КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№1 (9), 2020
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2020.9.6984
УДК 004.08; 005.4

Белей Олександр Ігорович
кандидат економічних наук, доцент, доцент кафедри Систем автоматизованого проектування
Національний університет «Львівська політехніка», Львів, Україна
ORCID: 0000-0003-4150-7425
Oleksandr.I.Belei@lpnu.ua

Сватюк Оксана Робертівна
кандидат економічних наук, доцент, доцент кафедри менеджменту та соціально-гуманітарних дисциплін
Львівський інститут Державний вищий навчальний заклад «Університет банківської справи», Львів, Україна
ORCID: 0000-0003-0099-2532
svatuk@gmail.com

РОЗРОБКА АЛГОРИТМУ ДЛЯ ШИФРУВАННЯ ПОВІДОМЛЕНЬ У СЕНСОРНИХ БЕЗПРОВІДНИХ МЕРЕЖАХ

Анотація. Здійснено аналіз фізичних характеристик вузла, на який може бути здійснена атака зловмисника. Запропоновано метод виявлення ушкодженого вузла з порушенням фізичних характеристик мережевого вузла, який базується на використанні ймовірнісних функцій, обчисленні довірчого інтервалу та ймовірності відхилення поточних показників від довірчого інтервалу. Його новизна полягає у можливості виявлення ушкодленого вузла шляхом оцінки потрапляння поточного значення функції в довірчий інтервал, при цьому не здійснюється порівняння функції розподілу поточного вузла з еталонним розподілом. Проведено аналіз фізичних параметрів мережевих вузлів для виявлення зловмисника на відміну від існуючих системи виявлення атак, що дозволяють виконати тільки аналіз мережевого трафіку. На основі розробленого алгоритму шляхом моделювання передачі хаотичних сигналів в безпровідній сенсорній мережі визначено ефективність виявлення атак через аналіз параметрів залишкової енергії та перевантаженості вузла, розширення діапазону атак, яким мережа здатна протидіяти порівняно з аналогами системи.
Під час моделювання поведінки безпровідної сенсорної мережі визначено, що процеси передачі даних носять хаотичний характер. Тому для підсилення безпеки передачі даних в хаотичним режимі нами запропоновано алгоритм шифрування з використанням динамічного хаосу, методів затримки координати та сингулярного спектрального аналізу. Здійснено порівняльний аналіз параметрів вхідної та вихідної послідовностей розробленого алгоритму шифрування на основі динамічного хаосу з стандартними алгоритмами шифрування даних. Встановлено, що параметри шифрування, які характерні для вихідних послідовностей алгоритму шифрування з використанням динамічного хаосу, не гірші за параметри шифрування, отримані для вихідних послідовностей стандартних алгоритмів шифрування. Оцінка навантаження вузлів за допомогою порогового аналізу їх поточних значень у довірчому інтервалі використовується для виявлення мережевих відхилень під час кібератаки. Розроблений алгоритм дозволяє здійснювати діагностику атак типу «Відмова в обслуговуванні» та «Сивілли» на початку їх появи та визначити можливі напрямки їх уникнення.

Ключові слова: атака; система виявлення атак; безпека; безпровідні сенсорні мережі; алгоритм шифрування; інформація; контроль; хаотичне відображення; динамічний хаос.

1. ВСТУП

Безпровідні сенсорні мережі широко використовуються для спостереження та управління об’єктами здалеку. У той же час, вузли мережі можуть розташовуватися за межами контрольованої зони та піддаватися впливу зловмисника. Також безпровідні

ISSN 2663 - 4023

сенсорні мережі мають велику кількість вразливостей, пов’язаних з передачею даних по незахищеним безпровідними каналам. У зв'язку з цим актуальним завданням є розробка методу, який дозволяє ефективно виявляти активні атаки зловмисником на основі аналізу мережевого трафіку та фізичних параметрів датчиків в безпровідній сенсорній мережі.

Розглядаючи алгоритми, що використовують динамічний хаос, важливо забезпечити хаотичний режим, який виявляється в отриманні хаотичних послідовностей алгоритму шифрування і обумовлений вимогами безпеки схеми шифрування.

У цій роботі ми пропонуємо та розглянемо два підходи до визначення стійкості вихідних послідовностей зашифрованої інформації. Перший з них ґрунтується на підході методів нелінійної динаміки, що дозволяє визначати параметри динамічної системи та їх зміни під час шифрування. Другий варіант, завдяки наявності детермінованого компонента в досліджуваних послідовностях, дозволяє використовувати підхід, заснований на сингулярному спектральному аналізі з визначенням динаміки інтенсивності основних компонентів.

Постановка проблеми. Для дослідження ми використовували вихідні послідовності, отримані для алгоритму шифрування, який ми розробили, використовуючи динамічний хаос, симетричний алгоритм блочного шифрування та стандартний симетричний алгоритм шифрування, а також послідовності введення чіткого тексту. Розроблений алгоритм шифрування на основі динамічного хаосу заснований на алгоритмі узагальненого блоку симетричного шифрування. Мережа Фейстеля використовується як основне перетворення, при якому нелінійна функція задається у вигляді хаотичної карти.

При використанні першого підходу до визначення випадковості проводиться аналіз рівня випадковості зашифрованих послідовностей шляхом побудови фазових портретів та використання методу відстроченої координати. Використання методу відстроченої координати як одного з методів нелінійної динаміки дозволяє визначити кількісні показники у вигляді кореляційного розміру d та ентропії Колмогорова K для кожної з досліджуваних послідовностей. Кореляційний розмір визначає область локалізації динамічної системи у фазовому просторі або кількість ступенів свободи зазначеної системи. Ентропія Колмогорова характеризує стійкість системи, виміряну швидкістю розбіжності її траєкторій у фазовому просторі. Візуальний аналіз проводиться відповідно до побудованих фазових портретів системи. Побудова фазових портретів дозволяє візуально визначити ступінь заповнення фазового простору.

При використанні другого підходу до визначення випадковості на основі методу сингулярного спектрального аналізу оцінюється кількісний параметр - рівень основних компонентів I. Для отримання візуальної інформації використовуються фазові діаграми, коли різні пари власних векторів або основних компонентів побудовано по осях x і y.

Мета статті. Метою дослідження є розробка методу, який дозволяє ефективно виявляти активні атаки зловмисника типу «Сивілли» на основі аналізу мережевого трафіку, та алгоритму шифрування передачі вихідних послідовностей на основі динамічного хаосу для безпровідних сенсорних мереж.

ISSN 2663 - 4023

2. АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ.

