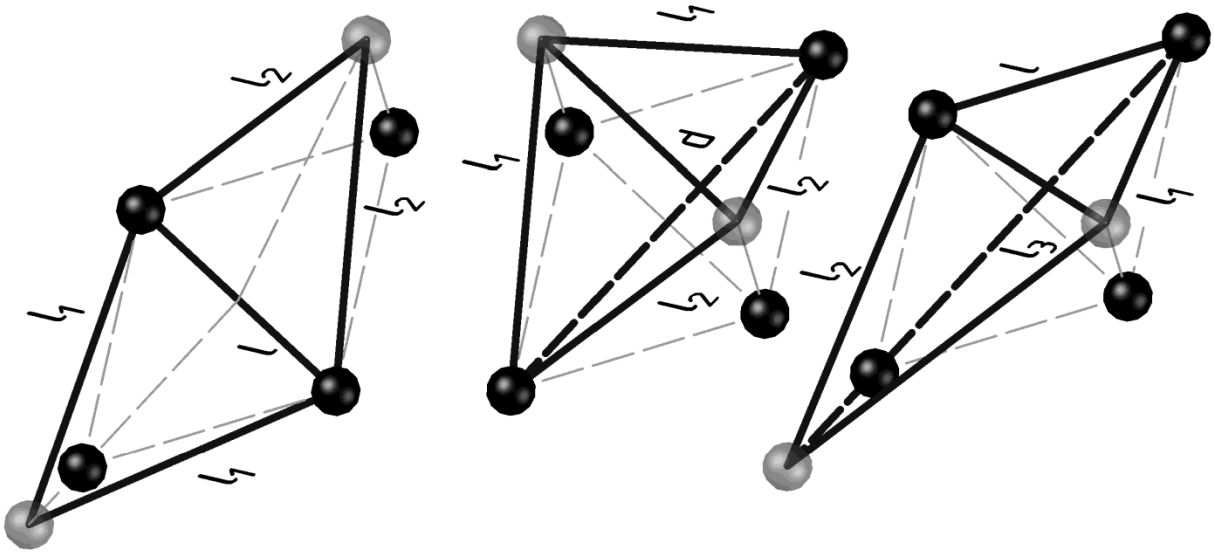
Якщо в кластері одночасно зазнають зміни параметри сигналів ІВ, які представлені СТ, що відносяться до різних класів, при цьому симплекси, до яких входять дані СТ не перетинаються і не дотикаються, наприклад СТ C_3, C_7 і C_{18}, то їх трансформацію можна розглядати одночасно. При цьому в області повної, часткової і нульової трансформації входять по шість симплексів.

4.3. Використання методу *[4C]* для візуалізації зміни параметрів сигналів двох ІВ

Якщо зміни параметрів зазнають одночасно сили сигналів двох ІВ представлених СТ в одному симплексі, можливими є трансформації при переміщенні СТ, які визначаються:

- двома ФЗ (рис. 4.4а);
- трьома ФЗ при розміщені СТ на кінцях малої діагоналі ромба, яка є також ФЗ (рис. 4.4б);
- трьома ФЗ для однієї СТ і двома ФЗ іншої при розміщенні СТ на кінцях однієї із сторін ромба (рис. 4.4в).

Для однозначного визначення області трансформації у приведених випадках доцільно використовувати методи візуалізації розглянуті нижче.



а) б) в)

Рис. 4.4. Типи трансформації симплекса при одночасній змінні параметрів сигналів двох ІВ

Якщо зміни параметрів сигналів зазнали одночасно два ІВ, СТ C_{13} і C_{18} яких знаходяться на серединах двох сусідніх сторін зовнішнього обвідного шестикутника кластера (рис. 4.5а) область трансформації складається із:
множини СТ $C_{tr} = \{C_1;\ C_5;\ C_6;\ C_7;\ C_9;\ C_{11};\ C_{12};\ C_{13};C_{14};\ C_{17};\ C_{18}\}$ і множини симплексів $S_{tr} = \{{}^{17}_{5}[C]^{11}_{18}; {}^{18}_{5}[C]^{12}_{6}; {}^{12}_{6}[C]^{13}_{1}; {}^{7}_{13}[C]^{14}_{1}; {}^{11}_{5}[C]^{18}_{6}; {}^{13}_{6}[C]^{7}_{1}\}$

Область повної трансформації складається із двох симплексів ${}^{17}_{5}[C]^{11}_{18}$ і ${}^{13}_{6}[C]^{7}_{1}$. Вони візуально утворюють дві трикутні піраміди типу а (рис. 4.5 а) з вершинами у двох СТ C_{13} і C_{18}, які і визначатимуть однозначно два ІВ, параметри сигналів, яких зазнали одночасно змін.

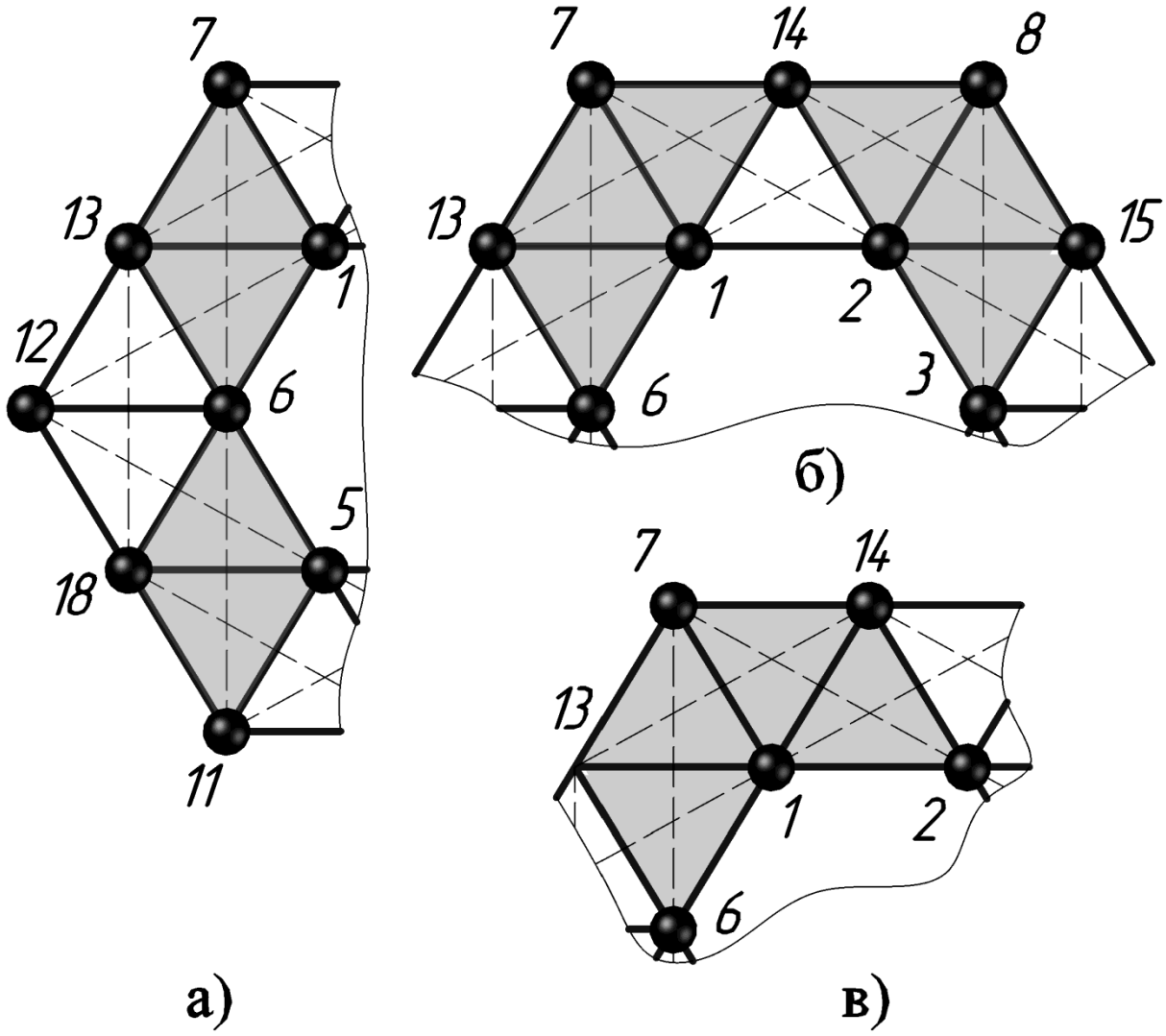


Рис. 4.5. Області повної трансформації кластера при одночасній зміні параметрів сигналів двох ІВ

Якщо зміни параметрів сигналів зазнали одночасно два ІВ, СТ яких знаходяться у кластері на сусідніх вершинах внутрішнього шестикутника, наприклад

C_1 і C_2, (рис. 4.5б), то область повної трансформації подібна до трансформації у випадку зміни параметрів сигналу одного ІВ, представленого СТ класу C_3. Область трансформації складається із:

- множини СТ $C_{tr} = \{C_1;\ C_2;\ C_3;\ C_5;\ C_6;\ C_7;\ C_8;\ C_{12};C_{13};\ C_{14};\ C_{15}\}$
- і множини симплексів $S_{tr} = \{{}_6^{12}[C]_1^{13}; {}_{13}^{7}[C]_1^{14}; {}_1^{7}[C]_2^{14}; {}_2^{14}[C]_{15}^{8}; {}_2^{15}[C]_3^{9}; {}_1^{14}[C]_2^{8}; {}_6^{13}[C]_1^{7}; {}_2^{8}[C]_3^{15}\}$
- Область повної трансформації складається із двох пар симплексів ${}_6^{13}[C]_1^{7}; {}_{13}^{7}[C]_1^{14}; {}_2^{14}[C]_{15}^{8}; {}_2^{8}[C]_3^{15}$. Вони здійснюють візуалізацію двох вказаних ІВ шляхом визначення двох зображень (рис. 4.5в) з вершинами у СТ C_1 і C_2.

В цьому випадку симплекс ${}_1^{7}[C]_2^{14}$ однозначно здійснює візуалізацію зміни параметрів сигналу ІВ представленого у кластері СТ C_1, а симплекс ${}_6^{13}[C]_1^{7}$ здійснює візуалізацію зміни параметрів сигналу ІВ представленого у кластері СТ C_{13}.

4.4. Метод фіктивних сигнальних точок (метод ФСТ)

Під час геометричного моделювання БСМ особливо важливим є одержання можливості однозначного визначення області повної трансформації кластера при зміні параметрів ІВ. Метод фіктивних сигнальних точок (ФСТ) дозволяє вирішити дане завдання, якщо одночасної зміни зазнали параметри сигналів кількох ІВ, СТ яких розміщені в одному кластері. В основу методу ФСТ покладено припущення, що у кластері, який здійснює візуалізацію нормальної роботи ІВ в результаті зміни параметрів сигналів відповідні ФЗ отримають видовження. В кінці видовження утворюється нове фіктивне положення сигнальної точки, яка в кластері представляє ІВ параметри сигналу, якого зазнали змін. Здійснивши такі ж самі видовження із іншими ФЗ, які з'єднують СТ із сусідніми СТ отримують наступні області повної трансформації (рис. 4.6):

- три фіктивні СТ, якщо СТ належить класу C_3;
- чотири фіктивних СТ, якщо СТ належать класу C_2;
- п'ять фіктивних СТ, якщо СТ належать класу C_1.

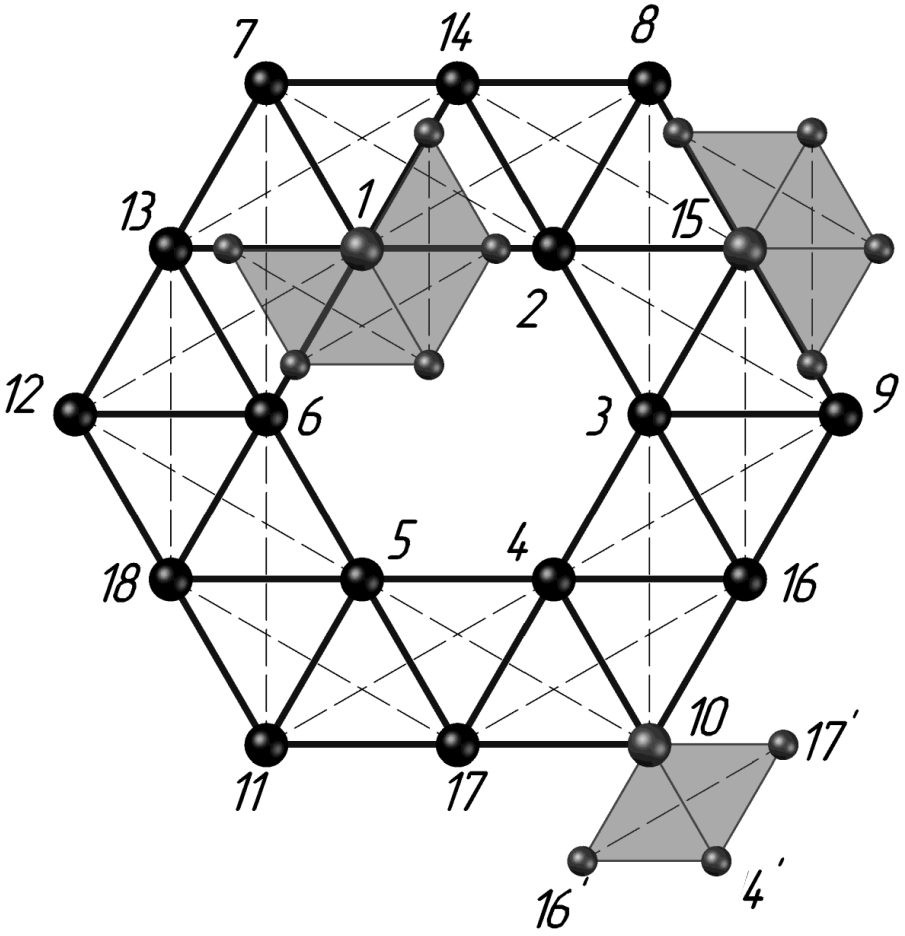
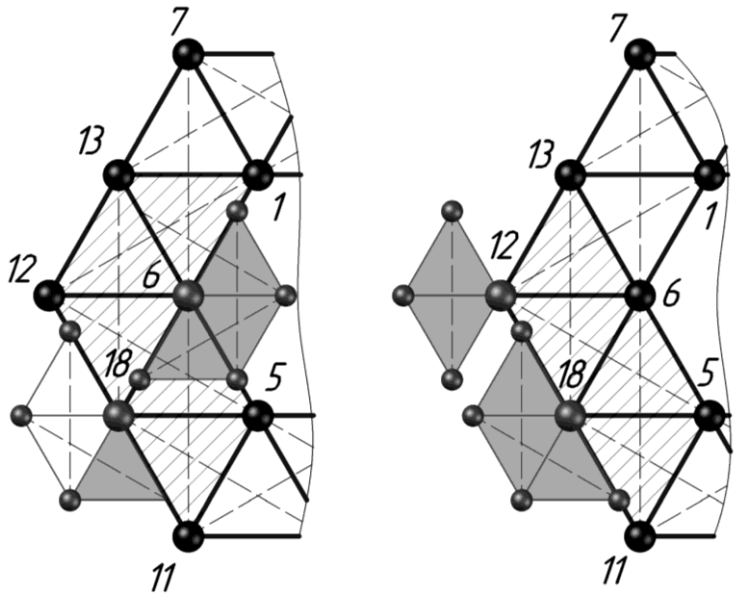


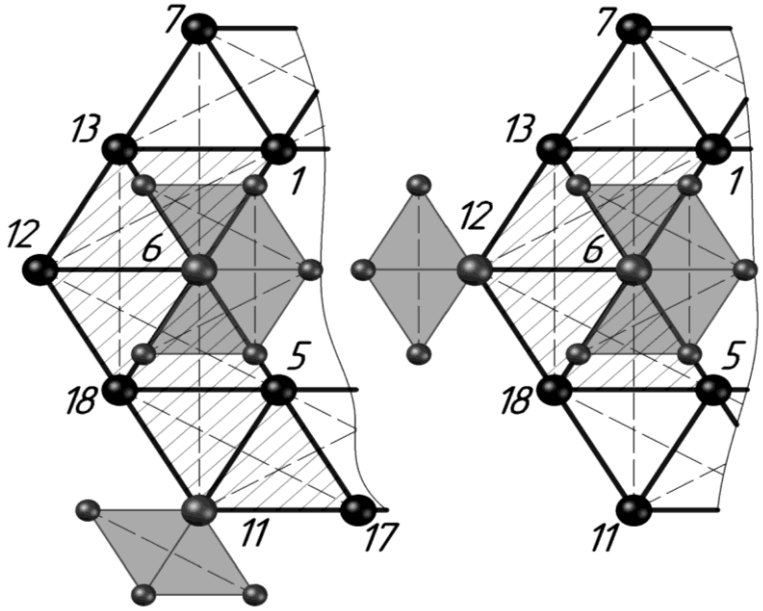
Рис. 4.6. Області повної трансформації за методом ФСТ

З’єднавши фіктивні СТ між собою із місцем розміщення СТ при стабільній роботі ІВ, отримують плоский геометричний об’єкт, який зі симетрією відносно початкового положення СТ відображає структуру області повної трансформації в кластері при зміні параметрів сигналів ІВ. Спроба з’єднати ФСТ в одну точку призводить до переміщення СТ, які представляють ІВ зі зміненими параметрами сигналів, у третій вимір і створення візуалізації тримірних геометричних об’єктів, які досліджувались метод *[С]* .

