

В. М. Ткачов¹, А. А. Коваленко¹, Г. А. Кучук², Я. С. Ні¹

¹ Харківський національний університет радіоелектроніки, Харків, Україна

² Національний технічний університет «Харківський політехнічний інститут», Харків, Україна

МЕТОД ЗАБЕЗПЕЧЕННЯ ЖИВУЧОСТІ ВИСОКОМОБІЛЬНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ

Анотація. В статті розглянуто особливості функціонування рухомих комп'ютерних мереж на базі малогабаритних літальних апаратів (високомобільні комп'ютерні мережі). Показано, що такі мережі, на відміну від стаціонарних або маломобільних, відрізняються низьким рівнем живучості при локальних пошкодженнях їх вузлів. **Метою** статті є розробка методу забезпечення живучості високомобільних комп'ютерних мереж в умовах деструктивного зовнішнього впливу, що призводить до локальної руйнації вузлів мережі або зв'язків між ними, з використанням методики оцінки живучості на всіх етапах функціонування мережі, шляхом зміни основної функції для реалізації всіх доступних стратегій функціонування мережі при визначенні критичних значень цілісності мережі та здатності її виконувати хоча б одну із доступних функцій. Отримані **результати** дозволяють: продовжити розвиток методики оцінки живучості комп'ютерних мереж в умовах деструктивного зовнішнього впливу; застосовувати розроблений метод для визначення критичних порогів живучості мережі відносно основної функції та зміни основної функції, відповідно до стратегій функціонування високомобільної мережі. Дослідження дозволяють зробити **висновки**, що запропонований метод може бути використаний на етапах проектування високомобільних комп'ютерних мереж, які характеризуються підвищеною живучістю та здатні функціонувати в умовах множинних локальних пошкоджень без катастрофічних руйнівних наслідків для структури мережі.

Ключові слова: живучість; комп'ютерна мережа; оцінка стану; реконфігурація; руйнівний вплив.

Вступ

Постановка проблеми. Стрімкий розвиток технологічної бази та доступність малогабаритних роботизованих платформ дозволяють використовувати відомі ройові алгоритми для створення рухомих систем реєстрації, обміну, збереження даних, до складу яких входить група вузлів, які взаємодіють між собою за єдиною стратегією [1, 2]. Одним із класів таких рухомих мереж є безпроводні літаючі комп'ютерні мережі (FANET), також відомі як високомобільні комп'ютерні мережі (ВМКМ) [3]. Основне призначення таких мереж – організація передачі даних в умовах швидкого розгортання мережі передачі даних на деякій площі, збору (реєстрації) інформації від стаціонарних вузлів – центрів полігрових мереж, розгорнутих на місцевості тощо. Найбільш уживаними сферами застосування ВМКМ є агропромисловий комплекс, метеорологія, служби з надзвичайних ситуацій, військово-оборонна сфера тощо [4, 5].

Одним з важливих питань, які виникають під час експлуатації такого класу мереж – забезпечення надійного функціонування протягом заданого часу, тобто виконання основної функції з можливістю перебудови стратегії функціонування при зміні змісту основної функції. Тобто в рамках стратегії ВМКМ може бути як одна, так і декілька функцій, які виконує мережа. Одним із способів досягнення цієї мети є забезпечення живучості ВМКМ [6]. Деструктивними чинниками є зовнішній вплив на елементи (вузли) ВМКМ (електромагнітне ураження, температурні чинники, інші види деструктивного впливу), внутрішні чинники, спричинені наслідками деструктивного впливу та руйнації вузлів або зв'язків між ними у структурі ВМКМ [7, 8]. Іншими словами, забезпечення живучості як окремо взятого елемента ВМКМ, так і мережі в цілому – є актуальною задачею при виконанні мережею функцій в рамках стратегії її функ-

ціонування. Досягнення результату пов'язано з такими задачами як моніторинг та оцінка стану ВМКМ, заходів щодо підвищення живучості ВМКМ в екстремальних умовах або дії деструктивних чинників

Живучість ВМКМ може забезпечуватися шляхом реалізації ряду технічних та організаційних заходів. До технічних заходів відносяться – удосконалення топології ВМКМ, використання підсистем моніторингу стану вузлів та захисту ВМКМ від зовнішнього деструктивного впливу, використання процедур автоматичної реконфігурації мережі. До організаційних заходів можна віднести удосконалення системи керування ВМКМ в нормальному та екстремальних режимах, наявність резервних стратегій щодо ліквідації наслідків відмов ВМКМ в залежності від руйнації мережі та перспектив виконання основної функції.

Таким чином, актуальною є науково-прикладна проблема забезпечення живучості високомобільної комп'ютерної мережі в умовах деструктивного впливу на її елементи.

Аналіз останніх досліджень і публікацій. У роботі [9] авторами представлені основні підходи для проведення кількісної оцінки живучості складних технічних систем, у тому числі, заснованих на оцінці співвідношення прямих та непрямих ризиків, співвідношення ймовірності катастрофічних відмов для систем різного рівня пошкодження. Авторами приведено приклад оцінки живучості технічних систем та обґрунтовано необхідність підвищення живучості для забезпечення безпеки складних технічних систем при екстремальних впливах. Однак, описаний підхід не може бути застосованим для мультифункціональних систем та мереж, коли основна функція може бути змінена в залежності від ступеню пошкодження системи або елементів. В такому випадку необхідне створення нової моделі та розрахунок її параметрів, на що не завжди є час. Тобто актуальність отриманих

розрахунків може бути втрачена у разі деградації системи та швидкої зміни її основної функції та визначення індексу живучості в залежності від нової функції. Іншими словами, мережа, як частина мегасистеми, яка в свою чергу має виконувати функції згідно глобальної стратегії, може мати наперед заданий набір функціональних задач, які можуть змінюватися в залежності від ступеню пошкодження системи або її елементів в рамках околу допустимих пошкоджень для виконання основної функції до досягнення нею критичного порогу.

