
NETWORK AND APPLICATION SECURITY

DOI 10.20535/2411-1031.2022.10.1.261121

УДК 004.7

ЮРІЙ ГОЛОВІН,
БОГДАН ПАСТУХ**ОЦІНКА ЕФЕКТИВНОСТІ ПРОТОКОЛІВ МАРШРУТИЗАЦІЇ В БЕЗПРОВОДОВИХ MESH-МЕРЕЖАХ**

Важливим напрямком в управлінні державою є створення єдиного інформаційного простору, що забезпечить зворотній зв'язок, своєчасне планування та узгодження дій різних підрозділів та структур держави для ефективного виконання поставлених завдань. Ці питання є дуже актуальними для збройних сил та інших силових структур держави. Технологія спільного управління багатьма доменами JADC2 (англ. Joint All-Domain Command and Control) була прийнята у 2022 році в якості важливої стратегії у збройних силах США та арміях країн НАТО. Передбачено, що JADC2 буде охоплювати всі гілки управління збройних сил з метою поєднання комунікацій різних пристроїв в загальній структурі командування та управління. Для досягнення успіху повинен підтримуватись постійний зв'язок між великою кількістю доменів, в тому числі датчиків та об'єктів управління – Інтернет-речей у військовій галузі із застосуванням штучного інтелекту AI/ML (англ. Artificial Intelligence/Machine learning). Зв'язок між елементами архітектури JADC2 на відповідних рівнях повинен забезпечуватись різними телекомунікаційними мережами з використанням різних фізичних каналів, таких як КХ та УКХ радіолінії, супутникового зв'язку, стаціонарних оптоволоконних лінії тощо. При цьому необхідно своєчасно передавати великі об'єми даних через глобальні мережі без втрати цілісності даних, тому мережі JADC2 повинні бути готові і до кібератак. Для вирішення зазначених завдань необхідний перехід від вже існуючих конвенційних мереж радіозв'язку до високошвидкісних на базі засобів широкосмугового доступу, в тому числі mesh-мереж MANET (англ. Mobile Ad hoc Network). Основними перевагами мереж MANET є: швидкість розгортання, низька вартість при високій ефективності мережі, можливість передачі даних на великі відстані без збільшення потужності передавача, стійкість до змін в інфраструктурі мережі, можливість швидкої реконфігурації в умовах несприятливих завад тощо. Протоколи маршрутизації в таких мережах є найбільш ефективними засобами вирішення проблеми якості обслуговування. В цій роботі представляються результати оцінки ефективності протоколів маршрутизації в mesh-мережах відповідно до вимог послуг, що надаються.

Ключові слова: mesh-мережа, класи обслуговування, протоколи маршрутизації, QoS, JADC2, рекомендації ITU-T.

Постановка проблеми. Топологія мереж MANET може змінюватися в процесі розгортання та експлуатації, тому вона потребує надійного та ефективного протоколу маршрутизації, що є достатньо складною задачею. Показники якості мереж (пропускна спроможність, затримка передачі інформації, навантаження на мережу) певною мірою визначаються ефективністю методів і технологій маршрутизації [1] - [3].

Важливим завданням в цих умовах є вибір (серед кількох наявних) і використання протоколу маршрутизації для MANET мереж, що забезпечить кращу продуктивність, меншу затримку та більшу надійність передачі даних в мережі [4] - [9].

Аналіз останніх досліджень і публікацій. За прогнозом компанії Cisco [5] трафік від безпроводових та мобільних пристроїв становитиме більше 70 відсотків загального трафіку IP-мереж вже до 2023 року, а кількість пристроїв, підключених до IP-мереж в 2 рази буде перевищувати чисельність населення.

Технічні норми на показники якості наведені у рекомендації ITU-T Y.1541 (вимоги до цільових значень показників продуктивності IP-мереж), розробленої Міжнародним Союзом електрозв'язку (ITU). При цьому рекомендації ITU-T фактично відповідають нормам та містять опис обчислення значень, необхідних характеристик якості мережі, яка моделюється.

MCE були розроблені також наступні рекомендації:

- Y.1540 – описують стандартні характеристики передачі даних в IP-мережах [7];
- Y.1221 – представлено загальний опис, завдання та процедури для управління трафіком та контролю навантаження в мережах, що базуються на IP.

