ISSN 1727-1290

KHARKIV NATIONAL UNIVERSITY OF RADIO ELECTRONICS

ACADEMY OF SCIENCES OF APPLIED RADIO ELECTRONICS

APPLIED RADIO ELECTRONICS

Scientific and Technical Journal 2013 Volume 12 № 2

Special issue devoted to problems of ensuring information security

CONTENTS

METHODOLOGY OF CREATING AND DEVELOPING ELECTRONIC DIGITAL WORLD AND CLOUD COMPUTING SECURITY

Gorbenko Yu.I. Problems and requirements to the grant of confidential services in European Union in the period of 2015–2030 184

Aulov I.F., Gorbenko I.D. Cloud computing and analysis of information security in the cloud 194

Pogrebnyak K.A., Povtariev D.V. Analysis of security of cloud data storage services 202

SYNTHESIS AND ANALYSIS OF SYMMETRIC TRANSFORMATIONS

Kazymyrov O. Extended criterion for absence of fixed points 209

Ruzhentsev V.I. On the method of proving the resistance of block ciphers to impossible differential attack 215

Khalimov G.Z. Strongly universal hashing 220

Khalimov G.Z. Estimates of complexity of universal hashing by algebraic curves 225

Lisitskaya I.V., Lisitsky K.E. On the reaching by iterative ciphers of a steady state characteristic of a random permutation 230

Dolgov V.I., Rodinko M.Yu. Block symmetric ciphers — random substitutions. Combinatorial indicators 236

Melnichuk E.D. Research of correlation between the new selection criteria and substitutions of modern block ciphers 240

Gorbenko I.D., Samoilova A.V. Analysis of block symmetric ciphers of international standard ISO/IEC 29192-2 247

Mordvinov R.I. Comparative analysis of methods and tools for testing random sequences NIST 800-22 and NIST 800-90B 250

ASYMMETRIC CRYPTOGRAPHIC TRANSFORMATIONS AND THEIR PROPERTIES

Kachko E.G., Balagura D.S., Pogrebnyak K.A., Gorbenko Yu.I. Research of methods of calculating of inversion in NTRU algorithm 254

Bondarenko M.F., Makutonina L.V. Computational complexity of algebraic lattice basic problems 258

Kotenko V.V., Kotenko S.V., Rumyantsev K.E., Gorbenko I.D. Optimization of information security processes in terms of virtualization relative to conditions of theoretical indecipherability 265

CONTENTS

(Continued from front cover)

Bessalov A.V., Dihtenko A.A., Yatsenko O.I. Parameters of cryptosystems on the Edwards curve above expansions of small simple fields 273

Bessalov A.V. Dividing a point by two for the Edwards curve over a simple field 278

Yesina M.V., Gorbenko I.D. Analyzing the complexity of cryptographic transformations in a group of points of elliptic curves according to a basis chosen 280

Bessalov A.V., Dihtenko A.A. Cryptographically resistant Edwards curves over prime fields 285

Ivanenko D.V. Methods to counteract side channel attacks on the NTRU cryptotransformations, based on energy consumption analysis 292

Balagura D.S., Baglaev I.A. Public key infrastructures with the use of NTRU cryptosystems 299

Proskurovskyi R.V. Analyzing the state of training specialists in the information security field 303

SYSTEMS AND MEANS OF INFORMATION SECURITY

Kotenko V.V., Kotenko S.V., Rumyantsev K.E., Gorbenko Yu.I. Continuous data protection strategy from the standpoint of virtualization of ensemble of keys on a formal relationship of ensembles 308

Alekseychuk A.N., Gryaznukhin A.Yu. A method of restoring systematic linear codes by samples of noisy code words 313

Kuznetsov A.A., Prihod'ko S.I., Bilal Hamse. Multidimensional Spectra for Describing Cascade Codes in the Frequency Domain 319

Smirnov A.A. Software model of a device of forming discrete signals with special correlation properties 333

Krasnobaev V.A., Mavrin M.A., Zamula A.A. Method for controlling data presented in residue classes 342

Nikolaenko S.V. Improving security of quantum direct secure communication protocol by XOR encryption 347

Zabolotnyi V.I., Zadorozhnaya E.V. Substantiation of choosing the methods of protection 351 of the production characteristics from competitive intelligence 351

Chyzh V.M., Karpinskiy M.P., Balaban S.M. Control and visualization of functional security of information systems using wireless sensor networks 356

Oleshko I.V. Improving of zero-knowledge protocol based on discrete logarithms 363

Харьковский национальный университет радиоэлектроники

Академия наук прикладной радиоэлектроники

ПРИКЛАДНАЯ РАДИОЭЛЕКТРОНИКА

Научно-технический журнал

Главный редактор
Бондаренко М. Ф.

Зам. главного редактора
Дохов А.И.
Чурюмов Г.И.

Редакционный совет

Гузь В.И., Довбня А.Н., Егоров А.М., Калугин В.В., Ковтуненко А.П., Кравченко В.И., Назаренко И.П. (Россия), Неклюдов И.М., Пресняк И.С., Симонов К.Г. (Россия), Симанков В.С. (Россия), Слипченко Н.И., Чабдаров Ш.М. (Россия), Яковенко В.М., Ярошенко В.С. (Россия)

Редакционная коллегия

Абрамович Ю.И. (США), Бодянский Е.В., Борисов А.В., Буц В.А., Бых А.И., Гомозов В.И., Жуйков В.Я., Зарицкий В.И., Кипенский А.В., Кульпа К. (Польша), Леховицкий Д.И., Литвинов В.В., Лукин К.А., Мачехин Ю.П., Модельский Й. (Польша), Нерух О.Г., Поляков Г.А., Ролинг Г. (Германия), Седышев Ю.Н., Серков А.А., Сухаревский О.И., Чурюмов Г.И., Шифрин Я.С., Шкварко Ю.В. (Мексика)

Адрес редакции:
Редакция журнала «Прикладная радиоэлектроника»
Харьковский национальный университет радиоэлектроники
просп. Ленина, 14, 61166, Харьков, Украина
Тел.: + 38 (057) 702 10 57
Факс: + 38 (057) 702 10 13
E-mail: are@kture.kharkov.ua
http://www.anpre.org.ua

© Харьковский национальный университет радиоэлектроники, 2013

СОДЕРЖАНИЕ

МЕТОДОЛОГИЯ СОЗДАНИЯ И РАЗВИТИЯ ЭЛЕКТРОННОГО ЦИФРОВОГО МИРА И БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Горбенко Ю.І. Проблеми та вимоги до надання довірчих послуг в Європейському Союзі в період 2015–2030 рр. 184