У роботі [10] авторами представлено імітаційну модель і результати моделювання процесу функціонування транспортної мережі зв'язку спеціального призначення з використанням математичного апарату дискретних ланцюгів Маркова в умовах дестабілізуючих інформаційних впливів. На основі одержаних ймовірно-часових характеристик процесу функціонування транспортної мережі зв'язку спеціального призначення, які становлять основу для дослідження даного процесу при різних варіантах дестабілізуючого інформаційного впливу та відновлення об'єктів транспортної мережі зв'язку спеціального призначення, авторами визначено оцінки коефіцієнта оперативної готовності мережі в різних умовах обстановки. Однак, цей підхід не в повній мірі може описати можливу сценарну траєкторію функціонування вузлів системи, які, внаслідок катастрофічного руйнування мережі, продовжують функціонувати без зв'язків між собою.

Метою статті є розробка методу забезпечення живучості ВМКМ в умовах деструктивного зовнішнього впливу, що призводить до локальної руйнації вузлів або зв'язків між ними в ВМКМ та оцінка показника живучості такої мережі.

Основна частина

Оцінка живучості високомобільної комп'ютерної мережі. На першому етапі вирішення поставленої задачі є доцільним проведення оцінки живучості ВМКМ з метою визначення напрямів заходів, які можуть підвищити показники живучості мережі.

Функціонування більшості складних технічних систем визначається співвідношенням навантаження та несучої здатності [9]. Відповідно живучістю ВМКМ є здатність мережі пропускати та обробляти потоки даних, які перерозподіляються в мережі після того, як, в результаті екстремального впливу, пошкоджуються окремі її елементи (вузли або канали передачі даних).

Нехай ВМКМ задана у вигляді такого кортежу:

$$S = \langle s_1, s_2, \dots, s_n \rangle, \quad (1)$$

де s – елементи (вузли) ВМКМ, які виконують функції, відповідно до стратегії ВМКМ.

$$s = \langle f_1, f_2, \dots, f_k \rangle, \quad (2)$$

де f – функції, які виконує вузол ВМКМ: реєстрація, обробка інформації, тимчасове зберігання даних, їх передача. Функції можуть змінюватися в залежності від задачі яка ставиться вузлу.

Сутність відмови вузла ВМКМ полягає в тому, що він перестає виконувати одну або більше функцій, яка визначена для виконання у певний проміжок часу. Якщо вузол може виконувати інші функції (визначається шляхом періодичної самодіагностики), які в конкретний проміжок часу не затребувані, то вузол, де-факто, перебуває у режимі очікування.

Таким чином, відповідно до стратегії функціонування ВМКМ, відмова вузла ініціює додаткові взаємодії між іншими вузлами мережі, наприклад, перебудова топології або зміна схеми маршрутизації потоків даних. В такому випадку критерієм живучості ВМКМ можна назвати її здатність перерозподіляти потоки даних та продовжувати виконання заданих їй функцій після того, як окремі її вузли виходять з ладу або не можуть виконувати затребувану від них функцію.

Існує ряд відомих методів оцінки живучості технічних систем [6-9], але специфіка їх побудови визначається класом технічних систем. Оскільки реальні вузли і канали передачі даних ВМКМ мають обмежену пропускну здатність при побудові більш досконалих моделей мереж, необхідно враховувати потоки даних, які циркулюють в ВМКМ. У разі пошкодження вузла або зниження пропускну здатності каналу передачі даних, потік, який проходить через сегмент ВМКМ, перенаправляється альтернативними шляхами. Це може призвести до переважання інших вузлів або каналів, що може призвести до більш швидкої їх деградації. Таким чином, будь-яке локальне пошкодження ВМКМ може привести до подальшого переважання інших вузлів мережі та їх подальшою відмовою. Подібні каскадні процеси можуть стати причиною масштабної руйнації структури ВМКМ, навіть якщо вузли можуть виконувати інші функції, які, однак не затребувані в рамках поточної стратегії функціонування ВМКМ. Тобто, ВМКМ з малою живучістю втрачають здатність виконувати основну функцію стрімко та катастрофічно, що може призвести до каскадних порушень в роботі більш високорівневих систем, до складу яких вони входять, або які обслуговують.

Таким чином, важливо оцінити, при яких значеннях локальних пошкоджень ВМКМ може відбутися катастрофічне порушення в роботі мережі. Але живучість ВМКМ неможливо оцінити, незалежно від діючих в мережі систем моніторингу і керування, кваліфікації осіб, що приймають рішення, адекватності технічних регламентів та інструкцій, так як всі ці фактори впливають на можливість обмежувати локальні наслідки локальних пошкоджень і запобігти катастрофічному руйнуванню ВМКМ, якщо мережі були заподіяні локальні пошкодження. Руйнівний вплив на ВМКМ, який наносить локальні пошкодження мережі, можуть мати різноманітну природу. При цьому аналіз живучості не повинен залежати від ініціюючих подій.