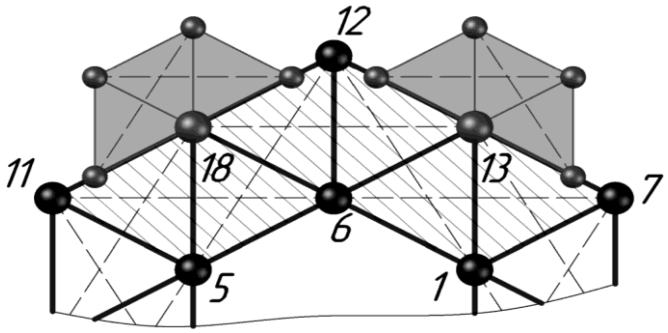
На рис. 4.7 показано деякі приклади повної трансформації при одночасній змін параметрів сигналів двох ІВ одного кластера: на рис. 4.7а представлено зміну параметрів сигналів двох ІВ, СТ яких знаходяться у вершині внутрішнього шестикутника і в середині сторони зовнішнього шестикутника; на рис. 4.7б зображено зміну параметрів сигналів ІВ, СТ яких знаходяться у вершині і середині зовнішнього шестикутника; на рис. 4.7в та 4.7г, з ілюстровано зміну параметрів сигналів ІВ, СТ яких знаходяться у вершинах зовнішнього та внутрішнього шестикутника; на рис. 4.7д представлено зміну параметрів сигналів ІВ, СТ яких знаходяться у серединах двох сусідніх сторін зовнішнього шестикутника.



а)



б)



в)

Рис. 4.7. Приклади використання методу ФСТ при зміні параметрів сигналів двох ІВ одного симплекса

4.5. Метод еталонних сигнальних точок (ЕСТ)

Запропоновані вище методи візуалізації процесів зміни параметрів сигналів ІВ розраховані для моделювання БСМ з ІВ яких можливо сформувати хоча б один повний кластер. Для візуалізації БСМ з обмеженою кількістю ІВ (>18) доцільно використовувати метод ЕСТ.

Метод еталонних сигнальних точок полягає в тому, що на першому етапі у *[C]* симплексі всі ФЗ визначаються одними і тими ж параметрами еталонного ІВ (ЕС). Таким чином утворюється симплекс із п'ятьма рівними ФЗ довжиною l і одним геометричним зв'язком, довжиною $d = \sqrt{3}l$. Такий *[C]* має форму ромба. Параметри підозрілого на зміну параметрів сигналу ІВ подаються у положення *[C]*, яке визначається трьома ФЗ (СТ малої діагоналі ромба).

Видовження трьох ФЗ спричинить трансформацію плоского *[C]* у тривимірний *[C]* у формі трикутної піраміди із вершиною у СТ, що визначає ІВ параметри сигналу, якого зазнали змін. Висота піраміди h, в цьому випадку, буде характеризувати ступінь зміни параметру сигналу ІВ (рис. 4.8).

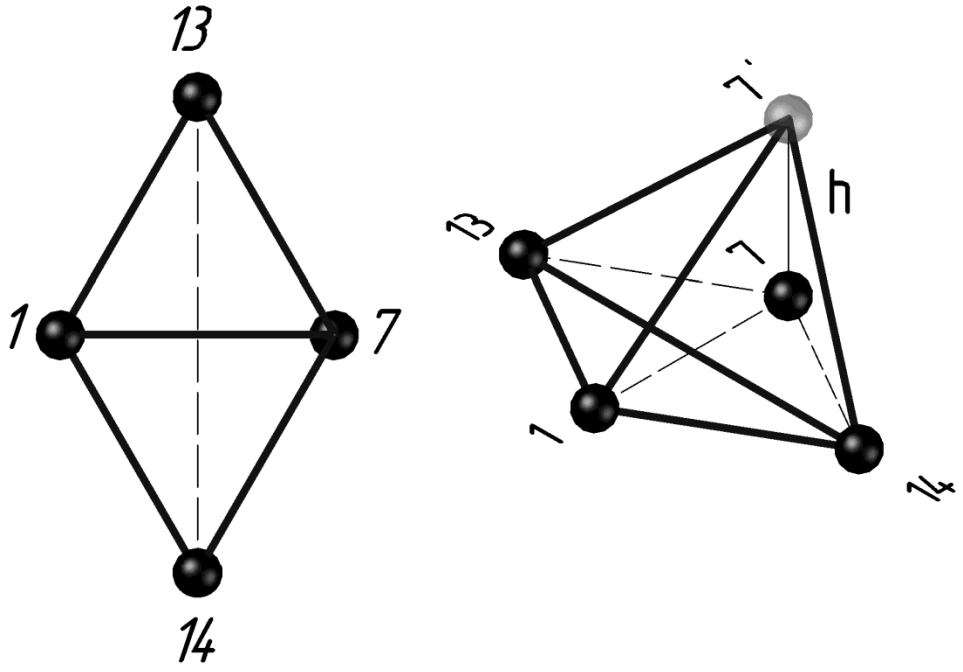


Рис. 4.8. Одинарний досліджуваний симплекс

Якщо внаслідок зміни параметрів сигналів кількох ІВ (на рисунку позначені *"e"*) утворюється область *ПТр*, то доцільно параметри кожного ІВ цієї області дослідити за допомогою такого еталонного ІВ. У цьому випадку можна утворити дослідницькі кластери, які складаються із двох, чотирьох, восьми,

шістнадцяти *[C]* , кожний з яких визначається трьома СТ, що перебувають у стані спокою. Четверта СТ кожного *[C]* буде давати характеристику величині зміни параметра сигналу ІВ (рис. 4.9, 4.10).

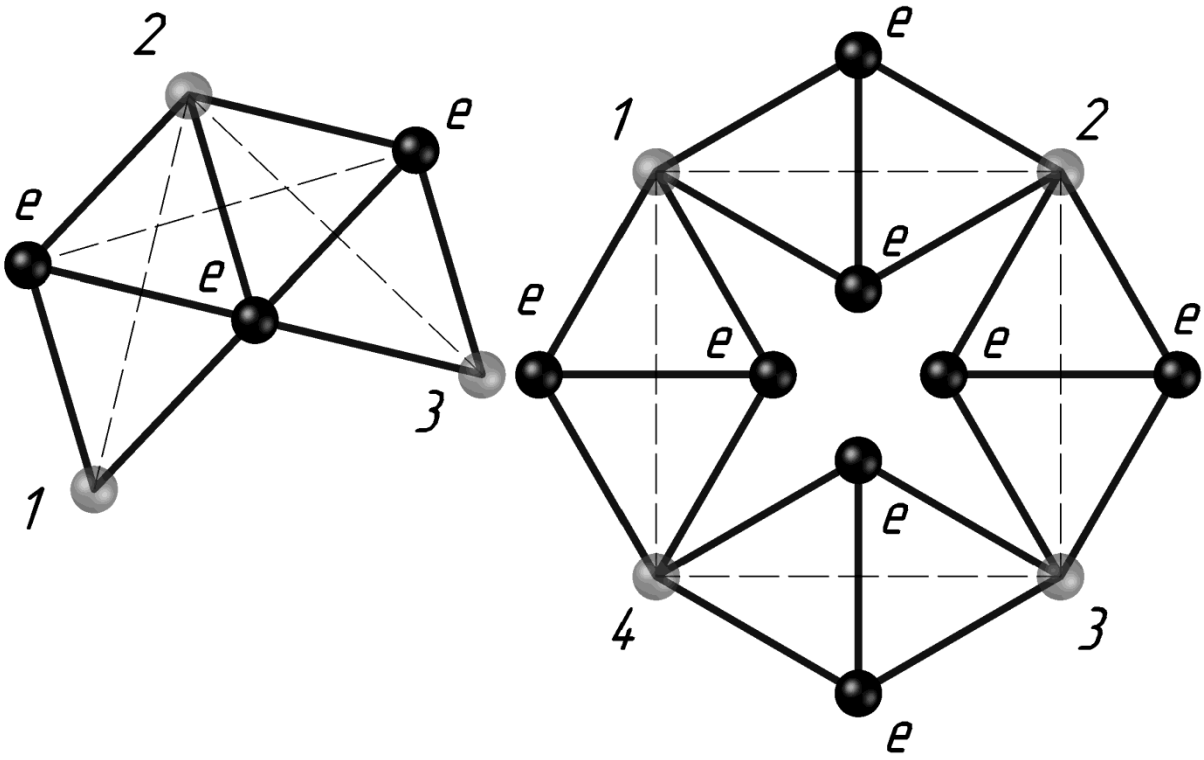


Рис. 4.9. Досліджувані кластери із двох і чотирьох *[C]*

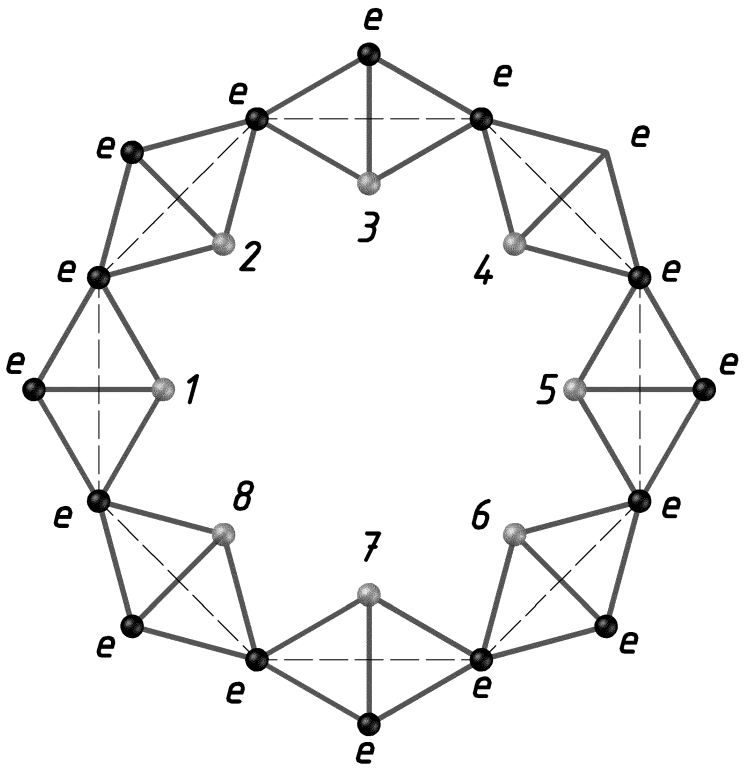


Рис. 4.10. Досліджувані кластери із восьми *[C]*

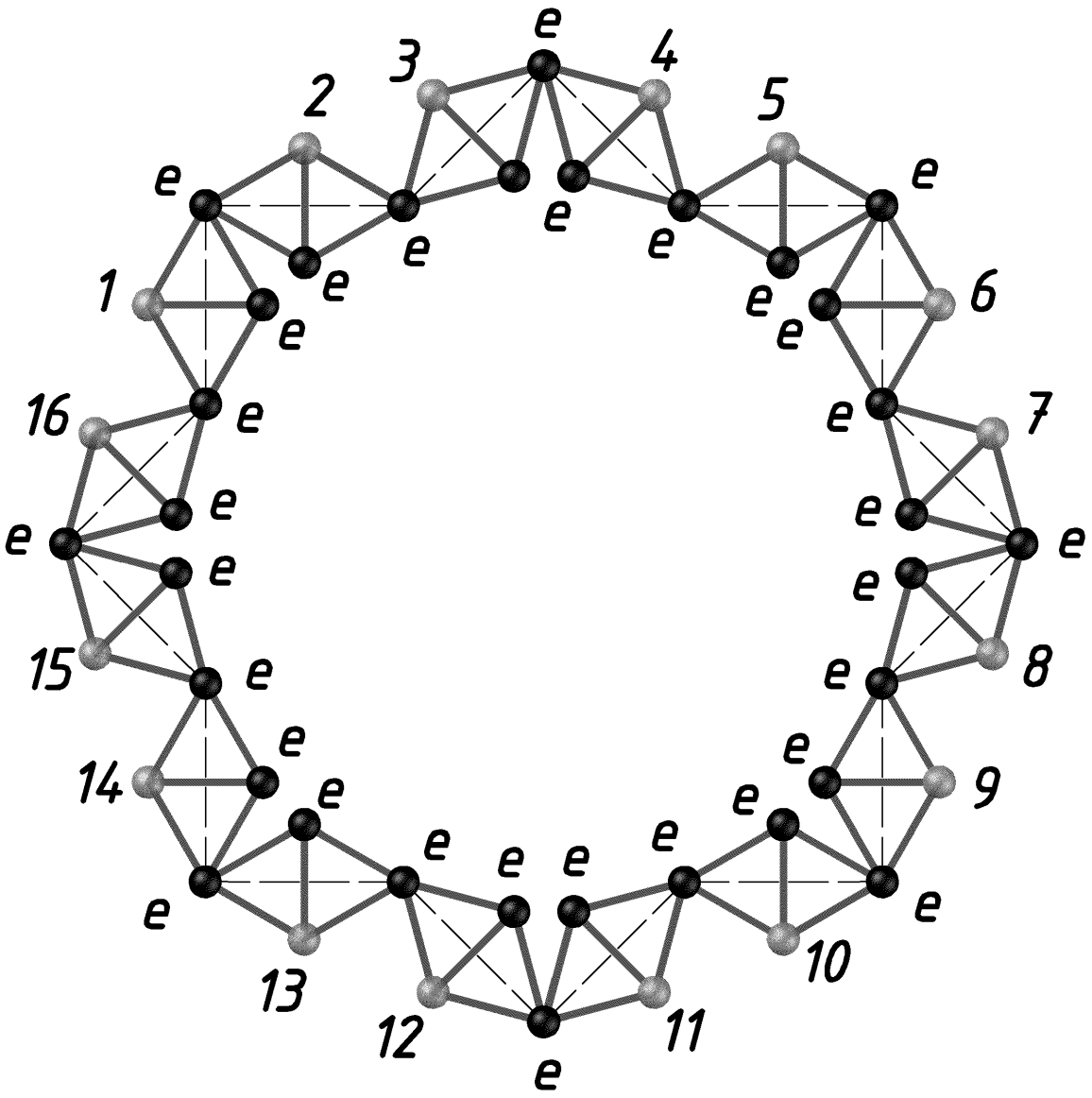
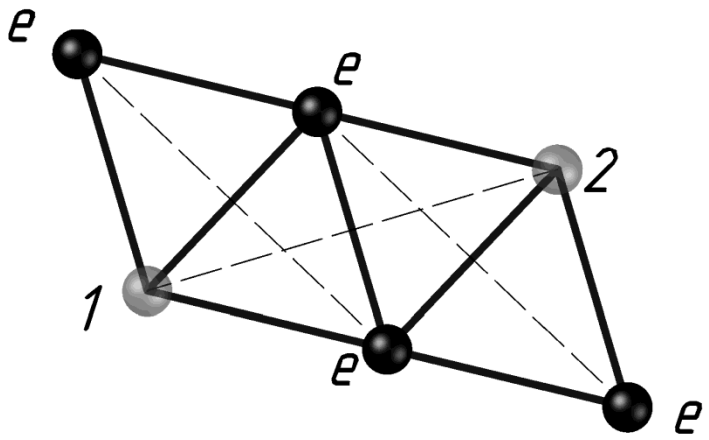
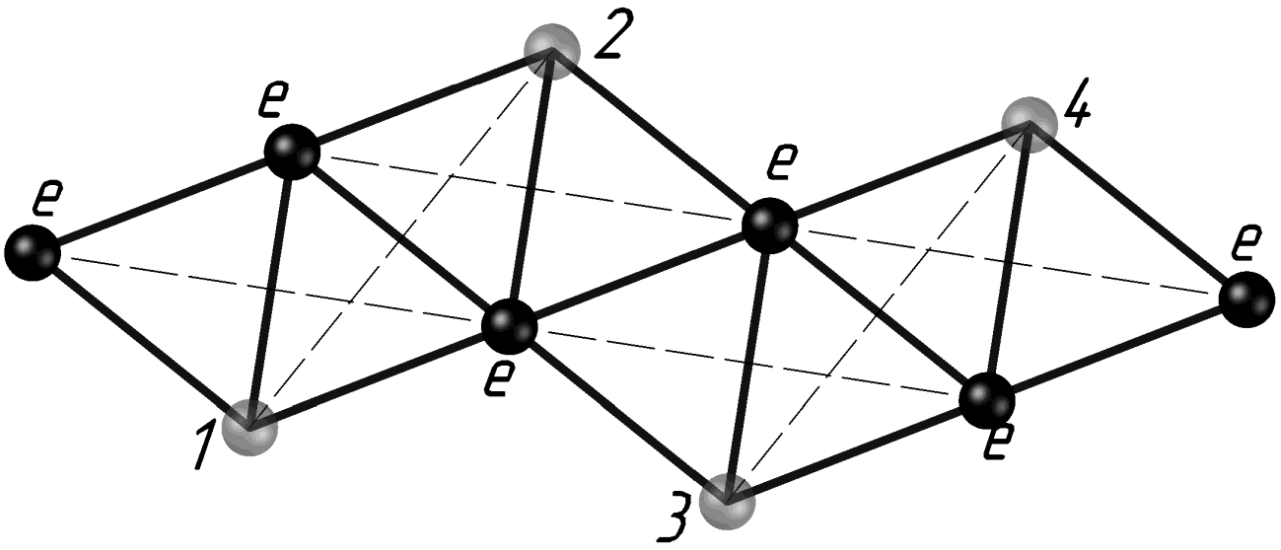


