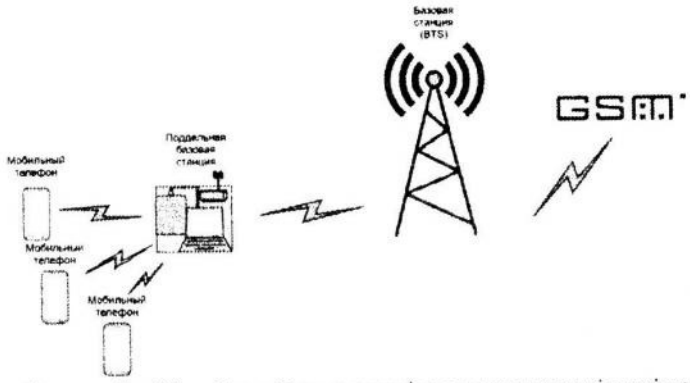

Рисунок 2 – Підроблена базова станція на уразливому ділянці мережі

На даний момент деталі алгоритму A5 / 1 стали відомі. Даний алгоритм не може вважатися безпечним для кінцевого користувача, так як може бути легко розшифрований будь-яким сучасним комп'ютером [2, 1].

За допомогою даної уразливості зловмисник може отримати доступ до: прослуховування дзвінків і sms-повідомлень абонентів GSM мережі; здійснення дзвінків і відправлення повідомлень від імені будь-якого абонента в радіусі дії підробленої базової станції.

Дана уразливість ставить під загрозу безпеку і анонімність користувачів GSM мереж, здійснення банківських операцій за допомогою мобільного телефону, двухфакторну аутентифікацію зокрема. Напрямком подальшої роботи ставиться дослідження уразливості з перехоплення трафіку шляхом моделювання базової станції на базі програмного означенної радіосистеми (SDR) і розробка алгоритму визначення довіреності до базової станції на моменті з'єднання, а також пошук і аналіз інших можливих варіантів розв'язання вразливості.

Література:

1. Patrik Ekdahl and Thomas Johansson. : Information Theory, 2001. Proceedings. IEEE International Symposium on., «Another Attack on A5 / 1» pp 284-289.

2. Marcin Olawski. «Security in the GSM network».

3. Anderson, Ross A5 - The GSM Encryption Algorithm, 1994.

4. Redl, Siegmund M .; Weber, Matthias K .; Oliphant, Malcolm W (February 1995). An Introduction to GSM. Artech House. ISBN 978-0-89006-785-7

УДК 004.045: 621.396.96

Обод А.І., Штих І.А.
ХНУРЕ
iryna.svyd@nure.ua
Науковий керівник – к.т.н., доц. Свид І.В.

СУМІСНА ОПТИМІЗАЦІЯ ОБРОБКИ ДАНИХ ОГЛЯДОВИХ СИСТЕМ СПОСТЕРЕЖЕННЯ ПОВІТРЯНОГО ПРОСТОРУ

Анотація. *Наводиться аналіз відомих методів поєднання даних оглядових систем спостереження повітряного простору на етапі третинної обробки та пропонується здійснювати поєднання даних в мережі систем спостереження на етапі сигнальних даних чи на етапі первинної обробки даних. Показано, що реалізація централізованої обробки сигнальних рішень та первинної обробки даних дозволяє здійснити сумісну оптимізацію обробки даних та підвищити показники якості інформаційного забезпечення користувачів системи контролю повітряного простору.*

Підвищення якості інформаційного забезпечення (ІЗ) користувачів системи контролю повітряного простору (ПП) неможливо без використання інформаційних технологій (ІТ) у процесі отримання, збору, обробки, зберігання й розповсюдження даних систем спостереження (СС) [1]. Завдання обробки даних від декількох джерел завжди залишається актуальною, оскільки дозволяє знизити похибки окремих вимірів і підвищити стійкість і достовірність спостережень. Мережевий принцип організації інформаційних систем (ІС) показав свої переваги при рішенні широкого кола завдань. ІЗ споживачів системи контролю повітряного простору (КПП) побудовано за мережевим принципом. Дійсно, третинна обробка інформації (ТОІ) передбачає об'єднання трас ПО, отриманих різними СС. Отже, у цьому випадку, СС ПП утворювали некогерентну несинхронну мережу СС ПП.

Третинна обробки даних СС це поєднання даних різних СС за однойменними ПО з метою поліпшення характеристик спостереження: виявлення; вимірювання координат і параметрів руху ПО. На цьому етапі обробки вирішується задача обробки даних СС ПП, що припускає виконання наступних функціонально закінчених операцій: приведення позначок місця розташування ПО до єдиної системи координат та до єдиного часу відліку; ототожнення (ідентифікація) траєкторій, отриманих від декількох джерел по тому самому ПО; обчислення параметрів об'єднаних (усереднених) траєкторій. Так як, звичайний час екстраполяції невеликий, тому застосовується лінійна екстраполяція.