Існує дві групи методів захисту безпровідних сенсорних мереж (БСМ) від активних атак зловмисником: системи виявлення атак та вторгнень та системи обчислення довіри [1]. Як спосіб захисту від активних атак зловмисником, у цій статті розглядається метод розрахунку довіри. Методи обчислення довіри дозволяють не тільки виявляти ненормальну поведінку та атаки в мережі, але й підтримувати довірені відносини між вузлами, що допомагає запобігти деяким типам атак [2]. На сьогодні існує два типи систем обчислення довіри: розподілена та централізована [3]. На основі аналізу атак [4] були виявлені найбільш шкідливі атаки, такі як «Відмова в обслуговуванні» [5], блокування вузла, блокування вузла умовами [6], тунелінг [7], атаки типу «Сивілли» [8]. Розподілені та централізовані системи для обчислення довіри мають свої переваги та недоліки [9], але загальним їх недоліком є неможливість протидіяти відмові у службі та атакам «Сивілли». Кожен тип методу може використовувати різний математичний апарат для обчислення довіри. Імовірнісні методи добре поєднуються з поняттям довіри, якщо довіра визначається як очікування, що мережевий вузол поводиться належним чином з іншими вузлами та виконує свої зобов'язання під час передачі даних, а також не заважає роботі інших вузлів та мережі як цілий [10].

На сучасному рівні розвитку інформаційних технологій велике значення мають питання захисту інформації в телекомунікаційних системах різного призначення. Напрямок, пов'язаний із шифруванням інформації в хаотичних системах, розвивається [11]. Використання динамічного хаосу для систем захисту інформації обумовлено здатністю хаотичних відображень забезпечувати секретність передачі зашифрованої інформації в блокових або потокових шифрах [12]. Детермінізм хаосу сприяє шифруванню інформації, а її випадковість робить систему стійкою до фальсифікації [13]. Такі властивості, як плутанина і розбризкування, характерні для традиційних крипто алгоритмів, реалізуються в хаотичних з використанням хаотичних відображень та подальших ітерацій.

В [14] було показано, що традиційні криптографічні системи можна розглядати в рамках синергетичного підходу, тобто як нелінійні динамічні системи $\langle F, X, K \rangle$. Під криптосистемою ми можемо зрозуміти динамічну систему з нелінійною функцією F, простором станів X і простором параметрів K. Нелінійна функція F задається за допомогою алгоритму, X - набір початкових станів, набір ключів.

У дослідженні [15] автором багато разів оцінюється захищеність алгоритму шифрування та виявляється, що алгоритм шифрування може бути ефективно розбитий лише одним відомим простим зображенням. Ефективність запропонованої відомої атаки в прямому тексті підтримується як суворим теоретичним аналізом, так і експериментальними результатами.

Як бачиом із наведених досліджень у сфері безпеки безпровідних сенсорних мереж та шифрування даних на основі динамічного хаосу, власне застосування алгоритмів шифрування передачі хаотичних сигналів для безпровідних сенсорних мереж немає.

ISSN 2663 - 4023

3. ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Для здійснення цих атак зловмиснику потрібно надіслати велику кількість пакетів, тому вузол повинен споживати велику кількість енергії. Порівнюючи рівень залишкової енергії *Q (E)* та навантаження вузла *L* залежно від загальної кількості пакетів за певний проміжок часу, можна побачити пропорційну закономірність. Для обчислення довірчого значення вузла враховуються параметри *L* та залишкова енергія *Q (E)*. Для того, щоб вузол вважався довіреним, рівень його залишкової енергії не повинен перевищувати максимальний заданий рівень енергії в мережі Emax і не був значно нижчим, ніж у сусідніх вузлів. При цьому рівень навантаження вузла не повинен значно перевищувати рівень навантаження сусідніх вузлів і не повинен бути нижчим за мінімально необхідний рівень навантаження. Ми використовуємо нормальний закон розподілу для показників перевантаженості *L* та залишкової енергії *Q (E)* для обчислення довірчих інтервалів та ймовірності того, що поточне значення потрапить у довірчий інтервал.

$$L_i(t) \sim N(\bar{L}, \sigma_L^2), Q(E)_i(t)) \sim N(\overline{Q(E)}, \sigma_{Q(E)}^2), \tag{1}$$

де $\sigma_{Q(E)}$, σ_L є загальним для групи кластерних вузлів; $\overline{\mathrm{Q(E)}}$, $\bar{\mathrm{L}}$ - математичне сподівання на навантаження та залишкову енергію вузла.

Використання нормального закону розподілу пояснюється тим, що він широко використовується в мережах чергування для представлення розподілу кількості вимог в інтервалі до середньої тривалості обслуговування, що аналогічно розподілу робочого навантаження та залишкової енергії вузла. А також був проведений аналіз кількісних діаграм для підтвердження цього факту. Щоб знайти довірчий інтервал, спочатку слід обчислити загальне середнє значення для залишкової енергії $Q(E)_i$ та навантаження *Li* для групи вузлів кластера для кожного часового інтервалу:

$$\overline{\mathrm{Q(E)}} = \frac{\sum Q(E)_i}{n}, \bar{\mathrm{L}} = \frac{\sum L_i}{n} \tag{2}$$

Далі потрібно обчислити дисперсію D та стандартне відхилення σ:

$$D_{Q(E)} = \frac{(\sum_i^n (Q(E)_i - \overline{Q(E)})^2}{n}, D_L = \frac{(\sum_i^n (L)_i - \bar{L})^2}{n} \tag{3}$$

де n - розмір вибірки; дисперсія *DQ (E)* для залишкової енергії *DL* дисперсія для перевантажень.

$$\sigma_{Q(E)} = \sqrt{D_{Q(E)}}, \sigma_L = \sqrt{D_L} \tag{4}$$

При визначенні достовірності важливо, щоб поточні значення вузла не виходили за довірчий інтервал, тобто навантаження на вузол та залишкова енергія не перевищували допустимих значень. Вузол обчислює нижню *bmin* та верхню границю *bmax* вузла, якому довіряють робоче навантаження та залишкову енергію *amin, amax,* відповідно до формул:

$$\alpha_{\min} = \overline{Q(E)} - \frac{t \cdot \sigma_{Q(E)}}{\sqrt{n}}, \alpha_{\max} = \overline{Q(E)} + \frac{t \cdot \sigma_{Q(E)}}{\sqrt{n}} \tag{5}$$

$$b_{\min} = \overline{Q(E)} - \frac{t \cdot \sigma_L}{\sqrt{n}}, b_{\max} = \overline{Q(E)} + \frac{t \cdot \sigma_L}{\sqrt{n}} \tag{6}$$

де $\frac{t \times \sigma}{\sqrt{n}}$ - точність оцінки; t - аргумент функції Лапласа; $\Phi(t) = \frac{\alpha}{2}$ - функція Лапласа; α - задана надійність