Аулов І.Ф., Горбенко І.Д. Хмарні обчислення та аналіз питань інформаційної безпеки в хмарі 194

Погребняк К.А., Повтарєв Д.В. Аналіз безпеки сервісів зберігання даних у хмарі 202

СИНТЕЗ И АНАЛИЗ СИМЕТРИЧНЫХ ПРЕОБРАЗОВАНИЙ

Kazymyrov O. Extended criterion for absence of fixed points 209

Руженцев В.И. О методе доказательства стойкости блочных шифров к атаке невыполнимых дифференциалов 215

Халимов Г.З. Строго универсальное хеширование 220

Халимов Г.З. Оценки сложности универсального хеширования по алгебраическим кривым 225

Лисицкая И.В., Лисицкий К.Е. О приходе итеративных шифров к стационарному состоянию, свойственному случайной подстановке 230

Долгов В.И., Родинко М.Ю. Блочные симметричные шифры — случайные подстановки. Комбинаторные показатели 236

Мельничук Е.Д. Исследование соответствия новым критериям отбора подстановочных конструкций современных БСШ 240

Горбенко І.Д., Самойлова А.В. Аналіз блокових симетричних шифрів міжнародного стандарту ISO/IEC 29192-2 247

Мордвінов Р.І. Порівняльний аналіз методів та засобів тестування випадкових послідовностей NIST 800-22 TA NIST 800-90B 250

АСИММЕТРИЧНЫЕ КРИПТОГРАФИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ И ИХ СВОЙСТВА

Качко Е.Г. , Балагура Д.С. , Погребняк К.А. , Горбенко Ю.И. Исследование методов вычисления инверсии в алгоритме NTRU 254

Бондаренко М.Ф., Макутоніна Л.В. Обчислювальна складність основних задач на алгебраїчних решітках 258

Котенко В.В., Котенко С.В., Румянцев К.Е., Горбенко И.Д. Оптимизация процессов защиты информации с позиций виртуализации относительно условий теоретической недешифруемости 265

Бессалов А.В., Діхтенко А.А., Яценко О.І. Параметри криптосистеми на кривій Едвардса над розширеннями малих простих полів 273

Бессалов А.В. Деление точки на два для кривой Эдвардса над простым полем 278

Єсіна М.В., Горбенко І.Д. Аналіз складності криптографічних перетворень у групі точок ЕК залежно від обраного базису 280

Бессалов А.В., Дихтенко А.А. Криптостойкие кривые Эдвардса над простыми полями 285

Іваненко Д.В. Методи протидії атакам на реалізації, які базуються на аналізі енергоспоживання, схеми направленого шифрування у кільцях зрізаних поліномів 292

Балагура Д.С., Баглаев И.А. Инфраструктуры открытых ключей с использованием криптосистем NTRU 299

Проскуровский Р.В. Аналіз стану підготовки фахівців у галузі «Інформаційна безпека» 303

СИСТЕМЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Котенко В.В., Котенко С.В., Румянцев К.Е., Горбенко Ю.И. Стратегия защиты непрерывной информации с позиций виртуализации ансамбля ключей на формальные отношения ансамблей 308

Алексейчук А.Н., Грязнухин А.Ю. Метод восстановления систематических линейных кодов по наборам искаженных кодовых слов 313

Кузнецов А.А., Приходько С.И., Билал Хамзе. Многомерные спектры для описания каскадных кодов в частотной области 319

Смирнов А.А. Программная модель устройства формирования дискретных сигналов с особыми корреляционными свойствами 333

Краснобаев В.А., Маврина М.А., Замула А.А. Метод контроля данных, представленных в классе вычетов 342

Николаенко С.В. Усиление безопасности методом гаммирования протокола квантовой прямой безопасной связи 347

Заболотний В.І., Задорожна Є.В. Обгрунтування вибору заходів захисту характеристик продукції від конкурентної розвідки 351

Чиж В.М., Карпінський М.П., Балабан С.М. Контроль та візуалізація стану функціональної безпеки інформаційних систем із застосуванням бездротових сенсорних мереж 356

Олешко І.В. Удосконалення протоколу нульових знань, заснованого на дискретних логарифмах 363

УДК 004.94

КОНТРОЛЬ ТА ВІЗУАЛІЗАЦІЯ СТАНУ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ ІЗ ЗАСТОСУВАННЯМ БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖ

В.М. ЧИЖ, М.П. КАРПІНСЬКИЙ, С.М. БАЛАБАН

Розглянуто важливість та складність організації ефективних методів контролю за станом надійності поширення інформації у бездротових сенсорних мережах. Запропоновано оригінальні методи контролю за параметрами сигналів окремих або компактно розташованих сенсорів та візуалізації атак на них. Обгрунтовано доцільність використання кластерної моделі зі симплексним покриттям його поля для візуалізації областей трансформації сенсорів, сигнали яких зазнали атак.

Ключові слова: функціональна безпека, інформаційні системи, сенсор, бездротова сенсорна мережа, кластер, візуалізація, трансформація, стаціонарна сигнальна точка, фіктивна сигнальна точка, еталонна сигнальна точка.

ВСТУП

Темпи розвитку та масштаби використання інформаційних систем (ІС), складовими частинами яких є бездротові сенсорні мережі (БСМ), ставлять перед їх розробниками ряд складних завдань. Особливе місце серед них займає забезпечення надійності роботи мережі та її захищеність, а також, безпека інформації. Успішне вирішення вказаних завдань значною мірою забезпечує наявність простих і ефективних методів контролю та візуалізації параметрів, що характеризують роботу ІС. Значну увагу,при цьому, приділяють виявленню і локалізації наслідків атак на сигнали сенсорів, які працюють у мережі. Але сьогодні відсутня інформація про методи контролю та візуалізації, які б дозволяли одночасно відслідковувати атаки на різні параметри сигналів.

Під візуалізацією функціональної безпеки ІС зі застосуванням БСМ розуміють контроль, виявлення і відображення атак на інформацію. Зокрема, в літературних джерелах [1, 2, 3, 4] наведено результати візуалізації атак типу «wormhole», які призводять до зміни сили сигналів у мережі. Така візуалізація дозволяє виявити вплив атаки на окремий сенсор, як який виступає інформаційний вузол (ІВ), або групу компактно розміщених сенсорів.