Одним із підходів до оцінки стану мережі під час деструктивного впливу є побудова сценарних дерев [11]. Враховуючи ступінь автономності елементів структури, доцільним є використання багатозарового дерева (рис. 1), на якому відображено гіллясту структуру. Структура показує, що існують ймовір-

ності, які можуть призвести до повної непрацездатності вузла ВМКМ або обмеження виконання ним деяких функцій. При досягненні критичних значень за кількістю пошкоджених вузлів, ВМКМ може приймати рішення щодо зміни стратегії та, відповідно, сутності виконуваної функції. Тобто, при

$$\sum_{s_n} J_0^{G',K'} \geq L, \quad (3)$$

де L – критичне значення кількості вузлів ВМКМ, які можуть виконувати поточну функцію в рамках стратегії функціонування мережі; стратегія ВМКМ змінюється, відповідно до можливостей вузлів виконувати нову функцію. Ця можливість наперед тестується вузлами, що і формує підстави для прийняття рішення про зміну стратегії. Якщо жодна із можливих стратегій є недосяжною для виконання внаслідок катастрофічної руйнації ВМКМ, приймається рішення про евакуацію вузлів, при цьому ВМКМ перестає існувати як цілісна система, а кожний вузол функціонує як незалежна сутність.

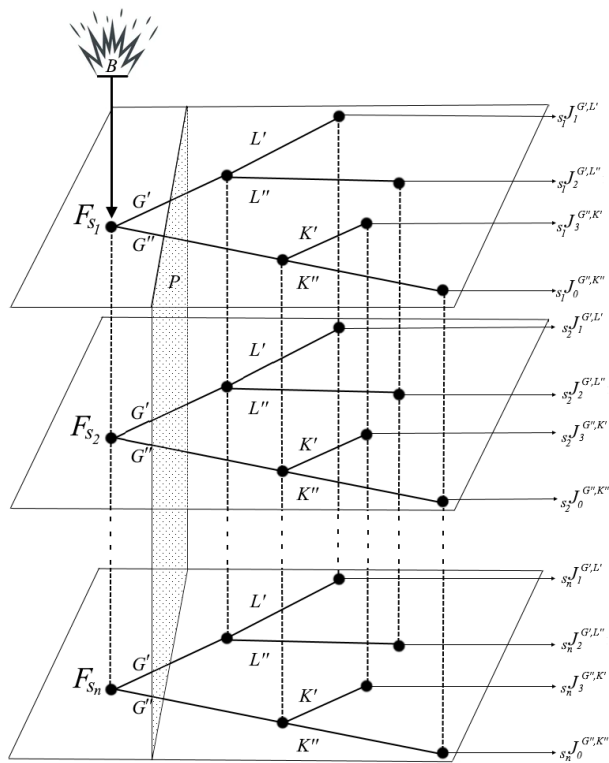


Рис. 1. Багатошарове сценарне дерево для ВМКМ, яка зазнає руйнівного впливу

Інші гілки дерева подій, наведені на рис. 1, показують, що накопичення значень вузлів у станах $s_n J_1^{G',L'}$, $s_n J_2^{G',L'}$, $s_n J_3^{G',K'}$ призводять до зміни стратегії функціонування ВМКМ, відповідно до правил, які задаються на етапі постановки задачі перед мережею. Виходячи з того, що показник надійності ВМКМ ξ_0 , яка не зазнавала деструктивного впливу буде визначатися як співвідношення математичного очікування до дисперсії, то показник надійності ВМКМ ξ_B , яка зазнала деструктивного впливу під час події B , – це співвідношення математичного спо-

дівання до середньоквадратичного відхилення запасу функціональності мережі. За таких визначень, індекс живучості за показником надійності, враховуючи [10], буде:

$$C = \xi_0 / \xi_B. \quad (4)$$

Виходячи зі структури дерева подій та враховуючи індекс живучості, заснований на співвідношенні ризиків прямих та непрямих збитків [10], оцінку живучості ВМКМ можна розрахувати як:

$$C_S = \frac{\int \int F_{S_n} q_{D|B}(\alpha | \beta) q_B(\alpha) d\beta d\alpha}{\int \int F_{S_n} q_{D|B}(\alpha | \beta) q_B(\alpha) d\beta d\alpha + \int \int F_{J_n} q_{D|B} P(G' | D = \beta) q_B(\alpha) d\beta d\alpha}, \quad (5)$$

де α, β – рівень деструктивного впливу і пошкодження елементів мережі; $q_B(\alpha)$ – щільність розподілу ймовірності деструктивного впливу.

У якості рішення задачі оцінки у даному вигляді можна використати метод Монте-Карло, а при модифікованих версіях ВМКМ при кількості вузлів менше п'яти – алгоритм імітації відпалу [12].

Для отримання більш точних оцінок живучості ВМКМ, необхідно удосконалювати моделі ескаляції аварій. Альтернативним підходом є використання простих моделей пошкодження мережі, які засновані на представленні мережі у вигляді графу. В такій постановці розглядаються, як правило, топологічні порушення в роботі ВМКМ, тобто вивчається вплив чинників на структуру мережі і, відповідно, розглядаються рішення реконфігурації топології мережі. Простота моделей пояснюється тим, що вузли мережі і канали передачі даних мережного графа можуть мати один з двох станів – робочий або неробочий. При цьому не враховується часовий фактор процесу розповсюдження пошкоджень і перерозподілу потоків. В такій моделі розповсюдження аварій – живучість ВМКМ може характеризуватися залежністю ступеня виконання мережею заданих функціональних обов'язків (рівня функціональності мережі) від кількості видалених вузлів або ребер (каналів передачі даних).

