Міністерство освіти і науки, молоді та спорту України

Тернопільський національний технічний університет імені Івана Пулюя

КАРПІНСЬКИЙ ВОЛОДИМИР МИКОЛАЙОВИЧ

УДК 004.94: 621.39

МЕТОДИ ТА АПАРАТНО-ПРОГРАМНІ ЗАСОБИ МОДЕЛЮВАННЯ ВІДБОРУ ІНФОРМАЦІЇ В БЕЗПРОВІДНИХ МЕРЕЖАХ ДАВАЧІВ СИСТЕМ ЕЛЕКТРОПОСТАЧАННЯ

01.05.02 – математичне моделювання та обчислювальні методи

Автореферат дисертації на здобуття наукового ступеня
кандидата технічних наук

Тернопіль-2012

Дисертацією є рукопис.

Робота виконана у Тернопільському національному технічному університеті імені Івана Пулюя Міністерства освіти і науки, молоді та спорту України.

Наукові керівники: доктор технічних наук, професор
Євтух Петро Сільвестрович,
Тернопільський національний технічний університет імені Івана Пулюя, завідувач кафедри систем електроспоживання та комп'ютерних технологій в електроенергетиці

доктор технічних наук, професор
Куритнік Ігор Петрович,
Університет в Бєльську-Бялій (Польща),
завідувач кафедри електротехніки та автоматики

Офіційні опоненти: доктор технічних наук, професор
Широчин Валерій Павлович,
Національний технічний університет України "Київський політехнічний інститут", професор кафедри обчислювальної техніки

доктор технічних наук, професор
Лупенко Сергій Анатолійович,
Тернопільський національний технічний університет імені Івана Пулюя, завідувач кафедри комп'ютерних систем та мереж

Захист відбудеться "_28_" вересня 2012 р. о "_11^{00}_" год. на засіданні спеціалізованої вченої ради К 58.052.01 у Тернопільському національному технічному університеті імені Івана Пулюя за адресою: 46001, м. Тернопіль, вул. Руська, 56, ауд.79.

З дисертацією можна ознайомитися в науково-технічній бібліотеці Тернопільського національного технічного університету імені Івана Пулюя за адресою: 46001, м. Тернопіль, вул. Руська, 56.

Автореферат розісланий "_27_" серпня 2012 р.

Учений секретар
спеціалізованої вченої ради Шелестовський Б.Г.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Гостра потреба в енергозбереженні диктує необхідність розвитку нових інформаційних технологій, що базуються на безпровідних сенсорних мережах (БСМ), які є найперспективнішими засобами для контролю енергоспоживання, будучи однією з основних складових моделі “інтелектуальних” електромереж. Неврахування загроз і відповідних атак на БСМ може не тільки призвести до аномального режиму функціонування стратегічно важливої “інтелектуальної” системи електропостачання, а й, як наслідок, вивести з ладу, наприклад, атомну електростанцію, що довели нещодавні спільні американо-ізраїльські випробування.

Важливим завданням є математичне моделювання спеціальних режимів роботи БСМ з врахуванням їх безпеки, що, у поєднанні з розвитком інтегрованих дистанційних давачів, належить до одного чільних наукових напрямків реалізації найважливіших викликів інженерії XXI сторіччя, визначених науковим фондом NSF, а також передбачених до виконання відповідною Постановою Президії НАН України.

Математичним моделям класичних систем і мереж, зокрема на підставі графів, присвячені праці багатьох вчених, серед яких: Бакулина М. А., Виноградов Д. В., Дунець Р. Б., Fax J., Jadbabaie A., Касьянов В. Н., Кочкаров А. А., Krzywdziński K., Lin Z., Olfati-Saber R., Панюкова Т. А., Парасюк І. М., Ren W., Сергієнко І. В., Скороходов В. А., Старостин Н. В., Tanner H., Фельк З. А., Чукарин А. В., Юрасов П. В. та ін.

Однак, за результатами аналізу наукових публікацій щодо моделювання БСМ систем електропостачання при відборі інформації виявлено проблемні науково-технічні питання, що потребують глибшого дослідження відомих моделей або створення нових і, в першу чергу, математичних моделей для оцінювання керованості та зв’язності сенсорних вузлів в розподіленій БСМ “інтелектуальної” системи електропостачання та моделей БСМ для оцінювання спостережуваності в умовах дії загроз із врахуванням напрямів інформаційних потоків, що враховували б особливості диспетчеризації “інтелектуальних” систем електропостачання, підвищували надійність їх функціонування та ефективність прийняття рішень оператора.

Необхідністю розробки комплексу моделей спеціальних режимів роботи БСМ та розв’язання зазначених задач математичного моделювання обумовлена актуальність теми дисертаційного дослідження, що має важливе прикладне значення для побудови ефективних “інтелектуальних” електромереж із застосуванням для диспетчеризації стійких до загроз БСМ.

Зв’язок роботи з науковими програмами, планами, темами. Дисертаційна робота виконувалася у Тернопільському національному технічному університеті імені Івана Пулюя (ТНТУ ім. І.Пулюя) за держбюджетним договором на виконання науково-дослідних робіт Міністерства освіти і науки, молоді та спорту України за темою “Виявлення та облік прихованого відбору електроенергії у високовольтних мережах методами комп’ютерних технологій” (ДР № 0109U002293) (2009-2011 рр., виконавець).

Мета і задачі дослідження. Метою дисертаційної роботи є удосконалення математичних моделей режимів функціонування безпровідних сенсорних мереж для забезпечення їх захисту від атак за рахунок використання методів візуалізації та зважених графів, які дозволять прогнозувати небезпечні стани та приймати адекватні рішення при збільшенні точності визначення місць розташування джерел інформації чи збурень, зменшенні часових та вартісних витрат на проведення модельних експериментів.

Основні задачі дослідження, відповідно до поставленої мети роботи, полягають у наступному.

1. Провести аналіз математичних моделей відбору інформації в безпровідних мережах давачів систем електропостачання з метою виявлення чинників, що істотно впливають на ефективність функціонування БСМ.

2. Дослідити та прокласифікувати моделі загроз, які зумовлюють аномальні режими роботи БСМ систем електропостачання, для виявлення найбільш критичних атак.

3. Проаналізувати та змодифікувати моделі режимів роботи БСМ на основі теорії зважених графів для отримання покращених якісних та кількісних показників зв’язності та спостережуваності в БСМ з врахуванням можливих загроз та збурювальних чинників.

4. Розробити ефективний метод візуалізації при моделюванні БСМ на основі побудови та семантичного аналізу топологічної поверхні сенсорної мережі для підвищення точності та зменшення часу виявлення місць збурень, на прикладі візуального виявлення атаки “червоточини”.

5. Створити апаратно-програмні засоби моделювання режимів відбору інформації та безпечного доступу в БСМ систем електропостачання для підвищення надійності їх роботи, зменшені часових та вартісних витрат на проведення модельних експериментів.

Об’єкт дослідження – процеси математичного моделювання режимів функціонування безпровідних сенсорних мереж в системах електропостачання для забезпечення їх захисту від атак.

Предмет дослідження – математичні моделі та засоби моделювання режимів функціонування безпровідних сенсорних мереж систем електропостачання для забезпечення їх захисту від атак і побудови методів та алгоритмів боротьби з цими атаками.

Методи дослідження. Теорія передавання інформації, теорія множин, теорія графів, теорія керування і теорія математичного моделювання для побудови математичних моделей режимів функціонування безпровідних сенсорних мереж, обчислювальна геометрія та обчислювальні методи для розробки методу візуального виявлення атаки червоточини в безпровідній сенсорній мережі, створення апаратно-програмних засобів моделювання відбору інформації та безпечного доступу в безпровідних мережах давачів систем електропостачання.

Наукова новизна роботи.