Рис. 4.11. Досліджувані кластери із шістнадцяти *[C]*

Можливі також комбінації кластерів із більшої кількості симплексів (рис. 4.12)



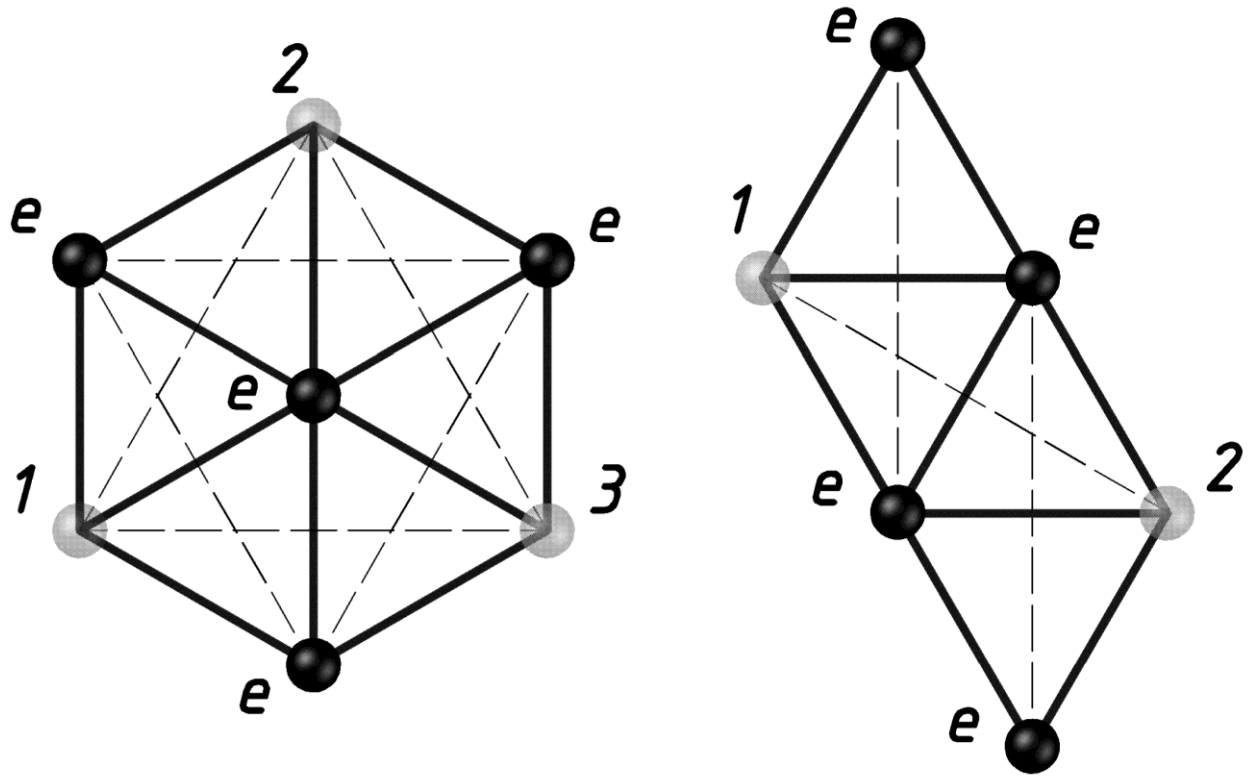
а)



б)

Рис. 4.12. Комбіновані досліджувані кластери

У розглянутих досліджуваних кластерах на один ІВ зі зміненими параметрами сигналу припадає два еталонних ІВ. Тому, з метою зменшення кількості еталонних ІВ, є можливість утворити інші типи кластерів, у яких крім утворення трикутних пірамід виникають інші тримірні симплекси у вигляді зігнутих по спільній стороні двох трикутників. Цілком зрозуміло, що об’єми таких тримірних симплексів дорівнюють нулю. Визначення геометричного зв’язку таких симплексів приводить до їх розгортки у плоский чотирикутник. На рис. 4.13 зображено два дослідні кластери, які складаються з семи (рис. 4.13а) та шести (рис. 4.13б) СТ. на три досліджуванні ІВ у першому випадку і два досліджувані ІВ у другому випадку, припадає чотири еталонні ІВ.



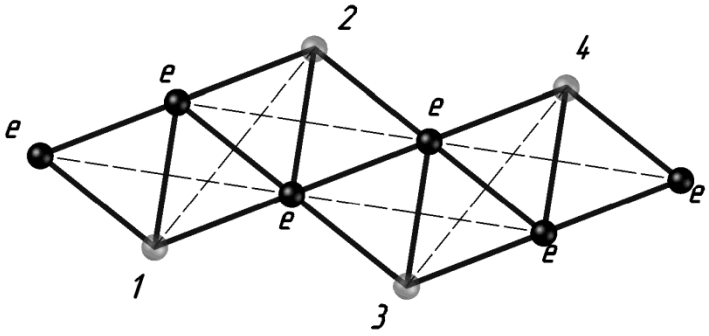
а) б)

Рис. 4.13. Досліджувані кластери з чотирма та шістьма еталонними ІВ

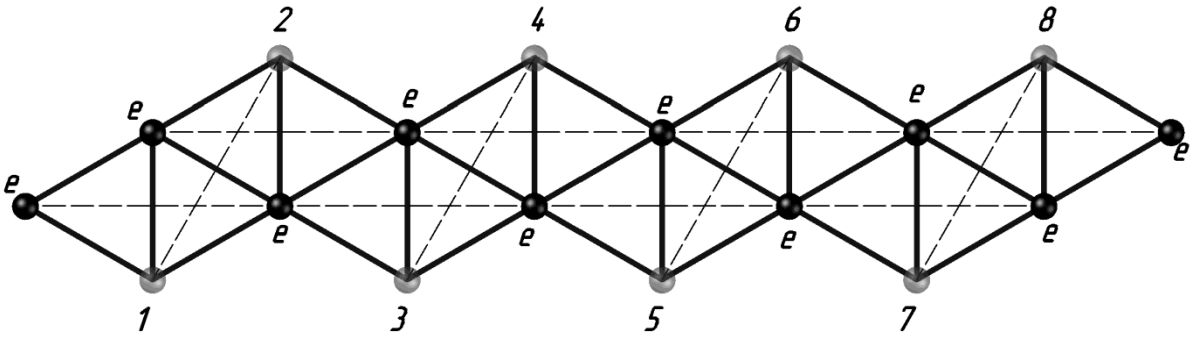
Наведені кластери дають можливість формувати складніші кластерні структури, в яких відбувається значне зменшення кількості еталонних ІВ. На рис. 4.14 показано кластерні структури для дослідження чотирьох (рис. 4.14а) та восьми (рис. 4.14б) ІВ.

Аналіз проведених досліджень дозволяє зробити висновок, що блок кластерної структури (рис. 4.14а) дає можливість формувати більш складні кластерні структури, в яких відбувається зменшення кількості еталонних ІВ на один досліджуваний ІВ. Послідовність відношень кількості еталонних ІВ до кількості досліджуваних ІВ має вигляд:

$$\frac{4}{2}=2;\ \frac{6}{4}=1{,}5;\ \frac{8}{6}=1{,}33;\ \frac{10}{8}=1{,}25;\ \ldots;\ \frac{2(n+1)}{2n};\qquad (4.1)$$



а)



б)

Рис. 4.14. Кластерні структури більш складних типів

Збільшуючи кількість початкових блоків (рис. 4.13а) до n в границі отримуємо одиницю:

$$\lim_{n\to\infty}\frac{2(n+1)}{2n}=\lim_{n\to\infty}\left(1+\frac{1}{n}\right)=1 \qquad (4.2)$$

Ефективність використання запропонованого методу візуалізації БСМ зростає зі збільшенням кількості ІВ, що піддаються контролю, оскільки при цьому відношення кількості еталонних ІВ до кількості контрольованих ІВ прямує до одиниці.

4.6. Оцінювання параметрів, які характеризують пошкодження сигналу ІВ

Характер змін у кластері, які спричинені тим, що ІВ перестає працювати у нормальному режимі, дає можливість визначити ступінь зміни параметрів його сигналу.

Відмінність від нуля об’єму і висоти симплекса, а також, утворення симплекса з відмінним від нуля об’ємом, вказує на те, що ІВ перестає працювати у нормальному режимі, тобто $\beta\neq 0$. Виникає можливість робити оцінювання

зміни параметрів сигналів ІВ за цими значеннями. Для початку приймають довжину l_0, яка відповідає шумовому сигналу $l_0 = l(\omega)$, за масштабну одиницю $(\,|\, l_0 = 1 \,|\,)$, що дає можливість, не втрачаючи інформативність, спростити викладки.

Квадрат об'єму трикутної піраміди в цьому випадку дорівнює:

$$(V_C^{\,2})_3 = -\frac{\Delta_3(C)}{288} \tag{4.3}$$

де $\Delta_3(C) = -6(2\alpha+1)^4\beta(\beta+4\alpha+2)$. (4.4)

Для знаходження висоти тримірного симплекса використовують подані вище залежності і одержують:

$$h = \frac{3(V_C)_3}{S_{осн}} = \frac{12(V_C)_3}{\sqrt{3}(2\alpha+1)^2} \tag{4.5}$$

$$\text{або } h^2 = -\frac{48(V_C^2)_3}{(2\alpha+1)^4} = -\frac{\Delta_3(C)}{6(2\alpha+1)^4} \tag{4.6}$$

Таким чином, отримуємо:

$$\Delta_3(C) = -6(2\alpha+1)^4\beta(\beta+4\alpha+2) \tag{4.7}$$

$$\text{і } \Delta_3(C) = -6h^2(2\alpha+1)^4, \tag{4.8}$$

$$\text{звідки } h^2 = \beta(\beta+4\alpha+2), \tag{4.9}$$

де $\alpha = \frac{1}{2}\left(\frac{l}{l_0}-1\right) > 0$ - коефіцієнт, який визначає, у скільки разів відрізняється відрізок, що характеризує сигнал Ω, від відрізка визначеного шумовим сигналом ω.

Отримання від'ємних значень h^2 і $(V_C^2)_3$ для від'ємних значень параметра β показує, що у випадку приглушення роботи ІВ атакуючим сигналом ($\beta < 0$) 4С стає уявним із уявними об'ємом і висотою. Тому додатне значення визначника Келі-Менгера характеризує приглушення ІВ атакуючим сигналом, а від'ємне значення – його підсилення. При видовженні ФЗ симплекс стає трикутною пірамідою із об'ємом $(V_C)_3$ і висотою h. При зменшенні ФЗ ($\beta < 0$) в комп'ютерній візуалізації можемо користуватися величиною $\Delta_3(C) = 6\,|h^2|(2\alpha+1)^4 > 0$, взявши при цьому $|h^2| = |\beta(\beta+4\alpha+2)|$ і здійснити

від'ємне локальне викривлення геометрії кластера, яке представимо заглибленнями навколо відповідної СТ із його максимальним значенням у цій точці. Зрозуміло, що в цьому випадку отримується штучно створена трикутна піраміда, в якої ребра при висоті не дорівнюють l_1, але основа такої піраміди така ж, а висота характеризує ступінь зміни параметру сигналу ІВ.

Зробивши довжину l_0, яка відповідає шумовому сигналу $l_0 = l(\omega)$, масштабною одиницею $(|l_0| = 1)$ і, враховуючи, що параметр β може набувати від'ємних, нульових і додатніх значень, записують отримані залежності у вигляді:

$h^2 = h(\beta)$і $(V_C^2)_3 = V(\beta)$:

$$(V_C^2)_3 = \eta\beta(\beta + 4\alpha + 2) \tag{4.10}$$

де $48\eta = (2\alpha + 1)^4$.

Для оцінювання рівня пошкодження сигналу окремого ІВ введемо чисельний коефіцієнт $\lambda = \lambda(\beta)$, який не має геометричного змісту, але характеризує стан змін у роботі ІВ. Враховуючи, що мінімальне значення β отримуємо при повному руйнуванні сигналу ІВ ($\beta = -\alpha$), будемо розглядати залежність $\lambda = \lambda(\beta)$ лише для $\beta \geq -\alpha$. Нехай ця залежність визначається співвідношенням, за яким коефіцієнт λ може бути від'ємним, додатним і дорівнювати нулю:

$$\lambda = \begin{cases} -\sqrt{|\beta(\beta + 4\alpha + 2)|} < 0, & -\alpha \leq \beta < 0, \\ 0, & \beta = 0, \\ \sqrt{\beta(\beta + 4\alpha + 2)} > 0, & \beta > 0. \end{cases} \tag{4.11}$$

Для мінімального значення $\beta = -\alpha$ отримуємо мінімальне значення

$$\lambda_{min} = -\sqrt{\alpha(3\alpha + 2)} \tag{4.12}$$

абсолютне значення якого вказує висоту штучно створеного тривимірного симплекса при повному руйнуванні сигналу ІВ атакованим сигналом.

Якщо, наприклад, нормальна робота ІВ визначається коефіцієнтом $\alpha = 10$, то отримаємо графік залежності, на якому по горизонтальній осі відкладено значення параметра сигналу атаки, а по вертикалі – коефіцієнт $\lambda = \lambda(\beta)$ (рис. 4.15).

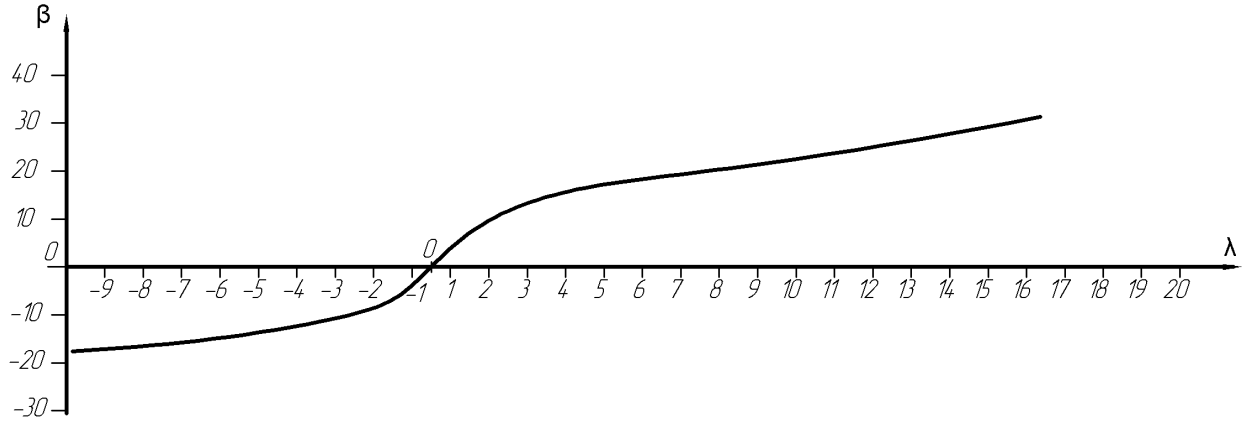


Рис. 4.15. Графік залежності $\lambda = \lambda(\beta)$

Для зручності візуального й чисельного оцінювання ступеня атаки на сигнал ІВ доцільно розглядати карту кластера у вигляді квадратної матриці D вісімнадцятого порядку, в якої стовпці і рядки є нечисловими характеристиками кластера: стовпці визначають $[C]$, а рядки – сигнальні точки. Елементами матриці будуть числові оцінювальні характеристики ступенів атак на сигнали ІВ, яким відповідають СТ кластера. Порожні клітинки визначають симплекси і сигнальні точки, які не задіяні в структурних змінах геометрії кластера. Клітинки з нулем визначають симплекси, трансформація яких здійснюється в межах двовимірного ЕКП.