Забезпечення живучості високомобільної комп'ютерної мережі. Виділяється два напрями рішення по зниженню ймовірності відмови ВМКМ: підвищення надійності її елементів та підвищення стійкості до локальних пошкоджень. Однак, запас живучості ВМКМ може бути недостатнім, щоб чинити опір катастрофічним руйнаціям мережі після нанесення їй локальних пошкоджень. Руйнації такого характеру найчастіше можуть виникати в ВМКМ з високим показником надмірності за рахунок позитивних зворотних зав'язків.

Аналіз та оцінка живучості ВМКМ показує, що до відмови ВМКМ призводять ланцюг подій, який складається з: екстремального впливу на мережу; локального пошкодження елементів мережі; ескаляція аварійного процесу, що призводить до ініціювання вторинних та каскадних відмов решти елементів мережі, та завершується відмовою мережі в цілому.

В існуючих рішеннях лежить визначення ймовірності виникнення екстремального впливу та конструктивний алгоритм, спрямований на підвищення живучості, щоб запобігти катастрофічним явищам руйнації ВМКМ [10, 11].

Існує велика кількість підходів до визначення ймовірності виникнення екстремального впливу, наприклад методи прогнозування, теорія випадкових процесів тощо [12], які добре себе зарекомендували.

Відповідно, пропонується новий підхід, який можна описати такою послідовністю кроків.

Крок 1. На початку планування роботи ВМКМ визначаються всі можливі стратегії та/або функції, які може виконувати ВМКМ, визначається мінімальний поріг цілісності структури мережі, який дозволяє виконувати задану функцію.

Крок 2. Власне, ВМКМ виконує задану їй функцію, відповідно до стратегії. Під час виконання відбувається моніторинг стану вузлів мережі, їх діагностика та самодіагностика. Нормальний режим функціонування характеризується відсутністю локальних пошкоджень ВМКМ та інформації про ймовірні пошкодження у найближчій перспективі.

Крок 3. У разі виникнення внутрішнього або зовнішнього впливу, який унеможливує, або частково обмежує виконання вузлами ВМКМ поставлених задач, відбувається оцінка можливості виконання основної функції мережею в цілому.

Ймовірність відмови ВМКМ можна визначити, використовуючи [10]:

$$P[S] = \{W_s\} \times [W_c] \times \{B\}, \quad (6)$$

де $\{W_s\}$ – вектор вразливості структури ВМКМ, який складається з умовних ймовірностей відмови мережі внаслідок локальних пошкоджень; $[W_c]$ – матриця локальної вразливості ВМКМ, яка складається з умовних ймовірностей локальних пошкоджень ВМКМ при різних руйнівних факторах впливу на мережу; $\{B\}$ – вектор загроз, який складається з ймовірностей виникнення та протікання різних руйнівних впливів.

Крок 4. Відповідно до заданих на початковому етапі критичних значень та результатів моніторингу стану структури ВМКМ та стану її вузлів, можуть прийматися наступні рішення: продовження виконання основної функції, діагностика ВМКМ щодо можливості виконання іншої функції, відповідно до пулу стратегій, зміна основної функції, евакуація вузлів ВМКМ, яка зазнала катастрофічної руйнації.

Крок 5. У разі зміни основної функції, відбувається реконфігурація вузлів ВМКМ, за необхідності, перебудовується схема маршрутизації потоків даних, встановлюється поріг цінності інформації, що реєструється.

Крок 6. Після виконання останньої функції, яка була визначена для ВМКМ, згідно алгоритмів, які задають стратегію функціонування ВМКМ, вузли мережі можуть: повернутися в точку постійного базування, самознищитися, знищити критично важливу інформацію, яка знаходиться на носію даних вузла, якщо стратегія не містить задачі повернення вузла.

Модельний експеримент. Розглянемо один із прикладів забезпечення живучості ВМКМ з використанням підходу, який запропоновано в роботі.

Нехай існує деяка ВМКМ S , яка складається з сукупності вузлів s_n , де $n = 1, 2, \dots, 16$ та каналів передачі даних між ними, виконує основну функцію реєстрації інформації на певній ділянці, яка характеризується високою ймовірністю виникнення деструктивних явищ B (рис. 2). При цьому вузли ВМКМ виконують функції, пов'язані з реєстрацією інформації f_1 , перетворенням (стисненням) f_2 , тимчасовим зберіганням f_3 , та передачею f_4 .

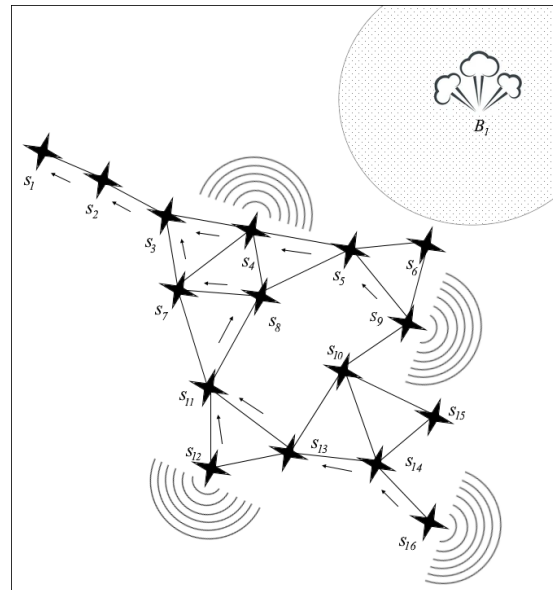


Рис. 2. Приклад ВМКМ, яка виконує функцію реєстрації інформації (зондування земної поверхні)

У деякий момент часу t_B виникає руйнівне явище B_1 , яке має високу швидкість поширення та протягом коротко часу досягає вузлів ВМКМ (рис. 3).