1. Удосконалено модель БСМ на основі методу зважених графів для оцінювання відтворення її топології та спостережуваності, яка відрізняється новою архітектурою та меншою складністю порівняно із ретрансляційною концепцією чи принципом

мобільного центрального вузла, що дозволяє мінімізувати обсяг обміну інформацією між сенсорними вузлами та центральним вузлом чи досягти незмінності обсягу обміном інформацією від відстані між сенсорними вузлами до центрального вузла.

2. Вперше одержано модифіковані моделі загроз, що зумовлюють аномальні режими роботи БСМ, а також моделі режимів протидії атакам на БСМ, які відрізняються застосуванням методу зважених графів відповідно до запропонованої класифікації атак, що дозволяє визначити шлях вдосконалення щодо виявлення найкритичніших атак і підвищити ефективність та результативність розроблюваних методів та засобів протидії потенційним загрозам.

3. Вперше розроблено візуалізаційний метод моделювання для виявлення потенційно небезпечних загроз маршрутизації в БСМ, який відрізняється внесенням та виконанням візуальних семантико-вимірювальних операцій, що дозволило частково автоматизувати та зменшити час на проведення аналізу та прийняття рішення по виявленню та локалізації загрози в БСМ згідно із запропонованою ознакою її ідентифікації, в тому числі для оперативного керування сенсорною мережею в протидіях певному типу атак.

Практичне значення одержаних результатів. На базі отриманих теоретичних результатів розроблено математичні моделі, методи та засоби моделювання режимів відбору інформації в безпровідних мережах давачів систем електропостачання, які можуть використовуватися під час експлуатації та вирішення задач диспетчеризації цих систем в різних режимах їх функціонування, включаючи аномальні, що викликані різного типу загрозами на сенсорну мережу.

На основі запропонованих методів реалізовано програмні засоби моделювання на мові C#, що дали можливість отримати відомості щодо характерних особливостей функціонування системи безпровідного передавання динамічного стрибкоподібного коду і створити комплексну апаратно-програмну систему безпечного доступу в БСМ.

Практична цінність роботи полягає у тому, що на отриманій експериментальній основі прикладу моделювання виявлення атаки “червоточини” в БСМ, реалізовано візуалізаційний метод викриття цієї атаки, завдяки чому поряд зі зменшенням часу прийняття рішення та розширенням функціональних можливостей, одночасно підвищена точність виявлення атаки червоточини, досягнуто абсолютної похибки визначення положення сенсорів в межах $\pm 7{,}5\ldots75 \cdot 10^{-2}$ м по відношенню до розмірів мережі та похибки інтерполяції під час згладжування реконструйованої топологічної поверхні сенсорної мережі $\pm 2\ldots3 \cdot 10^{-2}$ мкм, що є вкрай необхідним для рішення спеціальних задач, в яких сенсори розміщені в обмеженому просторі.

Додатковим фактором практичної цінності роботи є здійснення моделювання та імплементації швидкого перетворення Фур'є в системі типу Xilinx із застосуванням програмованих логічних матриць серії Virtex-5, завдяки чому підвищено вчетверо швидкодію та зменшено вдвічі енергоспоживання на відміну від аналога попередньої серії в БСМ.

Теоретичні та практичні результати дисертаційної роботи використані та впроваджені: при виконанні науково-дослідної роботи “Виявлення та облік прихованого відбору електроенергії у високовольтних мережах методами комп’ютерних технологій” (ДР № 0109U002293), що виконувалася в ТНТУ

ім. І.Пулюя, а також у навчальному процесі ТНТУ ім. І.Пулюя в курсі “Телеметрія та комп’ютерні технології в електроенергетиці” та Університету в Бєльську-Бялій, Польща (УББ) при викладанні дисциплін “Мережеві інформаційні технології” та “Безпека інформаційних технологій”, згідно з Договором про співпрацю між УББ і ТНТУ ім. І.Пулюя.

Особистий внесок здобувача. Основний зміст роботи, всі основні наукові положення, теоретичні та практичні розробки, висновки та рекомендації виконані автором особисто. В друкованих працях, опублікованих в співавторстві, здобувачеві належать: побудовано і реалізовано структуру, здійснено функціональну симуляцію та проведено верифікацію моделі засобу швидкого перетворення Фур'є для оброблення сигналів в режимі реального часу в безпровідній сенсорній мережі на основі демонстраційної плати типу Xilinx із застосуванням програмованих логічних матриць серії Virtex-5 [1], удосконалено модель захищеного безпровідного передавання динамічного стрибкоподібного коду у сенсорній мережі [2], сформульовано та обґрунтовано теоретико-графовий підхід до моделювання розподілених сенсорних мереж “інтелектуальних” систем електропостачання [4], обґрунтовано модель лідер-повторюваної топології гетерогенної безпровідної сенсорної мережі та проведено її оцінювання методами теорії графів, а також визначено достатні та необхідні умови для забезпечення зв’язності та керованості мережі [5], розроблено розширену класифікацію моделей атак на безпровідні сенсорні мережі відповідно до рівнів OSI (Open Systems Interconnection Reference Model) [7], розроблено моделі ідентифікації та локалізації збурювальних факторів-загроз відповідно до рівнів теоретичної моделі структури мережевої комунікації в безпровідній сенсорній мережі системи електропостачання [8], опрацьовано результати дослідження ефективності цифрового перетворення сигналів із застосуванням мікроконтролера з сімейства dsPIC [9, 28], проведено тестування системи безпечного передавання даних в телекомунікаційній мережі та опрацьовано отримані результати [10, 27], розроблено модель топології безпровідної персональної мережі та алгоритм вибору раціонального маршруту в цій мережі [11], оцінено рівень безпеки криптосистеми на еліптичних кривих [12], досліджено ризик витоку інформації про приватний ключ під час часового криптоаналізу методів піднесення до степеня за модулем [13], виконано оцінювання способів криптоаналізу шифрів на підставі еліптичних кривих із застосуванням програмованих логічних інтегральних схем [14], проведено аналіз методів та стандартів передавання даних у вимірювально-керуючих системах [15], розроблено обчислювальні методи, призначені для згладжування та візуалізації реконструйованої топологічної поверхні безпровідної сенсорної мережі при виявленні атаки червоточини, а також здійснено програмно-апаратну реалізацію методу [16], розроблено модуль безпровідного керування “інтелектуальної” системи електропостачання, зокрема призначеної для живлення ламп освітлення, який базується на компонентах трансивера ZigBee та мікроконтролера типу PIC24HJJ256 [17], отримано результати аналізу методів візуалізації атак в безпровідних сенсорних мережах та модель розповсюдження радіосигналу із врахуванням змішаного шуму, що описується функціями Бесселя з уявним аргументом нульового та вищих порядків [18], запропоновано та обґрунтовано локально-стохастичний

метод просторової кригінг-інтерполяції реконструйованої топологічної поверхні для моделювання візуального виявлення атаки червоточини в безпровідній сенсорній мережі моніторингу електротехнічних систем [19], побудовано та реалізовано засіб для моделювання безпечного безпровідного передавання інформації на підставі прототипної плати, побудованої на базі 16-бітного мікроконтролера типу PIC24FJ128, із під'єднаними схемами шифратора і дешифратора KeeLoq [22], проведено аналіз результатів дослідження системи оброблення та моделювання сигналів витоку інформації [23], розроблено модель оцінювання енергоефективності безпровідної мережі [24], розроблено підхід до збільшення безпеки комунікації приймодавачів в безпровідних сенсорних мережах [25], визначено структуру розподіленої обчислювальної системи для розв'язування задачі дискретного логарифму еліптичної кривої [26], створено програму, що базується на бібліотеках MPI2 та MIRACL, для оцінювання часу розв'язання дискретного логарифма на еліптичних кривих у багатопроцесорному середовищі з різними типами пам'яті [29], проаналізовано криптоатаки на підставі витоку інформації з побічних каналів та методи протидії їм [30], виконано аналіз результатів дослідження можливостей комунікації мікроконтролера типу DS80C400 MAXIM/Dallas в якості сервера в локальній мережі [31].