Для відслідковування атак на параметри сигналів окремих вузлів ІС запропоновано використання симплексно-кластерного моделювання ІС. [5, 6, 7]. При такому моделюванні передбачено створення візуалізованої форми реконструйованої топології мережі ІВ із використанням сітки рівносторонніх трикутників, у вершинах яких розміщені сигнальні точки (СТ), які представляють ІВ.

Створення методів аналізу роботи симплексно-кластерних моделей і візуалізації атак на параметри сигналів ІВ, які входять до даних моделей.

1. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

При стабільній роботі ІВ у «польових умовах» кластер (рис. 1), як це було відмічено в роботі [5], має геометрію двовимірного евклідового простору із функціональними зв'язками (ФЗ) довжиною l. Атака на ІВ сигналом ε змінює довжину ФЗ на величину $l_\varepsilon = l(\varepsilon)$ і, здійснює переміщення СТ, положення яких залежить від них.

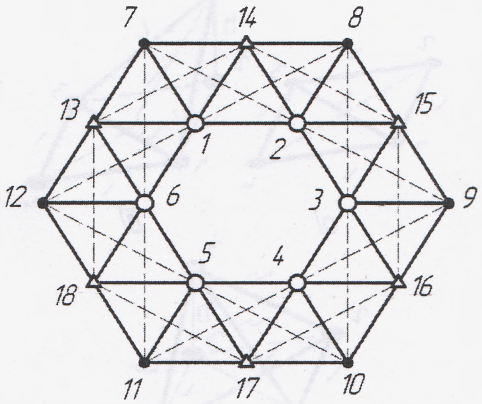

Рис. 1. Кластерна модель зі схемою поділу на симплекси [4С]

1.1. Метод 4-точкових симплексів (метод [4с])

Візуалізація атаки у кластері ґрунтується на можливості переміщення сигнальних точок у залежності від довжини ФЗ [5, 7]. Візуалізація реалізується завдяки покриттю поля кластера 4-точковими симплексами ([4С]). При стабільній роботі ІВ простір кластера заповнений ромбами, в яких п'ять відстаней між сигнальними точками є ФЗ довжиною l, а шоста відстань – друга діагональ ромба – геометричний зв'язок (ГЗ) довжиною $d = \sqrt{3}l$. Геометрія кластера при здійсненні атаки на один або декілька джерел інформації зміниться (відповідні ФЗ отримають видовження).

За даними довжин ФЗ, комп'ютер вибудує нові положення СТ кластера, відобразить трансформацію кластерного поля навколо СТ, і здійснить візуалізацію атакованих сенсорів у конфігураційному просторі комп'ютера.

В роботі [7] проаналізовано утворення областей трансформації при атаці на один і два сенсори.

При атаці на один сенсор утворяться три типи [4С] (рис. 2):

– [4С] з частковою трансформацією (ЧТр), яка визначається двома ФЗ із видовженнями $l_\varepsilon = l(\varepsilon)$ (рис. 2, *б*). В таких [4С] один трикутник знаходиться в області трансформації, а інший — поза нею. Трансформація симплекса призводить до утворення тривимірного геометричного об'єкта з нульовим об'ємом, складеного із двох трикутників, зігнутих вздовж спільної основи – функціонального зв'язку, який не змінюється і залишає нерухомими кінці відрізка (сигнальні точки);

– [4С] з повною трансформацією (ПТр) визначається трьома ФЗ із видовженнями $l_\varepsilon = l(\varepsilon)$ (рис. 2, *в*). Такі [4С] не можуть бути реалізованими у двовимірному просторі кластера. Вони утворять тривимірні геометричні об'єкти у вигляді трикутної піраміди. В основі піраміди знаходяться три нерухомі СТ, з'єднані двома функціональними зв'язками довжиною l і геометричним зв'язком довжиною $d = \sqrt{3}l$. Довжина висоти піраміди здійснює оцінку ступеня атаки на сенсор [5].

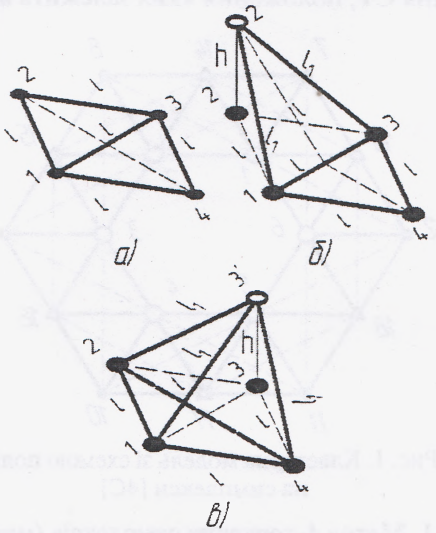

Рис. 2. Типи трансформації симплекса

В залежності від того, якому класу належить сигнальна точка, яка визначає атакований ІВ, отримуємо різні області трансформації у кластері (рис. 3).

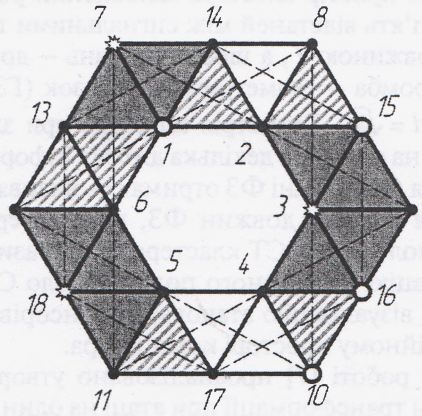

Рис. 3. Області трансформацій при атаці на сенсори, які представлені сигнальними точками різних класів

Якщо атаку здійснено на ІВ, представленими СТ, які є вершинами зовнішнього шестикутника (СТ – c_7, c_8, c_9, c_{10}, c_{11}, c_{12}), то в область трансформації входять три [4С]. При цьому один симплекс отримує ПТр, а два інші, які в перетині із цим симплексом мають його складові, отримують ЧТр. Всі інші 15 [4С] залишаться у вигляді первинних ромбів двовимірного простору кластера (рис. 3).

Якщо атаку здійснено ІВ, які у кластері представлені СТ – серединами сторін зовнішнього шестикутника(СТ – c_{13}, c_{14}, c_{15}, c_{16}, c_{17}, c_{18}), то в область трансформації попадають чотири [4С]. При цьому два симплекси отримують ПТр, а два інші, які в перетині із цими симплексами мають спільні складові, отримують ЧТр. Інші 14 [4С] зберігатимуть форму ромбів.