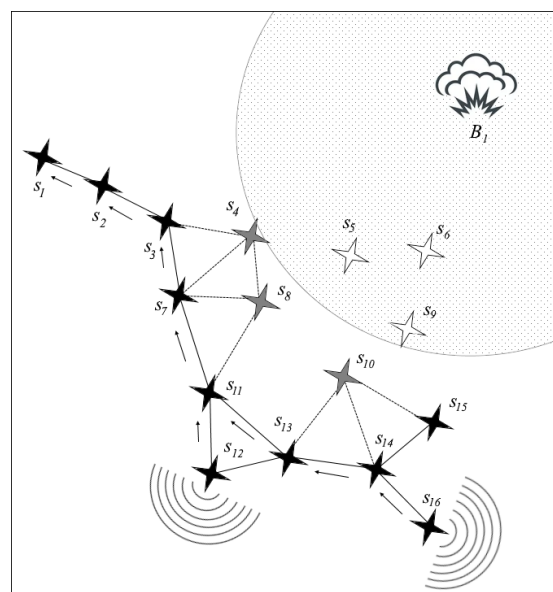


Рис. 3. Вплив руйнівного чинника на функціонування ВМКМ

Частина вузлів, під впливом такого впливу, втрачають свою функціональність та перестають бути частиною структури ВМКМ (s_5, s_6, s_9), тоді як вузли s_4, s_8, s_{10}, s_{15} отримують локальні пошкодження та не можуть виконувати поточну функцію реєстрації інформації. Матриця стану вузлів, можливості виконання ними функції щоразу оновлюється, тому ВМКМ завжди має представлення про свою структурну цілісність та можливість функціонування за визначеною стратегією.

Припустимо, через деякий час, деструктивний вплив B_1 набув свого пікового значення, вивівши з ладу частину вузлів високомобільних комп'ютерних мереж та у цей час виник інший чинник B_2 . Оцінка живучості та дерево подій, розглянуті вище, є підставою ініціювати перегляд стратегії функціонування ВМКМ.

Таким чином, перевизначається основні функція, а вузли ВМКМ реконфігуруються та починають виконувати нову функцію f_1' замість f_1 (рис. 4).

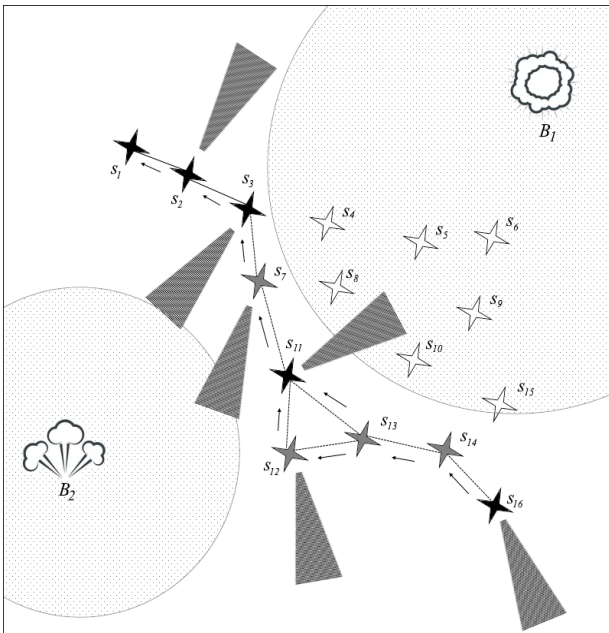


Рис. 4. Приклад реконфігурації ВМКМ – змінено спосіб реєстрації інформації

Результати модельного експерименту представлені у табл. 1.

Результати показують, за яких порогових значеннях відбувається перевизначення функцій, відповідно до нової стратегії та індекс живучості мережі з урахуванням (5).

Таким чином, модельний експеримент демонструє, що використання запропонованого методу дозволяє підвищити живучість високомобільних комп'ютерних мереж шляхом зміни основної функції на підставі даних моніторингу про деструктивний вплив на вузли. При цьому локальні пошкодження ВМКМ у вигляді виходу з ладу окремих її вузлів не спричиняють катастрофічної руйнації, про що свідчать теоретична оцінка показника живучості високомобільних комп'ютерних мереж.