$D =$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
R1	λ						λ						0	0				
R2		λ						λ						0	0			
R3			λ						λ						0	0		
R4				λ						λ						0	0	
R5					λ						λ						0	0
R6						λ						λ	0					0
R7	λ						0						λ					
R8	0	λ						0						λ				
R9		0	λ						0						λ			
R10			0	λ						0						λ		
R11				0	λ						0						λ	
R12					0	λ						0						λ
R13	λ	0				0	0							λ				
R14		λ	0					0							λ			
R15			λ	0					0							λ		
R16				λ	0					0							λ	
R17					λ	0					0							λ
R18	0					λ						0	λ					

Параметр λ якісно вказує на C, які трансформуються у тривимірний або в уявний симплекс. Кількісно параметр λ визначатиме значення параметру і характер атаки на сигнали ІВ (приглушення $(\lambda < 0)$ або підсилення $(\lambda > 0)$) за формулою

$$\lambda = \begin{cases} -h, & -\alpha \le \beta < 0, \\ 0, & \beta = 0, \\ h, & \beta > 0, \end{cases} \tag{4.13}$$

де $h = \dfrac{3V}{S_{осн}}$, $V = \begin{cases} \sqrt{|V_C^2|}, & -\alpha \le \beta < 0, \\ 0, & \beta = 0, \\ V_C & \beta > 0, \end{cases}$ $S_{осн} = \dfrac{S_C}{2} = \dfrac{\sqrt{3}}{4} l^2$

Література

1. Таненбаум Э. Компьютерные сети: Классика Computer Science / Э. Таненбаум, Д. Уэзеролл. – 5-те вид.,- М.: Питер, 2012. – 960с. – ISBN 978-5-459-00342-0.
2. Еркин А. Разработка распределенных систем контроля датчиков на основе защищенных низкопотребляющих беспроводных ZigBee-сетей на базе микроконтроллеров фирмы Jennic: [Электронный ресурс] / А. Еркин // Chipnews – 2010. – №1 – С. 1 – 9 – Режим доступу: http://chip-news.ru/ archive/ chipnews/ 201001/ZigBee.pdf – Назва з екрану.
3. Kurytnik I.P. Problems with Massive Data Storage in cardiac event monitoring using microcontroller dsPIC / I.P. Kurytnik, B. Borowik, W. Karpiński // Electrical Review. – 2009. – № 4. – P. 4 – 6. – ISSN 0033-2097.
4. Kurytnik I.P. Problems with Massive Data Storage in cardiac event monitoring using microcontroller dsPIC / I.P. Kurytnik, B. Borowik, W. Karpiński // Computational Problems of Electrical Engineering : 9th International Workshop CPEE'08, September 16-20, 2008. : Proceedings of Workshop. – Alushta (Crimea), Ukraine, 2008. – P. 130 – 132.
5. ZigBee Sensor Network for controlling the lightening system / B. Borowik, I.P. Kurytnik, B. Borowik, V. Karpinskyi // Knowledge in Telecommunication Technologies and Optics : 11th International Conference KTTO 2011, June 22nd - 24th 2011 : Proceedings of the 11th International Conference. – Szczyrk, Poland: Publisher VSB-Technical University of Ostrava, Czech Rebublic, 2011. – P. 117 – 120. – ISBN 978-80-248-2399-7.
6. Ермошкина Д.Д. Классификация беспроводных сенсорных сетей по видам нагрузки: [Електронний ресурс] / Д.Д. Ермошкина, А.Е. Кучерявый // T-Comm - Телекоммуникации и Транспорт. – 2011. – № 7. – С. 64 – 65. – Режим доступу до журн.: http://cyberleninka.ru/article/n/klassifikatsiya-besprovodnyh-sensornyh-setey-po-vidam-nagruzki – Назва з екрану.
7. Міночкін А.І. Методологія управління тактичними сенсорними мережами / А.І. Міночкін, В.А. Романюк // IV Науково-технічна конференція ВІТІ «Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення». – К.: ВІТІ НТУУ «КПІ», 2008. – С. 15 – 25.
8. Zheng J. Will 802.15.4 Make Ubiquitous Networking a Realisty?: A Discussion on a Potential Low Power, Low Bit Rate Standard / J. Zheng, M.J. Lee // IEEE

Communications Magazine. – 2004. – Vol. 42, Issue 6. – P. 140 – 146. – ISSN 0163-6804.

9. Зеляновський М.Ю. Математичні моделі для спеціалізованих та сенсорних мереж безпроводового доступу / М.Ю. Зеляновський, О.В. Тимченко // Моделювання та інформ. технології: зб. наук. пр. / НАН України, Ін-т пробл. моделювання в енергетиці. К., 2009. – Вип. 50. С. 192 – 200. Бібліогр.: 6 назв.
10. Баскаков С.С Беспроводные сенсорные сети на базе платформы MeshLogic / С.С. Баскаков , В.И. Оганов // Электронные компоненты. – 2006. – № 8. – С. 65 – 69.
11. Рагозин, Д.В. Моделирование синхронизированных сенсорных сетей / Д.В. Рагозин // Пробл. програмув. – 2008. – № 2-3. – С. 721 – 729. Текст: рос. – Бібліогр.: 12 назв.
12. Аникин А. Обзор современных технологий беспроводной передачи данных в частотных диапазонах ISM (Bluetooth, ZigBee, Wi-Fi) и 434/868 МГц [Електронний ресурс] / А. Аникин // Беспроводные технологии. – 2011. – № 4. – С. 6 – 12. – Режим доступу до журн.: http://www.wireless-e.ru/articles/technologies/2011_4_6.php – Назва з екрану.
13. Dragoş I. Săcăleanu Increasing lifetime in grid wireless sensor networks through routing algorithm and data aggregation techniques / Dragoş I. Săcăleanu, Dragoş M. Ofrim, Rodica Stoian, Vasile Lăzărescu // International Journal of Communications. – 2011. – Issue 4.: Volume 5. – P. 157 – 164.
14. В.А. Мочалов Стратегии размещения узлов сенсорной сети / Мочалов В.А., Турута Е.Н.; Московский технический университет связи и информатики // Материалы VII Международной научно-технической конференции. – М.: INTERMATIC, 23-27 ноября 2010 г. С.2 11 – 216.
15. Ishizuka M. Performance study of node placement in sensor networks / M. Ishizuka, M. Aida // 24th International Conference on Distributed Computing Systems Workshops. – Tokyo, 2004. – P. 598 – 603.: ISBN: 0-7695-2087-1.
16. Бунин С.Г. Перспективы беспроводных ячеистых сетей / С.Г. Бунин, А.И. Миночкин, В.А. Романюк // Зв'язок. – 2007. – № 5. – С. 20 – 24. – Режим доступу до журн.: http://viti.edu.ua/files/rom/2007/1_2007.pdf – Назва з екрану.
17. Романюк В.А. Мобільні радіомережі (manet) – Основа побудови тактичних мереж зв'язку / В.А. Романюк // Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення: Четверта науково-

технічна конференція, 22 листопада 2007 р.: доповіді та тези доповідей К.: "КПІ", 2007 р. – С. 15 – 28.

18. Плахтеев А.П. Моделирование и исследование процессов взаимодействия элементов беспроводных сенсорных сетей / А.П. Плахтеев, П.А. Плахтеев. // Радіоелектронні і комп'ютерні системи. –Х., 2010. № 6 (47). С. 20 – 24.
19. Карпінський В.П. Методи та апаратно-програмні засоби моделювання відбору інформації в безпровідних мережах давачів систем електропостачання: автореф. дис. на здобуття наук. ступеня канд. техн. наук: спец. 05.01.05 «Математичне моделювання» / Карпінський Володимир Петрович; Тернопіль. нац. техн. ун-т ім. Івана Пулюя. – Тернопіль, 2010. – 20 с.
20. Дорошенко, А.Е. О моделировании сенсорних сетей средствами високого уровня / А.Е. Дорошенко, К.А Жереб, Р.С. Шевченко // Проблеми програмування: Матеріали п'ятої Міжнар. наук.-практ. конф. з програмування Укр. ПРОГ 2006, м. Київ, 23-25 трав. 2006 р. – К.: НАН України. Ін-т програмних систем, 2006. – № 2-3. – С. 718 – 727. – ISSN 1727-4907.
21. Карпінський В.М. Теоретико-графовий підхід до моделювання розподілених безпровідних сенсорних мереж / В.М. Карпінський, П.С. Євтух, Я.І. Кінах // Вісник НТУУ “КПІ”. Інформатика, управління та обчислювальна техніка. – 2010. – № 52. – С. 27 – 32. – ISSN 0135-1729.
22. Голембо В. Аналіз способів організації переміщення мобільних вимірювальних агентів / В. Голембо, О. Бочкарьов, О. Кусьпісь // Вимірювальна техніка та метрологія. – 2008. – № 69. – С. 39 – 42.
23. Мельник А.О. Нові принципи побудови вимірювально-обчислювальних мереж на основі інтелектуальних агентів / А.О. Мельник, В.А. Голембо, О.Ю. Бочкарьов // Вісник Нац. ун-ту «Львівська політехніка» «Комп’ютерні системи та мережі». – 2003. – № 492. – С. 100 – 107.
24. Multiagent system for intruders’ detection and tracking: tasks and solutions / A. Melnyk, V. Golembo, A. Botchkariov, O. Kuspis // Aktualne Problemy w Elekrotechnice i Informatyce : Konferencja, Ameliówka, 17-18 czerwca 2005 r.: Wydawnictvo Politechniki Swiętokrzyskiej. – Kielcy, 2005. – P. 109 – 114.
25. Проблема самоорганізації багатоагентної системи виявлення та відстеження порушників / А.О. Мельник, В.А. Голембо, О.Ю. Бочкарьов, О.П. Кусьпісь // Вісник Нац. ун-ту «Львівська політехніка» «Комп’ютерні системи проектування». – 2005 – № 548. – С. 11 – 15.

26. Чижденко Р.Н. Агентный подход в задаче управления динамическим объектом / Р.Н. Чижденко // Інформаційні технології та комп'ютерна інженерія : Міжнар. наук.-практ. конф., 19-21 травня 2010 р. : тези доп. – Вінниця, 2010. – С. 68 – 69.
27. Євтух П. Побудова моделей сенсорних мереж та їх оцінювання методами теорії графів / П. Євтух, В. Карпінський, Я. Кінах // Вісник Тернопільського національного технічного університету. – 2010. – Том 15, № 4. – С. 146 – 154. – ISSN 1727-7108.
28. Boguslaw Filipowicz Zastosowanie przykladowego algorytmu stadnego: [Електронний ресурс] / Boguslaw Filipowicz, Joanna Kwiecien* // AUTOMATYKA. – 2010. – Tom 14. – P. 885 – 891. – Режим доступу: http://journals.bg.agh.edu.pl/AUTOMATYKA/2010-03-2/Auto19.pdf – Назва з екрану.
29. Novel type of phase transitions in a system of self-driven particles / Vicsek T., Czirok A., Jacob E. B. [et al.] // Physical Review Letters. – 1995. – Vol. 75. – P. 1226 – 1229.
30. Рибальський О.В. Основи теорії виявлення слідів цифрової обробки фонограм : автореф. дис. на здобуття наук. ступеня д-ра техн. наук : спец. 05.13.21 «Системи захисту інформації» / Рибальський Олег Володимирович; Державний ун-т інформаційно-комунікаційних технологій. – К., 2005. – 33 с.
31. Fax J. Information flow and cooperative control of vehicle formations / J. Fax, R. Murray // IEEE Transactions on Automatic Control. – 2004. – Vol. 49. – P. 1465 – 1476.
32. Jadbabaie A. Coordination of groups of mobile autonomous agents using nearest neighbor rules / A. Jadbabaie, J. Lin, A.S. Morse // IEEE Transactions on Automatic Control. – 2003. – Vol. 48. – P. 988 – 1001.
33. Lin Z. Local control strategies for groups of mobile autonomous agents / Z. Lin, M. Broucke, B. Francis // IEEE Transactions on Automatic Control. – 2004. – Vol. 49, No 4. – P. 622 – 629.
34. Olfati-Saber R. Flocking for multi-agent dynamic systems: Algorithms and theory / R. Olfati-Saber // IEEE Transactions on Automatic Control. – 2006. – Vol. 51. – P. 401 – 420.
35. Ren W. Consensus of information under dynamically changing interaction topologies / W. Ren, R. Beard // The American Control Conference, June 30-July 2 2004 : Proceedings of Conf., vol. 6. – 2004. – P. 4939 – 4944.

36. Tanner H. Stable flocking of mobile agents, part II : Dynamic topology / H. Tanner, A. Jadbabaie, G. Pappas // Decision and Control : The 42nd IEEE Conference CDC 03, 9-12 Dec. 2003 : Proceedings of Conf. – Maui, Hawai, USA. – P. 2016 – 2021.
37. Borowik B. Tracing and building of topology in Wireless Network Sensors / B. Borowik, M. Mikulski, V. Karpinskyi // Вісник Хмельницького національного університету. – 2008. – № 4 (113). – С. 7 – 12.
38. Дунець Р.Б. Знаходження шляху обходу вершин дугами при візуалізації топологій на площині / Р.Б. Дунець, Т.М. Басюк // Вісник Нац. ун-ту «Львівська політехніка» «Комп'ютерні системи та мережі». – 2007. – С. 43 – 48.
39. Карпінський М. Передавання даних у вимірювально-керуючих системах: методи, стандарти та класифікація засобів / М. Карпінський, М. Мікульскі, В. Карпінський // Вісник Тернопільського державного технічного університету. – 2007. – Том 12, № 3. – С. 113 – 119.
40. Касьянов В.Н. Графы в программировании: обработка, визуализация и применение / В.Н. Касьянов, В.А. Евстегнеев. – СПб.: БХВ, 2003. – 1104 с. – ISBN 5-94157-184-4.
41. Кочкаров Азрет Ахматович. Новые теоретико-графовые подходы в моделировании сложных систем : дис. ... канд. физ.-мат. наук : 05.13.18 / Кочкаров Азрет Ахматович. – М., 2005. – 118 с.
42. Кулаков О.Ю. Програмно-апаратна організація GRID-систем на основі технології віртуальних мереж : автореф. дис. на здобуття наук. ступеня канд. техн. наук : спец. 05.13.05 «Компютерні системи та компоненти» / Кулаков Олексій Юрійович; Нац. техн. ун-т України «Київ. політехн. ін-т». – Київ, 2010. – 22 с.
43. Панюкова Татьяна Анатольевна. Задачи маршрутизации специального вида в плоских графах : Свойства, алгоритмы, программное обеспечение : дис. ... канд. физ.-мат. наук : 05.13.17 / Панюкова Татьяна Анатольевна. – Челябинск, 2006. – 127 с.
44. Парасюк І.М. Моделе-орієнтовані методи побудови та оцінювання програмних архітектур на основі нечітких графів / І.М. Парасюк, С.В. Єршов // Проблеми програмування. – 2008. – № 2-3. – С. 181 – 190.
45. Сергієнко І.В. Нечіткий трансформаційний підхід до розробки програмних систем / І.В. Сергієнко, І.М. Парасюк, С.В. Єршов // Проблеми програмування. – 2004. – № 2-3. – С. 122 – 132.

46. Скороходов Владимир Александрович. Математические модели и алгоритмы на графах с нестандартной достижимостью : дис. ... канд. физ.-мат. наук : 05.13.18 / Скороходов Владимир Александрович. – Ростов на/Д, 2004. – 145 с.
47. Старостин Николай Владимирович. Разработка и исследование гибридных методов решения задач проектирования систем и устройств информатики, моделируемых графовыми моделями : дис. ... канд. техн. наук : 05.13.17 / Старостин. Николай Владимирович. – Н. Новгород, 2001. – 123 с.
48. Фельк Зинаида Александровна. Построение автоматизированных моделей систем по эквивалентным схемам методами аналогий и теории графов : дис. ... канд. техн. наук : 05.13.12 / Фельк Зинаида Александровна. – Челябинск, 2005. – 292 с.
49. Чукарин Алексей Валерьевич. Применение теории графов к решению задачи маршрутизации в цифровых сетях : дис. ... канд. физ.-мат. наук : 05.13.17 / Чукарин Алексей Валерьевич. – М., 2004. – 129 с.
50. Novel type of phase transitions in a system of self-driven particles / Vicsek T., Czirok A., Jacob E. B. [et al.] // Physical Review Letters. – 1995. – Vol. 75. – P. 1226 – 1229.
51. Кузин А.В. Компьютерные сети: Учебное пособие / А.В. Кузин . – М.: Форум, Инфра, 2011. – 192с. : ISBN: 978-5-16-004609-9.
52. Баскаков С. Стандарт ZigBee и платформа MeshLogic:эффективность маршрутизации в режиме «многие к одному» / С. Баскаков // Первая миля. – 2008. – Выпуск № 2-3. С. 32 – 37. – Режим доступу до журн.: http://www.lastmile.su/files/article_pdf/2/article_2100_315.pdf. – Назва з екрану.
53. Карпінський М.П. Геометричне моделювання у графічному представленні сенсорних мереж / М.П. Карпінський, С.М. Балабан, В.М. Чиж // Прикладна геометрія та інженерна графіка: Доповіді VIIміжнародної науково-практичної конференції. К.: Віпол, 2011. Вип. 87. С.154 – 158.
54. TinyOS: An Operating System: [Електронний ресурс] / P. Levis, S. Madden, J. Polastre, at al // Ambient Intelligence. – 2005. – P. 115 – 148. – Режим доступу: http://www.cs.berkeley.edu/~culler/papers/ai-tinyos.pdf – Назва з екрану.
55. Сергиевский М. Беспроводные сенсорные сети [Електронний ресурс] / Максим Сергиевский // Компьютер Пресс. – 2007. – № 8. – С. 60 – 63. – Режим доступу: http://www.compress.ru/article.aspx?id=17950. – Назва з екрану.