Якщо атаку здійснено на сенсори, які представлені у кластері СТ – вершинами внутрішнього шестикутника (СТ – c_1, c_2, c_3, c_4, c_5, c_6), то в область трансформації входять п'ять [4С]. При цьому три симплекси отримують ПТр, а два, які в перетині із цими симплексами мають спільні геометричні складові, отримують ЧТр. 13 симплексів кластера не задіяні в трансформаційних процесах і зберігають початкову форму ромба.

Необхідно зазначити, що рис. 3 можна розглядати, як одночасну атаку на три сенсори, які в кластері представлені сигнальними точками c_3, c_7 і c_{18}. Аналіз показує, що в області повної, часткової і нульової трансформації входять по 6 [4С].

На рис. 4 зображено області повної трансформації у кластері при здійсненні атак на ІВ, представлених сигнальними точками різних класів, а на рис. 5, відповідні візуальні зображення областей ПТр

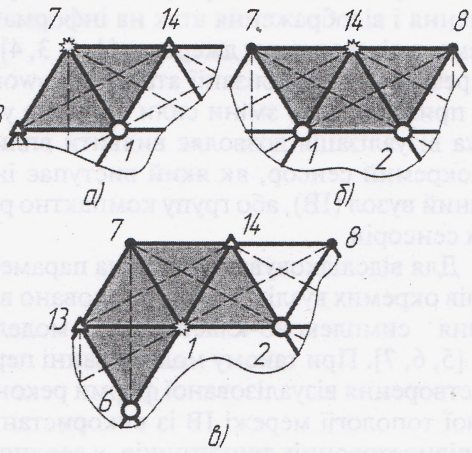

Рис. 4. Області трансформації кластера при атаці на один сенсор

В роботі [7] визначено також області трансформації кластера при одночасній атаці на два ІВ, які належать одному [4С] (рис. 6).

При атаці на два сенсори одного [4С] кластера можливими є випадки переміщення двох СТ (рис. 6), які визначаються: двома ФЗ (рис. 6, *а*); трьома ФЗ при розміщенні СТ на кінцях малої

діагоналі ромба, яка є також ФЗ (рис. 6, *б*); трьома ФЗ для однієї СТ і двома ФЗ для іншої при розміщенні сигнальних точок на кінцях однієї із сторін ромба (рис. 6, *в*).На рис. 7 зображено області ПТр кластера при таких трансформаціях [4С].

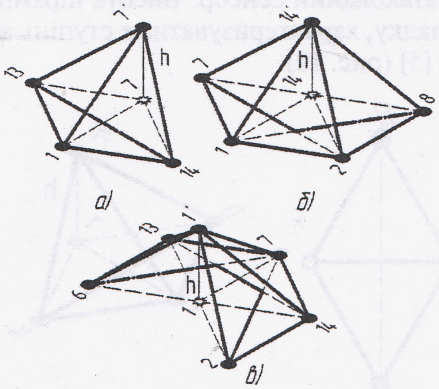

Рис. 5. Візуальне зображення областей трансформації за методом [4С]

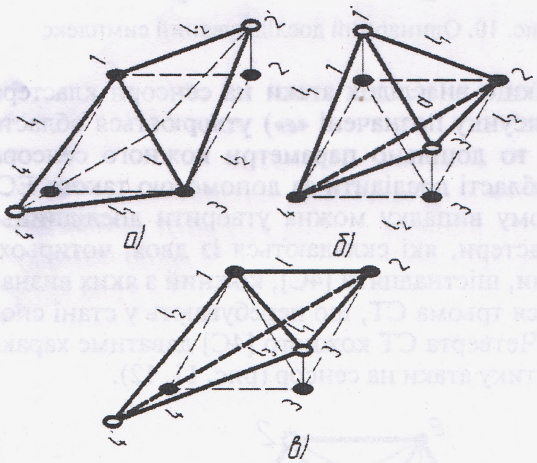

Рис. 6. Типи трансформації [4С] при двох атакованих сенсорах

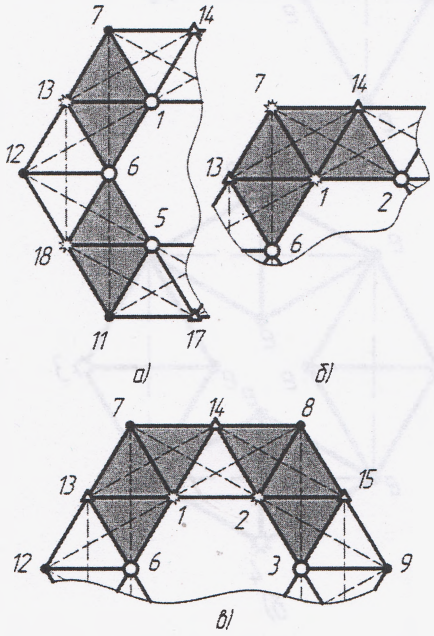

Рис. 7. Області ПТр кластера при атаці на два сенсори в одному [4С]

1.2. Метод фіктивних сигнальних точок (метод ФСТ)

Основним завданням, яке виникає при розгляді методу [4С], є необхідність однозначного визначення області ПТр кластера при здійсненні атак на сенсори. Задача визначення області ПТр вирішується використанням методу фіктивних сигнальних точок (ФСТ). За цим методом у кластері, який здійснює візуалізацію роботи сенсорів, при виникненні нестандартної роботи сенсора,функціональні зв'язки отримують видовження. В кінці видовження утворюється нове фіктивне положення СТ, яка у кластері представляє атакований сенсор. Здійснивши такі ж самі видовження із іншими ФЗ, які з'єднують СТ із сусідніми СТ, ми отримаємо (рис. 8): три ФСТ атакованого сенсора, якщо СТ знаходиться у вершині зовнішнього шестикутника кластера; чотири ФСТ атакованого сенсора, якщо СТ знаходиться на середині сторін зовнішнього шестикутника; п'ять ФСТ атакованого сенсора, якщо сигнальна точка є вершиною внутрішнього шестикутника.

З'єднавши ФСТ між собою і з місцем розміщення СТ при стабільній роботі сенсора, отримуємо плоскі геометричні об'єкти, які із симетрією відносно початкового положення СТ відображують структуру області ПТр у кластері при атаках на сенсори. Спроба з'єднати ФСТ в одну точку призводить до переміщення СТ атакованих сенсорів у третій вимір і створення візуалізації тривимірних геометричних об'єктів, які досліджувались методом [4С].