Поєднання даних за однойменними ПО при цьому може здійснюватися на етапах: обробки сигнальних даних; первинної обробки інформації (ПОІ); вторинної обробки інформації (ВОІ).

У більшості відомих системах обробки даних ТОІ здійснюється на етапі об'єднання трас ПО. Дійсно, в обчислювальному відношенні переважно спочатку прокладати траєкторії ПО незалежно за даними кожного джерела, а на наступному етапі – етапі третинної обробки – використовувати їх для підвищення якості даних, що надається особі яка приймає рішення. Траєкторії кожного ПО, що спостерігається з різних ракурсів кількома СС, при узагальненні дозволяють не тільки точніше визначати і передбачати місце розташування об'єкта, а й оперативно відслідковувати поточні значення похибки кожного джерела вимірювань.

Задачі ТОІ на рівні трас вирішуються двома основними методами [2]: мозаїчна обробка; мультирадарна обробка.

При мозаїчній обробці кожній СС виділяється своя зона огляду, що не перетинається із зонами огляду інших СС. Для формування єдиного формуляра ПО використовується інформація тільки від однієї СС.

До недоліків даного методу відноситься задача супроводу траєкторій ПО при перетинанні границь зон огляду, а також не використання переваги перекриття зон виявлення сусідніх СС.

При мультирадарній обробці використовуються всі доступні СС для формування єдиного формуляра ПО.

Мультирадарна обробка повинна забезпечити стабільний супровід ПО і формування картини повітряної обстановки шляхом аналізу інформації, що надходить від декількох ІС. Як правило, ІС володіють різними характеристиками, так що в конкретних умовах може бути більш ефективний той чи інший радар. За інших рівних умов на великих відстанях буде ефективний радар, що володіє більшою потужністю. В областях великої щільності руху і підвищеної маневреності ПО необхідний радар з невеликим періодом огляду. Крім того, ефективність радара залежить від його розташування щодо навколишніх завад. Будинки, природний рельєф та інші елементи навколишньої місцевості можуть екранувати, відображати або перевідбивати випромінювання, в результаті чого в певних областях з'являються численні хибні відмітки (або пропадають справжні). Тому для отримання найбільш інформативної картини бажано використовувати інформацію від декількох СС, причому враховувати особливості цих радарів та їх можливості стосовно конкретних ділянок

зони дії системи КПП. Результатом мультирадарної обробки є мультирадарні траєкторії, розраховані з реальних за спеціальними алгоритмами. Залежно від обставин при формуванні мультирадарної траєкторії може використовуватися траєкторія тільки від одного радара або відразу від декількох радарів, вимірювання яких усереднюється з різними ваговими коефіцієнтами.

Задача ототожнення позначок вирішується у два етапи.

На першому етапі позначки групуються за їх потраплянням у строб припустимих відхилень, що визначається погрішностями оцінки координат. Потім проводиться ототожнення позначок та їх об'єднання.

Якщо в строб попадають позначки від багатьох СС, що належать декільком ПО, то задача групування вирішується в такий спосіб:

- складаються всі можливі варіанти групування;
- обчислюються різниці координат у кожній групі;
- обчислюється кореляційна матриця помилок $\vec{C}_i^{-1}$, як сума кореляційних матриць помилок координат, що групуються;
- для кожного варіанта групування складається квадратична форма $\vec{Q}_i = \vec{Z}_i^T \vec{C}_i^{-1} \vec{Z}_i$ та приймається варіант групування, для якого значення $\vec{Q}_i$, мінімальне.

Нехай, наприклад, у строб припустимих відхилень потрапили дві позначки з векторами параметрів $\vec{W}_{1,1}$ і $\vec{W}_{1,2}$ отримані від першої СС, і одна позначака з векторами параметрів $\vec{W}_2$ від другої СС. Кореляційні матриці помилок відповідно рівні $\vec{C}_1^{-1}$ і $\vec{C}_2^{-1}$.