Для залишкової енергії верхня межа інтервалу завжди дорівнює E_{max}, оскільки вузли можуть мігрувати з кластеру в кластер, і нові вузли можуть з'являтися з максимальним значенням залишкової енергії, щоб уникнути помилок першого виду, цей фактор повинен враховувати. Розрахунок нижньої межі довірчого інтервалу проводиться лише для значення залишкової енергії. Оскільки нижня межа завантаження вузла виявляється відповідно до мінімально необхідної кількості пакетів, переданих через вузол під час сеансу зв'язку. Далі, обчислення ймовірності потрапляння в довірчий інтервал поточного навантаження та залишкової енергії вузла, за формулами:

$$b_{\min} = \overline{Q(E)} - \frac{t \cdot \sigma_L}{\sqrt{n}}, b_{\max} = \overline{Q(E)} + \frac{t \cdot \sigma_L}{\sqrt{n}} \quad (7)$$

$$P_{Q(E)}(\alpha_{\min} < Q(E)_i < \alpha_{\max}) =$$

$$= \Phi\left(\frac{\alpha_{\max} - \overline{Q(E)_b}}{\sigma_{Q(E)_b}}\right) - \Phi\left(\frac{\alpha_{\min} - \overline{Q(E)_b}}{\sigma_{Q(E)_b}}\right) \quad (8)$$

$$P_L(\alpha_{\min} < L_i < \alpha_{\max}) =$$

$$= \Phi\left(\frac{\alpha_{\max} - \overline{L_b}}{\sigma_{L_b}}\right) - \Phi\left(\frac{\alpha_{\min} - \overline{L_b}}{\sigma_{L_b}}\right) \quad (9)$$

де Ф - функція Лапласа; $P_{Q(E)}$, P_L - ймовірність отримання залишкової енергії вузла та рівня навантаження вузла в межах довірчого інтервалу.

Для обчислення стандартного відхилення та математичного очікування необхідно скоротити інтервал, на який обчислюється значення, та врахувати лише попередні L_{i-1}, $Q(E)_{i-1}$ та поточні Li, $Q(E)_i$ значення вузла. Якщо взяти значення протягом усього часового інтервалу, стандартне відхилення зростає занадто сильно, через велику різницю між початковим та кінцевим значеннями. Крім того, математичне очікування не дасть точного значення. Якщо ми візьмемо значення сусідніх інтервалів, то це дозволить нам оцінити, чи потрапляє поточне значення в довірчий інтервал без втрати точності обчислення. Для отримання достовірного значення необхідно використовувати комбінацію *PQ(E), PL* значень прямого довірчого значення *Tcent*, представлений алгоритм комбінування значень довіри за допомогою теореми Баєса. Як результат, формула для обчислення значення довіри прийме вигляд:

$$T_{cent} = P_{Q(E)} \times P_L . \quad (10)$$

4. МЕТОДИКА ДОСЛІДЖЕННЯ

Для проведення експериментального дослідження та оцінки ефективності системи управління обороною була розроблена динамічна модель безпровідної сенсорної мережі (БСМ). Для реалізації концептуальної моделі БСМ була обрана система моделювання NS-2. Аналіз експериментальних даних проводився за допомогою програми аналізу даних та оцінки довіри у БСМ.

Оцінка ефективності проводилася на основі наявності помилок 1-го та 2-го роду

при виявленні зловмисника. Помилка першого типу - хибний позитив, який виникає в результаті блокування довіреного вузла. Це значення обчислюється відповідно до наступного виразу:

$$P_{1error} = \frac{n_{error1}}{N_{all}} \quad (11)$$

де n_{error1} кількість інтервалів часу для всіх довірених вузлів мережі, при яких рівень довіри не перевищував 0,5; n_{error1} - загальна кількість часових інтервалів для всіх надійних хостів.

Помилка другого роду - помилковий позитив, який виникає внаслідок не виявлення шкідливого вузла. Імовірність виникнення помилок другого роду обчислюється так:

$$P_{2error} = \frac{n_{error2}}{N_{all2}} \quad (12)$$

де n_{error2} кількість інтервалів часу для всіх шкідливих вузлів мережі, на яких рівень довіри перевищує 0,5; N_{all2} - загальна кількість часових інтервалів для всіх надійних хостів.

В атаці «Відмова в обслуговуванні» зловмисник надсилає пакети в мережу з більшою інтенсивністю, ніж довірені вузли, в той час як зловмисник надсилає пакети з інтенсивністю 24 пакети/сек, а довірений вузол 0,9 пакетів/сек. Більше того, основна мета цієї серії експериментів - оцінка рівня помилкових позитивних результатів при наявності великої кількості шкідливих вузлів. Хибний позитив може виникнути через те, що велика кількість шкідливих вузлів має велике навантаження і межі довірчого інтервалу зміщуються, щоб довірений вузол не потрапляв у них. Крім того, під час нападу збільшується і навантаження надійного вузла, що може призвести до помилок першого виду. Перша серія експериментів була проведена для випадку, коли початковий рівень енергії E_{max} для шкідливих вузлів та для довірених вузлів був однаковим. У цьому випадку один вузол зловмисника цілеспрямовано атакував один довірений вузол. У першому рядку табл. 1 відображається ймовірність виникнення помилки першого виду. Виникнення помилок першого типу пов'язане з тим, що рівень перевантаженості довірених вузлів збільшується через збільшення отриманих пакетів. Далі рівень помилкових позитивних результатів знижується, оскільки рівень завантаженості нападників значно збільшується.

Таблиця 1

Ймовірність помилки атаки 1-го роду (*P1error*) «Відмова в обслуговуванні»

Надлишок початкової енергії вузлами зловмисників	Кількість вузлів зловмисника,%								
	5	**10**	**20**	**25**	**30**	**35**	**40**	**45**	**50**
E_{max}	0,09	0,07	0	0	0	0	0	0	0
1,5 E_{max}	0,03	0,02	0,05	0,02	0,02	0,02	0,02	0,02	0,01
2 E_{max}	0,04	0,02	0,04	0	0	0,02	0	0	0

Виникнення помилок другого роду пов’язане з тим, що зі збільшенням кількості зловмисників до 50%, верхня межа довірчого інтервалу значно зростає, що призводить до зниження рівня виявлення зловмисників. У табл. 2 показана ймовірність помилок другого роду при зміні двох параметрів: початковий рівень енергії та кількість вузлів зловмисника. Виявлення зловмисника відбувається у всіх випадках експерименту.

Ефективність виявлення зменшується, коли кількість шкідливих вузлів наближається до порогу 50 %.