56. Dragoş I. Săcăleanu Increasing lifetime in grid wireless sensor networks through routing algorithm and data aggregation techniques / Dragoş I. Săcăleanu, Dragoş M. Ofrim, Rodica Stoian, Vasile Lăzărescu // International Journal of Communications. – 2011. – Issue 4.: Volume 5. – P. 157 – 164.
57. Карпінський М. Перспективні засоби моделювання безпроводових сенсорних мереж для мінімізації енерговитрат [Текст] / М. Карпінський,С. Балабан, В. Чиж // Матеріали першої науково-технічної конференції «Інформаційні моделі системи та технології». – Тернопіль, 20 травня 2011 р. – С. 36.
58. Чиж, В. Геометричне моделювання деяких атак на сигнали у безпроводових сенсорних мережах / В. Чиж, О. Демчишин, М. Карпінський, С. Балабан // Матеріали 14-ої міжнародної науково-практичної конференції, «Прикладна геометрія та інженерна графіка» – Мелітополь : ТДАУ, 2012. – Вип. 4. – С. 195 – 201. – Текст: укр. – Бібліогр.: 10 назв.
59. Chinh T. Delaunay-triangulation based complete coverage in wireless sensor networks / Chinh T. Vu, Yingshu Li // PERCOM 09 Proceedings of the 2009 IEEE International Conference on Pervasive Computing and Communications – 2009 P. 1 – 5. ISBN 978-1-4244-3304-9.
60. Reda ElHakim. Interactive 3D visualization for wireless sensor networks [Електронний ресурс] / Reda ElHakim, Mohamed ElHelw // The Visual Computer – 2011. – Volume 21 Режим доступу до журн. :http://www.springerlink.com/content/k4p6728468463149. – Назва з екрану.
61. Карпінський В.М. Безпровідні сенсорні мережі: особливості моделювання та візуалізації топології при загрозах // Сучасна спеціальна техніка. – 2011. – № 2 (25). – С. 55 – 60.
62. Weaponizing Wireless Networks: An Attack Tool for Launching Attacks against Sensor Networks [Електронний ресурс] / Thanassis Giannetso , Tassos Dimitriou, Neeli R. Prasad, Aalborg Un. – Barcelona, 2010. – 46p. – Режим доступу до журн.: https://media.blackhat.com/bh-eu-10/presentations/Giannetsos/BlackHat-EU-2010-Giannetsos-Weaponizing-Wireless-Networks-slides.pdf. – Назва з екрану.
63. A. Becher Tampering with Motes: Real-World Physical Attacks on Wireless Sensor Networks / Becher A., Benenson Z., Dornseif M. // Security in Pervasive Computing : Lecture Notes in Computer Science. – Berlin: Springer Berlin Heidelberg, 2006. – P. 104 – 118.: ISBN 978-3-540-33376-0.

64. Пат. 64391 Україна, МПК H04W 12/00. Спосіб візуалізації атаки червоточини в безпровідній сенсорній мережі [Текст] / Карпінський В.М., Євтух П.С. (Україна), Боровік Б.Л., Карпінський М.П. (Польща); заявник та патентовласник Тернопільський національний технічний університет ім. Івана Пулюя. – № u 2011 03578; заявл. 25.03.11; опубл. 10.11.2011, Бюл. № 21. – 4 с.
65. Пат. 103955 Україна, МПК H04W 12/12. Спосіб візуалізації параметрів сигналів інформаційних вузлів / Александер М.Б., Чиж В.М., Карпінський М.П., Балабан С.М. Карпінський В.М.; власник патенту Тернопільський національний технічний університет ім. Івана Пулюя (Україна), Академія технічно-гуманістична в Бєльску-Бялей (Польща). – № u 2015 05858 ; за-явл. 15.06.15 ; опубл. 12.01.2016, Бюл. № 11. – 6 с.
66. Скворцов А.В. Триангуляция Делоне и её применение / С.А. Владимирович. Томск : Изд-во Том ун-та, 2002. – 128с. ISBN: 5-7511-1501-5.
67. Voronoi G.M. Nouvelles applications des paramètres continus à la théorie des formes quadratiques. Deuxième mémoire. Recherches sur les parallélloèdres primitifs / G.M. Voronoi // Journal für die reine und angewandte Mathematik. – Volume134. P.198-287. ISSN 0075-4102; 1435-5345.
68. Препарата Ф. Вычислительная геометрия : Введение / Ф. Препарата, М. Шеймос М.: Мир, 1989. – 478 с. – ISBN5-03-001041-6.
69. Бугрименко Д. Управление беспроводной ЛВС и определение местоположения абонента [Електронний ресурс] / Д. Бугрименко // Cisco Expo 2006 ежегодная конференция по информационным технологиям в Москве. – Режим доступу: http://old.ciscoexpo.ru/moscow/2006/rus/download.shtml. – Назва з екрану.
70. Raport merytoryczny z realizacji zadań badawczych grupy tematycznej «Systemy bezprzewodowe i mobilne oraz ich bezpieczeństwo» [Електронний ресурс]: Projekt PBZ-MNiSzW-02/II/2007 «Usługi i sieci teleinformatyczne następnej generacji – aspekty techniczne, aplikacyjne i rynkowe» : Sprawozdanie / Kier. prof. dr hab. inż. A.R. Pach // Kraków, 23.06.2008. – 250 s. – Режим доступу : https://pbz.itl.waw.pl/raporty/pdf/GT02/GT02-Raport_zbiorczy.pdf/ – Назва з екрану
71. Richard I. Hartleya Triangulation / Richard I. Hartleya, Peter Sturmb // Computer Vision and Image Understanding. – November 1997. – Volume 68. – P. 146 – 157. – ISSN: 1077-3142.

72. Пат. 82896 Україна, МПК H04W 12/12. Спосіб симплексного моделювання: патент на корисну модель /Чиж В.М., Демчишин О.І., Карпінський М.П., Балабан С.М.; власник патенту Тернопільський національний технічний університет ім. Івана Пулюя (Україна), Академія технічно-гуманістична в Бєльску-Бялей (Польща). – № u 2012 13971; заявл. 07.12.12; опубл. 27.08.2013, Бюл. № 16. – 4 с.
73. Карпінський М.П. Класифікація атак на безпроводові сенсорні мережі і шляхи їх візуалізації / М. Карпінський, С. Балабан, В. Чиж. // Вісник Тернопільського національного технічного університету [науковий журнал] – Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя, 2012. – С. 191 – 197
74. Мироненко В. [Электронний ресурс] : Киберпреступность / В. Мироненко. – 2011. – Режим доступу: http://www.3dnews.ru/software-news/ kiberprestupnost-nanosit-velikobritanii-16327-mlrd-ubitkov-ezhegodno. – Назва з екрану
75. Скопа О.О. Аналіз розвитку сучасних напрямів інформаційної безпеки автоматизованих систем/ О.О. Скопа, Н.Ф. Казакова // Системи обробки інформації. – Х.: Харківський ун-т Повітряних Сил ім. І. Кожедуба, 2009. – Випуск 7 (81). – С. 48 – 53. – ISSN 1681-7710.
76. A. S. K. Pathan Security in wireless sensor networks: issues and challenges / A. S. K. Pathan, Hyung-Woo Lee ; Choong Seon Hong // ICACT 2006. The 8th International Conference . – Advanced Communication Technology, 20-22 Feb. 2006 . – Volume:2. – P. 1043 – 1048. – ISBN:89-5519-129-4.
77. Tworzenie powszechnego środowiska inteligentnego sensoringu (ST) [Електронний ресурс]: Praca nr 10300086, 06300046, 12300046, 67300016 / Kierownik pracy dr inż. Jacek Jarkowski // Warszawa: Instytut Łączności, 2006. – 71 s. – Режим доступу: http://www.itl.waw.pl/publikacje_pliki/ statutowe/ pliki/272.pdf/ – Назва з екрану.
78. Чернобыль, Припять, Чернобыльская АЭС и зона отчуждения [Електронний ресурс]. – Режим доступу: http://chornobyl.in.ua/uk/chernobyl-pozar.html
79. Security for Sensor Networks / J. Undercoffer, S. Avancha, A. Joshi, J. Pinkston // Central Asia Deep Ice-Coring Project (CADIP) : The CADIP Research Symposium, 25-26 Oct. 2002 : Proceedings of Symposium. – University of Maryland, Baltimore County, USA. – P. 1 – 11.

80. Євтух П.С. Модель та інформаційні технології ідентифікації і локалізації загроз функціонуванню безпровідних сенсорних мереж / П.С. Євтух, В. Врона, В.М. Карпінський // Вісник Східноукраїнського національного університету імені Володимира Даля. – 2009. – № 6 [136], Частина 1. – С. 196 – 200. – ISSN 1998-7927.
81. Karlof C. Secure routing in wireless sensor networks: attacks and countermeasures / C. Karlof, D. Wagner // Elsevier's Ad Hoc Networks Journal, Special Issue on Sensor Network Applications and Protocols. – 2003. – N 1 (2-3). – P. 293 – 315.
82. The Sybil Attack in Sensor Networks: Analysis & Defenses / J. Newsome, E. Shi, D. Song, A. Perrig // Information Processing in Sensor Networks – IPSN'04: Third International Symposium : April 26-27, 2004 : Proceedings of Symposium. – Berkeley, California, USA. – P. 259 – 268. – ISBN 1-58113-846-6.
83. Win K. S. Analysis of Detecting Wormhole Attack in Wireless Networks / K. S. Win // World Academy of Science, Engineering and Technology. – 2008. – Vol. 48. – P. 422-428. – ISSN 2070-3724.
84. Kalita H.K. Wireless Sensor Network Security Analysis / H.K. Kalita, A. Kar // International Journal of Next-Generation Networks (IJNGN). – 2009. – Vol. 1, No 1.– P. 1 – 10. – ISSN 0975-7252.
85. Ngai E. C. H. On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks / E. C. H. Ngai, J. Liu, M.R. Lyu // Communications – ICC 2006 : IEEE International Conference, 11-15 June 2006, Istanbul : Proceedings of Conference. – Vol. 8. – P. 3383-3389. – ISBN 1-4244-0355-3.
86. Raymond David Richard. Denial-of-Sleep Vulnerabilities and Defenses in Wireless Sensor Network MAC Protocols : Ph.D. Diss.: Computer Engineering / Raymond David Richard. – Blacksburg, Virginia Polytechnic Institute and State University. – 2008. – 210 p. – Bibliogr. : P. 180 – 187.
87. Sharif W. New Variants of Wormhole Attacks for Sensor Networks / W. Sharif, C. Leckie // Australian Telecommunication Networks and Applications Conference – ATNAC 2006 : Conference, 4-6 December 2006 : Proceedings of Conference. – Melbourne, Australia. – P. 26 – 30. – ISBN/ISSN 0977586103.
88. Kurytnik I.P. Bezprzewodowa sieć sensorów / I.P. Kurytnik, M. Mikulski, W. Karpiński // Pomiary Automatyka Kontrola. – 2010. – Vol. 56, Nr 6. – S. 548 – 551. – ISSN 0032-4140.

89. Apparatus and method for visualizing environmental conditions in a data center using wireless sensor networks : патент США 702/188 : МПК6 G06F15/00 / Ramin Y., Pandey R.; власник патенту SynapSense Corporation. – № US20100280796A1 ; опубл. 04.11.10. – 19 с. : іл.
90. Огляд засобів і технологій контролю вузлів комп'ютерної мережі / Юдін О.М., Гроза П.М., Сомов С.В., Тесленко О.В. // Системи озброєння і військова техніка. – 2009. – № 4 (20). – С. 182 – 189. – ISSN 1997-9568.
91. Modeling a sensor network design to secure a network against attack : патент США 380/278; 340/539.22; 370/338 : МПК6 H04L9/00 / Roy S. S. R., Mukhopadhyay D., Thejaswi PS C.; власник патенту Honeywell International Inc, Morristown, NJ (US). – № US007804962B2; опубл. 28.09.10. – 22 с. : іл.
92. Remote monitoring of pipelines using wireless sensor network : патент США 73/49.1; 73/40.5 R; 73/86; 73/865.9; 702/113 : МПК6 G01M3/28; G01N17/00 / Sabata A., Brossia S. – № US007526944B2; опубл. 05.05.09. – 6 с. : іл.
93. Sensor networks for monitoring pipelines and power lines : патент США 340/870.01; 370/252; 73/49.1 : МПК6 G08C17/00 / Twitchell R.W. Jr.; власник патенту Terahop Networks, Inc, Alpharetta, GA (US). – № US007705747B2; опубл. 27.04.10. – 13 с. : іл.
94. Sensor networks for pipeline monitoring : патент США 340/870.07; 340/854.5; 73/40.5 R; 73/49.1 : МПК6 H04Q5/00 / Twitchell R.W. Jr.; власник патенту Terahop Networks, Inc, Alpharetta, GA (US). – № US007830273B2; опубл. 09.11.10. – 13 с. : іл.
95. Sensor network system : патент США 455/412.1; 455/456.1; 455/435.1 : МПК6 H04L12/58 / Kato H., Miyao T.; власник патенту Hitachi, Ltd., Tokyo (JP). – № US007680486B2; опубл. 16.03.10. – 24 с. : іл.
96. System and program product for signal transmission between a sensor and a controller in a wireless sensor network : патент США 340/539.1; 340/870.01; 343/757; 455/69 : МПК6 G08B1/08 / Coronel P. E., Furrer S.; Shott W. H.; власник патенту International Business Machines Corporation, Armonk, NY (US). – № US007782188B2; опубл. 24.08.10. – 16 с. : іл.
97. Multiple-path wormhole interconnect : патент США 340/870.01; 370/252; 73/49.1 : МПК6 H04Q 11/00; H04L12/28; G06F15/173 / Hesse J.E.; власник патенту Interactic Holdings, LLC, NY (US). – № US007382775B2; опубл. 03.06.08. – 93 с. : іл.

98. NetTopo: A framework of simulation and visualization for wireless sensor networks / Lei Shua, Manfred Hauswirthb, Han-Chieh Chaoc, Min Chend, Yan Zhange, // Ad Hoc Networks. – Elsevier, July 2011. – Volume 9, Issue 5. – P. 799 – 820.
99. Karbowski K. Podstawy rekonstrukcji elementów maszyn i innych obiektów w procesach wytwarzania / K. Karbowski. – Kraków: Politechnika Krakowska im. Tadeusza Kościuszki, 2008. – 152 s. – ISBN 978-83-61312-59-8.
100. Borowik B. Method of attacks visualization in wireless sensor networks / B. Borowik, V. Karpinskyi, I.P. Kurytnik // Knowledge in Telecommunication Technologies and Optics : 11th International Conference KTTO 2011, June 22nd - 24th 2011 : Proceedings of the 11th International Conference. – Szczyrk, Poland: Publisher VSB-Technical University of Ostrava, Czech Rebublic, 2011. – P. 223 – 225. – ISBN 978-80-248-2399-7.
101. Євтух П.С. Моделювання візуалізаційного виявлення атак у сенсорній мережі моніторингу електротехнічних систем / П.С. Євтух, В.М. Карпінський // Проблеми енергоресурсозбереження в електротехнічних системах. Наука, освіта і практика. Наукове видання. – Кременчук: КНУ, 2011. – Вип. 1/2011 (1). – С. 322 – 323. – ISSN 2221-5190.
102. Groenen P. J. F. Multidimensional Scaling [Електронний ресурс] / P. J. F. Groenen, M. van de Velden // Report EI 2004-15, Erasmus University Rotterdam. – Режим доступу до журн.: http://publishing.eur.nl/ ir/repub/asset/ 1274/ei200415.pdf. – Назва з екрану.
103. KruskalJ. B. Multidimensional scaling by optimizing goodness of fit to a nonmetric hypothesis / J.B. Kruskal // Psychometrika. – Springer-Verlag, March 1964. – Volume 29, Issue 1. – P. 1 – 27. – ISSN 0033-3123.
104. Тормосов Ю.М. Геометрія моделей багатовимірного шкалювання / Ю.М. Тормосов, К.Р. Сафіуліна // Праці ТДАТУ, 2010. – Вип. 4, Т. 48. – С. 44 – 47.
105. Diversitas Cybernetica / [red. R. Klempous]. – Warszawa : WKŁ, 2005. – 232 s. – ISBN 83-206-1595-X.
106. Маковейчук О.М. Об’єктивна оцінка якості обробки зображень / О.М. Маковейчук // Системи озброєння і військова техніка. – 2008. – № 3. – С. 135 – 136. – Режим доступу до журн.: http://nbuv.gov.ua/j-pdf/soivt_2008_3_38.pdf. – Назва з екрану.