Наведені рекомендації визначають характеристики, що найбільше впливають на відповідність якості обслуговування між джерелом і адресатом, а саме:

- затримка;
- джитер;
- надійність;
- втрати пакетів;
- пропускна спроможність.

Незважаючи на те, що у рекомендації Y.1540 відсутні норми продуктивності мережі в частині пропускної спроможності, тим не менш, Y.1541 посиляється на можливість її визначення відповідно до дескриптора трафіку [4] – набору параметрів потоку трафіку між інтерфейсами відправника та одержувача, визначеного ITU-T Y.1221.

У розділі про спроможності передачі IP трафіку (IP transfer capabilities) ITU-T Y.1221(06/2010) виділяють п'ять типів пропускної спроможності [8]:

- Dedicated bandwidth (DBW) – пропускна спроможність застосунків з високими вимогами гарантованої та своєчасної доставки пакетів (наприклад, застосунків реального часу);
- Statistical bandwidth (SBW) – пропускна спроможність для програм, які не мають жорстких вимог до затримок мережі, головна вимога – гарантована доставка пакетів адресату;
- Best-effort (BE) – пропускна спроможність для застосунків, які не висувають високих вимог до рівня затримки та гарантії доставки пакетів адресату;
- Delay-sensitive statistical bandwidth (DSBW) – пропускна спроможність для застосунків, які не висувають високі вимоги до рівня затримки в мережі та гарантії доставки пакетів, але не пред'являють жодних вимог до варіативності затримки;
- Conditionally dedicated bandwidth (CDBW) – пропускна спроможність застосунків з високими вимогами до затримки та певного рівня втрат пакетів, а характеристики продуктивності цього типу може бути недостатнім для застосунків реального часу, (наприклад, відеотрансляції високої якості, але при цьому достатнім для передачі голосу або відео низької якості).

Також рекомендацією Y.1541 [6] визначається відповідність класів обслуговування та застосунків, що використовують інфраструктуру мережі (табл. 1).

Виходячи з наведених рекомендацій MCE (ITU), були визначені вимоги до продуктивності цільової мережі залежно від призначення застосунків, що використовують mesh-мережу [6], [7], [8]:

- мінімальний інтервал часу спостереження за потоком;
- шість класів якості обслуговування та відповідність кожному класу типів застосунків;
- максимальні граничні значення затримки доставки та джитера всередині кожного класу;
- максимальні значення коефіцієнтів втрачених пакетів (IPLR);
- максимальні значення коефіцієнтів пошкоджених пакетів (IPER);
- значення рівня пропускної спроможності при тестуванні мережі з потоком VoIP.

Отриманий набір значень було використано в якості контрольних значень при проведенні експерименту із моделлю mesh-мережі. Для визначеності будемо використовувати параметри, що вказані у рекомендації MCE Y.1541 та наведені в табл. 2.

Таблиця 1 – Типи застосунків згідно з класом обслуговування

№ класу	Застосунки
клас 0	застосунки реального часу, які мають високі вимоги до затримки та джітеру (наприклад, IP телефонія (VoIP), телеконференція (VTC))
клас 1	застосунки реального часу, які мають високі вимоги до джітеру, але не потребують малу затримку
клас 2	застосунки, які потребують малу затримку (наприклад, інтерактивні застосунки, телеметрія)
клас 3	інтерактивний обмін даними в застосунках, що не потребують малу мережеву затримку
клас 4	застосунки, що здійснюють передачу великого об'єму даних, але не потребують малу затримку в мережі (наприклад, потокове відео, що буферізується)
клас 5	застосунки, вимоги яких задовольняють будь-які значення затримки та джітеру

Таблиця 2 – Значення параметрів робочих характеристик мережі та відповідність їх класам обслуговування (класи QoS)

Параметр робочої характеристики мережі	Класи обслуговування QoS				
	Клас 0	Клас 1	Клас 2	Клас 3	Клас 4
IPTD, мс	100	400	100	400	1000
IPDV, мс	50	50	50+	50+	50+
IPLR	0,001	0,001	0,001	0,001	0,001
IPER	0,0001	0,0001	0,0001	0,0001	0,0001

Метою статті є підвищення якості обслуговування в mesh-мережах шляхом динамічної зміни протоколів маршрутизації в залежності від параметрів мережі. Наукова задача полягає у обґрунтуванні імітаційної моделі дослідження mesh-мережі та аналізу показників якості мережі при застосуванні різних протоколів маршрутизації для оптимізації її функціонування з різними застосунками.