Таблиця 2

Ймовірність помилки нападу 2-го роду (*P2error*) «Відмова в обслуговуванні»

Надлишок початкової енергії вузлами зловмисників	Кількість вузлів зловмисника,%								
	5	10	20	25	30	35	40	45	50
E_{max}	0,09	0,07	0	0	0	0	0	0	0
1,5 E_{max}	0,03	0,02	0,05	0,02	0.02	0,02	0,02	0,02	0,1
2 E_{max}	0,04	0,02	0,04	0	0	0,03	0	0	0

Найвища ефективність виявлення спостерігається, коли перевищення початкового рівня енергії знаходиться в інтервалі *Emax<Ei<2Emax*.

Під час атаки типу «Сивілли», нападник, схоже, є декількома об'єктами в системі.

У цьому випадку зловмисник виявляється вузлами і намагається захопити найбільший вплив мережею. Основна мета експерименту - оцінити можливість виявлення атаки типу «Сивілли» за заданих умов та ефективність виявлення цієї атаки при зміні параметрів атаки. У табл. 3 представлена оцінка ймовірності помилки першого і другого роду залежно від зміни показників кількості вузлів зловмисника та кількості вузлів, сприйнятливих до атаки. Якщо в мережі є 1 шкідливий вузол, найефективніше виявлення зловмисника спостерігається, коли кількість жертв становить 15 %. Тобто зловмисник впливає на невелику частину мережі. Далі, шкідливий вузол намагається взяти під дію інші вузли. У той же час ефективність знижується, оскільки вузли знаходяться в важкодоступній близькості від зловмисника.

Найефективніше виявлення зловмисника спостерігається, коли зловмисник перенаправляє всі пакети довколишніх вузлів до себе, для того, щоб здійснити атаку, потрібно було 4 вузли зловмисника.

Таблиця 3

Ймовірність помилки 1-го роду (P1error) атаки типу «Сивілли»

Кількість вузлів нападника	Кількість вузлів, сприйнятливих до нападу,%								
	5	10	20	30	40	50	60	65	70
1	0	0	0,1	0,06	0,04	0,08	0,06	0,06	0,06
2	0,05	0,04	0,05	0,04	0,05	0,04	0,04	0,03	0,04
3	0	0	0	0	0	0,08	0,04	0,08	0,06
4	0,05	0,05	0,01	0,01	0,01	0,01	0,06	0,08	0,07

Для дослідження ми використовували вихідні послідовності, отримані для алгоритму шифрування та послідовності вхідного простого тексту. Ми розробили алгоритм на основі моделі динамічного хаосу, блочного та стандартного симетричного шифрування. Розроблений алгоритм шифрування на основі динамічного хаосу заснований на узагальненому алгоритмі шифрування симетричного блоку. Мережа Фейстеля використовується як основне перетворення, при якому нелінійна функція позначається у вигляді хаотичної карти.

Відповідно до методу відстроченої координати, вихідна послідовність алгоритму шифрування представлена у вигляді:

$$x_1, x_2, ..., x_n \tag{13}$$

де $x_n = x\,(np)$, p - крок вибірки, n - ціле число.

Ця послідовність генерує m-мірні вектори, що лежать у m-мірному фазовому

просторі:

$$\overline{x_i^T} = (x_i, ..., x_{i+m-1}) \quad (14)$$

де *T* - знак транспонування.

Стан системи у відтвореному *m*-мірному фазовому просторі визначається m-мірними точками для кожної реалізації *x (p)*:

$$x_i^m = m^{\frac{1}{2}}(x_i, x_{i+1}, ..., x_{i+m-1}) \quad (15)$$

Кореляційний інтеграл *Cm (l)* - це функція, рівна ймовірності того, що відстань між двома реконструйованими векторами x_i менше l.

Кореляційний розмір *d* визначається:

$$d = \lim_{r \to 0} \left[\frac{\lg C_m(r)}{\lg r} \right] \quad (16)$$

де *Cm(r)* - інтеграл кореляції, *r* - розмір комірки перегородки або коефіцієнт подібності.

Інтеграл кореляції записується:

$$C_m(r) = \lim_{N \to \infty} \frac{1}{N^2} \sum_{i,j=1}^{N} \theta(r - |\overline{x_i} - \overline{x}_j|) \quad (17)$$

де $\theta = 0$ в $t \le 0, \theta = 0.5$, в $t = 0, \theta = 1$, в $t \ge 0, \theta$ - функція *Heaviside, N* - кількість точок, використаних для оцінки розмірності.

Виявлено, що для малих значень r поведінку функції *Cm(r)* можна розписати:

$$C_m(r) = r^d \quad (18)$$

де *d* - параметр, близький до фрактальної розмірності дивного атрактора, *r* - параметр подібності.

Для вивчення реалізацій відкритих та зашифрованих текстових повідомлень використовується метод сингулярного спектрального аналізу, алгоритм якого зводиться до наступного.

Нехай наведено часовий ряд $\{x_i\}_{i-1}^N$, утворений послідовністю *N* рівних відстаней деякої функції *f (t)*.

1. Сканування одновимірного на багатовимірний ряд. В якості першого ряду матриці *X* використовуються значення *M* (довжина гусениці) послідовності, починаючи з першого члена.

Значення послідовності використовуються як другий рядок матриці, починаючи від x_2 до x_{M+1}. Останній рядок матриці з числом $k = N - M + 1$ формується з останньої послідовності *M* елементів. Ця матриця, елементи якої можна розглядати як *M*-мірний часовий ряд, який відповідає *M*-мірній траєкторії в *M*-розмірному просторі *k-1* одиниць.

2. Аналіз основних компонентів: сингулярне розкладання зразкової матриці коваріації. Обчислюється матриця, яка є матрицею коваріації поза центром $V = (\frac{1}{k}) X^T X$.

Визначаються власні значення та власні вектори матриці V $V = P \wedge P^T$, її розширення де *L* - діагональна матриця, по діагоналі якої знаходяться низхідні власні значення, а *P* - ортогональна матриця власних векторів матриці *V*.

Матриця P може розглядатися як матриця переходу до основного компонента

ISSN 2663 - 4023

$XP = Y = (y_1, y_2, ..., y_m)$. Якщо використовується часовий ряд випадкових чисел, то власні значення матриці V є вибірковими дисперсіями відповідних головних компонентів, а їх квадратні корені - вибіркові засоби. Для аналізу основних складових недооцінених рядів використовується графічне зображення власних значень деяких функцій.

3. Враховуючи властивості матриці P, можна представити матрицю ряду X у вигляді $X = YP^T$. Отримуємо розширення матриці ряду на ортогональні компоненти.