Апробація результатів дисертації. Основні положення та результати дисертаційної роботи доповідалися і обговорювалися на: XV Міжнародному семінарі метрологів „Методи і техніка перетворення сигналів при фізичних вимірюваннях МСМ'07" (Львів-Ряшів, 2007 р.), V, VI, VII та VIII Міжнародних науково-практичних конференціях "Інформаційні технології та безпека в управлінні" (ITSM'2008-ITSM'2011) (Крим, 2008-2011 рр.), 9th International Conference "Modern Problems of Radio Engineering, Telecommunications and Computer Science" (TCSET'2008) (Львів-Славсько, 2008), 12 науковій конференції Тернопільського державного технічного університету імені І. Пулюя (Тернопіль, 2008), 9th International Workshop "Computational Problems of Electrical Engineering" (CPEE'08) (Алушта, 2008), Xth International Conference "The Experience of Designing and Application of CAD Systems in Microelectronics" (CADSM 2009) (Львів-Поляна, 2009), VII Міжнародній науково-практичній конференції "Проблеми впровадження інформаційних технологій в економіці" (Ірпінь, 2009) , IV Міжнародній науково-технічній конференції DESSERT'2009 (Кіровоград, 2009), Всеукраїнськській науковій конференції Тернопільського державного технічного університету ім. І.Пулюя (Тернопіль, 2009 р.), 4th International Conference "Advanced Computer Systems and Networks: Design and Application" (ACSN-2009) (Львів, 2009), VI науково-практичному семінарі "Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС, навчальному процесі, взаємодії з іншими службами" (Львів, 4 грудня 2009 р.), Міжнародній науково-практичній конференції "Інформаційні технології та комп'ютерна інженерія" (ITKI 2010) (Вінниця, 2010), XI Науковій конференції "Czujniki Optoelektroniczne i Elektroniczne" (COE 2010) (Наленчув, Польща, 2010), 3 Міжнародній науково-технічній конференції "Підвищення ефективності енергоспоживання в електротехнічних пристроях і системах" (Луцьк – Шацькі озера, 2010), XIII International Conference "Problems of Energy and Resource Saving in Electrical Systems. Science, Education and

Practice" (PEES 2011) (Кременчук, 2011), 11th International Conference "Knowledge in Telecommunication Technologies and Optics" (KTTO 2011) (Щирк, Польща, 2011).

Наукові результати дисертаційної роботи розглядалися та обговорювалися в Державному технологічному університеті (м. Черкаси), Університеті в Бєльську-Бялій (Польща). В цілому роботу апробовано у Національному технічному університеті імені Івана Пулюя (м. Тернопіль), Національному технічному університеті України "Київський політехнічний інститут" (м. Київ), Прикарпатському національному університеті імені Василя Стефаника (м. Івано-Франківськ), Східноукраїнському національному університеті ім. В. Даля (м. Луганськ), Державному економічному університеті (м. Одеса).

Публікації. Основні результати дисертаційних досліджень опубліковані в 30 наукових роботах і одному патенті, 15 із них – наукові статті, 11 з яких – статті у наукових фахових виданнях України, 1 наукова стаття у збірнику наукових праць Технічного інституту Державної вищої технічної школи у Новому Сончі (Польща) та 3 наукові статті в центральних закордонних наукових журналах (інформація про яких та друковані в них анотації статей і/або статті розміщені в мережі Інтернет, а також міжнародних базах даних IEE INSPEC, SCOPUS, ULRICHSWEB, INDEX COPERNICUS, GOOGLE SCHOLAR, BAZTECH та до складу редколегій яких входить достатня кількість професорів, докторів технічних наук за профілем дисертації, з них 2 статті у журналі з філадельфійського списку (ISI Master Journal List), імпакт-фактор якого становить 0.242), та 15 – публікації в матеріалах конференцій і семінару, з них 11 міжнародних конференцій.

Структура та обсяг роботи. Дисертаційна робота складається із вступу, чотирьох розділів, висновків, списку використаних джерел із 232 найменувань і додатків. Загальний обсяг дисертації становить 208 сторінок, з яких основний зміст викладений на 178 сторінках, містить 45 рисунків, 4 таблиці.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі наведено загальну характеристику роботи, обґрунтовано її актуальність, сформульовано її мету та основні задачі досліджень, визначено методи вирішення поставлених задач, сформульовано наукову новизну роботи та практичну цінність одержаних результатів, викладено короткий зміст роботи. Наведені дані про впровадження результатів роботи, її апробацію та публікації.

У першому розділі наведено аналіз моделей відбору інформації в безпровідних мережах давачів системах електропостачання. Проаналізовано типи безпровідних мереж, їх компоненти та прикладні особливості застосування. Показано, що перспективним, з точку зору надання якості послуг та енергоощадності, є безпровідне передавання вимірювально-керуючих даних на короткі та середні відстані за допомогою гомогенних і гетерогенних БСМ. Обґрунтовано, що для вирішення завдань їх надійного функціонування доцільно модифікувати теоретико-графові підходи моделювання режимів роботи БСМ.

Розглянуто моделі гомо- та гетерогенних БСМ за характером оцінювання топологічного стану, моніторингу та керування при відборі з них інформації для керування електропостачанням в "інтелектуальних" електромережах. Здійснено порівняльний аналіз різних моделей БСМ, в тому числі призначених для розв'язання

задачі взаємного узгодження в сенсі моніторингу та керування гомогенної мережі, в якій топологічний стан, зокрема положення кожного сенсорного вузла описано моделлю в дискретному часі $k = \{0, 1, 2, ...\}$:

$$x_i(k+1) = x_i(k) + u_i(k), \tag{1}$$

де $u_i(k)$ – приріст відстані, що відповідає вхідному радіосигналу $u_i(t)$ для *i*-го вузла ϑ_i, кількість сусідніх сенсорів якого становить *n* в момент часу $t \in [0, \infty)$.

Оцінено зв'язність вузлів для координованого керування в комутованих топологіях БСМ із врахуванням динамічно змінюваної матриці суміжності. Сформовано вимоги до побудови моделі гібридного контролю топологічного стану БСМ в дво- та тривимірному просторі з теоретико-інформаційної точки зору.

Проведено аналіз і дослідження моделей класів гетерогенних БСМ: а) заснованих на однорангових топологіях і багаторівневих структурах лідер-послідовник, б) побудованих на розподілених в просторі комплектах сенсорних вузлів, кожен з яких інтегрований з мікропроцесором, трансивером (приймодавачем), а в деяких випадках виконавчим механізмом.

Обґрунтовано переваги та недоліки підходів для побудови моделей координації чи узгодження в розподіленій БСМ – багатоетапної передачі, в якій беруть участь декілька проміжних вузлів-ретрансляторів, на основі мобільних центральних вузлів, із застосуванням узгоджувального розподіленого фільтру Кальмана, на підставі стохастичного методу для формування оптимальних маршрутів, з пакетним виділенням каналів. Розглянуто типи безпровідних мереж, прикладні аспекти застосування БСМ, поділ засобів включно з інтерфейсами, комп'ютерними та телекомунікаційними мережами, методи і стандарти відбору інформації в системах електропостачання, зокрема при безпровідному передаванні вимірювально-керуючих даних на короткі та середні відстані.

Сформовано вимоги до модифікації та побудови покращених моделей відбору інформації в безпровідних мережах давачів системах електропостачання, приймаючи до відома потенційну піддатливість БСМ та рекомендації фонду NFS і НАН України як одного з 14-ти пріоритетних наукових напрямків розвитку інженерії цього сторіччя із врахуванням загроз та забезпеченням комплексного захисту інформації, включаючи ефективні методи виявлення атак та прийняття рішення по локалізації зловмисника із застосуванням удосконалених теоретико-графових підходів.