Для досягнення мети роботи необхідно було виконати наступні завдання:

- проаналізувати особливості протоколів маршрутизації в mesh-мережах;
- провести оцінку вимог до якості надання послуг в IP-мережах відповідно до рекомендацій МСЕ(ITU);
- проаналізувати програмне забезпечення імітаційного моделювання процесів в mesh-мережах;
- розробити програмне забезпечення для аналізу результатів моделювання мережі та визначення їх відповідності класам обслуговування згідно рекомендаціям МСЕ.

Виклад основного матеріалу дослідження. Mesh-мережі MANET (Mobile Ad hoc NETWORK) відносять до децентралізованих автономних безпроводових мереж, що мають можливість самостійно налаштовуватися. Мобільні безпроводові вузли мережі можуть довільно переміщуватися та з'єднуватися між собою випадковим чином, утворюючи довільну топологію.

Після достатньо великих дослідницьких робіт по MANET, в тому числі і в межах проекту Internet Engineering Task Force (IETF), все ще не існує повної форми стандартів до таких мереж. Протоколи маршрутизації для MANET продовжують досліджувати з метою підвищення пропускної спроможності мереж та оптимізації їх застосування для різних застосунків.

Протоколи маршрутизації поділяють на протоколи реактивної (RMP) та проактивної (PMP) маршрутизації, а також – гібридні.

Реактивні протоколи передбачають розсилання запиту на маршрутизацію по всій мережі, що викликає значну затримку і переважно підходять для вузлів з високою мобільністю або вузлів, які рідко передають дані. До таких протоколів для mesh-мереж відносять AODV та DSR.

Проактивні протоколи маршрутизації забезпечують хорошу надійність поточної топології мережі та низьку затримку щодо маршруту. Прикладом є протокол OLSR. Гібридні протоколи об'єднують переваги двох попередніх типів маршрутизації.

AODV (Ad hoc On-demand Distance Vector) – це реактивний протокол маршрутизації “на вимогу” – процес визначення маршруту зніщується тільки тоді, коли з'являються пакети даних для передачі відсутній маршрут до вузла призначення. В якості транспортного протоколу використовується UDP. Алгоритм AODV забезпечує простий спосіб отримання інформації про зміну ситуації лінії зв'язку.

Наприклад, якщо зв'язок між вузлами пошкоджений (рис.1), то повідомлення надсилаються лише потерпілим вузлам мережі та скасовуються всі маршрути через цей пошкоджений вузол. Це дозволяє будувати одно адресні маршрути від джерела до місця призначення, тому мережевий трафік мінімальний.

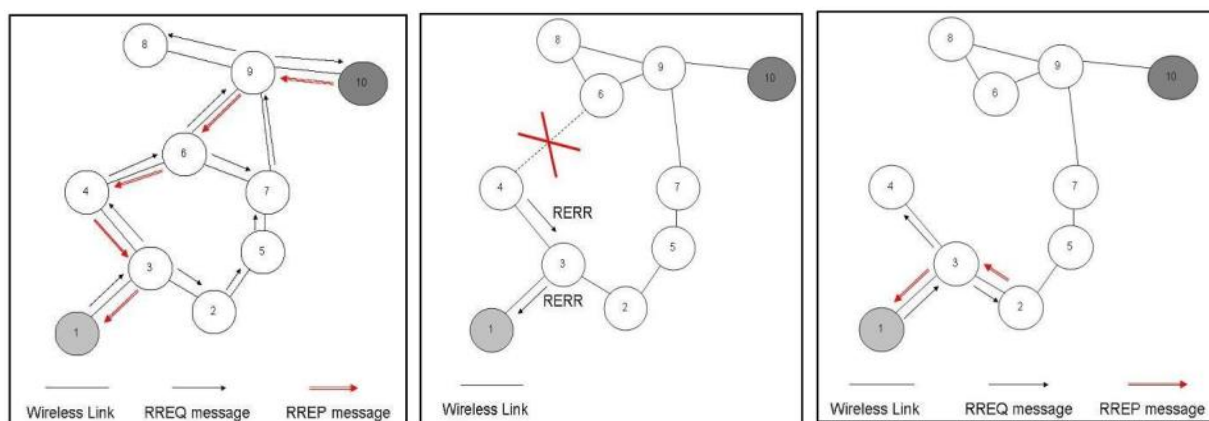


Рисунок 1 – Процес визначення та оновлення маршруту протоколом AODV між джерелом повідомлення (вузол 1) та вузлом призначення (10)

Протокол AODV забезпечує швидку адаптацію до умов динамічного з'єднання та зміни конфігурації мережі, низькі витрати на обробку та пам'ять, низьке службове навантаження в мережі.