У той же час перетворення $y_i = XP_i$ - це лінійне перетворення початкового процесу з використанням дискретного перетворення згортки:

$$y_i[l] = \sum_{q=1}^{M} x_{lq} p_{jq} = \sum_{q=1}^{M} x_{l+q-1} p_{jq...} \quad (19)$$

Алгоритм генерує набір лінійних фільтрів, налаштованих на компоненти вихідного процесу. Власні вектори матриці V виконують роль перехідних функцій відповідних фільтрів.

Візуально-аналітичне вивчення власних векторів та основних компонентів, отриманих в результаті лінійної фільтрації, дає інформацію про структуру досліджуваного процесу та його властивості.

Для отримання візуальної інформації використовуються фазові діаграми, коли різні пари власних векторів або головних компонентів побудовані по осях x і y. З ортогонально власних векторів та основних компонентів випливає, що зсув фаз між такими парами становить $\pm \pi / 2$.

4. Відновлення одновимірного ряду. Процедура відновлення заснована на декомпозиції $X = YP^T$. Відновлення здійснюється за основними компонентами, якщо при застосуванні формули $X = Y * P$ матриця отримується з матриці Y шляхом знецінення всіх невизначених компонент.

Таким чином, ми можемо отримати апроксимацію матриці рядів, в яких ми перетинаємось, або інтерпретованої частини цієї матриці.

5. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Під час обчислювального експерименту з використанням методу відкладених координат та методу сингулярного спектрального аналізу були отримані параметри вихідних послідовностей розробленого алгоритму шифрування, алгоритмів блочного та стандартного симетричного шифрування сигналів. На рис. 1 представлені графіки кореляційного виміру d та ентропії Колмогорова K вхідних та вихідних послідовностей. Вони отримуються за допомогою шифрування довільного фрагмента простого тексту за допомогою розробленого алгоритму шифрування та блочного симетричного шифрування.

ISSN 2663 - 4023

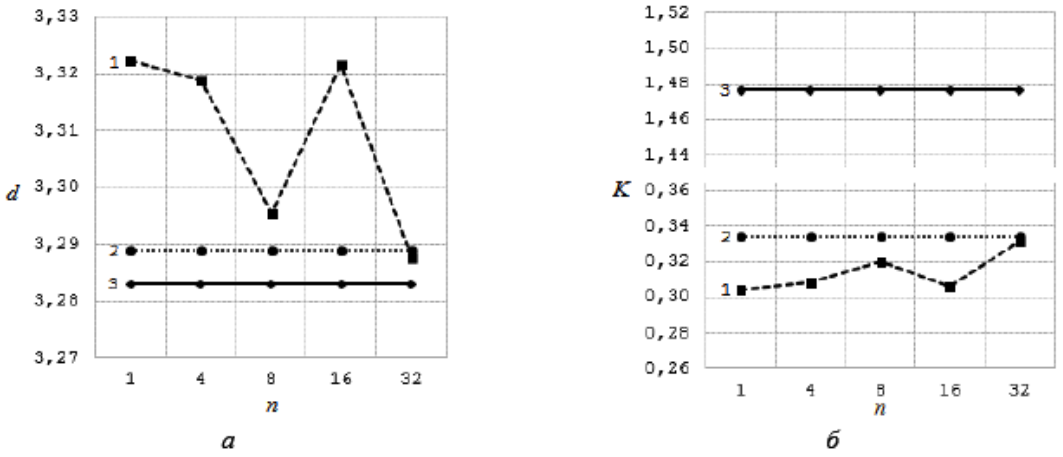

Рис. 1. Графіки залежності величини кореляційного розміру d (а), ентропія Колмогорова K (б) вихідних послідовностей алгоритму шифрування з використанням динамічного хаосу (крива 1), блочного симетричного алгоритму (крива 2), вхідні послідовності (крива 3) на кількість раундів n перетворення основи в роботі зчеплення блоку шифру

Використання інформаційних параметрів дозволяє ідентифікувати відмінності у послідовності виходу алгоритму шифрування щодо введення. Зокрема, в режимі роботи WSN значення кореляційного розміру для вихідної послідовності перевищують значення для вхідної послідовності на 4,0–4,6 %, а значення ентропії Колмогорова для вихідної послідовності становлять відповідно 20,0–21,8 % значення для входу.

Як видно з графіків, показаних на рис. 2, в захваті блоку шифру, для інтервалу, пов'язаного з інтервалом кількості раундів базової трансформації (1–32 раунда), виводяться послідовності виходів, отримані розробленим алгоритмом шифрування. більш високий ступінь випадковості, ніж вихідні послідовності, отримані алгоритмом блочного симетричного шифрування.

Використання цих інформаційних параметрів також дозволяє ідентифікувати області визначення у вихідних послідовностях, які можуть бути сформовані, коли елементи алгоритму шифрування не хаотичні, що неможливо виявити, проаналізувавши показники Ляпунова. Зокрема, поведінка логістичного відображення в алгоритмі шифрування для певних значень параметру управління потрапляє в область з детермінованою динамікою, що робить цей алгоритм вразливим до атак на основі відомого простого тексту. Значення кореляційного виміру та ентропії Колмогорова для відповідних вихідних послідовностей значно відрізнятимуться від значень за наявності динамічного хаосу.

На рис. 2 представлені фазові портрети простого тексту та відповідні зашифровані послідовності, отримані за допомогою розробленого алгоритму шифрування та блочного симетричного алгоритму. Кількість раундів базового перетворення розробленого алгоритму становить 16, а для блочного симетричного - 14.

ISSN 2663 - 4023

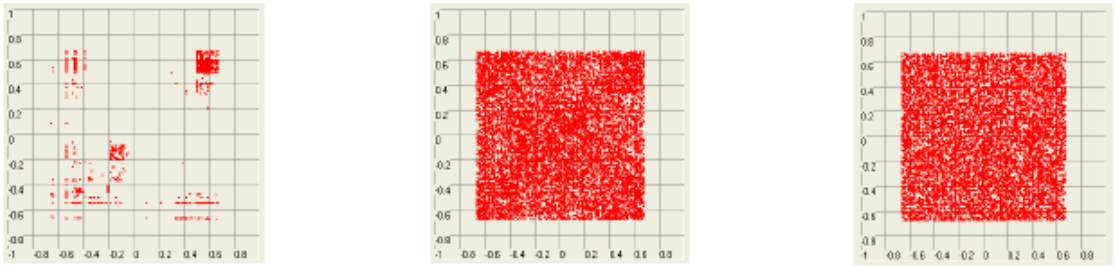

Рис. 2. Фазові портрети вхідних даних: (а) вихідних послідовностей, отриманих за допомогою розробленого алгоритму шифрування; (б) блочний симетричний алгоритм; (в) під час керування блоком шифру

Результати, отримані методом затримки координат та побудова фазових портретів вхідних (звичайний текст) та вихідних (зашифрованих) послідовностей, дозволяють зробити висновок про те, що: розмір кореляції, ентропія Колмогорова можна використовувати як параметри для визначення ступеня випадковості вихідні послідовності та фазові портрети для візуального аналізу при застосуванні алгоритму шифрування з використанням динамічного хаосу (табл. 4).