У другому розділі подано результати розроблення автором моделей теоретико-графового підходу до моделювання розподілених БСМ. Дисертантом здійснено розподілене оцінювання топологічного стану в гетерогенних мережах на основі графів. Проведено аналіз моделей загроз режиму роботи БСМ та способів моделювання візуального виявлення цих загроз.

Проведено теоретичні дослідження процесів функціонування компонентів БСМ в умовах дії збурювальних факторів моделюванням на основі орієнтованого зваженого графа $G(V, E, w)$, 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, $|V(G)|$ і $|E(G)|$ – порядок і розмір графа, $|\ |$ – символ для позначення кардинального числа (рис. 1).

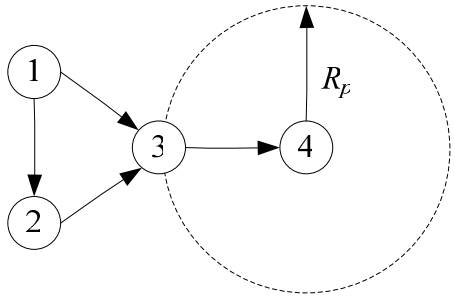


Рис. 1. Орієнтований граф на вузлах $V=\{1, 2, 3, 4\}$ з набором дуг $E=\{(1, 2), (1, 3), (2, 3), (3, 4)\}$ з R_p-кругом суміжності

Співставлено граф взаємодії з наявними інформаційними потоками, в якому вузли відповідають сенсорам, а дуги – доступним міжсенсорним каналам зв'язку. Отримано математичну модель залежності швидкості передачі даних від часу та відстані між вузлами, ґрунтуючись на правилі найближчих сусідів, суть якої зводиться до оптимізації міжсенсорної комунікації за критерієм швидкодії:

$$v_*\left(\Delta t_{ij}, \Delta x_{ij}\right) = \frac{\beta_i \sum\limits_{j \in n} w_{ij}\left(x_i(t) - x_j(t)\right)}{\Delta t_{ij}\ v_{пот}}, \qquad (2)$$

де $x_i(t) \in \Re^n$ – вектор стану сенсора ϑ_i в момент часу t, що характеризує його положення, виражене, зокрема, у відстані; β_i, w_{ij} – вагові коефіцієнти, що визначаються для конкретної БСМ; n – 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; $v_*\left(\Delta t_{ij}, \Delta x_{ij}\right)$ – швидкість передачі даних у відносних одиницях, причому $\Delta x_{ij} = \left(x_i(t) - x_j(t)\right)$.

Показано, 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.

Сформовано алгоритм оцінювання топологічного стану гетерогенної БСМ:

$$\frac{dx_i}{dt} = \beta_i \sum_{j \in n(i)} w_{ij}(x)\ f\left(x_j(t) - x_i(t)\right),\ x_i(0) = u_i,\ i = 1, ..., n, \qquad (3)$$

де $u_i \in \Re$ – вихідний радіосигнал давача вузла (вершини) ϑ_i, $i = \{1, ..., n\}$; x_i – в даному випадку радіосигнал суміжного компонента, пов'язаного з вершиною ϑ_i.

Ґрунтуючись на сформованому алгоритмі, центральні вузли здійснюють вибірку даних спостереження

$$y(t) = \varphi(x(t)), \qquad y(t) \in \Re^q,\ q << n, \qquad (4)$$

де q – наявна кількість центральних вузлів, причому $x(t) = \left[x_1(t), ..., x_n(t)\right]^T$,

та задача в подальшому зводиться до однозначного визначення $u = [u_1, ..., u_n]^T$ із $y(t)$ шляхом розв'язання системи рівнянь

$$\begin{cases} \dot{x} = -L(G_s)x,\ x(0) = u, \\ y = Mx, \end{cases} \tag{5}$$

де $L(G_s)$ – лапласівська матриця графу, що відповідає БСМ, (надалі використовується позначення L_s); $M \in \Re^{q \times n}$ – матриця даних моніторингу.

Доведено, що система (5) стійка та $x_i(t)$ збігається до $\sum_1^n u_i / n$ для всіх $i \in \{1, n\}$ та $w_{ij} = const$. Ґрунтуючись на теорії керування та припущенні спостережуваності системи $(-L_s, M)$, показано, що можна повністю відновити її початковий стан $x(0)$ на підставі даних моніторингу $y(t)$.

Інший алгоритм моніторингу на основі (5) та нескладний спосіб відновлення інформації, виходячи з наявних статичних параметрів, полягає у розв'язанні системи

$$\begin{cases} \dot{x} = Ax,\ x(0) = x_0, \\ y = Mx, \end{cases} \tag{6}$$

де A – матриця суміжності графа.

Надано відмінності графовій моделі архітектури мережі, яка полягає в тому, що в БСМ інформаційні потоки спрямовані від сенсорних вузлів до центрального вузла, тоді як у лідер-повторюваній топології інформаційні потоки напрямлені від лідерів до послідовників. Показано, що завдяки такій кластерній архітектурі мережі є можливість зменшити обсяг переданої інформації, а це в свою чергу збільшує швидкодію, надійність та покращує інші техніко-економічні показники функціонування БСМ. Сформульовано достатню умову для не повністю керованої БСМ. Подано теоретичну інтерпретацію із застосуванням графів для задач керованості та спостережуваності.

Обґрунтовано, що удосконалити методи моделювання візуального виявлення атак в мережі, а також поліпшити розуміння та ілюстрацію потенціалу запропонованих в подальшому методів та апаратно-програмних засобів можна в нерозривному поєднанні з розробкою більш детальної класифікації моделей атак на БСМ, що наведено в третьому розділі дисертації.

У третьому розділі здійснено моделювання режимів роботи БСМ. Зокрема, розширено класифікацію моделей атак на БСМ. Удосконалено моделювання режимів протидії атакам на БСМ методами теорії нечітких орієнтованих зважених графів. Одержано ознаку ідентифікації зловмисного вузла у БСМ, що полягає в обчисленні подібності зв'язків сусідів між двома підозрілими вузлами і дає змогу автоматизувати процес виявлення атаки. Розроблено моделі та методи запобігання загрозам на БСМ, суть яких зводиться до поєднання заходів безпеки, включно з криптографічними методами, та технологій моніторингу БСМ і теоретико-графових засад на рівнях теоретичної моделі структури мережевої комунікації, методів тріангуляції та візуалізації. Розроблено запатентований автором метод моделювання візуального виявлення атаки червоточини в БСМ.

Запропоновано ідентифікацію та класифікацію моделей атак в БСМ за критеріями зв'язку з різними рівнями моделі OSI та характером впливу (активні та пасивні). Описано модель топології БСМ і особливості моделювання режимів протидії атакам на ці мережі. Розглянуто адекватність пристосування моделі до динамічних змін структурної та алгоритмічної організації систем і методів моделювання БСМ в цих умовах, забезпечуючи подальше функціонування мережі, особливо за наявності таких небезпечних атак маршрутизації, якими є вибране переадресування, воронкова атака, атаки Сибіли чи червоточини.

Оцінено: а) адаптацію зміннокодової системи, в якій передбачено динамічний код і зміну ключа, для моделювання безпеки в БСМ систем електропостачання; б) підхід до пришвидшення виявлення атак в БСМ та прийняття оператором рішення по їх локалізації шляхом підвищення швидкодії цифрового оброблення сигналів із застосуванням швидкого перетворення Фур'є (ШПФ) в спеціально десигнованому компоненті, що зумовило необхідність проведення в четвертому розділі дисертації функціональної симуляції та верифікації моделей засобів ШПФ.

Розроблено вперше метод безпечної локалізації вузлів в БСМ відповідно до схем моделей розподілу криптографічних ключів і методів тріангуляції. Суть методу полягає у визначенні розміщення вузла та захисті його розташування. Представлено підхід до виявлення атак маршрутизації в БСМ, що об'єднує заходи безпеки та методи візуалізації, згідно з ним здійснюється моніторинг зв'язності сусідів між безпровідними вузлами та змін в топології мережі, а також визначаються підозрілі вузли через візуалізацію аномалій, викликаних підробленими ідентичностями.