DSR (Dynamic Source Routing Protocol) є простим та достатньо ефективним реактивним протоколом маршрутизації та заснований на маршрутизації від джерела повідомлення. При цьому саме джерело визначає ідеальну послідовність вузлів мережі, через які воно буде здійснювати передачу пакетів до пункту призначення. Виявлення та підтримка маршруту – дві основні особливості цього протоколу. Кожний мобільний вузол в DSR повинен зберігати в своїй пам'яті декілька альтернативних кеш-маршрутів (рис. 2), завдяки чому в мережі зменшується службове навантаження із-за відсутності необхідності широкомовних запитів.

При цьому протокол DSR не є ефективним для мереж з великою кількістю вузлів або для мереж, топологія яких динамічно змінюється, що притаманно для мобільних mesh-мереж.

OLSR (Optimized Link-State Routing) – оптимізована маршрутизація за станом з'єднання. Це проактивний протокол маршрутизації, який також називають протоколом із таблицею, оскільки він постійно зберігає та оновлює свою таблицю маршрутизації. Протокол відстежує таблицю маршрутизації, щоб забезпечити маршрут у разі потреби. Використовується спосіб оптимізації розсилки мережевої інформації про стани – MPR (Multipoint Relay), при якому тільки визначені вузли багатоточкової ретрансляції передають в мережу маршрутні пакети (рис. 3). Завдяки такому методу скорочується трафік широкомовного розсилання в мережі.

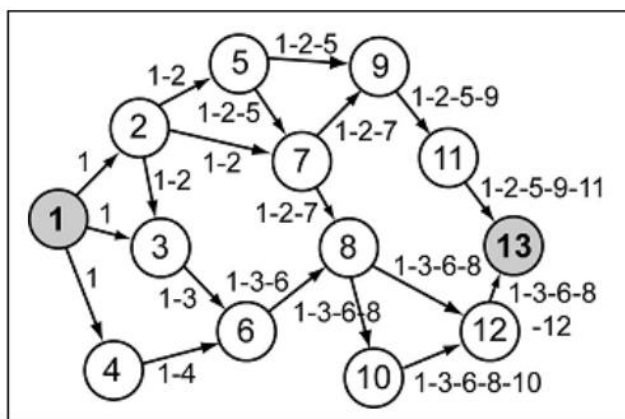


Рисунок 2 – Приклад запису під час виявлення маршруту в DSR між вузлами 1 та 13

Цей алгоритм має гарну реакцію на всілякі несподівані події, а саме:

- раптові відмови та відновлення ліній або вузлів;
- несправність та ремонт вузлів мережі;
- небезпечні дії “зовнішнього середовища”, що призводять до блокування певних елементів системи;
- приєднання та від’єднання вузлів та ліній при зміні їх місцеположення.

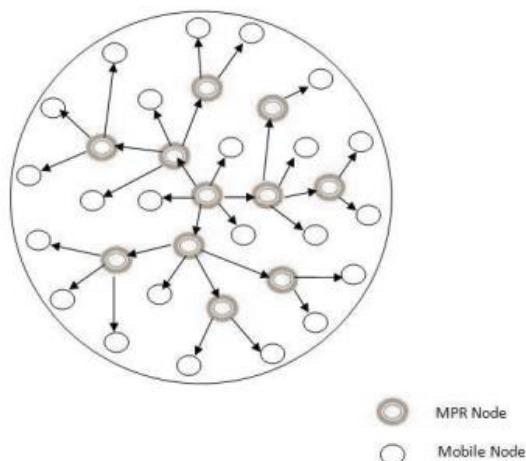


Рисунок 3 – Розміщення MPR-вузлів в мережі з OLSR

Гібридний протокол для безпроводових mesh-мереж HWMP (Hybrid Wireless Mesh Protocol) є стандартним протоколом для маршрутизації (стандарт 802.11s) та реалізований на канальному рівні (на основі MAC-адрес) моделі OSI. Він є гібридним, оскільки поєднує в собі два режими побудови маршрутів, які можуть бути використані як окремо, так і одночасно в одній мережі:

- 1) реактивний режим – побудова маршрутних таблиць у вузлах mesh-мережі безпосередньо перед передачею даних (“на вимогу”);
- 2) проактивний режим – регулярна процедура оновлення інформації у маршрутних таблицях вузлів усієї мережі.