Таблиця 4

Рівень основних компонентів *I*

№ основного компонента	1000	999	998	997	996	995	994	993
Вхідні послідовності	0,3530	0,3530	0,3036	0,3035	0,2989	0,2979	0,2934	0,2934
Вихідниі послідовності розробленого алгоритму шифрування з використанням динамічного хаосу з кількістю ітерацій *z = 8 (2)*	0,2203	0,2202	0,2122	0,2118	0,2081	0,2080	0,2028	0,2027
Вихідниі послідовності розробленого алгоритму шифрування з використанням динамічного хаосу з кількістю ітерацій *z = 64 (3)*	0,226	0,2258	0,2250	0,2250	0,2109	0,2108	0,2015	0,2014
Стандартний симетричний алгоритм шифрування	0,1899	0,1893	0,1880	0,1879	0,1841	0,1840	0,1821	0,1820
Блочний симетричний алгоритм шифрування	0,2287	0,2287	0,2179	0,2177	0,2135	0,2134	0,2083	0,2081

Використовуючи другий підхід до визначення випадковості на основі методу сингулярного спектрального аналізу, в процесі дослідження ми оцінили кількісний параметр - рівень основних компонентів вхідних послідовностей, вихідні послідовності алгоритму шифрування, розробленого нами за допомогою алгоритму динамічного хаосу, алгоритм блочного та стандартного симетричного шифрування. Для аналізу візуальної інформації використовуються фазові діаграми, коли різні пари власних векторів або головних компонентів побудовані вздовж осей *x* та *y*. У таблиці показані результати обчислювального експерименту за таких умов: довжина аналізованих послідовностей *N = 10000*, довжина гусениці *M = 1000*, кількість ітерацій змінилося *z=8, z=64*.

Як видно з таблиці, для вхідних послідовностей (1) рівень основних компонентів I перевищує значення для показників досліджуваних вихідних послідовностей (2–5) більш ніж на 50 %. Порівняльний аналіз показує, що для вихідних послідовностей розробленого алгоритму шифрування з використанням динамічного хаосу рівень основних компонентів *I* практично збігається з продуктивністю алгоритмів шифрування стандартного та блочного шифрування в режимі БСМ. Фазові діаграми пар власних векторів з числами 1000 і 999, 1000 і 998 для вхідних послідовностей, вихідних послідовностей розробленого алгоритму (кількість ітерацій *z = 8*) та

ISSN 2663 - 4023

розробленого алгоритму наведені на рис. 3.

Для фазових діаграм вихідних послідовностей розробленого алгоритму шифрування (рис. 3, д, е) характерно наявність “шумних” фігур, на відміну від діаграм простого тексту (рис. 3 , а, б, в, г).

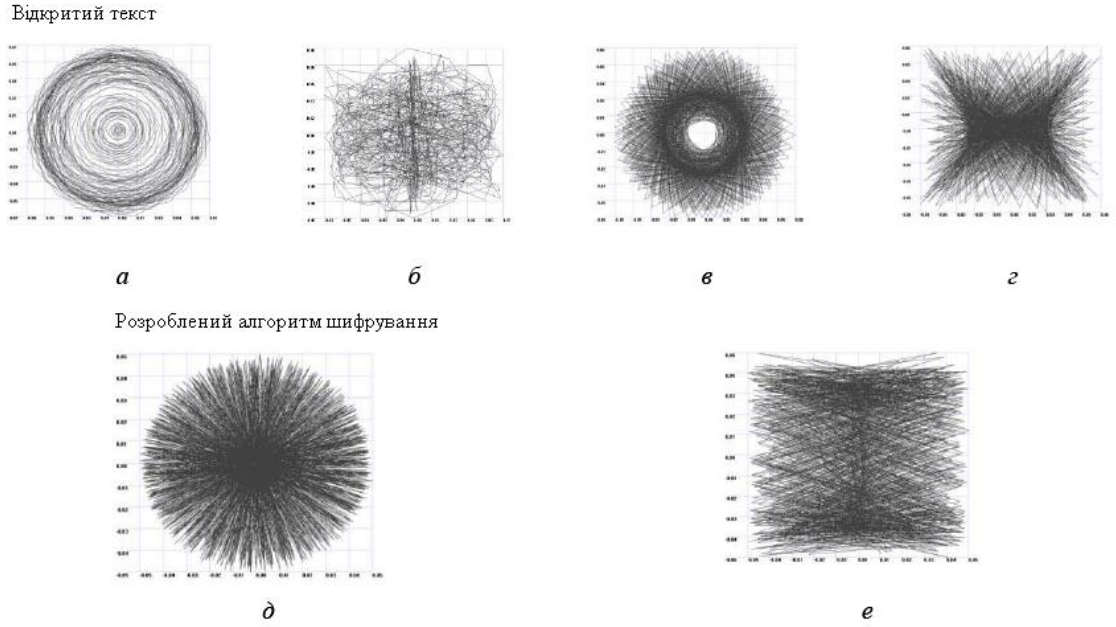

Рис. 3. Фазові діаграми пар власних векторів з числами 1000 і 999, 1000 і 998: для вхідних послідовностей (а) і (б); вихідні послідовності розробленого алгоритму з використанням динамічного хаосу з кількістю ітерацій z = 8 (в) і (г), вихідні послідовності розробленого алгоритму (д) і (е) при аналізі послідовностей методом сингулярного спектрального аналізу

Таким чином, використання методу сингулярного спектрального аналізу, застосованого до вхідних послідовностей, а також для виведення послідовностей алгоритму шифрування з використанням динамічного хаосу. В БСМ ми можемо встановити якісні критерії у вигляді фазові діаграми, а також кількісний критерій рівня основних компонентів для визначення випадковості послідовностей алгоритмів шифрування.

6. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

В результаті досліджень було встановлено, що для управління випадковістю вихідних послідовностей алгоритмів шифрування за допомогою хаотичних сигналів можна використовувати метод затримки координат та метод сингулярного спектрального аналізу. Показано, що такі параметри, як розмір кореляції, ентропія методом Колмогорова затримки координат, можуть використовуватися як критерії для визначення ступеня випадковості вихідних послідовностей та фазові портрети для візуального аналізу з використанням алгоритму шифрування з використанням хаотичних сигналів. Параметр рівня основних компонентів методу сингулярного спектрального аналізу та фазових діаграм рекомендується використовувати як засіб визначення випадковості вихідних послідовностей алгоритму шифрування з використанням хаотичних сигналів.