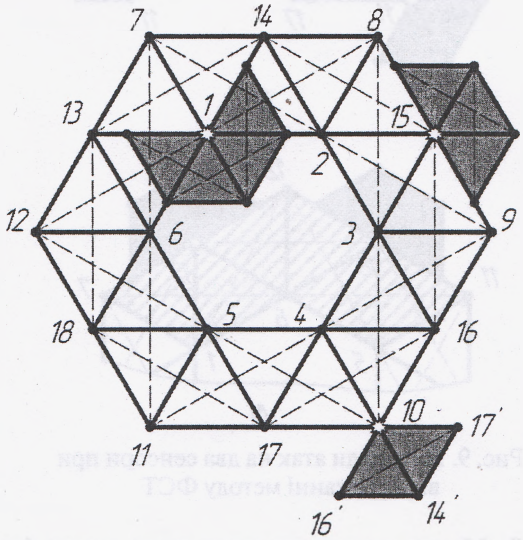

Рис. 8. Одинарний дослідний симплекс

На рис. 9 показано деякі приклади атак на два сенсори одного симплекса: рис. 9, *а* представляє атаку на два сенсори, сигнальні точки яких є вершиною внутрішнього шестикутника і серединою сторони зовнішнього шестикутника; рис. 9, *б* – атаку на сенсори, представлені сигнальними точками, одна з яких є вершиною, а інша – серединою зовнішнього шестикутника; рис. 9, *в* і 9, *г*

представляють атаки на сенсори, якщо СТ є вершинами зовнішнього і внутрішнього шестикутників; рис. 9, *д* – атаку на сенсори, представлені СТ, які є серединами двох сусідніх сторін зовнішнього шестикутника.

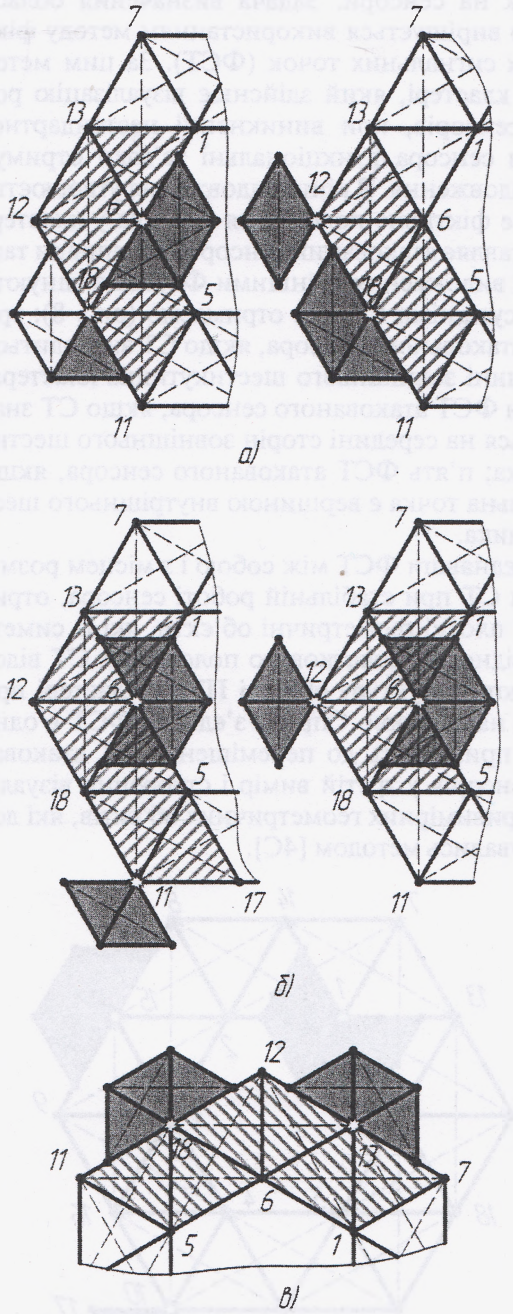

Рис. 9. Приклади атак на два сенсори при використанні методу ФСТ

1.3. Метод еталонних сигнальних точок (метод ЕСТ)

Метод еталонних сигнальних точок полягає в тому, що на першому етапі у 4-точковому симплексі всі ФЗ визначаються одними і тими ж параметрами еталонного сенсора (ЕС). Таким чином утворюється симплекс із п'ятьма рівними ФЗ довжиною l і одним геометричним зв'язком, довжиною $d = \sqrt{3}l$. Такий [4С]має форму ромба. Параметри підозрілого на атакованість сенсора подаються у положення [4С], яке визначається трьома ФЗ(СТ малої діагоналі ромба).

Видовження трьох ФЗ спричинить трансформацію плоского [4С] у тривимірний [4С] у формі трикутної піраміди із вершиною у СТ, що визначає атакований сенсор. Висота піраміди, в цьому випадку, характеризуватиме ступінь атаки на сенсор [5] (рис. 10).

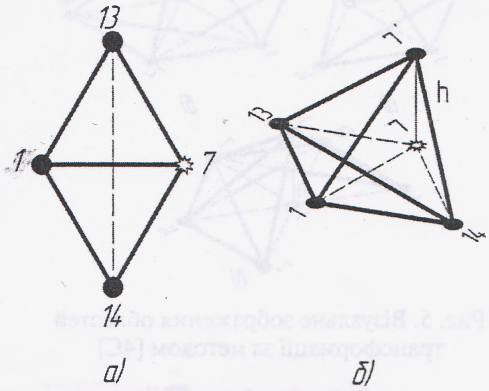

Рис. 10. Одинарний досліджуваний симплекс

Якщо внаслідок атаки на сенсори кластера (на рисунку позначені «*е*») утворюється область ПТр, то доцільно параметри кожного сенсора цієї області дослідити за допомогою такого ЕС. У цьому випадку можна утворити дослідницькі кластери, які складаються із двох, чотирьох, восьми, шістнадцяти [4С], кожний з яких визначається трьома СТ, що перебувають у стані спокою. Четверта СТ кожного [4С] даватиме характеристику атаки на сенсор (рис. 11, 12).