Розроблено ефективний засіб моделювання виявлення атак маршрутизації в БСМ згідно з інтегрованими моделями безпеки та методами візуалізації. Основу засобу становить контролер, в якому накопичуються статистичні дані про топологію БСМ, ідентифікуються та виявляються підозрілі вузли. Система зосереджується на візуалізації та спостереженні важливих моделей інформації про топологію мережі. Впроваджено інтелектуальні алгоритми для виявлення потенційних аномальних подій і забезпечення додаткових методів перевірки.

Сформульовано ознаку ідентифікації зловмисного вузла $I_{n1,n2}$ на підставі зібраної інформації про топологію БСМ з врахуванням подібності зв'язків між двома підозрілими суміжними вузлами *n1* та *n2*:

$$I_{n1,n2} = \left(R_{n1}^{T} \cap R_{n2}^{T}\right) / \left(R_{n1}^{T} \cup R_{n2}^{T}\right), \quad 0 \le I_{n1,n2} \le 1. \qquad (7)$$

де R_{n1}^{T} – набір сусідів вузла *n1* в оновленій мережевій топології *T*.

Запропонована ознака ідентифікації зловмисного вузла $I_{n1,n2}$ за допомогою вагових коефіцієнтів 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 змогу контролеру автоматично виявляти атаку, а оператору – спростити процедуру виявлення зловмисного вузла та пришвидшити прийняття рішення щодо його подальшої локалізації на підставі відповідного списку сенсорних вузлів, сформованого на підставі вищезгаданої ознаки $I_{n1,n2}$.

Розроблено модель системи безпеки БСМ, що полягає у моніторингу топології мережі згідно з розробленим удосконаленим методом виявлення атаки та міжкомпонентній взаємодії систем безпеки та візуалізації шляхом 3D- і 2D-переглядів та порівняння структур у вікні моделі організації взаємодії, а також здійснено аналіз результатів моделювання по виявленню атаки маршрутизації. Адекватність удосконаленого методу підтверджено результатами комп'ютерного моделювання, здійсненого протягом двох етапів: 1) на першому етапі використано модель ns-2 (Network Simulator) для симуляції процедури викриття суміжного вузла, а також розголошення топології до контролера; 2) під час другого етапу здійснено спробу виявлення атаки маршрутизації і знаходження підроблених ідентичностей, а також проведено відповідне тестування.

Висвітлено метод моделювання візуального виявлення атаки червоточини в БСМ, новизна якого підтверджена отриманням покращених результатів, висвітленням у публікаціях та захищена патентом. В даному методі передбачено виконання таких етапів та математичних числень: вимірювання відстані між сенсорами на підставі рівня потужності прийнятого радіосигналу; реконструювання топологічної поверхні БСМ та обчислення віртуального положення кожного сенсора з унаочненням зображення; згладжування реконструйованої топологічної поверхні БСМ на підставі методу з комп'ютерною графікою із застосуванням просторової кригінг-інтерполяції.

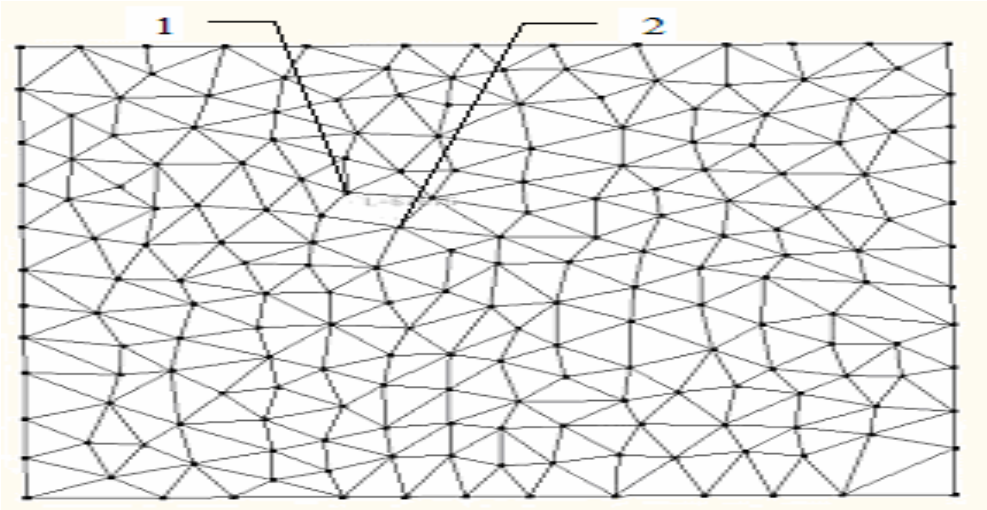
У четвертому розділі подано результати розробки та дослідження методів і програмно-апаратних засобів моделювання відбору інформації в БСМ. Наведено систему моделювання безпечної комунікації в БСМ. Розглянуто реалізацію запатентованого способу моделювання візуального виявлення атаки червоточини в БСМ. Висвітлено результати функціональної симуляції та верифікації моделі засобу ШПФ для оброблення сигналів в БСМ в режимі реального часу, як додаткового фактора для практичної цінності щодо підвищення швидкодії та зменшення енергоспоживання в БСМ.

Виконано верифікацію моделі архітектури засобу ШПФ, здійснивши попередньо його функціональну симуляцію на програмованій логічній інтегральній схемі серії Virtex-5 із наведенням часових діаграм роботи пристрою в середовищі Xilinx ISE 11.1. Аналіз результатів проведеної верифікації зазначеної моделі свідчить про збільшення вчетверо швидкодії ШПФ в порівнянні з відомим аналогом попередньої серії, що є достатнім для оброблення сигналів в БСМ в реальному часі.

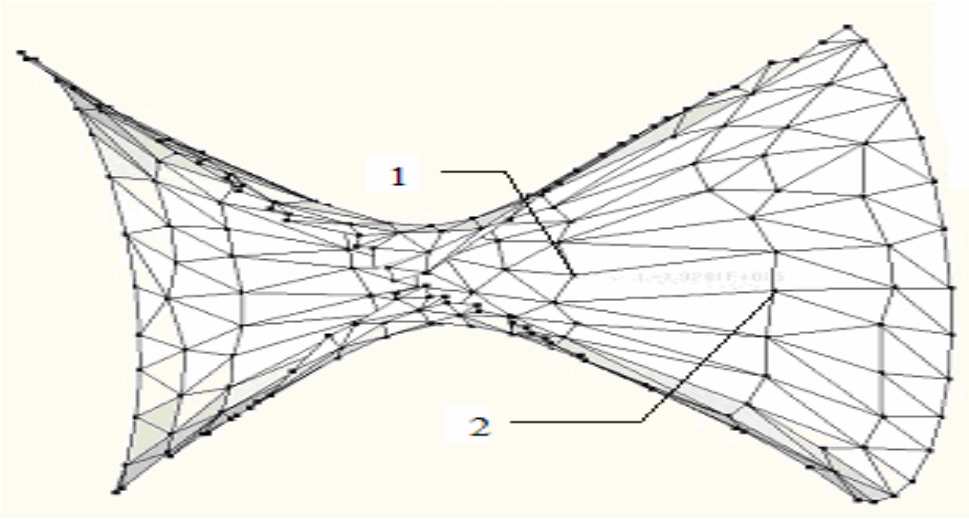
Проведено проектування та виконано діючу систему моделювання безпечної комунікації в БСМ на підставі прототипної плати, побудованої на базі 16-бітного мікроконтролера PIC24FJ128, та мікроелектронних пристроїв KeeLoq – шифратора HCS410, в якому реалізується криптографічний алгоритм KeeLoq на основі симетричного 32-бітного блокового шифру з 64-бітним ключем, та дешифратора HCS500. Створено комп'ютерну програму-симулятор KeeLoq Dumping Konsole на мові C#, яка дає змогу реалізувати запропонований метод організації та оптимізації процесу моделювання захищеного безпровідного передавання інформації шляхом її шифрування і розшифрування, а також здійснювати моніторинг чергових переприйомів і проводити детальний аналіз наступних кадрів передавання.