Порівняльний аналіз параметрів методів запізнілого координатного та

сингулярного спектрального аналізу вхідних та вихідних послідовностей алгоритмів шифрування з використанням хаотичних сигналів, блочного та стандартного симетричного шифрування показав значні відмінності в параметрах вхідних та вихідних послідовностей; практичний збіг за рівнем основних компонентів в роботі захвату блоку шифрів; вдосконалення параметрів кореляційного виміру та ентропії Колмогорова для алгоритму шифрування з використанням динамічного хаосу, який, в цілому, може послужити основою для рекомендацій щодо використання цих методів при розробці вимог до інформаційної безпеки.

В результаті дослідження було розроблено метод оцінки показників навантаження вузлів. Перевага полягає в тому, що в БСМ існує велика ймовірність не тільки мережевих нападів, але й атак, спрямованих на порушення фізичної активності вузла.

Визначений поріг помилок, коли кількість шкідливих вузлів становить менше 70%, дозволяє визначати вузли та блокувати їх досить точно. Коли кількість шкідливих вузлів становить понад 70%, точність виявлення зменшується, і, як правило, в реальній ситуації, коли вузли мережі розташовані на досить великій відстані один від одного і їх кількість вимірюється тисячами вузлів, для зловмисника досить складно перевищувати поріг навіть на 50% шкідливих вузлів у мережі. У той же час, розподілені та централізовані системи обчислення довіри не в змозі протидіяти атак типу «Сивілли» та «Відмова в обслуговуванні», оскільки вони аналізують лише успішні або невдалі хост-події, і при здійсненні цих типів атак зловмисник не видає невдалих.

Тому наше наступне дослідження зосередиться на розробці методів ранньої діагностики та протидії атакам «Відмова в обслуговуванні», зокрема, атакам типу «Сивілли».

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] I. Artyshchuk, O. Belej and N. Nestor, "Designing a Generator of Random Electronic Message Based on Chaotic Algorithm," *2019 IEEE 15th International Conference on the Experience of Designing and Application of CAD Systems (CADSM)*, Polyana, Ukraine, 2019, pp. 1-5, doi: 10.1109/CADSM.2019.8779306.

[2] O. Belej, I. Artyshchuk, W. Sitek, “The Controlling of Transmission of Chaotic Signals in Communication Systems Based on Dynamic Models,” in: *CEUR Workshop Proceedings*, vol. 2353, pp. 1-15, 2019.

[3] K. Govindan and P. Mohapatra, "Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey," in *IEEE Communications Surveys & Tutorials*, vol. 14, no. 2, pp. 279-298, Second Quarter 2012, doi: 10.1109/SURV.2011.042711.00083.

[4] V. Deepali, H. Manas, Ch. Shringarica, “Exponential Trust-Based Mechanism to Detect Black Hole Attack in Wireless Sensor Network,” in: *International Journal of Soft Computing and Engineering (IJSCE) Proceedings*, p. 14-16, 2014.

[5] M. Momani, “Bayesian Fusion Algorithm for Inferring Trust in Wireless Sensor,” *Networks. Journal of Networks*, vol. 5 (7), pp. 815-822, 2010, doi**:** 10.4304/jnw.5.7.815-822.

[6] E. Schoch, M. Feiri, F. Kargl, M. Weber, “Simulation of Ad Hoc Networks: ns–2 compared to JiST/SWANS, SIMUTools,” in: *proceedings of the 1st International Conference on Simulation Tools and Techniques for Communications*, Networks and Systems & Workshops, Marseille, France, 2008. doi**:** 10.1145/1416222.1416263.

[7] D. Koll, J. Li, J. Stein and X. Fu, "On the state of OSN-based Sybil defenses," *2014 IFIP Networking Conference*, Trondheim, 2014, pp. 1-9, doi: 10.1109/IFIPNetworking.2014.6857128.

[8] H. Liu, Chao Ma and R. Walshe, "An adaptive membership protocol against sybil attack in unstructured P2P networks," *IET International Conference on Information and Communications Technologies (IETICT 2013)*, Beijing, China, 2013, pp. 29-34, doi: 10.1049/cp.2013.0031.

[9] O. Belej, T. Lohutova and M. Banaś, "Algorithm for Image Transfer Using Dynamic Chaos," *2019 IEEE 15th International Conference on the Experience of Designing and Application of CAD Systems*

(CADSM), Polyana, Ukraine, 2019, pp. 1-5, doi: 10.1109/CADSM.2019.8779285.

[10] R. R. Devi and M. Hemalatha, "Sybil node identification algorithm using connectivity threshold for secured community mining in social network," *2013 IEEE International Conference on Computational Intelligence and Computing Research*, Enathi, 2013, pp. 1-4, doi: 10.1109/ICCIC.2013.6724148.

[11] T. Silawan and C. Aswakul, "SybilComm: Sybil community detection using persuading function in IoT system," *2016 International Conference on Electronics, Information, and Communications (ICEIC)*, Da Nang, 2016, pp. 1-4, doi: 10.1109/ELINFOCOM.2016.7563012.

[12] L. Sun, H. Ma, D. Fang, J. Niu, W. Wang, "Advances in Wireless Sensor Networks," in: *Revised Selected Papers of the 8th China Conference,* Xi'an, China, 2015, doi**:** 10.1177/1550147718763220.

[13] S. Guo, K. Liu, C. Chen, H. Huang, "Wireless Sensor Networks," in: *Proceedings of the 13th China Conference on Wireless Sensor Networks,* Chongqing, China, , 2019.

[14] F. A. Kadhim, G. H. A. Majeed and R. S. Ali, "Proposal new s-box depending on DNA computing and mathematical operations," *2016 Al-Sadeq International Conference on Multidisciplinary in IT and Communication Science and Applications (AIC-MITCSA)*, Baghdad, 2016, pp. 1-6, doi: 10.1109/AIC-MITCSA.2016.7759926.