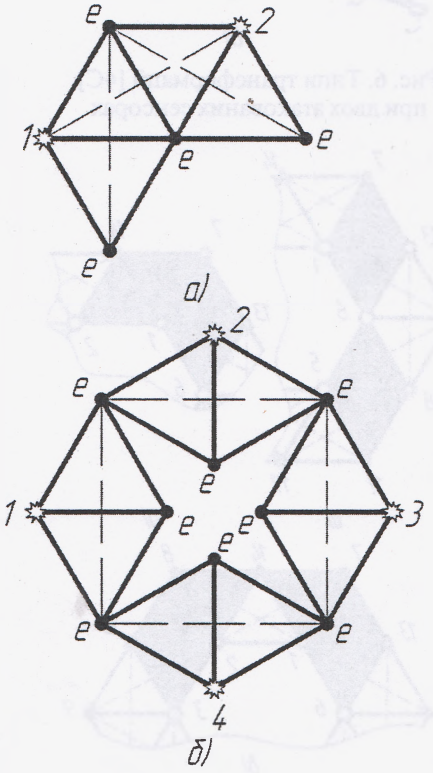

Рис. 11. Досліджувані кластери із двох і чотирьох [4С]

діагоналі ромба, яка є також ФЗ (рис. 6, *б*); трьома ФЗ для однієї СТ і двома ФЗ для іншої при розміщенні сигнальних точок на кінцях однієї із сторін ромба (рис. 6, *в*).На рис. 7 зображено області ПТр кластера при таких трансформаціях [4С].

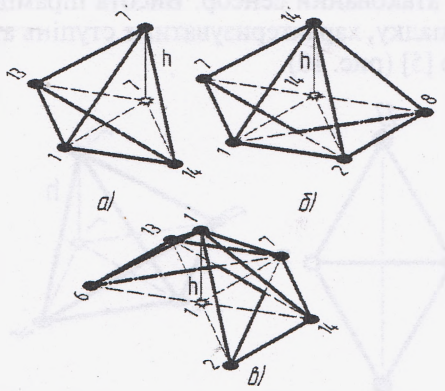

Рис. 5. Візуальне зображення областей трансформації за методом [4С]

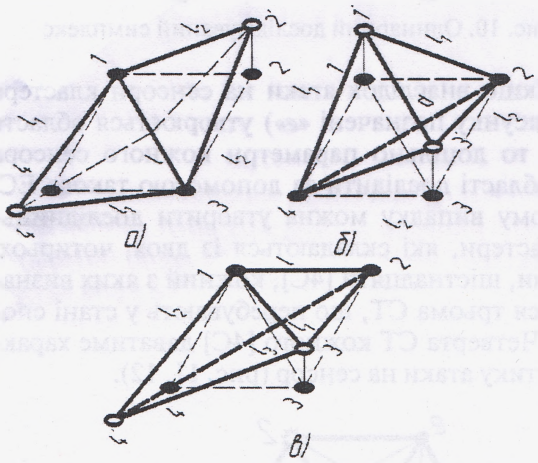

Рис. 6. Типи трансформації [4С] при двох атакованих сенсорах

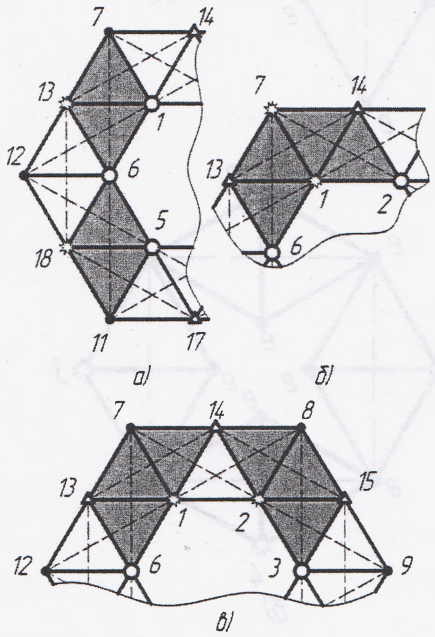

Рис. 7. Області ПТр кластера при атаці на два сенсори в одному [4С]

1.2. Метод фіктивних сигнальних точок (метод ФСТ)

Основним завданням, яке виникає при розгляді методу [4С], є необхідність однозначного визначення області ПТр кластера при здійсненні атак на сенсори. Задача визначення області ПТр вирішується використанням методу фіктивних сигнальних точок (ФСТ). За цим методом у кластері, який здійснює візуалізацію роботи сенсорів, при виникненні нестандартної роботи сенсора,функціональні зв'язки отримують видовження. В кінці видовження утворюється нове фіктивне положення СТ, яка у кластері представляє атакований сенсор. Здійснивши такі ж самі видовження із іншими ФЗ, які з'єднують СТ із сусідніми СТ, ми отримаємо (рис. 8): три ФСТ атакованого сенсора, якщо СТ знаходиться у вершині зовнішнього шестикутника кластера; чотири ФСТ атакованого сенсора, якщо СТ знаходиться на середині сторін зовнішнього шестикутника; п'ять ФСТ атакованого сенсора, якщо сигнальна точка є вершиною внутрішнього шестикутника.

З'єднавши ФСТ між собою і з місцем розміщення СТ при стабільній роботі сенсора, отримуємо плоскі геометричні об'єкти, які із симетрією відносно початкового положення СТ відображують структуру області ПТр у кластері при атаках на сенсори. Спроба з'єднати ФСТ в одну точку призводить до переміщення СТ атакованих сенсорів у третій вимір і створення візуалізації тривимірних геометричних об'єктів, які досліджувались методом [4С].

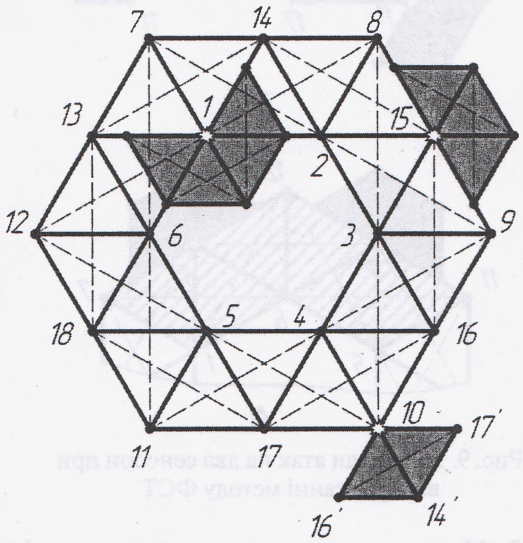

Рис. 8. Одинарний дослідний симплекс

На рис. 9 показано деякі приклади атак на два сенсори одного симплекса: рис. 9, *а* представляє атаку на два сенсори, сигнальні точки яких є вершиною внутрішнього шестикутника і серединою сторони зовнішнього шестикутника; рис. 9, *б* – атаку на сенсори, представлені сигнальними точками, одна з яких є вершиною, а інша – серединою зовнішнього шестикутника; рис. 9, *в* і 9, *г*

Розглянуті дослідні кластери (рис. 11, 12) характеризуються тим, що в них на один досліджуваний сенсор припадає два ЕС.