Таблиця 1 – Результати модельного експерименту

Вузол	Функціональна траєкторія
s_1	$\{f_4 t_1\} \rightarrow \{f_4 t_2\} \rightarrow \{f_4 t_3\}$
s_2	$\{f_4 t_1\} \rightarrow \{f_4 t_2\} \rightarrow \{(f_4, f_1') t_3\}$
s_3	$\{f_4 t_1\} \rightarrow \{f_4 t_2\} \rightarrow \{(f_4, f_1') t_3\}$
s_4	$\{(f_4, f_1) t_1\} \rightarrow \{f_3 t_2\} \rightarrow \{0 t_3\}$
s_5	$\{f_4 t_1\} \rightarrow \{0 t_2\} \rightarrow \{0 t_3\}$
s_6	$\{f_4 t_1\} \rightarrow \{0 t_2\} \rightarrow \{0 t_3\}$
s_7	$\{f_4 t_1\} \rightarrow \{f_4 t_2\} \rightarrow \{(f_4, f_3, f_1') t_3\}$
s_8	$\{f_4 t_1\} \rightarrow \{f_3 t_2\} \rightarrow \{0 t_3\}$
s_9	$\{(f_4, f_1) t_1\} \rightarrow \{0 t_2\} \rightarrow \{0 t_3\}$
s_{10}	$\{1 t_1\} \rightarrow \{0 t_2\} \rightarrow \{0 t_3\}$
s_{11}	$\{f_4 t_1\} \rightarrow \{f_4 t_2\} \rightarrow \{(f_4, f_1') t_3\}$
s_{12}	$\{(f_4, f_1) t_1\} \rightarrow \{(f_4, f_1) t_2\} \rightarrow \{(f_4, f_3, f_1') t_3\}$
s_{13}	$\{f_4 t_1\} \rightarrow \{f_4 t_2\} \rightarrow \{(f_4, f_3) t_3\}$
s_{14}	$\{f_4 t_1\} \rightarrow \{f_4 t_2\} \rightarrow \{(f_4, f_3) t_3\}$
s_{15}	$\{1 t_1\} \rightarrow \{1 t_2\} \rightarrow \{0 t_3\}$
s_{16}	$\{(f_4, f_1) t_1\} \rightarrow \{(f_4, f_1) t_2\} \rightarrow \{(f_4, f_1') t_3\}$

Висновки

В результаті проведеної роботи поставлена і успішно вирішена науково-прикладна задача розробки методу, який дозволяє забезпечити живучість високомобільної комп'ютерної мережі, призначеної для функціонування в екстремальних умовах з рядом чинників, які можуть чинити локальний пошкодження мережі, шляхом механізму визначення порогових значень неможливості виконання основної функції та її зміни для реалізації всіх доступних стратегій функціонування мережі при визначенні критичних значень цілісності мережі та здатності її виконувати хоча б одну із доступних функцій, які задаються на початковому етапі. Метод включає в себе оцінку живучості ВМКМ в нормальному та екстремальному режимах функціонування, організаційні заходи. Зокрема, досягнуто такі результати:

- сформульована науково-прикладна задача забезпечення живучості високомобільної комп'ютерної мережі;
- отримала подальший розвиток методика оцінки живучості комп'ютерних мереж в умовах деструктивного зовнішнього впливу;
- розроблено метод визначення критичних порогів живучості мережі відносно основної функції та зміни основної функції, відповідно до стратегій функціонування ВМКМ;
- проведено модельні експерименти з дослідженням ефективності використання розробленого методу.

Запропонований метод може бути використаний при на етапах планування використання високомобільних комп'ютерних мереж в середовищі з високою ймовірністю деструктивних впливів на елементи

мережі для розробки спеціальних стратегій функціонування мережі з метою збереження накопичених даних, вчасної передачі та цілісності елементів мережі.

У якості подальшої дослідницької роботи за даним напрямком пропонується провести експериментальні дослідження на базі реального обладнання з метою пошуку нових закономірностей, які неможливо або вкрай складно передбачити внаслідок деградації

апаратної складової під час нормального функціонування високомобільних комп'ютерних мереж протягом тривалого часу [13], а також є необхідним для більш повного розуміння траєкторій гілок сценарного дерева, застосувати інші алгоритмічні підходи, такі як метод невизначених множників Лагранжа при розрахунку порогових значень, коли необхідно виконувати реконфігурацію вузлів [14].