[15] Y. Liu, J. Tang, T. Xie, "Cryptanalyzing a RGB image encryption algorithm based on DNA encoding and chaos map," *Optics & Laser Technology*, *60*, pp.111-115, 2014, doi: 10.1016/j.optlastec.2014.01.015.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (9), 2020
ISSN 2663 - 4023

Oleksandr Belei
Ph.D. in Economics, Associate professor, Associate professor of Department of Computer-Aided Design
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: 0000-0003-4150-7425
Oleksandr.I.Belei@)lpnu.ua

Oksana Svatiuk
Ph.D. in Economics, Associate professor, Associate professor of Department of Management and Socio-Humanities Department
Lviv Educational and Scientific Institute School of Business Administration «Banking University», Lviv, Ukraine
ORCID: 0000-0003-0099-2532
svatuk@gmail.com

DEVELOPMENT OF ALOGORITHM FOR ENCRYPTION OF MESSAGES IN THE WIRELESS SENSOR NETWORK

Abstract. An analysis of the physical characteristics of the node, which can be attacked by an attacker. A method of detecting a damaged node with a violation of the physical characteristics of the network node, which is based on the use of probability functions, calculation of the confidence interval and the probability of deviation of current values from the confidence interval. Its novelty lies in the possibility of detecting a damaged node by estimating the current value of the function in the confidence interval, without comparing the distribution function of the current node with the reference distribution. The analysis of physical parameters of network nodes for detection of the malefactor in contrast to existing systems of detection of attacks which allow to carry out only the analysis of network traffic is carried out. Based on the developed algorithm by modeling the transmission of chaotic signals in a wireless sensor network, the effectiveness of attack detection is determined through the analysis of residual energy and node congestion parameters, expanding the range of attacks that the network is able to counteract compared to system analogues.
During the simulation of the behavior of the wireless sensor network, it was determined that the data transmission processes are chaotic. Therefore, to enhance the security of data transmission in a chaotic mode, we have proposed an encryption algorithm using dynamic chaos, coordinate delay methods and singular spectral analysis. A comparative analysis of the parameters of the input and output sequences of the developed encryption algorithm based on dynamic chaos with standard data encryption algorithms is performed. It is established that the encryption parameters that are characteristic of the original sequences of the encryption algorithm using dynamic chaos are not worse than the encryption parameters obtained for the source sequences of standard encryption algorithms. Estimation of node load by means of threshold analysis of their current values in the confidence interval is used to detect network deviations during a cyberattack. The developed algorithm allows to diagnose attacks such as "Denial of Service" and "Sibyl" at the beginning of their appearance and to determine possible ways to avoid them.

Keywords: attack; attack detection system; security; wireless sensor networks; encryption algorithm; information; control; chaotic reflection; dynamic chaos.

REFERENCES (TRANSLATED AND TRANSLITERATED)

[1] I. Artyshchuk, O. Belej and N. Nestor, "Designing a Generator of Random Electronic Message Based on Chaotic Algorithm," 2019 IEEE 15th International Conference on the Experience of Designing and Application of CAD Systems (CADSM), Polyana, Ukraine, 2019, pp. 1-5, doi: 10.1109/CADSM.2019.8779306.

[2] O. Belej, I. Artyshchuk, W. Sitek, “The Controlling of Transmission of Chaotic Signals in Communication Systems Based on Dynamic Models,” in: CEUR Workshop Proceedings, vol. 2353, pp. 1-15, 2019.

[3] K. Govindan and P. Mohapatra, "Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey," in IEEE Communications Surveys & Tutorials, vol. 14, no. 2, pp. 279-298, Second Quarter 2012, doi: 10.1109/SURV.2011.042711.00083.

[4] V. Deepali, H. Manas, Ch. Shringarica, “Exponential Trust-Based Mechanism to Detect Black Hole Attack in Wireless Sensor Network,” in: International Journal of Soft Computing and Engineering (IJSCE) Proceedings, p. 14-16, 2014.

[5] M. Momani, “Bayesian Fusion Algorithm for Inferring Trust in Wireless Sensor,” Networks. Journal of Networks, vol. 5 (7), pp. 815-822, 2010, doi: 10.4304/jnw.5.7.815-822.

[6] E. Schoch, M. Feiri, F. Kargl, M. Weber, “Simulation of Ad Hoc Networks: ns–2 compared to JiST/SWANS, SIMUTools,” in: proceedings of the 1st International Conference on Simulation Tools and Techniques for Communications, Networks and Systems & Workshops, Marseille, France, 2008. doi: 10.1145/1416222.1416263.

[7] D. Koll, J. Li, J. Stein and X. Fu, "On the state of OSN-based Sybil defenses," 2014 IFIP Networking Conference, Trondheim, 2014, pp. 1-9, doi: 10.1109/IFIPNetworking.2014.6857128.

[8] H. Liu, Chao Ma and R. Walshe, "An adaptive membership protocol against sybil attack in unstructured P2P networks," IET International Conference on Information and Communications Technologies (IETICT 2013), Beijing, China, 2013, pp. 29-34, doi: 10.1049/cp.2013.0031.

[9] O. Belej, T. Lohutova and M. Banaś, "Algorithm for Image Transfer Using Dynamic Chaos," 2019 IEEE 15th International Conference on the Experience of Designing and Application of CAD Systems (CADSM), Polyana, Ukraine, 2019, pp. 1-5, doi: 10.1109/CADSM.2019.8779285.

[10] R. R. Devi and M. Hemalatha, "Sybil node identification algorithm using connectivity threshold for secured community mining in social network," 2013 IEEE International Conference on Computational Intelligence and Computing Research, Enathi, 2013, pp. 1-4, doi: 10.1109/ICCIC.2013.6724148.

[11] T. Silawan and C. Aswakul, "SybilComm: Sybil community detection using persuading function in IoT system," 2016 International Conference on Electronics, Information, and Communications (ICEIC), Da Nang, 2016, pp. 1-4, doi: 10.1109/ELINFOCOM.2016.7563012.

[12] L. Sun, H. Ma, D. Fang, J. Niu, W. Wang, “Advances in Wireless Sensor Networks,” in: Revised Selected Papers of the 8th China Conference, Xi'an, China, 2015, doi: 10.1177/1550147718763220.

[13] S. Guo, K. Liu, C. Chen, H. Huang, “Wireless Sensor Networks,” in: Proceedings of the 13th China Conference on Wireless Sensor Networks, Chongqing, China, , 2019.

[14] F. A. Kadhim, G. H. A. Majeed and R. S. Ali, "Proposal new s-box depending on DNA computing and mathematical operations," 2016 Al-Sadeq International Conference on Multidisciplinary in IT and Communication Science and Applications (AIC-MITCSA), Baghdad, 2016, pp. 1-6, doi: 10.1109/AIC-MITCSA.2016.7759926.

[15] Y. Liu, J. Tang, T. Xie, "Cryptanalyzing a RGB image encryption algorithm based on DNA encoding and chaos map, " Optics & Laser Technology, 60, pp.111-115, 2014, doi: 10.1016/j.optlastec.2014.01.015.