З метою зменшення їхньої кількості є можливість утворити інші типи кластерів, у яких крім утворення трикутних пірамід виникають і інші тривимірні симплекси, складові яких стають гранями трикутних пірамід.

На рис. 13 зображено дослідні кластери, які складаються із шести, десяти і 18-ти СТ для дослідження, відповідно, двох; чотирьох та восьми атакованих ІВ.

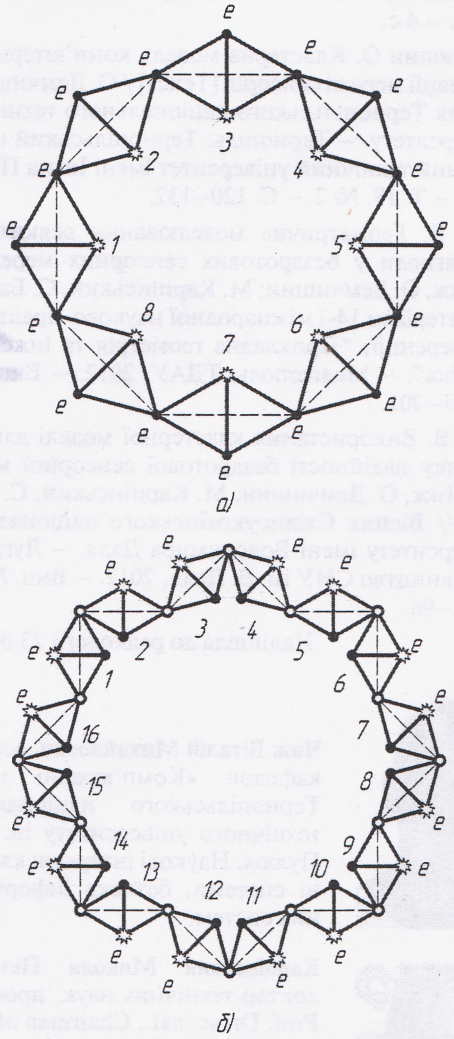

Рис. 12. Досліджувані кластери із восьми і шістнадцяти [4С]

Блок типу (рис. 13, *а*) дає можливість формувати більш складні кластерні структури, в яких відбувається зменшення кількості еталонних сенсорів (рис. 13, *б*, 13, *в*).

Можна скласти послідовність відношень кількості еталонних сенсорів до кількості досліджуваних сенсорів:

$$\frac{4}{2}=2,\quad \frac{6}{4}=1{,}5,\quad \frac{8}{6}=\frac{4}{3}\approx 1{,}33,$$

$$\frac{10}{8}=1{,}25\ldots,\quad \frac{2(n+1)}{2n},\ldots$$

Збільшуючи кількість початкових блоків *n* типу рис. 13, *а*, ми в границі отримаємо одиницю:

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

Це означає, що при великій кількості блоків відношення кількості еталонних сенсорів до кількості досліджуваних сенсорів близьке до одиниці.

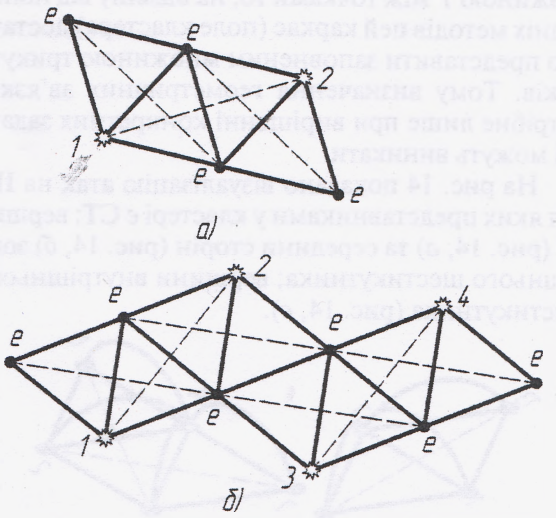

Рис. 13. Кластерні структури більш складних типів

1.4. Метод стаціонарних сигнальних точок (метод ССТ)

Цей метод дозволяє реалізувати інший вид візуалізації атак на ІВ, які моделюються кластером у конфігураційному просторі комп'ютера. Він ґрунтується на тому, що первинне положення СТ фіксується у кластері. Утворена плоска структура кластера із стабільно визначеними положеннями СТ і ФЗ між ними стає жорстким плоским каркасом. Сигнальні точки залишаються нерухомими і при здійсненні атак на ІВ. Зміна характеру роботи ІВ або групи ІВ спричиняє зміну довжин відповідних ФЗ.

Стаціонарність СТ у кластері перетворює ФЗ із відрізків у дуги кіл, які з'єднують сигнальну точку атакованого ІВ із сусідніми СТ. Таким чином, область ПТр кластера складатиметься із групи взаємозв'язаних трикутників, дві сторони кожного з яких перетворюються на дуги, що з'єднують СТ із точкою – представником атакованого ІВ. Сама ж область трансформації отримає локальне викривлення у вигляді, подібному до раковини молюска. Необхідно відмітити, що при використанні такої візуалізації зникає поняття часткової трансформації. Крім цього, якщо необхідно визначити горизонтальний зв'язок, то він знаходитиметься у плоскому полі каркасу кластера і не змінює своєї довжини.

Це нагадує ситуацію, коли на нерухомий каркас натягнути гумову плівку, зафіксовану у 18-ти точках і по периметру, який визначає ФЗ, які не змінюються внаслідок здійснення атаки. Змінені у довжині, внаслідок атаки на ІВ, ФЗ стають

дугами кіл, відділеними хордами, довжиною l. Дуги мають своїм початком зафіксовану СТ – представника атакованого ІВ. Кінці дуг фіксуються у сигнальних точках, які визначають ФЗ у створеному при стабільній роботі ІВ каркасу кластера.

Внаслідок того, що при створенні кластера із стабільною роботою ІВ, положення сигнальних точок визначається функціональними зв'язками довжиною l між точками то, на відміну від попередніх методів цей каркас (поле кластера) достатньо представити заповненим множиною трикутників. Тому визначення геометричних зв'язків потрібне лише при вирішенні конкретних задач, які можуть виникати.

На рис. 14 показано візуалізацію атак на ІВ, для яких представниками у кластері є СТ: вершини (рис. 14, *а*) та середини сторін (рис. 14, *б*) зовнішнього шестикутника; вершини внутрішнього шестикутника (рис. 14, *в*).