Реалізовано метод моделювання візуального виявлення атаки червоточини в БСМ, сенсори якої сформовано на модулях XBee виробництва фірми Digi International шляхом програмування стеку XBee на програмному рівні. Передбачено функціонування сенсорів в рамках протоколу ZigBee згідно зі стандартом IEEE 802.15.4. При цьому застосовано вбудовану програму типу ZB20, яка базується на специфікації ZigBee PRO Feature Set. Проведено проектування БСМ на розміщених у просторі 201 сенсорах з інтегрованими антенами. Дану БСМ охоплено поверхнею розмірами: 750 м по осі аплікат та 750 м по осі ординат. БСМ введено в два режими функціонування: без наявності атаки червоточини та за наявності атаки червоточини для температури довкілля в межах від +5°C до +30°C і вологості від 30% до 70%.

Здійснено комп'ютерний моделюючий експеримент у сформованій БСМ за характером атаки червоточини, в якій брало участь два зловмисні сенсорні вузли, що активувалися по одному на кожному з кінців тунелю. Отримано серію графічних візуалізованих форм топологічних поверхонь БСМ за результатами комп'ютерного моделювання (частина з них – рис. 2, 3). На рисунках позначено оцифрованими позиціями точки, у яких розміщені сенсори, та додатково вказано відстань між сенсорами і площу охопленої сенсорною мережею поверхні.

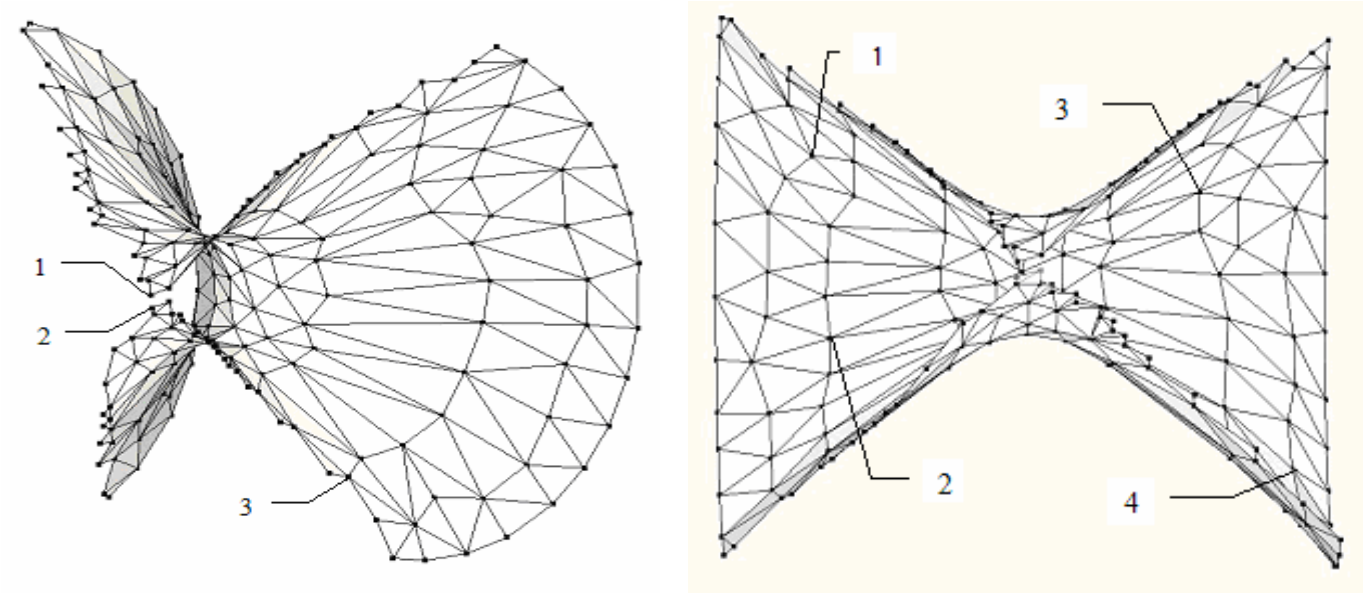


а)



б)

Рис. 2. Візуалізована форма згладженої реконструйованої топологічної поверхні БСМ: а) без наявності атаки червоточини; б) за наявності атаки червоточини



а) б)

Рис. 3. Вигляд збоку (а) та спереду (б) візуалізованої форми згладженої реконструйованої топологічної поверхні БСМ під впливом атаки червоточини

Аналізуючи отримані ілюстрації, бачимо, що атака червоточини:

- зумовила суттєву зміну відстані між двома сусідніми сенсорами 1 і 2 з 67,6147 м (рис. 2 а) на 192,908 м (рис. 2 б);
- спотворила топологічну поверхню сенсорної мережі (див. попарно рис. 2 а і рис. 2 б, рис. 3 а і рис. 3 б);
- викликала зміну площі топологічної поверхні сенсорної мережі з $5{,}625 \cdot 10^5$ м^2 на $6{,}631 \cdot 10^5$ м^2 (рис. 3 б).

Показано, що реалізація запропонованого запатентованого способу дає змогу автоматизувати процес виявлення атаки червоточини та пришвидшити прийняття рішення оператором по локалізації зловмисного вузла. Досягнуто підвищення точності виявлення атаки червоточини з отриманням абсолютної похибки визначення положення сенсорів в межах $\pm 7{,}5 \ldots 75 \cdot 10^{-2}$ м по відношенню до розмірів мережі та похибки інтерполяції під час згладжування реконструйованої топологічної поверхні сенсорної мережі $\pm 2 \ldots 3 \cdot 10^{-2}$ мкм. Слід зазначити, що для рішення одних задач таке забезпечення високої точності не є актуальним, тоді як для інших завдань, особливо спеціальних, це має важливе значення.

У додатках наведено акти впровадження результатів дисертаційної роботи, опис моделі засобу оброблення сигналів в безпровідній сенсорній мережі, код комп'ютерної програми KeeLoq Dumping Konsole на мові C#, а також засоби, опис і результати моделювання візуалізаційного виявлення атаки червоточини в безпровідній сенсорній мережі.

ВИСНОВКИ

У дисертаційній роботі отримано нові науково-обґрунтовані результати розв'язання актуального наукового завдання – побудови удосконалених методів та засобів моделювання відбору інформації в безпровідних мережах давачів систем електропостачання на підставі способів візуалізації та зважених графів, що має

істотне значення для підвищення ефективності їх функціонування та стійкості до зловмисних атак. Основні наукові результати, висновки та рекомендації полягають у наступному:

1. Показано тісний зв'язок безпровідних мереж з системами електропостачання та виділено клас безпровідних гомо- та гетерогенних сенсорних мереж, які забезпечують, поряд з переходом до якісно нового локально-оптимального параметричного рівня відбору інформації в системах електропостачання, відчутне заощадження електроенергії, підвищення надійності електропостачання та зниження екологічних навантажень.

2. За результатами аналізу математичних моделей відбору інформації в безпровідних мережах давачів “інтелектуальних” систем електропостачання виявлено чинники, які істотно впливають на ефективність їх функціонування, що дало змогу обґрунтувати та сформулювати основні вимоги до графової моделі для оцінювання керованості сенсорних вузлів на стадіях проектування та експлуатації в цих умовах.

3. Виконано оцінювання зв’язності розподіленої БСМ з отриманням низки необхідних умов, відповідно до концепції якої кожний сенсорний вузол вільно переміщується за зближувально-подібною схемою в локальній інформаційній системі, що дозволяє центральним вузлам оцінити первинну дійсну інформацію шляхом спостереження невеликої групи сенсорів, завдяки чому розв’язано задачу забезпечення зв’язності.