107. Світличний О.О. Основи геоінформатики : навч. посіб. / О.О. Світличний, С.В. Плотницький. – Суми : ВТД «Університетська книга», 2006. –295 с. – ISBN 966-680-234-1.
108. Bowling G. Kriging [Електронний ресурс] / G. Bowling. – Kansas : Kansas Geological Survey. – 2005. – C&PE 940. – 21 p. – Режим доступу : http://people.ku.edu/~gbohling/cpe940/Kriging.pdf. – Назва з екрану.
109. Дэвис Дж.С. Статистический анализ данных в геологии. В 2 кн. Кн. 1 : пер. с англ. / Дж.С. Дэвис ; под ред. Д.А. Родионова. – Москва: Недра, 1990. – 319 с.
110. Іщук О.О. Просторовий аналіз і моделювання в ГІС: навч. посіб. / О.О. Іщук, М.М. Коржнев, О.Є. Кошляков ; за ред. акад. Д.М. Гродзинського. – К. : ВПЦ “Київський університет”, 2003. – 200 с.
111. Попова М.А. Онтологічний інтерфейс як засіб представлення інформаційних ресурсів в ГІС - середовищі [Електронний ресурс] / М.А. Попова, О.Є. Стрижак // Ученые записки Таврического национального университета имени В.И.Вернадского. – 2013. – Том 26. – С. 127 – 135. – Режим доступу: http://sn-geography.crimea.edu/arhiv/2013/uch_26_1geo/014_popo.pdf. – Назва з екрану.
112. Основы геоинформатики. В 2 кн. Кн. 1: учеб. пособ. для студ. вузов / Е.Г. Капралов, А.В. Кошкарев, В.С. Тикунов [и др.] ; под ред. В.С. Тикунова. – М.: Издательский центр “Академия”, 2004. – 352 с.
113. Stein M.L. Interpolation of spatial data: some theory for kriging / Michael Leonard Stein. – New York, NY [u.a.]: Springer, 1999. – 249p. – ISBN 978-0-387-98629-6.
114. Абракітов В.Е. Картографування шумового режиму центральної частини міста Харкова / В.Е. Абракітов. – Х.: ХНАМГ, 2010. – 266 с. – ISBN 978-966-695-178-9.
115. Guiyun Liu An indicator kriging method for distributed estimation in wireless sensor networks [Електронний ресурс] / Liu Guiyun, Bugong Xu, Hongbin Chen // International Journal of Communication Systems. – 2014. – Volume 27, Issue 1. – P.68-80. – Режим доступу до журн.: http://www.readcube.com/articles/10.1002%2Fdac.2344?r3_referer=wol&tracking_action=preview_click&show_checkout=1&purchase_referrer=onlinelibrary.wiley.com&purchase_site_license=LICENSE_EXPIRED. – Назва з екрану.

116. Половко А. Интерполяция. Методы и компьютерные технологии их реализации: Научное издание / А.М. Половко, П.Н. Бутусов. – Санкт-Петербург: БХВ-Петербург, 2004. – 320с. – ISBN 5941574932.
117. Карпінський М. Моделювання та графічне представлення об'ємних безпроводових сенсорних мереж / М. Карпінський, С. Балабан, В. Чиж // XV Наукова конференція Тернопільського національного технічного університету імені Івана Пулюя . – Тернопіль: Видавництво Тернопільського національного технічного університету імені Івана Пулюя, 2011. – С. 73.
118. Giannetsos T. Weaponizing Wireless Networks: An Attack Tool for Launching Attacks against Sensor Networks / Thanassis Giannetsos, Tassos Dimitriou, Neeli R. Prasad; 2010. – Режим доступудо журн.: http://www.ait.gr/export/sites/default/ait_web_site/faculty/tdim/various/attackTool-BlackHat10.pdf. – Назва з екрану.
119. Perkins C.E., Mobility Support in IPv6 / Perkins C.E., Johnson D.B. // Proceedings of the 2Nd Annual International Conference on Mobile Computing and Networking MobiCom: MobiCom '96. – New York: ACM, 1996. – P. 27 – 37. – ISBN 0-89791-872-X.
120. Шнитман В.З. Реализация функций мобильности в протоколе IPv6 и анализ их безопасности [Електронний ресурс]: Российская Академия Наук Институт системного программирования / В.З. Шнитман. – М., 2004. – 35с. – Режим доступу: http://ipv6.ispras.ru/mobile_rev.pdf. – Назва з екрану.
121. Karlof C. Secure routing in wireless sensor networks: attacks and countermeasures / C. Karlof, D. Wagner // Elsevier’s Ad Hoc Networks Journal, Special Issue on Sensor Network Applications and Protocols. – 2003. – N 1 (2-3). – P. 293 – 315.– ISBN - 978-3-540-36410-8.
122. Чиж В. Метод стаціонарних сигнальних точок як засіб аналізу та візуалізації залишкової енергії інформаційних вузлів у безпроводових сенсорних мережах з автономним живленням / В. Чиж, М. Карпінський, С. Балабан // Матеріали 15-ої міжнародної науково-практичної конференції, "Прикладна геометрія та інженерна графіка" – Мелітополь: ТДАУ, 2013. – Вип. 4. – С. 225 – 232.
123. Кучерявый А.Е. Выбор головного узла кластера в однородной беспроводной сенсорной сети [Текст] / А.Е. Кучерявый, А. Салим // Электросвязь: Научно-

технический журнал по проводной и радиосвязи, телевидению и радиовещанию. – М.: Общество с ограниченной ответственностью «Инфо-электросвязь» 2009. N 8. С. 32 – 36.

124. Чиж В. Алгоритм побудови та дослідження структури кластера при геометричному моделюванні безпроводових сенсорних мереж / В. Чиж, О. Демчишин, М. Карпінський, С. Балабан // Збірник наукових праць «Будівництво та техногенна безпека» – Сімферополь: Національна академія природоохоронного та курортного будівництва, 2012. – Вип. 41. – С. 246 – 251.
125. Курс физики: учебник для вузов: в 2 т. / под ред. В.Н. Лозовского. СПб.: Лань, 2000. ISBN 5-8114-0288-0. Т. 2. 2000. 591 с. ISBN 5-8114-0287-2.
126. Долуханов М.П. Распространение радиоволн: Учебник для вузов. / М.П. Долуханов.[4-е изд.]. М.: Связь, 1972. 336 с.
127. Методи геометричного моделювання безпроводових сенсорних мереж для аналізу сили сигналів інформаційних вузлів / М.П. Карпінський , В.М. Чиж, С.М. Балабан, Т.О. Яремчук // Вісник Східноукраїнського національного університету імені Володимира Даля. – Луганськ: Видавництво СНУ ім. Володимира Даля, 2013. – Вип. № 15 (204), ч. 1. – С. 69 – 76 ISSN 1998-7927.
128. Балабан С. Вибір методу візуалізації сили сигналів інформаційних вузлів у безпроводових сенсорних мережах / С. Балабан, В. Чиж, Александер М. // Природничі науки та інформаційні технології: XVII наукова конференція, 20-21 листопада 2013 р.: тези доповідей / Тернопільський національний технічний університет ім. Івана Пулюя. – Тернопіль, 2013. – С. 19
129. Пат. 82896 Україна, МПК H04W 12/12. Спосіб симплексного моделювання: патент на корисну модель / Чиж В.М., Демчишин О.І., Карпінський М.П., Балабан С.М.; власник патенту Тернопільський національний технічний університет ім. Івана Пулюя (Україна), Академія технічно-гуманістична в Бєльску-Бялей (Польща). – № u 2012 13971; заявл. 07.12.12; опубл. 27.08.2013, Бюл. № 16. – 4 с.
130. Мандельброт, Бенуа. Фрактальная геометрия природы / Бенуа Мандельброт; – Ижевск: Институт компьютерных исследований, 2010. – 756 с. – ISBN 978-5-93972-872-0.
131. Шредер, М. Фракталы, хаос, степенные законы. / М. Шредер – Ижевск: РИЦ «Регулярная и хаотическая динамика», 2001. – 528 с. – ISBN 5-93972-041-2.
132. Пат. 93269 Україна, МПК H04W 12/12. Спосіб кластерного моделювання безпроводової сенсорної мережі / Чиж В.М., Карпінський М.П., Бала-

бан С.М.; власник патенту Тернопільський національний технічний університет ім. Івана Пулюя (Україна), Академія технічно-гуманістична в Бєльску-Бялей (Польща). – № u 2014 03919 ; заявл. 14.04.14 ; опубл. 25.09.2014, Бюл. № 18. – 6 с.

133. Чиж В. Метод аналізу та візуалізації залишкової енергії : Збірник тез доповідей / В. Чиж, С. Балабан, О. Демчишин // XVI НАУКОВОЇ КОНФЕРЕНЦІЇ Тернопільського національного технічного університету імені Івана Пулюя. – Тернопіль: Вид-во ТНТУ імені Івана Пулюя, 5-6 грудня 2012 р. – С. 66.
134. Пат. 103955 Україна, МПК H04W 12/12. Спосіб візуалізації параметрів сигналів інформаційних вузлів / Александер М.Б., Чиж В.М., Карпінський М.П., Балабан С.М. Карпінський В.М.; власник патенту Тернопільський національний технічний університет ім. Івана Пулюя (Україна), Академія технічно-гуманістична в Бєльску-Бялей (Польща). – № u 2015 05858 ; заявл. 15.06.15 ; опубл. 12.01.2016, Бюл. № 11. – 6 с.
135. Моделювання безпроводових сенсорних мереж на підставі кластерів / В.М. Чиж, С.М. Балабан, О.М. Карпінська, В.М. Карпінський // Інформаційна безпека. – Луганськ: Видавництво СНУ ім. Володимира Даля, 2013. – № 1 (9). – С. 155 – 164. – ISSN 2224-9613.
136. Чиж В.М. Контроль та візуалізація стану функціональної безпеки інформаційних систем із застосуванням безпроводових сенсорних мереж / В.М. Чиж, М.П. Карпінський, С.М. Балабан // Прикладна радіоелектроніка – Х.: Харківський національний університет радіоелектроніки, 2013 – Т. 12, № 2 С. 356 – 362. ISSN 1727-1290
137. Кулаков Ю.И. Теория физических структур. (Математические начала физической герменевтики) / Ю.И. Кулаков. М., 2004. – 847 с.
138. Wireless sensor network design for tactical military applications : Remote large-scale environments / S.H. Lee, Daej S. Lee, H. Song, H.S. Lee // MILCOM 2009 – 2009 IEEE Military Communications Conference. – Boston, MA , 18-21 Oct. 2009 . – P. 1 – 7 . – ISBN:978-1-4244-5238-5.
139. Чиж В. Використання кластерної моделі для розрахунку надійності безпроводової сенсорної мережі / В. Чиж, О. Демчишин, М. Карпінський, С. Балабан // Інформаційна безпека – Луганськ: Видавництво СНУ ім. В. Даля, 2012. – Вип. № 1 (7). – С. 83 – 89. ISSN 2224-9613.
140. Чиж В. Геометричне моделювання деяких атак на сигнали у безпроводових сенсорних мережах / В. Чиж, О. Демчишин, М. Карпінський, С. Балабан //

Матеріали 14-ої міжнародної на-уково-практичної конференції, «Прикладна геометрія та інженерна графіка» – Мелітополь: ТДАУ, 2012. – Вип. 4. – С. 195 – 201.

141. Карпінський М.П. Аналітичний метод дослідження величини зміни параметрів сигналів у безпроводових сенсорних мережах / М.П. Карпінський, В.М. Чиж, С.М. Балабан // Вісник національного університету «Львівська політехніка». Львів: Видавництво Львівської політехніки, 2014. – № 806. – С. 88 – 93.
142. Карпінський М. Аналіз параметрів сигналів як засіб підвищення безпеки безпроводових інформаційних систем: Наукове видання / Микола Карпінський, Марек Александер, Віталій Чиж, Степан Балабан // Матеріали ІІІ-ої міжнародної науково-технічної конференції. Львів: Видавництво Української академії друкарства, 05-06 червня 2014 р. С. 74 – 75.
143. Deo N. Teoria grafów i jej zastosowanie w technice i informatyce / N. Deo. – Warszawa: PWN, 1980. – 607 s. – ISBN 83-01-00544-0.
144. Kościelnik D. Overview of the Methods for Information Broadcast in ad-hoc Wireless Networks / D. Kościelnik, J. Stępień // Telecommunication Review. – 2010. – No 5. – P. 168 – 173.
145. Encyclopedia of Wireless and Mobile Communications / Edit. by B. Furht. – London: Taylor & Francis Group, 2011. – 1856 p. – ISBN 978-1-4200-4326-6.
146. Korn G.A. Matematyka dla pracowników naukowych i inżynierów. W 2 cz. Cz. 1: tłum. z ang. M. Krawczyk, T. Krawczyk, L. Szymanowski / G.A. Korn, T.M. Korn. – Warszawa: PWN, 1983. – 556 s. – ISBN 83-01-03446-7.
147. Le Boudec J.-Y. Perfect Simulation and Stationarity of a Class of Mobility Models / J.-Y.Le Boudec, M. Vojnovic // Computer Communications : 24th Annual Joint Conference of the IEEE Computer and Communications Societies INFOCOM 2005, 13-17 March 2005 : Proceedings of the Conference, Vol. 4. – Miami, FL, USA. – P. 2743 – 2754. – ISBN 0-7803-8968-9.
148. Boneh D. On the importance of checking cryptographic protocols for faults (extended abstract) / D. Boneh, R.A. DeMillo, R.J. Lipton // Lecture Notes in Computer Science: Proc. jf Advances in Cryptology. EUROCRYPT'97 (W. Fumy, Ed.). – Konstanz, Germany: Springer-Verlag, 1997. – N 1233. – P. 37 – 51.
149. Карпінський В.М. Імітаційне моделювання процесів виявлення та ізолювання негативних збурювальних чинників в безпровідних сенсорних мережах / В.М. Карпінський // Підвищення ефективності енергоспоживання в

електротехнічних пристроях і системах: 3-я міжнарод. наук.-техн. конф., 28-30 червня 2010 р. : тези доп. – Луцьк – Шацькі озера, 2010. – С. 102 – 104.

150. Широчин В.П. Захист інформації в комп'ютерних системах / В.П. Широчин. – К.: Корнейчук, 2009. – 288 с.
151. Bućko M. [Електронний ресурс]: Ataki na bezprzewodowe sieci sensoryczne / M. Bućko. – Режим доступужурн.: http://hack.pl/felietony/ ataki_na_ bezprzewodowe_sieci_sensoryczne_46. – Назва з екрану.
152. Aleman E. KEELOQ™ with AES Microcontroller-Based Code Hopping Encoder [Електронний ресурс] / E. Aleman, M. Stuckey // DS01265A : Microchip Technology Inc., 2009. – 12 p. – Режим доступу: http://ww1.microchip.com/ downloads/en/AppNotes/01265B.pdf – Назва з екрану.
153. Bogdanov A. Cryptanalysis of the KeeLoq block cipher [Електронний ресурс] / A. Bogdanov // Cryptology ePrint Archive, Report 2007. – 12 p. – Режим доступу : http://eprint.iacr.org/2007/055.pdf. – Назва з екрану.
154. Courtois N.T. Algebraic and Slide Attacks on KeeLoq / N.T. Courtois, G.V. Bard, D. Wagner // Fast Software Encryption – 15th International Workshop : FSE 2008, February 10-13, 2008: Proceedings. – Lausanne, Switzerland. – Lecture Notes in Computer Science (LNCS). – Vol. 5086: Springer, 2008. – P. 97 – 115. – ISBN: 3-540-71038-8.
155. Courtois N.T. Periodic Ciphers with Small Blocks and Cryptanalysis of KeeLoq / N.T. Courtois, G.V. Bard, A. Bogdanov // Tatra Mt. Mathematical Publications. – 2008. – N 41. – P. 167 – 188.
156. A Practical Attack on KeeLoq / Indesteege S., Keller N., Dunkelman O. [et al.] // The Theory and Applications of Cryptographic Techniques – Advances in Cryptology : 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques EUROCRYPT 2008, April 13-17, 2008: Proceedings. – Istanbul, Turkey. – LNCS. Vol. 4965: Springer, 2008. – P. 1 – 18. – ISBN 978-3-540-78966-6.
157. Lyons R.G. Wprowadzenie do cyfrowego przetwarzania sygnałów / R.G. Lyons. – Wyd. 2. – Warszawa : WKŁ, 2010. – 648 s. – ISBN: 9788320617641.
158. Zhang Y. Intrusion detection in wireless ad-hoc networks / Y. Zhang, W. Lee // Mobile Computing and Networking : 6th Annual International Conference ACM MobiCom, August 06-11, 2000 : Proceedings of Conference. – Boston, MA, USA. – P. 275 – 283. – ISBN:1-58113-197-6.