СПИСОК ЛІТЕРАТУРИ

1. Яровий О. В. Системи управління безпілотними літальними апаратами для здійснення моніторингу наземних об'єктів. *Системи управління, навігації та зв'язку*. 2018. Вип. 3 (49). С. 33-38. DOI: <https://doi.org/10.26906/SUNZ.2018.3.033>.
2. Харченко В. С., Ястребенецкий М. А., Фесенко Г. В., Саченко А. А., Кочан В. В. Система послеварийного моніторингу АЭС с использованием БПЛА: модели надежности. *Ядерна та радіаційна безпека*. 2017. № 4. С. 50-55.
3. Talak R., Karaman S., Modiano E. Capacity and delay scaling for broadcast transmission in highly mobile wireless networks. *IEEE Transactions on Mobile Computing*. 2019. 19(9). P. 1-10. DOI: <https://doi.org/10.1145/3084041.3084045>.
4. Nagchaudhuri A., Mitra M., Hartman C., Ford T., Pandya J. Mobile Robotic Platforms to Support Smart Farming Efforts at UMES. *2018 14th IEEE/ASME Int. Conf. on Mechatronic and Emb. Systems and Appl. (MESA)*. 2018, July. P. 1-7. IEEE.
5. Alghamdi Y., Munir A., La H. M. Architecture, Classification, and Applications of Contemporary Unmanned Aerial Vehicles. *IEEE Consumer Electronics Magazine*. 2021. DOI: <https://doi.org/10.1109/MCE.2021.3063945>.
6. Додонов А. Г., Ландэ Д. В. Живучесть информационных систем. Киев : Наук. думка, 2011. 256 с.
7. Ruban I. V., Churyumov G. I., Tokarev V. V., Tkachov V. M. Provision of Survivability of Reconfigurable Mobile System on Exposure to High-Power Electromagnetic Radiation. *Selected Papers of the XVII Int. Scientific and Practical Conf. on Information Technologies and Security (ITS 2017)*. CEUR Workshop Processing, Kyiv, Ukraine, November 30, 2017. Pp. 105-111.
8. Churyumov G., Tokarev V., Tkachov V., Partyka S. Scenario of interaction of the mobile technical objects in the process of transmission of data streams in conditions of impacting the powerful electromagnetic field. *2018 IEEE second international conference on Data Stream Mining & Processing (DSMP)*. 2018, August. P. 183-186. IEEE.
9. Махутов Н. А., Петров В. П., Резников Д. О. Оценка живучести сложных технических систем. *Проблемы безопасности и чрезвычайных ситуаций*. 2009. № 3. С. 47-66.
10. Канаев А. К., Муравцов А. А., Субботин Д. В., Ефремов С. П. Модели функционирования транспортной сети связи специального назначения с учетом динамического изменения структуры сети в условиях дестабилизирующих информационных воздействий. *Вопросы оборонной техники*. Серия 16. 2019. № 7-8. С. 90-98.
11. Махутов Н. А., Резников Д. О. Оценка уязвимости технических систем и ее место в процедуре анализа риска. *Проблемы анализа риска*. 2008. Т. 5, № 3. С. 72-85.
12. Кошевой Н. Д., Бельмега А. В., Чистикова З. Э. Применение алгоритма имитации отжига для оптимизации многофакторных планов эксперимента. *Системи обробки інформації*. 2015. № 6. С. 103-106.
13. Ткачов В. М., Мігін Д. С., Дух Я. В. Підвищення живучості мережної складової рою БПЛА. *Комп'ютерні інтелектуальні системи та мережі*. Мат. XI Всеукраїнської науково-практичної WEB конференції аспірантів, студентів та молодих вчених (21-23 березня 2018 р.). Кривий Ріг: ДВНЗ «Криворізький національний університет», 2018. С. 98-100.
14. Kovalenko A., Kuchuk H., Tkachov V. Method of ensuring the survivability of computer network on the basis of VPN-tunneling. *Системи управління, навігації та зв'язку*. 2018. Вип. 1 (63). С. 90-95. DOI: <https://doi.org/10.26906/SUNZ.2021.1.090>.

REFERENCES

1. Yaroviy, O. (2018), "Systems of management of unavailable flighting apparatus for implementation of monitoring of ground object", *Control, Navigation and Communication Systems*, Is. 1(49), pp. 33-38. DOI: <https://doi.org/10.26906/SUNZ.2018.3.033>.
2. Kharchenko, V. S., Yastrebenetskiy, M. A., Fesenko, G. V., Sachenko, A. A. and Kochan, V. V. (2017), "System of NPP post-accident monitoring using UAVs: reliability models", *Nuclear and radioactive safety*, No. 4, pp. 50-55.
3. Talak, R., Karaman, S. and Modiano, E. (2019), "Capacity and delay scaling for broadcast transmission in highly mobile wireless networks", *IEEE Transactions on Mobile Computing*, 19(9), pp 1-10, DOI: <https://doi.org/10.1145/3084041.3084045>.
4. Nagchaudhuri, A., Mitra, M., Hartman, C., Ford, T. and Pandya, J. (2018), "Mobile Robotic Platforms to Support Smart Farming Efforts at UMES", *2018 14th IEEE/ASME Int. Conf. on Mechatronic and Emb. Systems and Appl. (MESA)*, pp. 1-7.
5. Alghamdi, Y., Munir, A. and La, H. M. (2021), "Architecture, Classification, and Applications of Contemporary Unmanned Aerial Vehicles", *IEEE Consumer Electronics Magazine*, DOI: <https://doi.org/10.1109/MCE.2021.3063945>.
6. Dodonov A.G. and Lande, D.W. (2011), *Information Systems Survivability*, Nauk. dumka, Kyiv, 256 p.
7. Ruban, I. V., Churyumov, G. I., Tokarev, V. V. and Tkachov, V. M. (2017), "Provision of Survivability of Reconfigurable Mobile System on Exposure to High-Power Electromagnetic Radiation", *Selected Papers of the XVII Int. Scientific and Practical Conf. on Information Technologies and Security (ITS 2017)*, CEUR Workshop Processing, Kyiv, Ukraine, pp. 105-111.
8. Churyumov, G., Tokarev, V., Tkachov, V. and Partyka, S. (2018), "Scenario of interaction of the mobile technical objects in the process of transmission of data streams in conditions of impacting the powerful electromagnetic field", *2018 IEEE second international conference on Data Stream Mining & Processing (DSMP)*, pp. 183-186, IEEE.
9. Makhutov, N.A., Petrov V.P. and Reznikov, D.O. (2009), "Assessment of the survivability of complex technical systems", *Problems of safety and emergency situations*, no. 3, pp. 47-66.
10. Kanaev, A.K., Muravtsov, A.A., Subbotin, D.V. and Efremov, S.P. (2019), "Models of the functioning of a special-purpose communication transport network, taking into account the dynamic changes in the structure of the network in conditions of destabilizing information influences", *Problems of defense technology*, Series 16, No. 7-8, pp. 90-98.
11. Makhutov, N.A. and Reznikov, D.O. (2008), "Assessing the vulnerability of technical systems and its place in the risk analysis procedure", *Problems of risk analysis*, vol 5, no. 3, pp. 72-85.