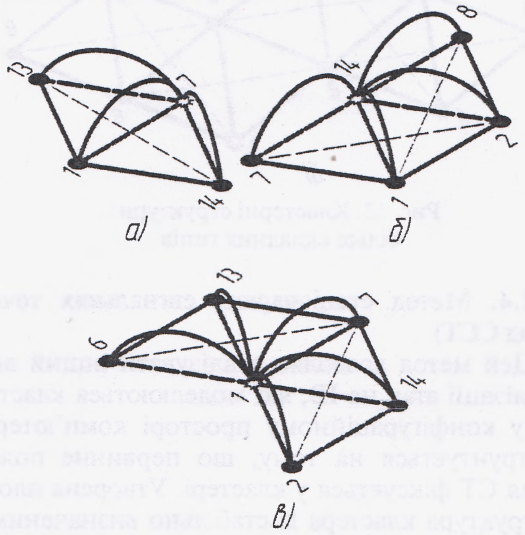

Рис. 14. Візуальне зображення областей повної трансформації за методом ССТ

ВИСНОВКИ

Доведено доцільність у процесі моделювання БСМ розглядати як модель кластер у вигляді плоскої замкнутої шестикутної геометричної структури, складеної із 18 сигнальних точок, з'єднаних за допомогою 36 однакових відрізків. Розглянуто чотири методи виявлення і дослідження областей трансформації кластера при здійсненні атаки на один і два сенсори, які представлені у кластері сигнальними точками одного 4-точкового симплекса.

Література

1. Majid Meghdadi. A Survey of Wormhole-based Attack sand their Counter measures in Wireless Sensor Networks [Електронний ресурс] // Department of Electrical Engineering IndianInstitute of Technology. – New Delhi, 2011. – Volume 28 Режим доступу: http://www.tr.ietejournals.org/ article. asp?issn= 0256-4602; year = 2011; volume=28;issue=2;spage=89;epage=102;aulast=Meghdadi. – Назва з екрану.
2. A. Becher. Tampering with motes: Real-world physical attacks on wireless sensor networks / A. Becher, Z. Benenson, M. Dornseif // volume 3934 of Lecture Notesin Computer Science, In J. A. Clark, R. F. Paige, F. Polack, and P. J. Brooke, editors, SPC, – 2006. – Pages 104-118.
3. Hyunsang Choi. Fast detection and visualization of network attacks on parallel coordinates / Hyunsang Choi, Heejo Lee, Hyogon Kim // Computers & Security. – July 2009. – Issue 5. – Pages 276–288
4. Пат. на корисну модель 64391 Україна: МПК H04W 12/00 Спосіб візуалізації [Текст] / Карпінський В.М., Євтух П.С., Боровік Б.Л., Карпінський М.П.; власник патенту Тернопільський національний технічний університет ім. І. Пулюя. – № u 2011 03578; заявл. 25.03.11; опубл. 10.11.2011, Бюл. № 21. – 4 с.
5. Демчишин О. Кластерна модель комп'ютерної візуалізації мережі сенсорів [Текст] / О. Демчишин // Вісник Тернопільського національного технічного університету. – Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя, 2012. – Т. 18, № 2. – С. 120–132.
6. Чиж В. Геометричне моделювання деяких атак на сигнали у бездротових сенсорних мережах / В. Чиж, О. Демчишин, М. Карпінський, С. Балабан // Матеріали 14-ї міжнародної науково-практичної конференції, "Прикладна геометрія та інженерна графіка". – Мелітополь: ТДАУ, 2012. – Вип. 4. – С. 195–201.
7. Чиж В. Використання кластерної моделі для розрахунку надійності бездротової сенсорної мережі / В. Чиж, О. Демчишин, М. Карпінський, С. Балабан // Вісник Східноукраїнського національного університету імені Володимира Даля. – Луганськ: Видавництво СНУ ім. В. Даля, 2012. – Вип. № 8. – С. 92–96.

Надійшла до редколегії 23.04.2013

Чиж Віталій Михайлович, аспірант кафедри «Комп'ютерні науки» Тернопільського національного технічного університету ім. Івана Пулюя. Наукові інтереси: кластерні системи, безпека інформаційних систем.

Карпінський Микола Петрович, доктор технічних наук, професор, Prof. Dr. sc. nat., Chairman of Computer Science Division of University of Bielsko-Biala, Bielsko-Biała. Наукові інтереси: спеціалізовані комп'ютерні мережі, безпровідні інформаційні технології та системи їх безпеки.

Балабан Степан Миколайович, кандидат технічних наук, доцент, доцент кафедри «графічного моделювання» Тернопільського національного технічного університету імені Івана Пулюя. Наукові інтереси: енергозберігаючі технології, екологічні проблем і проблем геометричного моделювання.

УДК 004.94

Контроль и визуализация состояния функциональной безопасности информационных систем с применением беспроводных сенсорных сетей / В.М. Чиж, М.П. Карпинский, С.М. Балабан // Прикладная радиоэлектроника: науч.-техн. журнал. – 2013. – Том 12. – № 2. – С. 356–362.

В статье рассмотрены важность и сложность организации эффективных методов контроля за состоянием надежности распространения информации в беспроводных сенсорных сетях. Предложены оригинальные методы контроля параметров сигналов отдельных или компактно расположенных сенсоров и визуализации атак на них. Обоснована целесообразность использования кластерной модели с симплексным покрытием его поля для визуализации областей трансформации сенсоров, сигналы которых подверглись атакам.

Ключевые слова: функциональная безопасность, информационные системы, сенсор, беспроводная сенсорная сеть, кластер, визуализация, трансформация, стационарная сигнальная точка, фиктивная сигнальная точка, эталонная сигнальная точка.

Ил.: 14. Библиогр.: 06 наим.

UDC 519:616-079.4:616.5

Control and visualization of functional security of information systems using wireless sensor networks / V.M. Chyzh, M.P. Karpinskiy, S.M. Balaban // Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. – № 2. – P. 356–362.

The importance and complexity of organizing effective methods of monitoring the status of the reliability of propagating information in wireless sensor networks are examined. Original methods of controlling signal parameters of individual or compactly disposed sensors and visualization methods of attacks on them are proposed. Authors substantiated using a cluster model with simplex coverage of its field to visualize areas of transformation of sensors whose signals were subjected to attacks.

Keywords: functional security, information systems, sensor, wireless sensor network, cluster visualization, transformation, fixed alarm point, dummy alarm point, reference signal point.

Fig.: 14. Ref.: 06 items.