159. Anjum F. Signature based Intrusion Detection for Wireless Ad-Hoc Networks: A Comparative study of various routing protocols / F. Anjum, D. Subhadrabandhu, S. Sarkar // Vehicular Technology : The IEEE 58th Conference VTC, Oct. 6-9, 2003 : Proceedings of Conference. – Morristown, NJ, USA. – P. 2152 – 2156. – ISBN:0-7803-7954-3.
160. Bhuse V. Anomaly intrusion detection in wireless sensor networks / V. Bhuse, A. Gupta // Journal of High Speed Networks, 2006. – No 1 (15). – P. 33 – 51.
161. Hall J. Using mobility profiles for anomaly based intrusion detection in mobile networks / J. Hall, M. Barbeau, E. Kranakis // Mobile Computing, Networking and Communications : NDSS'05 Preconference Workshop on Wireless and Mobile Security, August 2005 : Proceedings of Workshop. – Montreal, Kanada. – P. 22 – 24.
162. Wang W. Visualization Assisted Detection of Sybil Attacks in Wireless Networks / W. Wang, A. Lu // Visualization for Computer Security : 3rd International Workshop VizSEC'06, November 3, 2006: Proceedings of Workshop. – Alexandria, VA, USA. – P. 51 – 60. – ISBN:1-59593-549-5.
163. Бойко Ю.М. Концептуальні особливості реалізації безпровідних сенсорних мереж [Електронний ресурс] / Ю.М. Бойко, В.М. Локазюк, В.В. Мішан // Вісник Хмельницького національного університету. – 2010. – № 2. – С. 94 – 97. – Режим доступу до журн.: http://journals.khnu.km.ua/ vestnik/ pdf/ tech/ 2010_2/18boy.pdf . – Назва з екрану.
164. Kulesza W. Bezprzewodowe sieci sensorowe – aspekty metrologiczne, telekomunikacyjne i energetyczne / W. Kulesza // Biuletyn Techniczno-Informacyjny OŁ SEP. – 2010. – Nr 3 (50). – S. 2 – 8. – ISSN 1428-8966.
165. Курітник І.П. Безпровідна трансляція інформації: переклад з польськ. В. Карпінський та У. Яциковська / І.П. Курітник, М. Карпінський. – Тернопіль: Крок, 2010. – 376 с. – ISBN 978-966-2362-16-9.
166. Карпінський В.М. Безпровідні сенсорні мережі: особливості моделювання та візуалізації топології при загрозах / В.М. Карпінський // Сучасна спеціальна техніка. – 2011. – № 2 (25). – С. 55 – 60.
167. Algorithms and Protocols in Wireless Sensor Networks / Edited by Prof. Azzedine Boukerche. – Hoboken, NJ : John Wiley & Sons, Inc., 2008. – 544 p. – ISBN 978-0-471-79813-2.
168. A framework for maintaining formations based on rigidity / T. Eren, P. Belhumeur, B. Anderson, A. Morse // International Federation of Automatic Control

(IFAC) : 15th IFAC World Congress : 21-26 July 2002 : Proceedings of Congress, Vol. # 15, Part # 1. – Barcelona, Spain. – P. 2752-2757. – ISBN 978-3-902661-74-6.

169. Networking issues in wireless sensor networks / D. Ganesan D., Cerpa A., Ye W. [et al.] // Journal of Parallel and Distributed Computing (JPDC), Special issue on Frontiers in Distributed Sensor Networks. – 2004. – Volume 64, Issue 7. – P. 799 – 814.
170. Law Y.W. How to secure sensor networks / Y.W. Law, P.J.M. Havinga // Sensor Networks and Information Processing : The 2005 International Conference, 5-8 Dec. 2005 : Proceedings of the Conference. – Melbourne, Australia. – P. 89 – 95.
171. Євтух П.С. Підхід до збільшення безпеки безпровідних комунікаційних технологій / П.С. Євтух, Р.Б. Трембач, В.М. Карпінський // Проблеми впровадження інформаційних технологій в економіці : VII міжнар. наук.-практ. конф., 23-24 квітня 2009 р. : тези доп. – Ірпінь, Україна, 2009. – С. 243 – 244.
172. The security of data transmission over telecommunication networks based on advanced data encryption methods / M. Karpinski, M. Aleksander, G. Litawa, V. Karpinskyi // Electrical Review. – 2009. – N 4. – P. 19 – 21. – ISSN 0033-2097.
173. The Security of Data Transmission over Telecommunication Networks Based on Advanced Data Encryption Methods / M. Karpinski, M. Aleksander, G. Litawa, V. Karpinskyi // Computational Problems of Electrical Engineering : 9th International Workshop CPEE'08, September 16-20, 2008 : Proceedings of the Workshop. – Alushta (Crimea), Ukraine). – P. 71 – 73.
174. Yih-Chun H. Wormhole attacks in wireless networks / H. Yih-Chun, A. Perrig, D. Johnson // IEEE Journal on Selected Areas in Communications (JSAC). – 2006. – Vol. 24, Issue 2. – P. 370 – 380. – ISSN:0733-8716.
175. Poovendran R.A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks / R. Poovendran, L. Lazos // ACM Journal on Wireless Networks. – 2007. – Vol. 13 , Issue 1. – P. 27 – 59. – ISSN 1022-0038.
176. Бакулина Мария Алексеевна. Средства разработки и анализа алгоритмов решения задач структурного синтеза на графах : дис. ... канд. техн. наук : 05.13.11 / Бакулина Мария Алексеевна. – М., 2006. – 133 с.

177. Виноградов Дмитрий Владимирович. Метод и алгоритм автоматизированной обработки графовых моделей динамических систем в структурах автоматического управления : дис. ... канд. техн. наук : 05.13.01 / Виноградов Дмитрий Владимирович. – М., 2002.
178. Дунець Р.Б. Математичні моделі та методи аналізу й синтезу топологій комп'ютерних видавничо-поліграфічних систем : автореф. дис. на здобуття наук. ступеня д-ра техн. наук : спец. 01.05.02 «Математичне моделювання та обчислювальні методи» / Дунець Роман Богданович; Нац. ун-т «Львів. Політехніка». – Львів, 2005. – 36 с.
179. Юрасов Павел Владиславович. Алгоритмизация оптимального проектирования информационных сетей на основе слабосвязных графов : дис. ... канд. техн. наук : 05.13.12 / Юрасов Павел Владиславович. – Воронеж, 2000. – 133 с.
180. Roosta T. Taxonomy of Security Attacks in Sensor Networks and Countermeasures / T. Roosta, S. Shieh, S. Sastry // System Integration and Reliability Improvements : The First IEEE International Conference SIRI 2006, 13-15 Dec. 2006 : Proceedings of Conference. – Hanoi, Vietnam. – P. 13 – 15.
181. Karlof C. Tinysec: a link layer security architecture for wireless sensor networks / C. Karlof, N. Shastry, D. Wagner // Embedded Networked Sensor Systems : The Second ACM Conference SenSys 2004, 3-5 Nov. 2004 : Proceedings of Conference. – Baltimore, Maryland, USA. – P. 162 – 175. – ISBN:1-58113-879-2.
182. Hoesel L.V. A lightweight medium access protocol (LMAC) for wireless sensor networks: reducing preamble transmissions and transceiver state switches [Електронний ресурс] / L.V. Hoesel, P. Havinga // Networked Sensing Systems : The First International Workshop INSS'04, 22-23 June 2004 : Proceedings of Conference. – Tokyo, Japan. – Режим доступу: http://eprints.eemcs.utwente.nl/12718/01/VanHoesel_INSS04_048.pdf. – Назва зекрану.
183. Wood A. Denial of service in sensor networks / A. Wood, J. Stankovic // IEEE Computer. – 2002. – Vol. 35, No. 10. – P. 54 – 62. – ISSN: 0018-9162.
184. Wood A.A jammed-area mapping service for sensor networks / A. Wood, J. Stankovic, S.H. Son // The Real-Time Systems : 24th IEEE Symposium RTSS'03, 3-5 Dec. 2003 : Proceedings of Symposium. – Cancun, Mexico. – P. 286 – 297. – ISBN: 0-7695-2044-8
185. Hu N. Security for fixed sensor networks / N. Hu, R.K. Smith, P.G. Bradford // The 42nd ACM Southeast Regional Conference, 2-3 April 2004 : Proceedings of Conference. – Huntsville, Alabama, USA. – P. 212-213. – ISBN:1-58113-870-9.

186. A key management scheme for wireless sensor networks using deployment knowledge / Du W., Deng J., Han Y.S. [et al.] // Computer Communications : 23rd Annual Joint Conference of the IEEE Computer and Communications Societies INFOCOM 2004, 7-11 March 2004 : Proceedings of Conference. – Hong Kong. – P. 586 – 597.
187. A pairwise key predistribution scheme for wireless sensor networks / Du W., Deng J., Han Y.S. [et al.] // ACM Transactions on Information and System Security (TISSEC). – 2005. – Volume 8, Issue 2. – P. 228 – 258.
188. Chan H. Random key redistribution schemes for sensor networks / H. Chan, A. Perrig, D. Song // Security and Privacy: The IEEE Symposium, 11-14 May 2003 : Proceedings of Symposium. – Oakland, CA, USA. – P. 197 – 213. – ISBN: 0-7695-1940-7.
189. Eltoweissy M. Group key management scheme for large-scale sensor networks / M. Eltoweissy, A. Wadaa, S. Olariu, L. Wilson // Journal of Ad Hoc Networks, Special Issue on Data Communications and Topology Control in Ad Hoc Networks. – 2005. – Vol. 3, Issue 5. – P. 668 – 688.
190. Eschenauer L. A key-management scheme for distributed sensor networks / L. Eschenauer, V. Gligor // Computer and Communication Security : The 9th ACM Conference CCS 2002, 18-22 Nov. 2002 : Proceedings of Conference. – Washington DC, USA. – P. 41 – 47.
191. Liu D. Establishing pairwise keys in distributed sensor networks / D. Liu, P. Ning, R. Li // ACM Transactions on Information and System Security (TISSEC). – 2005. – Vol. 8, Issue 1. – P. 41 – 77.
192. Pietro R. Random key-assignment for secure wireless sensor networks / R. Pietro, L. Mancini, A. Mei // Security of ad hoc and Sensor Networks : The 1st ACM Workshop SANS, 31 Oct. 2003 : Proceedings of Workshop. – Fairfax, VA, USA. – P. 62 – 71.
193. Securing sensor networks with location-based keys / Y. Zhang, W. Liu, W. Lou, Y. Fang // Wireless Communications and Networking : IEEE Conference WCNC 2004, 21-25 March 2004 : Proceedings of Conference. – Atlanta, GA, USA. – P. 1909 – 1914.
194. Zia T.A. A secure triple-key management scheme for wireless sensor networks / T.A. Zia, A.Y. Zomaya // Computer Communications : 25th Annual Joint Conference of the IEEE Computer and Communications Societies INFOCOM 2006, 23-24 April 2006 : Proceedings of Conference. – Barcelona, Spain. – P. 1 – 2.

195. Sastry N. Secure verification of location claims / N. Sastry, U. Shankar, D. Wagner // Wireless Security : The 2nd ACM Workshop, 19 Sept. 2003 : Proceedings of Workshop. – San Diego, CA, USA. – P. 1 – 10.
196. Карпінський В.М. Візуалізаційне моделювання безпровідних сенсорних мереж / В.М. Карпінський // Вісник Східноукраїнського національного університету імені Володимира Даля. – 2010. – № 9 [151]. – С. 259 – 266. – ISSN 1998-7927.
197. Proceedings of IEC Workshop on Internet Simulations with the NS simulator, 2000 [Електронний ресурс] : The Network Simulator – ns-2. – Режим доступу: http://isi.edu/nsnam/ns. – Назва з екрану.
198. Hu Y.-C. Wormhole detection in wireless ad hoc networks / Y.-C. Hu, A. Perrig, D.B. Johnson // Technical Report No TR01-384. – Houston, TX (USA) : Rice University, Department of Computer Science. – 2002.
199. The TESLA Broadcast Authentication Protocol / A. Perrig, R. Canetti, J.D. Cygar, D. Song // CryptoBytes. – 2002. – Vol. 5, No. 2. – P. 2 – 13.
200. Rajasegarar S. Anomaly detection in wireless sensor networks / S. Rajasegarar, C. Leckie, M. Palaniswami // IEEE Wireless Communications. – IEEE, Aug. 2008. – Volume:15, Issue: 4 . – P. 34 – 40. – ISSN :1536-1284.
201. Аникин А. Обзор современных технологий беспроводной передачи данных в частотных диапазонах ISM (Bluetooth, ZigBee, Wi-Fi) и 434/868 МГц [Електронний ресурс] / А. Аникин // Беспроводные технологии. – 2011. – № 4. – С. 6 – 12. – Режим доступу до журн.: http://www.wireless-e.ru/articles/ technologies/2011_4_6.php – Назва з екрану.
202. Жук О.В., Романюк В.А., Сова О.Я. Система управління тактичними сенсорними мережами // Збірник наукових праць ВІТІ НТУУ, К.: „КПІ”. – 2008. – № 2. – С. 88 – 96.
203. Зеляновський М.Ю. Математичні моделі для спеціалізованих та сенсорних мереж безпроводового доступу / М.Ю. Зеляновський, О.В. Тимченко // Моделювання та інформ. технології: зб. наук. пр. / НАН України, Ін-т пробл. моделювання в енергетиці. - К., 2009. – Вип. 50. - С. 192 – 200.
204. Баскаков С.С. Беспроводные сенсорные сети на базе платформы MeshLogic / С.С. Баскаков , В.И. Оганов // Электронные компоненты. – 2006. – № 8. – С. 65 – 69.

205. Рагозин, Д.В. Моделирование синхронизированных сенсорных сетей / Д.В. Рагозин // Пробл. програмув. – 2008. – № 2-3. – С. 721 – 729. Текст: рос. – Бібліогр.: 12 назв.
206. Wireless sensor networks: a survey / I.F. Akyildiz,W. Su, Y. Sankarasubramaniam, E. Cayirci; Georgia Institute of Technology // Computer Networks. – Atlanta, 15 March 2002. – Volume 38. – P. 393 – 422.
207. Dragoş I. Săcăleanu Increasing lifetime in grid wireless sensor networks through routing algorithm and data aggregation techniques / Dragoş I. Săcăleanu, Dragoş M. Ofrim, Rodica Stoian, Vasile Lăzărescu // International Journal of Communications. – 2011. – Issue 4.: Volume 5. – P. 157 – 164.
208. В.А. Мочалов Стратегии размещения узлов сенсорной сети / Мочалов В.А., Турута Е.Н.; Московский технический университет связи и информатики // Материалы VII Международной научно-технической конференции. – М.: INTERMATIC, 23-27 ноября 2010 г. – С. 211 – 216.
209. Ishizuka M. Performance study of node placement in sensor networks / M. Ishizuka, M. Aida // 24th International Conference on Distributed Computing Systems Workshops. – Tokyo, 2004. – P. 598 – 603.: ISBN:0-7695-2087-1.
210. Бунин С.Г. Перспективы беспроводных ячеистых сетей / С.Г.Бунин, А.И. Миночкин, В.А. Романюк // Зв'язок. – 2007. – № 5. – С. 20 – 24. – Режим доступу до журн.: http://viti.edu.ua/files/rom/2007/1_2007.pdf – Назва з екрану.
211. Романюк В.А. Мобільні радіомережі (manet) – Основа побудови тактичних мереж зв'язку / В.А. Романюк // Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення: Четверта науково-технічна конференція, 22 листопада 2007 р.: доповіді та тези доповідей – К.: "КПІ", 2007 р. – С. 15 – 28.
212. Дорошенко, А.Е. О Моделировании сенсорних сетей средствами високого уровня / А.Е. Дорошенко, К.А Жереб, Р.С. Шевченко // Проблеми програмування: Матеріали п'ятої Міжнар. наук.-практ. конф. з програмування Укр. ПРОГ 2006, м. Київ, 23-25 трав. 2006 р. – К.: НАН України. Ін-т програмних систем, 2006. – № 2-3. – С. 718 – 727. – ISSN 1727-4907.
213. Плахтеев А.П. Моделирование и исследование процессов взаимодействия элементов беспроводных сенсорных сетей / А.П. Плахтеев, П.А. Плахтеев. // Радіоелектронні і комп'ютерні системи. – Х., 2010. – № 6 (47). – С. 20 – 24.

214. С. Сысоева MEMS компоненты, движения, беспроводные применения, энергосбережение и технологические инновации – в фокусе выставки Sensors Expo&Conference 2008 / Сысоева С. // Компоненты и технологии. – 2008. – № 8 – С. 51 – 56. – Режим доступу до журн.: http: // kit-e.ru/ articles/sensor/ 2008_08_51.php. – Назва з екрану.
215. Кузин А.В. Компьютерные сети: Учебное пособие / А.В. Кузин . – Форум, Инфра-М, 2011. – 192 с.: ISBN: 978-5-16-004609-9.
216. Баскаков С. Стандарт ZigBee и платформа MeshLogic:эффективность маршрутизации в режиме «многие к одному» [Електронний ресурс] / С. Баскаков // Первая миля. – 2008. – Выпуск #2-3. – С. 32 – 37. – Режим доступу до журн.: http://www.lastmile.su/files/article_pdf/2/article_2100_315.pdf. – Назва з екрану.
217. Сергиевский М. Беспроводные сенсорные сети [Електронний ресурс] / Максим Сергиевский // Компьютер Пресс. – 2007. – №8. – С. 60 – 63. – Режим доступу до журн.: http://www.compress.ru/article.aspx?id=17950. – Назва з екрану.
218. Сергиевский М. Беспроводные сенсорные сети [Електронний ресурс] / Максим Сергиевский // Компьютер Пресс. – 2008. – № 4. – С. 154 – 156. – Режим доступу до журн.: http://www.sapr.ru/Article.aspx?id=18943. – Назва з екрану.
219. Курс физики: учебник для вузов: в 2 т. / под ред. В.Н. Лозовского. – СПб.: Лань, 2000. – ISBN 5-8114-0288-0. Т. 2. – 2000. – 591 с. ISBN 5-8114-0287-2.
220. Долуханов М.П. Распространение радиоволн: Учебник для вузов. / М.П. Долуханов.[4-е изд.]. – М.: Связь, 1972. – 336 с.
221. Чиж В. Алгоритм побудови та дослідження структури кластера при геометричному моделюванні безпроводових сенсорних мереж / В. Чиж, О. Демчишин, М. Карпінський, С. Балабан // Збірник наукових праць «Будівництво та техногенна безпека» – Сімферополь: Національна академія природоохоронного та курортного будівництва, 2012. – Вип. 41. – С. 246 – 251.
222. Săcăleanu, D.I. Increasing lifetime in grid wireless sensor networks through routing algorithm and data aggregation techniques. / D.I. Săcăleanu, D.M. Ofrim, R. Stoian, & V. Lăzărescu // International Journal of Communications. – 2011. – Volume 5. P. 157 – 164.
223. Чиж В. Геометричне моделювання деяких атак на сигнали у безпроводових сенсорних мережах / В. Чиж, О. Демчишин, М. Карпінський, С. Балабан // Матеріали 14-ої міжнародної науково-практичної конференції, «Прикладна

геометрія та інженерна графіка» – Мелітополь : ТДАУ, 2012. – Вип. 4. – С. 195 – 201.