4. Розроблено удосконалену математичну модель БСМ на підставі процесо-подійного підходу із застосуванням зважених графів для оцінювання відтворення її топології та спостережуваності з врахуванням можливих загроз і збурювальних чинників, якій у порівнянні з моделями на основі ретрансляційної концепції чи принципу мобільного центрального вузла, притаманна менша складність та гнучка архітектура, що дає змогу мінімізувати обсяг інформації обміну між сенсорними вузлами та центральним вузлом або досягти незмінності обсягу інформації обміну від відстані до центрального вузла.

5. Розроблено модифіковані моделі загроз, що викликають аномальні режими функціонування БСМ, та моделі режимів протидії зловмисним атакам на ці мережі, які відрізняються застосуванням методу зважених графів для удосконалення структурної та алгоритмічної організації систем відбору інформації згідно із запропонованою класифікацією атак, завдяки чому визначено шлях вдосконалення щодо виявлення найкритичніших атак, підвищено ефективність та результативність розроблюваних методів та засобів протидії потенційним загрозам.

6. Розроблено метод моделювання візуального виявлення потенційно небезпечних атак маршрутизації в БСМ, що дає змогу частково автоматизувати та зменшити час на проведення аналізу та прийняття рішення по виявленню з підвищеною точністю та локалізації загрози відповідно до запропонованої ознаки її ідентифікації.

7. Створено апаратно-програмні засоби моделювання режимів відбору інформації та безпечного доступу в БСМ систем електропостачання, на підставі досліджень яких установлено, що внесення та виконання семантико-вимірювальних операцій із застосуванням локально-стохастичного методу просторової кригінг-

інтерполяції у запропонованому візуалізаційному методі моделювання дозволяє зменшити в 2-4 рази похибку вимірювання відстані між сенсорами, в 2-3 рази підвищити точність згладжування реконструйованої топологічної поверхні БСМ та оперативно керувати сенсорною мережею в протидіях певного типу атак, зокрема атаки "червоточини". При цьому досягнуто абсолютної похибки визначення положення сенсорів $\pm 7{,}5\ldots75 \cdot 10^{-2}$ м по відношенню до розмірів мережі та похибки інтерполяції під час згладжування реконструйованої топологічної поверхні БСМ $\pm 2\ldots3 \cdot 10^{-2}$ мкм, що є вкрай необхідним для вирішення спеціальних задач, в яких сенсори розміщені в обмеженому просторі.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Wrona W. Aspects of Fast Fourier Transform simulation for applications requiring operation in real time / W. Wrona, V. Karpinskyi, M. Bogusz // Вісник Східноукраїнського національного університету імені Володимира Даля. – 2011. – № 7 (161), Частина 1. – С. 296-304. – ISSN 1998-7927.

2. Карпінський В. Моделювання захищеного безпровідного передавання інформації в сенсорній мережі / В. Карпінський, Б. Антош, Т. Яремчук // Вісник Тернопільського національного технічного університету. – 2011. – Том 16, № 2. – С. 196-202. – ISSN 1727-7108.

3. Карпінський В. М. Безпровідні сенсорні мережі: особливості моделювання та візуалізації топології при загрозах // Сучасна спеціальна техніка. – 2011. – № 2 (25). – С. 55–60.

4. 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. – ISSN 0135-1729.

5. 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. – ISSN 1727-7108.

6. 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.

7. Kurytnik I. P. Bezprzewodowa sieć sensorów / I. P.Kurytnik, M. Mikulski, W. Karpiński // Pomiary Automatyka Kontrola. – 2010. – Vol. 56, Nr 6. – P. 548-551. – ISSN 0032-4140.

8. 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.

9. 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. – N 4. – P. 4-6. – ISSN 0033-2097.

10. 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.

11. 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.

12. Cryptographic system security level based on elliptic curves / M. Karpinski, M. Aleksander, G. Litawa, V. Karpinskyi // Вісник Східноукраїнського національного університету імені Володимира Даля. – 2008. – No 8 (126), Частина 1. – С. 94-98.

13. Карпінський М. П. Система для проведення криптоаналізу / М. П. Карпінський, Л. О. Дубчак, В. М. Карпінський // Праці Луганського відділення Міжнародної Академії Інформатизації. – 2008. – № 1 (16). – С. 134-137.

14. Litawa G. Zaawansowana kryptoanaliza szyfrów opartych na krzywych eliptycznych z zastosowaniem układów programowalnych FPGA / G. Litawa, W. Karpiński // Prace naukowe Instytutu Technicznego Państwowej Wyższej Szkoły Zawodowej w Nowym Sączu. – Praca zbiorowa pod red. dr inż. Marka Aleksandra. – Nowy Sącz: Wydawca Państwowa Wyższa Szkoła Zawodowa w Nowym Sączu. – 2007. – S. 175-185. – ISBN 978-83-60822-31-9.

15. 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.

16. Спосіб візуалізації атаки черв'яка в безпровідній сенсорній мережі: патент на корисну модель 64391 : МПК H04W 12/00 / Карпінський В. М., Євтух П. С., Боровік Б. Л., Карпінський М.П. ; власник патенту Тернопільський національний технічний університет ім. І. Пулюя (Україна). – № u 2011 03578 ; заявл. 25.03.11 ; опубл. 10.11.2011, Бюл. № 21. – 4 с.

17. 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. – Pp. 117-120. – ISBN 978-80-248-2399-7.

18. 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. – Pp. 223-225. – ISBN 978-80-248-2399-7.

19. Євтух П. С. Моделювання візуалізаційного виявлення атак в сенсорній мережі моніторингу електротехнічних систем / П. С. Євтух, В. М. Карпінський // Проблеми енергоресурсозбереження в електротехнічних системах. Наука, освіта і практика: XIII міжнарод. конф. PEES 2011, 18-20 травня 2011 р. : тези доп., №1/2011 (1). – Кременчук, 2011. – С. 322-323.

20. 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.

21. Карпінський В. М. Вибрані аспекти безпеки та моделювання безпровідних сенсорних мереж / В. М. Карпінський // Інформаційні технології та комп'ютерна інженерія: міжнарод. наук.-практ. конф. ITKI 2010, 19-21 травня 2010 р. : тези доп. – Вінниця, 2010. – С. 241-242. – ISBN 978-966-641-356-0.

22. Карпінський В. М. Система моделювання безпечної комунікації в безпровідній сенсорній мережі / В. М. Карпінський, Б. Л. Боровік, Б. Антош // Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС, навчальному процесі, взаємодії з іншими службами : VI наук.-практ. семінар, 4 грудня 2009 р. : матеріали наук.-практ. сем. – Львів: Львівський державний університет внутрішніх справ, 2009. – С. 232-240.

23. Karpinskyi V. Side-Channel Signal Processing and Modeling / V. Karpinskyi, L. Korkishko, M. Karpinski // Advanced Computer Systems and Networks: Design and Application (Сучасні комп'ютерні системи та мережі: розробка та використання) : 4th International Conference ACSN-2009, November 9-11th, 2009 : Proceedings of the Conference. – Lviv, Ukraine, 2009. – Pp. 199-202. – ISBN 978-966-345-190-9.

24. Євтух П. Безпровідні мережі: класифікація, моделі, енергоефективність та безпека / П. Євтух, В. Карпінський, Л. Дубчак // Всеукраїнська наукова конференція Тернопільського державного технічного університету імені Івана Пулюя, 13–14 травня 2009 р. : матеріали конф. – Тернопіль, 2009. – С. 128. – ISBN 966-305-007-7.

25. 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.

26. Aleksander M. Distributed computing system which solve an elliptic curve discrete logarithm problem / M. Aleksander, G. Litawa, V. Karpinskyi // The Experience of Designing and Application of CAD Systems in Microelectronics : Xth International Conference CADSM 2009, 24-28 February 2009 : Proceedings of the Conference. – Lviv-Polyana, Ukraine: Publishing House Vezha&Co, 2009. – Pp. 378-380. – ISBN 978-966-2191-05-9.