Можливі два варіанти групування:

$$1)\ \vec{Z}_1 = \left\| \begin{matrix} \vec{Q}_{1,2} \to \vec{Q}_2 \\ \vec{Q}_{1,2} \end{matrix} \right\|, \quad 2)\ \vec{Z}_2 = \left\| \begin{matrix} \vec{Q}_{1,1} \\ \vec{Q}_{1,2} \to \vec{Q}_2 \end{matrix} \right\|.$$

Кореляційні матриці помилок для першого й другого варіантів групування однакові й визначаються як

$$\vec{C}_0^{-1} = \vec{C}_1^{-1} + \vec{C}_2^{-1}$$

Конкуруючі квадратичні форми:

$$\vec{Q}_1 = \vec{Z}_1^T \vec{C}_0^{-1} \vec{Z}_1 = \vec{Z}_1^T \vec{C}_0^{-1} \vec{Z}_1; \vec{Q}_2 = \vec{Z}_2^T \vec{C}_0^{-1} \vec{Z}_2.$$

Якщо $\vec{Q}_1 < \vec{Q}_2$, обирається перший варіант і навпаки.

Для m СС і n ПО число варіантів групування можна визначити як

$$k = (m-1)!n!.$$

Із цієї формули видно, що воно різко зростає зі збільшенням m та n.

Задача формування одиничних вимірів вирішується усередненням координат ПО з вагами, обернено пропорційними дисперсіям помилок одиничних вимірів кожної СС.

Якщо сигнальні або первинні дані, отримані в окремих пунктах спостереження, передати і зосередити в деякому центрі обробки, то це об'єднання дозволить використовувати в інтересах поліпшення характеристик спостереження не тільки додаткову енергетику, але і кореляційні зв'язки прийнятих сигналів, а також просторову подобу первинних даних про один об'єкт від різних джерел, обумовлене наявністю ПО в певній точці простору.

Основою об'єднання сигнальних даних є наявність розсіяного або випроміненого ПО сигналу в просторі, що набагато перевершує за розмірами обмежений простір однопозиційного спостереження.

Остання задача третинної обробки вирішується методами, розглянутими при вторинній обробці.

Проведемо оцінку результатів поєднання сигнальних даних в мережі СС ПП з трьома пунктами прийому. На кожному пункті прийому здійснюється виявлення сигналів, рішення про яке передається на пункт сумісної обробки на якому здійснюється:

- поєднання рішень про виявлення сигналів (критерії 1/3;2/3;3/3);

- виявлення ПО;
- виявлення зав'язки траси ПО.

Будемо вважати, що виявлення ПО здійснюється за правилом $K/N = 12/25$, а зав'язка траси ПО - $l/m = 2/3$.

Характеристики виявлення траси ПО при поєднанні на рівні виявлення сигналів наведені на рис. 1. Ймовірність хибної тривоги дорівнює $F = 10^{-3}$.

Проведемо оцінку результатів поєднання виявлених ПО в мережи СС ПП з трьома пунктами прийому. На кожному пункті прийому здійснюється виявлення сигналів та виявлення ПО рішення про яке передається на пункт сумісної обробки на котрій здійснюється:

- поєднання рішень про виявлення ПО (критерії 1/3;2/3;3/3);
- виявлення зав'язки траси ПО.

Характеристики виявлення траси ПО при поєднанні на рівні виявлення ПО наведені на рис. 2.

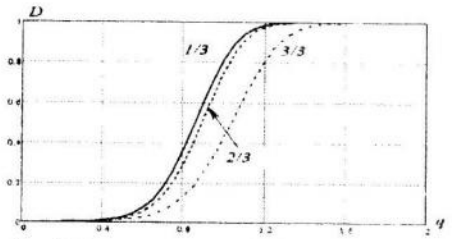

Рис. 1. Поєднання даних на рівні сигнальних рішень

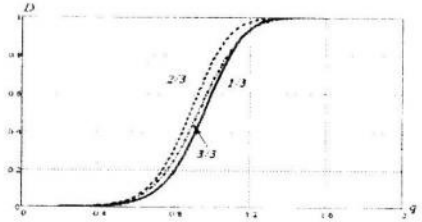

Рис. 2. Поєднання даних на рівні ПОІ

Наведені розрахунки показують, що поєднання рішень про однойменні ПО більш доцільно здійснювати на рівні виявлення ПО для більш жорстких логік обробки і навпаки.

Висновки

Отримані показники якості інформаційного забезпечення користувачів системи КПП показали доцільність використання сумісної обробки даних СС ПП при широкому застосуванні ІТ на етапах поєднання сигнальних рішень та первинної обробки даних.

Література:

1. Фарина А. Цифровая обработка радиолокационной информации / А. Фарина, Ф. Студер. – М.: Радио и связь, 1993. – 319 с.

2. Моделювання аеронавігаційних систем. Оброблення інформації та прийняття рішень у системі керування повітряним рухом: навч. посіб./ В.М. Васильєв, В.П. Харченко. – К.: НАУ. – 180 с.