Існує чотири типи кадрів у HWMP, які безпосередньо беруть участь у процесі виявлення шляху (рис. 4):

- 1) шлях запити – Path Request (PREQ);
- 2) шлях відповіді – Path Reply (PREP);
- 3) помилка шляху – Path Error (PERR);
- 4) кореневе оголошення – Root Announcement (Rann).

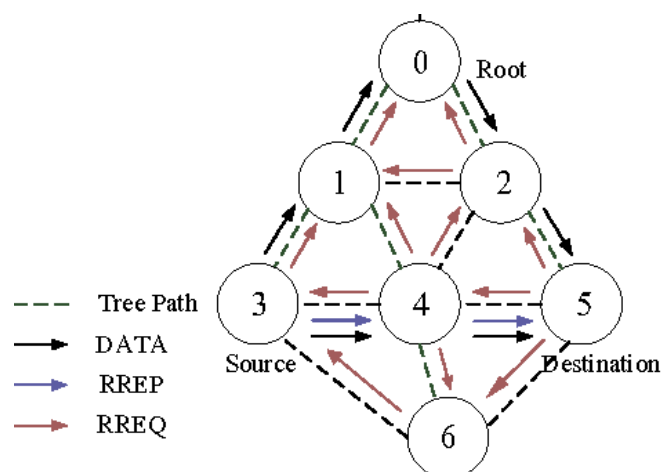


Рисунок 4 – Реалізація процесів маршрутизації в протоколі HWMP

Результати аналізу особливостей функціонування протоколів маршрутизації OLSR, DSR, AODV та HWMP наведені в табл. 3.

Таблиця 3 – Порівняльна характеристика протоколів маршрутизації

Характеристики та властивості протоколів	Протоколи маршрутизації			
	AODV	DSR	OLSR	HWMP
Тип протоколу	реактивний	реактивний	проактивний	гібридний
Рівень моделі OSI	мережевий	мережевий	мережевий	канальний
Придатність до великих мереж	+	-	+	+
Швидко реагують на зміну топології мережі	+	-	+	+
Придатні для мобільних мереж	+	-	+	+
Навантаження мережі службовим трафіком	низьке	високе	низьке	низьке

Для аналізу протоколів маршрутизації було обрано імітаційне моделювання, тому що виникає необхідність імітації роботи mesh-мережі у часі при можливості зміни деяких параметрів мережі, а саме: розміру мережі (кількості хостів), протоколів маршрутизації. Для імітаційного моделювання роботи mesh-мережі може бути використано різне програмне забезпечення, а саме:

- *NS-3 (Network Simulator)*, в якому реалізовані реактивні та проактивні механізми протоколів маршрутизації mesh-мереж, такі як, AODV, OLSR, але відсутні протоколи DSR та HWMP;

- *OMNeT++* – це модульна модель, що розширюється та заснована на компонентах бібліотеки моделювання C++ і платформа, що, в першу чергу, призначена для створення мережесимуляторів для сенсорних та бездротових однорангових мереж, фотонних мереж, моделювання продуктивності, інтернет-протоколів; пропонується інтегроване середовище розробки на основі Eclipse, графічне середовище виконання та багато інших інструментів та існують розширення для моделювання в реальному часі, емуляції мережі, інтеграції з базами даних, інтеграції з SystemC та інших функцій; серед недоліків можна зазначити відсутність графічного інтерфейсу для створення моделі і налаштування параметрів мережі, а також необхідність володіння мовою програмування C++;

– *Common Open Research Emulator (CORE)* – це інструмент для емуляції мереж на одній або кількох машинах, має функцію підключення емульованої мережі до реальних мереж та складається з графічного інтерфейсу для відображення топології та модулів Python для створення сценаріїв емуляції мережі; серед недоліків можна зазначити відсутність параметрів, які будуть визначені в результаті моделювання;

– *OPNET Modeler* та інші програмні інструменти.