224. Chinh T. Delaunay-triangulation based complete coverage in wireless sensor networks / Chinh T.Vu, Yingshu Li // PERCOM 09 Proceedings of the 2009 IEEE International Conference on Pervasive Computing and Communications – 2009 – P. 1 – 5. – ISBN: 978-1-4244-3304-9.
225. A. Becher Tampering with Motes: Real-World Physical Attacks on Wireless Sensor Networks / Becher A., Benenson Z., Dornseif M. // Security in Pervasive Computing : Lecture Notes in Computer Science. – Berlin: Springer Berlin Heidelberg, 2006. – P. 104 – 118.: ISBN 978-3-540-33376-0.
226. Карпінський М.П. Геометричне моделювання у графічному представленні сенсорних мереж / М.П. Карпінський, С.М. Балабан, В.М. Чиж // Прикладна геометрія та інженерна графіка: Доповіді VIIміжнародної науково-практичної конференції. – К.: Віпол, 2011. – Вип. 87. – С.154 – 158.
227. Detecting Wormhole Attacks in Wireless Sensor Networks / Yurong Xu, Guanling Chen, James Ford, Fillia Makedon. – Springer US. – Volume 253. – P. 267-279. – ISBN: 978-0-387-75461-1.
228. Tun Zaw Wormhole attack detection in wireless sensor networks [Електронний ресурс] / Zaw Tun, Aung Htein Maw // World Academy of Science, Engineering and Technology 46 2008. – P. 545 – 550. – Режим доступу до журн.: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.193.3856&rep=rep1&type=pdf. – Назва з екрану.
229. Скворцов А.В. Триангуляция Делоне и её применение / С.А. Владимирович. – Томск: Изд-во Томского ун-та, 2002. – 128с. – ISBN: 5-7511-1501-5.
230. Резаи В. Создание беспроводных сетей мониторинга промышленного производства [Електронний ресурс] / В. Резаи // Комп'ютерні засоби, мережі та системи. – 2009. – № 8. – Режим доступу до журн.: http://www.dasd.com.ua/kzms/2009/2009_st12.pdf. – Назва з екрану.
231. Voronoi G.M. Nouvelles applications des paramètres continus à la théorie des formes quadratiques. Deuxième mémoire. Recherches sur les parallélloèdres primitifs / G.M. Voronoi // Journal für die reine und angewandte Mathematik. – Volume134. – P. 198 – 287. - ISSN 0075-4102; 1435-5345.
232. Препарата Ф. Вычислительная геометрия: Введение / Ф. Препарата, М. Шеймос – М.: Мир, 1989. – 478 с. – ISBN5-03-001041-6.

233. TOSSIM: accurate and scalable simulation of entire TinyOS applications / Philip Levis, Nelson Lee, Matt Welsh, David Culler // SenSys '03 Proceedings of the 1st international conference on Embedded networked sensor systems . – New York, NY, USA, 2003. – P. 126 – 137 . – ISBN:1-58113-707-9.
234. .Сергиевский М.В. Беспроводные сенсорные сети: эмуляция работы: [Електронний ресурс] / М.В. Сергиевский, С.Н. Сыроежкин // Компьютер Пресс. – 2008. – Часть 4. – http://compress.ru/article.aspx?id=19782 - Назва з екрану.
235. Карпінський М.П. Класифікація атак на безпроводові сенсорні мережі і шляхи їх візуалізації / М. Карпінський, С. Балабан, В. Чиж. // Вісник Тернопільського національного технічного університету [науковий журнал] – Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя, 2012. – С. 191 – 197.
236. Kurytnik I.P. Bezprzewodowa sieć sensorów / I.P. Kurytnik, M. Mikulski, W. Karpiński // Pomiary Automatyka Kontrola. – Warszawa: Wydawnictwo PAK, 2010. – Vol. 56, Nr 6. – P. 548 – 551. – ISSN 0032-4140.
237. Eriksson J. TrueLink: A Practical Countermeasure to the Wormhole Attack in Wireless Networks / J. Eriksson, S.V. Krishnamurthy, M. Faloutsos // Proceedings of the 2006 IEEE International Conference on Network Protocols. – Santa Barbara, CA, 12-15 Nov. 2006. – P. 75 – 84. – ISBN:1-4244-0593-9.
238. Perkins C.E., Mobility Support in IPv6 / Perkins C.E., Johnson D.B. // Proceedings of the 2Nd Annual International Conference on Mobile Computing and Networking MobiCom: MobiCom '96. – New York: ACM, 1996. – P. 27 – 37. – ISBN 0-89791-872-X.
239. Зацепин Д.В. Особенности применения технологии unitesk для тестирования функций мобильности в протоколе IPV6: [Електронний ресурс] / Д.В. Зацепин, В.З. Шнитман // Труды Института системного программирования РАН. - 2007. - № 1, т. 13. – С. 143 – 170. – Режим доступу: http://cyberleninka.ru/article/n/osobennosti-primeneniya-tehnologii-unitesk-dlya- testirovaniya-funktsiy-mobilnosti-v-protokole-ipv6 – Назва з екрану.
240. Пат. 64391 Україна, МПК H04W 12/00. Спосіб візуалізації атаки червоточини в безпровідній сенсорній мережі [Текст] / Карпінський В.М., Євтух П.С. (Україна), Боровік Б.Л., Карпінський М.П. (Польща); заявник та патентовласник Тернопільський національний технічний університет ім. Івана Пулюя. – № u 2011 03578 ; заявл. 25.03.11 ; опубл. 10.11.2011, Бюл. № 21. – 4 с.

241. Wang W. Visualization of Wormholes in Sensor Networks / W. Wang, B. Bhargava // Wireless Security: Workshop ACM WiSE'04. – New York, NY, USA: ACM, 2004. – P. 51 – 60.: ISBN 1-58113-925-X.
242. Євтух П.С. Моделювання візуалізаційного виявлення атак у сенсорній мережі моніторингу електротехнічних систем / П.С. Євтух, В.М. Карпінський // Проблеми енергоресурсозбереження в електротехнічних системах. Наука, освіта і практика. Наукове видання. – Кременчук: КНУ, 2011. – Вип. 1/2011 (1). – С. 322 – 323. – ISSN 2221-5190.
243. Карпінський В.М. Теоретико-графовий підхід до моделювання розподілених безпровідних сенсорних мереж / В.М. Карпінський, П.С. Євтух, Я.І. Кінах // Вісник НТУУ «КПІ». Інформатика, управління та обчислювальна техніка. – 2010. – № 52. – С. 27 – 32. – ISSN 0135-1729.
244. Карпінський В.М. Безпровідні сенсорні мережі: особливості моделювання та візуалізації топології при загрозах /В.М. Карпінський // Сучасна спеціальна техніка. – 2011. – № 2 (25). – С. 55 – 60.
245. Бугрименко Д. Управление беспроводной ЛВС и определение местоположения абонента [Электронний ресурс] / Д. Бугрименко // Cisco Expo 2006 ежегодная конференция по информационным технологиям в Москве. – Режим доступу: ftp://cs.gin.by/upload/scaner/WRLS-UWN-RRM-LBS.pdf. - Назва з екрану.
246. Raport merytoryczny z realizacji zadań badawczych grupy tematycznej «Systemy bezprzewodowe i mobilne oraz ich bezpieczeństwo» [Электронный ресурс]: Projekt PBZ-MNiSzW-02/II/2007 «Usługi i sieci teleinformatyczne następnej generacji – aspekty techniczne, aplikacyjne i rynkowe» : Sprawozdanie / Kier. prof. dr hab. inż. A. R. Pach // Kraków, 23.06.2008. – 250 s. – Режим доступу :https://pbz.itl.waw.pl/raporty/pdf/GT02/GT02-Raport_zbiorczy.pdf. - Назва з екрану.
247. Lee D.T. Two algorithms for constructing a Delaunay triangulation / D.T. Lee, B.J. Schachter // International Journal of Computer & Information Sciences. – Kluwer Academic Publishers-Plenum Publishers, June 1980. – Volume 9, Issue 3. – P. 219 – 242. – ISSN: 0091-7036.
248. Delaunay Triangulation as a New Coverage Measurement Method in Wireless Sensor Network [Електронний ресурс] / Hassan Chizari, Majid Hosseini, Timothy Poston [та ін.] // MDPI. – Basel, Switzerland: Published by MDPI AG,

15 March 2011. – 11 (3). – P. 3163 – 3176. – Режим доступу до журн.: http://www.mdpi.com/1424-8220/11/3/3163/htm. – Назва з екрану.

249. Світличний О.О. Основи геоінформатики : навч. посіб. / О.О. Світличний, С.В. Плотницький. – Суми : ВТД «Університетська книга», 2006. –295 с. – ISBN 966-680-234-1.
250. Bowling G. Kriging [Електронний ресурс] / G. Bowling. – Kansas : Kansas Geological Survey. – 2005. – C&PE 940. – 21 p. – Режим доступу: http://people.ku.edu/~gbohling/cpe940/Kriging.pdf. - Назва з екрану.
251. Дэвис Дж. С. Статистический анализ данных в геологии. В 2 кн.: пер. с англ. / Дж. С. Дэвис ; под ред. Д.А. Родионова. – М.: Недра, 1990. Кн. 1. - 1990. 319 с. – ISBN: – 0-471-08079-9.
252. Дэвис Дж. С. Статистический анализ данных в геологии. В 2 кн. Кн. 1 : пер. с англ. / Дж. С. Дэвис ; под ред. Д.А. Родионова. – М.: Недра, 1990. Кн. 2. – 1990. 425 с. – ISBN: – 5-247-02122-1
253. Іщук О.О. Просторовий аналіз і моделювання в ГІС : навч. посіб. / О.О. Іщук, М.М. Коржнев, О.Є. Кошляков ; за ред. акад. Д.М. Гродзинського. – К.: ВПЦ «Київський університет», 2003. – 200 с.
254. Karlof C. Secure routing in wireless sensor networks: attacks and countermeasures / C. Karlof, D. Wagner // Elsevier’s Ad Hoc Networks Journal, Special Issue on Sensor Network Applications and Protocols. – 2003. – N 1 (2-3). – P. 293 – 315.– ISBN – 978-3-540-36410-8
255. Karbowski K. Podstawy rekonstrukcji elementów maszyn i innych obiektów w procesach wytwarzania / K. Karbowski. – Kraków: Politechnika Krakowska im. Tadeusza Kościuszki, 2008. – 152 p. – ISBN 978-83-61312-59-8.
256. BohlingG. Kriging [Електроний русурс] / Geoff Bohling.– 2005. – 20 с. -Режим доступу до журн.: http://www.ems-i.com/gmshelp/Interpolation/ Interpolation_Schemes/Kriging/Kriging.htm – Назва з екрану.
257. Основы геоинформатики. в 2 т.: учеб. пособ. для студ. вузов / Е.Г. Капралов, А.В. Кошкарев, В.С. Тикунов [и др.] ; под ред. В.С. Тикунова. – М.: Издательский центр «Академия», 2004. Т. 1. – 2004. 352 с. – ISBN: 5-7695-1443-4.
258. Абракітов В.Е. Картографування шумового режиму центральної частини міста Харкова / В.Е. Абракітов. – Х.: ХНАМГ, 2010. – 266 с. – ISBN 978-966-695-178-9.

259. Umer M. Spatial interpolation in wireless sensor networks: localized algorithms for variogram modeling and Kriging / Muhammad Umer , Lars Kulik, Egemen Tanin // GeoInformatica. – Springer US, January 2010. – 14. – P. 101 – 134. – ISSN: 1384-6175.
260. Interpolation for wireless sensor network coverage / R. Tynan, G. M. P. O'Hare, D. Marsh, D. O'Kane // The Second IEEE Workshop on Embedded Networked Sensors, 2005. EmNetS-II. – Sydney, Qld., Australia: IEEE, 31-31 May 2005. – P. 123 – 131 . – ISBN: 0-7803-9246-9.
261. Чиж В. Метод стаціонарних сигнальних точок як засіб аналізу та візуалізації залишкової енергії інформаційних вузлів у безпроводових сенсорних мережах з автономним живленням / В. Чиж, М. Карпінський, С. Балабан // Матеріали 15-ої міжнародної науково-практичної конференції, «Прикладна геометрія та інженерна графіка» – Мелітополь: ТДАУ, 2013. – Вип. 4. – С. 225 – 232.
262. Кучерявый А.Е. Выбор головного узла кластера в однородной беспроводной сенсорной сети [Текст] / А.Е. Кучерявый, А. Салим // Электросвязь: Научно-технический журнал по проводной и радиосвязи, телевидению и радиовещанию. – М.: Общество с ограниченной ответственностью «Инфо-электросвязь» 2009. - N 8. – С. 32 – 36.
263. Методи геометричного моделювання безпроводових сенсорних мереж для аналізу сили сигналів інформаційних вузлів / М.П. Карпінський, В.М. Чиж, С.М. Балабан, Т.О. Яремчук // Вісник Східноукраїнського національного університету імені Володимира Даля. – Луганськ: Видавництво СНУ ім. Володимира Даля, 2013. – Вип. № 15 (204), ч.1. – С. 69 – 76. – ISSN 1998-7927.
264. Чиж В.М. Контроль та візуалізація стану функціональної безпеки інформаційних систем із застосуванням безпроводових сенсорних мереж / В.М.Чиж, М.П. Карпінський, С.М. Балабан // Прикладная радиоэлектроника – Х.: Харьковский национальный университет радиоэлектроники, 2013 – Т. 12, № 2 С. 356 – 362. – ISSN 1727-1290.
265. Моделювання безпроводових сенсорних мереж на підставі кластерів / В.М. Чиж, С.М. Балабан, О.М. Карпінська, В.М. Карпінський // Інформаційна безпека. – Луганськ: Видавництво СНУ ім. Володимира Даля, 2013. – № 1 (9). – С. 155 – 164. – ISSN 2224-9613.
266. Кулаков Ю.И. Теория физических структур. (Математические начала физической герменевтики) / Ю.И. Кулаков. – Новосибирск: Альфа Виста, 2004. – 851 с. – ISBN 5-88119-008-4.

267. Чиж В. Алгоритм побудови та дослідження структури кластера при геометричному моделюванні безпроводових сенсорних мереж / В. Чиж, О. Демчишин, М. Карпінський, С. Балабан // Збірник наукових праць «Будівництво та техногенна безпека» – Сімферополь: Національна академія природоохоронного та курортного будівництва, 2012. – Вип. 41. – С. 246 – 251.
268. Мандельброт Бенуа. Фрактальная геометрия природы / БенуаМандельброт. – Ижевск : Институт компьютерных исследований, 2010. – 756 с. – ISBN 978-5-93972-872-0.
269. Шредер М. Фракталы, хаос, степенные законы. / М. Шредер. – Ижевск: РИЦ «Регулярная и хаотическая динамика», 2001. – 528 с. – ISBN 5-93972-041-2.
270. Моделювання безпроводових сенсорних мереж на підставі кластерів / В.М. Чиж С.М. Балабан О.М. Карпінська В.М. Карпінський // Інформаційна безпека. – Луганськ: Видавництво СНУ ім. Володимира Даля, 2013. – № 1 (9). – С. 155 – 164. – ISSN 2224-9613.

Для нотаток

Для нотаток

Наукове видання

Александер М.Б., Балабан С.М., Карпінський М.П.,
Райба С.А., Чиж В.М.

Інформаційна безпека в середовищі безпроводових сенсорних мереж

МОНОГРАФІЯ

Редактор *Є.І. Гриценко*
Комп'ютерне верстання *А.П. Катрич*

Формат 60х90/16. Обл. вид. арк. 6,34 Тираж 300 пр. Зам. № 2718.

Видавництво Тернопільського національного
технічного університету імені Івана Пулюя.
46001, м. Тернопіль, вул. Руська, 56.
Свідоцтво суб'єкта видавничої справи ДК № 4226 від 08.12.11.