12. Koshevoy, N.D., Belmega, A.V. and Chistikova, Z.E. (2015), "Application of the simulated annealing algorithm for optimization of multivariate experimental designs", *Information processing systems*, No. 6, pp. 103-106.
13. Tkachov, V.M., Mitin, D.E. and Spirit, J.W. (2018), "Improving the survivability of the network component of the UAV swarm", *Computer Intelligent Systems and Networks*, Kryvyi Rih National University, Kryvyi Rih, pp. 98-100.
14. Kovalenko, A., Kuchuk, H. and Tkachov, V. (2021), "Method of ensuring the survivability of the computer network based on VPN-tunneling", *Control, Navigation and Communication Systems*, Is. 1(63), pp. 90-95. DOI: <https://doi.org/10.26906/SUNZ.2021.1.090>.

Received (Надійшла) 15.02.2021

Accepted for publication (Прийнята до друку) 28.04.2021

ВІДОМОСТІ ПРО АВТОРІВ / ABOUT THE AUTHORS

Ткачов Віталій Миколайович – кандидат технічних наук, доцент, доцент кафедри електронних обчислювальних машин, Харківський національний університет радіоелектроніки, Харків, Україна;

Vitalii Tkachov – Candidate of Technical Sciences, Associate Professor, Associate Professor of Department of Electronic Computers, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine;

e-mail: vitalii.tkachov@nure.ua, ORCID ID: <http://orcid.org/0000-0002-6524-9937>.

Коваленко Андрій Анатолійович – доктор технічних наук, професор, завідувач кафедри електронних обчислювальних машин, Харківський національний університет радіоелектроніки, Харків, Україна;

Andriy Kovalenko – Doctor of Technical Sciences, Professor, Head of Department of Electronic Computers, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine;

e-mail: andriy.kovalenko@nure.ua; ORCID ID: <http://orcid.org/0000-0002-2817-9036>.

Кучук Георгій Анатолійович – доктор технічних наук, професор, професор кафедри обчислювальної техніки та програмування, Національний технічний університет "Харківський політехнічний інститут", Харків, Україна;

Heorhii Kuchuk – Doctor of Technical Sciences, Professor, Professor of Computer Science and Programming Department, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine;

e-mail: kuchuk56@ukr.net; ORCID ID: <http://orcid.org/0000-0002-2862-438X>.

Ні Яна Самвелівна – кандидат технічних наук, старший викладач кафедри електронних обчислювальних машин, Харківський національний університет радіоелектроніки, Харків, Україна;

Iana Ni – Candidate of Technical Sciences, Senior Lecturer of the Department of Electronic Computers, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine;

e-mail: yana.movsesian@nure.ua; ORCID ID: <http://orcid.org/0000-0002-1352-700X>.

Метод обеспечения живучести высокомобильной компьютерной сети

В. Н. Ткачев, А. А. Коваленко, Г. А. Кучук, Я. С. Ни

Аннотация. В статье рассмотрены особенности функционирования подвижных компьютерных сетей на базе малогабаритных летательных аппаратов (высокомобильные компьютерные сети). Показано, что такие сети, в отличие от стационарных или маломобильных, отличаются низким уровнем живучести при локальных повреждениях их узлов. **Целью статьи** является разработка метода обеспечения живучести высокомобильных компьютерных сетей в условиях деструктивного внешнего воздействия, что приводит к локальному разрушению узлов сети или связей между ними, с использованием методики оценки живучести на всех этапах функционирования сети, путем изменения основной функции для реализации всех доступных стратегий функционированием сети при определении критических значений целостности сети и способности ее выполнять хотя бы одну из доступных функций. **Полученные результаты** позволяют: продолжить развитие методики оценки живучести компьютерных сетей в условиях деструктивного внешнего воздействия; применять разработанный метод для определения критических порогов живучести сети относительно основной функции и изменения основной функции, согласно со стратегией функционированием высокомобильных сетей. Исследования позволяют сделать выводы, что предложенный метод может быть использован на этапах проектирования высокомобильных компьютерных сетей, характеризующихся повышенной живучестью и способных функционировать в условиях множественных локальных повреждений без катастрофических разрушительных последствий для структуры сети.

Ключевые слова: живучесть; компьютерная сеть; оценка состояния; реконфигурация; разрушительное воздействие.

Method of ensuring the survivability of highly mobile computer networks

Vitalii Tkachov, Andriy Kovalenko, Heorhii Kuchuk, Iana Ni

Abstract. The article discusses the features of the functioning of mobile computer networks based on small-sized aircraft (highly mobile computer networks). It is shown that such networks, in contrast to stationary or low-mobile ones, have a low level of survivability in case of local damage to their nodes. **The purpose of the article** is to develop a method for ensuring the survivability of highly mobile computer networks under conditions of destructive external influences, which leads to local destruction of network nodes or links between them, using the method of assessing survivability at all stages of network functioning, by changing the main function to implement all available strategies for the functioning of the network when determining the critical values of the integrity of the network and its ability to perform at least one of the available functions. The results obtained allow: to continue the development of theoretical research in the development of strategies for managing highly mobile computer networks in extreme situations; to develop an applied solution to ensure the survivability of highly mobile computer networks by building multifunctional or redundant structures, increasing the value of their redundancy. The studies allow us to **conclude** that the proposed method can be used at the design stages of highly mobile computer networks, characterized by increased survivability and capable of functioning in conditions of multiple local damages without catastrophic destructive consequences for the network structure.

Keywords: survivability; computer network; condition assessment; reconfiguration; destructive impact.