Різні методи та середовища моделювання можуть давати різні результати для оцінки продуктивності та інших характеристик мережі. В якості програмного забезпечення для вузлів mesh-мереж було обрано відкриту операційну систему Contiki, вихідний код до якої представлений в відкритому доступі в мережі Інтернет. Ця операційна система позиціонується, як операційна система пристроїв Інтернету речей (IoT) із обмеженою пам'яттю, потужністю та пропускнуою здатністю. ОС Contiki підтримує стек протоколів для IP мереж, а також для mesh-мереж. За прогнозами спеціалістів [2] Contiki буде основною операційною системою, на базі якої можна створити модель з великою кількістю вузлів для IoT.

Для задачі імітаційного моделювання mesh-мережі в роботі було застосовано програмне забезпечення *COOJA Simulator*, яке має зрозумілий графічний інтерфейс, а також інтеграцію з ОС Contiki (рис. 5). В програмі була задана конфігурація моделі мережі для коректної роботи, а також інструменти моделювання, скрипти для генерації випадкових координат, запуску та зупинки моніторингу, а також для генерації інших змінних.

За допомогою інструменту Radio messages COOJA Simulator можна відстежити такі параметри мережі:

- кількість переданих пакетів;
- час, за який передавалися пакети;
- вузол відправки;
- вузол приймання;
- інформація, яка передавалася.

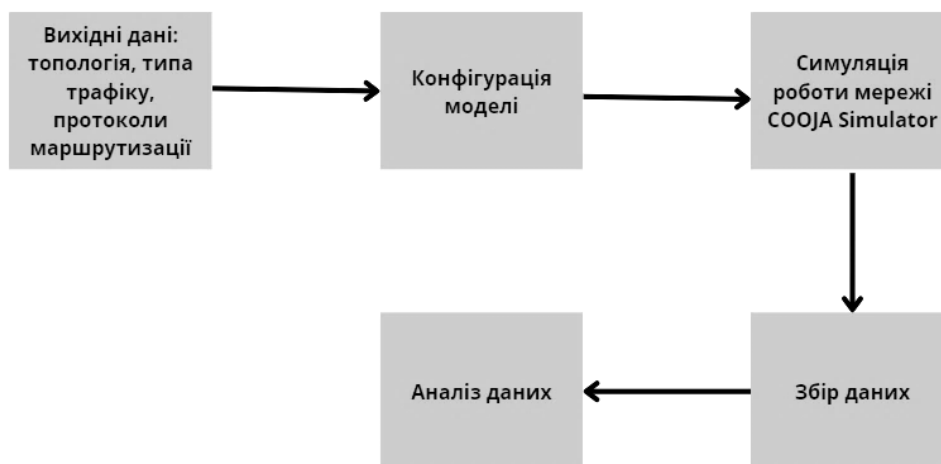


Рисунок 5 – Етапи вирішення задачі

Для моделювання була створена типова mesh-мережа, що складається з 21 хоста, які розташовуються в довільному порядку відносно координат X та Y, що відображено на графічному інтерфейсі програми (рис. 6). За необхідністю кількість вузлів та параметри можуть змінюватись в залежності від початкових даних мережі, що аналізується.

При дослідженні функціонування мережі здійснювався моніторинг протягом 10-ти секундного інтервалу, як достатнього інтервалу часу для встановлення з'єднання “кожний з кожним”. Під час моделювання були розраховані основні робочі характеристики мережі при використанні різних протоколів маршрутизації: OLSR, DSR, AODV та HWMP [10], [11].