27. 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). – Pp. 71-73.

28. 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. – Pp. 130-132.

29. Карпінський В. Розв'язання проблеми дискретного логарифму паралельним методом Ро-Поларда на підставі бібліотек MPI2 і MIRACL / В. Карпінський,

Ґ. Літава, І. Якименко // Дванадцята наук. конф. Тернопільського державного технічного університету імені І. Пулюя, 14-15 травня 2008 : Матеріали конф. – Тернопіль, 2008. – С. 93.

30. Коркішко Т. Криптоатаки на підставі витоку інформації з побічних каналів і протидія їм / Т. Коркішко, Л. Коркішко, В. Карпінський // Дванадцята наук. конф. Тернопільського державного технічного університету імені І. Пулюя, 14-15 травня 2008 : Матеріали конф. – Тернопіль, 2008. – С. 97.

31. Kurytnik I. Communications capabilities of the DS80C400 MAXIM/Dallas microcontroller as a server in the LAN environment / I. Kurytnik, B. Borowik, W. Karpinsky // Modern Problems of Radio Engineering, Telecommunications and Computer Science : 9th International Conference TCSET'2008, 19-23 February 2008 : Proceedings of the Conference. – Lviv-Slavsko, Ukraine: Publishing House of Lviv Polytechnic National University, 2008. – Pp. 423-425.

АНОТАЦІЯ

Карпінський В. М. Методи та апаратно-програмні засоби моделювання відбору інформації в безпровідних мережах давачів систем електропостачання. – На правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 01.05.02 – математичне моделювання та обчислювальні методи. – Тернопільський національний технічний університет імені Івана Пулюя, Тернопіль, 2012.

Дисертацію присвячено побудові удосконалених методів та засобів моделювання відбору інформації в безпровідних мережах давачів систем електропостачання на підставі способів візуалізації та зважених графів для прогнозування небезпечних станів та прийняття адекватних рішень при збільшенні точності визначення місць розташування джерел інформації чи збурень, зменшення часових та вартісних витрат на проведення модельних експериментів, а також підвищення ефективності функціонування мереж та їх стійкості до зловмисних атак.

Розроблено та запатентовано метод моделювання візуального виявлення потенційно небезпечних атак маршрутизації в безпровідних сенсорних мережах, який дає змогу частково автоматизувати та зменшити час на проведення аналізу і прийняття рішення по виявленню з підвищеною точністю та локалізації атак. Створено апаратно-програмні засоби моделювання режимів відбору інформації та безпечного доступу в безпровідних сенсорних мережах систем електропостачання.

Ключові слова: модель мережі, модель атаки, візуальне моделювання, безпровідна сенсорна мережа, зважений граф, система електропостачання.

АННОТАЦИЯ

Карпинский В. Н. Методы и аппаратно–программные средства моделирования отбора информации в беспроводных сетях датчиков систем электроснабжения. – На правах рукописи.

Диссертация на соискание ученой степени кандидата технических наук по специальности 01.05.02 – математическое моделирование и вычислительные

методы. – Тернопольский национальный технический университет имени Ивана Пулюя, Тернополь, 2012.

Диссертация посвящена построению усовершенствованных методов и средств моделирования отбора информации в беспроводных сетях датчиков систем электроснабжения на основании способов визуализации и взвешенных графов для прогнозирования опасных состояний и принятия адекватных решений при увеличении точности определения мест расположения источников информации или возмущений, уменьшения временных и стоимостных затрат на проведение модельных экспериментов, а также повышения эффективности функционирования сетей и их устойчивости к злонамеренным атакам.

Разработано и запатентовано метод моделирования визуального обнаружения потенциально опасных атак маршрутизации в беспроводных сенсорных сетях, который позволяет частично автоматизировать и сократить время на проведение анализа и принятие решения по выявлению с повышенной точностью и локализации атак. Создано аппаратно-программные средства моделирования режимов отбора информации и безопасного доступа в беспроводных сенсорных сетях систем электроснабжения.

Ключевые слова: модель сети, модель атаки, визуальное моделирование, беспроводная сенсорная сеть, взвешенный граф, система электроснабжения.

ANNOTATION

Karpinskyi V. M. Methods and hardware-software means of selection information modeling in wireless sensor networks of electric power supply systems. – Submitted as a Manuscript.

The thesis for obtaining a scientific degree of the candidate of technical sciences by speciality 01.05.02 – Mathematical modeling and computational methods. – Ternopil Ivan Puluj National Technical University. – Ternopil, 2012.

Thesis is dedicated to the improved modeling tools and methods construction of information removal in wireless sensor networks of power supply systems based on methods of visualisation and weighted graphs to predict dangerous conditions and opportunity of making appropriate decisions while increasing the accuracy of information sources or disturbances location definition, reducing time and cost values of the model experiments, and also enhance efficiency of the networks functioning and persistence to malicious attacks.

Relevant scientific and technical task for mathematical modeling of information selection in the "intelligent" power networks was formulated, were demonstrated a close relations with wireless networks that includes the class of homo- and wireless heterogeneous sensor networks. Latest supports, together with the conversion to a high-grade new locally-optimal parametric level of information selection in the power-supply system, noticeable energy savings, increased reliability of electricity supply and reduce environmental loads.

Was proved the expediency using of graph model information selection in a distributed wireless sensor networks of "intelligent" power supply systems for the controllability evaluation of sensor nodes on the stages of their design and exploitation.

An improved mathematical model of wireless sensor network was developed based on process-event approach using weighted graphs to estimate topology reconstruction and observability.

A modified models threats, that cause abnormal modes of wireless sensor network functioning, and resistance modes model against malicious attacks on these networks which differ using the method of weighted graphs to improve the structural and algorithmic system organization of information selection according with the proposed attacks classification by criteria of communications on different levels of the OSI model and the nature of the impact (active and passive) were developed and investigated.

Were substantiated structural and algorithmic organization of systems and modeling methods of wireless sensor networks in terms condition of existing threats to the functioning of the network, that allows to increase speed, reliability, resistance against to attacks and to improve other technical and economic parameters of the network functioning. Was developed a convenient tool of modeling for detection routing attack in networks according with integrated security models and methods of visualization.

Identifying feature of malicious sensor node was formulated based on collected information about network topology, taking into account the similarity relations between two suspicious neighbor nodes, that clearly identifies and provides an analytical formula component by which attack can be detected automatically. Adequacy of the improved method was confirmed by computer modeling, carried out in two stages.

The application of information technologies of visual modeling for monitoring, detection and localization of attacks in wireless sensor networks was substantiated. Modeling method of visual detection of potentially dangerous routing attacks in wireless sensor networks was developed, which includes the executing of such steps and mathematical calculations: measuring the distance between sensors based on the power level of the received signal; reconstructing topological network surface by multidimensional scaling and calculation virtual position of each sensor; smoothing the reconstructed topological network surface using triangulation and kriging-interpolation, visualization of smoothed reconstructed topological network surface and its analysis using attack binary detection of malicious node identifying by the proposed feature. This allows partially automate and reduce time for analysis and making decision for attack identifying with high accuracy and attacks localization. The method is patented.

Developed and implemented an effective system for secure communication modeling in wireless sensor networks based on the prototype board, constructed on the basis of the 16-bit microcontroller type PIC24FJ128, encoder and decoder HCS410 HCS500. A computer program for simulation was created in C# language.

Carried out a computer modeling experiment on visual detection of worm attacks in designed wireless sensor network based on the patented method. Sensor network formed by the XBee modules by programming the XBee stack at the program level. Foreseen sensors functioning within the ZigBee protocol in accordance with the standard IEEE 802.15.4. Thus used a built-in program ZB20 type, based on the ZigBee PRO Feature Set specification.

Key words: network model, attack model, visual modeling, wireless sensor network, weighted graph, power supply system.