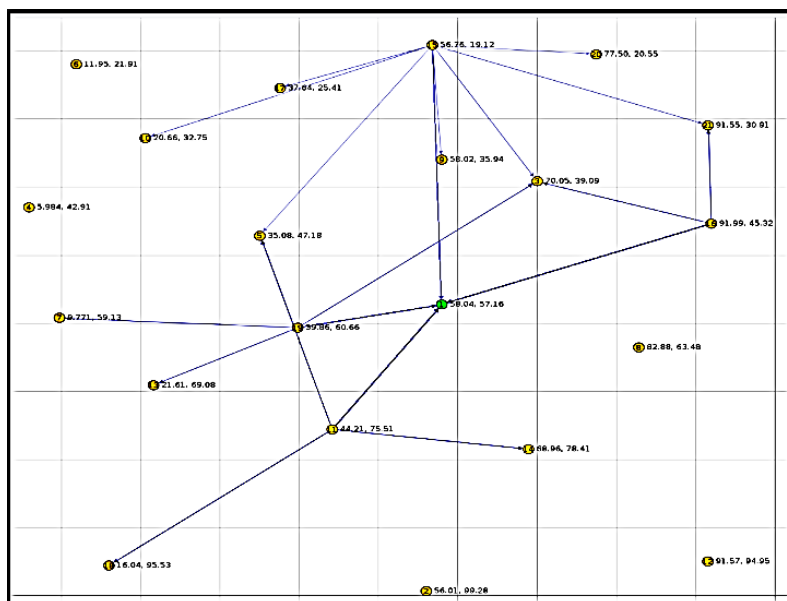


Рисунок 6 – Розташування хостів mesh-мережі на графічному інтерфейсі COOJA Simulator

Для автоматизації процесу аналізу результатів розрахунків параметрів мережі для різних протоколів маршрутизації та їх відповідності класам QoS згідно з рекомендаціями МСЕ було розроблено програмне забезпечення на основі мови програмування *Python*.

Результати розрахунків відображаються у вигляді гістограм (рис. 7) показників параметрів обраної mesh-мережі для кожного із протоколів маршрутизації та надаються рекомендації по застосуванню протоколів маршрутизації згідно з класом обслуговування для відповідної конфігурації мережі.

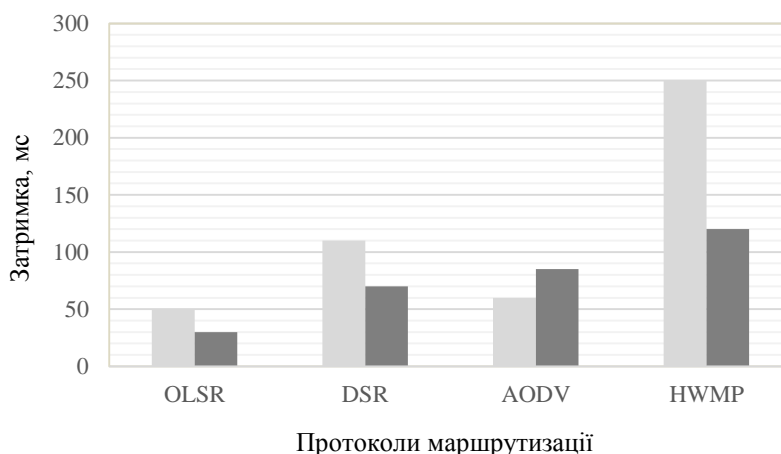


Рисунок 7 – Приклад відображення результатів розрахунку характеристик mesh-мережі

Результати розрахунків імітаційного моделювання можуть бути застосовані для оптимізації mesh-мережі шляхом зміни протоколів маршрутизації в залежності від параметрів мережі у відповідності до необхідного класу обслуговування.

Висновки. Робота присвячена аналізу методів маршрутизації в mesh-мережах з метою оптимізації їх роботи для різних параметрів мережі і відповідних класів обслуговування QoS. Були розглянуті основні класи протоколів маршрутизації в mesh-мережах, серед яких є проактивний, реактивні та гібридний.

Були проаналізовані рекомендації ITU-T Y.1541, ITU-T Y.1540, ITU-T Y.1221 та висунуті вимоги до затримки в мережі, джитеру, втрати пакетів, якості обслуговування в mesh-мережах.

Виходячи з наведених рекомендацій МСЕ (ITU), були визначені вимоги до продуктивності мережі залежно від типу трафіку застосунків та сервісів, що використовують mesh-мережу.

Створено імітаційну модель mesh-мережі та розраховані параметри для протоколів маршрутизації OLSR, DSR, AODV, HWMP з використанням програмного забезпечення COOJA Simulator на базі ОС Kontiki. Розроблено програмне забезпечення для аналізу результатів розрахунків та їх відповідності класам обслуговування відповідно до вимог рекомендацій ITU-T для оптимізації мережі.

У перспективах подальших досліджень планується продовження дослідження імітаційної моделі mesh-мережі з метою наближення її топології до реальної, проведення аналізу залежності робочих характеристик мережі від її топології та розмірів з метою надання рекомендацій по застосуванню протоколів маршрутизації для досягнення відповідних класів обслуговування в мережі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

- [1] I. Demydov, Y. Klymash, M. Brych, and M. Klymash, “The Structural-Functional Synthesis of IoT Service Delivery Systems by Performance and Availability Criteria”, *Internet of Things and Engineering Applications*, Canada, May, 2017, vol. 2, iss. 1, pp. 1-13, doi: <http://dx.doi.org/10.23977/iotea.2017.21001>.
- [2] A. Karimi, S. Abedini, F. Zarafshan, and S.A. Al-Haddad, “Cluster Head Selection Using Fuzzy Logic and Chaotic Based Genetic Algorithm in Wireless Sensor Network”, *Journal of Basic and Applied Scientific Research*, no. 3 (4), pp. 694-703, 2013.
- [3] J. Ghosh, and A. Acharya, “Cluster ensembles”, *Wiley Interdisciplinary Reviews, Data Mining and Knowledge Discovery*, vol. 1 (4), pp. 305-315, 2011, doi: <https://doi.org/10.1002/9781118445112.stat08170>.
- [4] P.-J. Chuang, and Y.-J. Jiang, “Effective neural network-based node localisation scheme for wireless sensor networks”, *Wireless Sensor Systems, IET*, vol. 4, iss. 2, pp. 97-103, 2014, doi: <https://doi.org/10.1049/iet-wss.2013.0055>.
- [5] Cisco Annual Internet Report (2018–2023). [Online]. Available: <https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.pdf>. Accessed on: Jan. 15, 2022.
- [6] ITU-T Y.1541. [Online]. Available: <https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11462&lang>. Accessed on: Jan. 03, 2022.
- [7] ITU-T Y.1540. [Online]. Available: <https://www.itu.int/rec/T-REC-Y.1540> Accessed on: Jan. 05, 2022.
- [8] ITU-T Y.1221. [Online]. Available: <https://www.itu.int/rec/T-REC-Y.1221/en>. Accessed on: Jan. 27, 2022.
- [9] Summary of the Joint All-Domain Command and Control Strategy. Department of Defense USA, March 2022. [Online]. Available: <https://www.defense.gov/News/Releases/Release/Article/2970094/dod-announces-release-of-jadc2-implementation-plan>. Accessed on: Dec. 03, 2021.
- [10] S. Ali, and A. Ali, “Performance Analysis of AODV, DSR and OLSR in MANET”, Department of Electrical Engineering with emphasis on Telecommunication Blekinge Institute of Technology, Sweden 2009. [Online]. Available: <http://www.diva-portal.org/smash/get/diva2:833565/FULLTEXT01.pdf>. Accessed on: Jan. 11, 2022.
- [11] N. P. Bobade, and N. N. Mhala, “Performance evaluation of AODV and DSR on-demand routing protocols with varying MANET size”, *International Journal of Wireless & Mobile Networks (IJWMN)*, vol. 4, no. 1, February 2012, doi: <http://dx.doi.org/10.5121/ijwmn.2012.4113>.

Стаття надійшла до редакції 08.02.2022.

REFERENCE

- [1] I. Demydov, Y. Klymash, M. Brych, and M. Klymash, “The Structural-Functional Synthesis of IoT Service Delivery Systems by Performance and Availability Criteria”, *Internet of Things and Engineering Applications*, Canada, May, 2017, vol. 2, iss. 1, pp. 1-13, doi: <http://dx.doi.org/10.23977/iotea.2017.21001>.
- [2] A. Karimi, S. Abedini, F. Zarafshan, and S. A. Al-Haddad, “Cluster Head Selection Using Fuzzy Logic and Chaotic Based Genetic Algorithm in Wireless Sensor Network”, *Journal of Basic and Applied Scientific Research*, no. 3 (4), pp. 694-703, 2013.
- [3] J. Ghosh, and A. Acharya, “Cluster ensembles”, *Wiley Interdisciplinary Reviews, Data Mining and Knowledge Discovery*, vol. 1 (4), pp. 305-315, 2011, doi: <https://doi.org/10.1002/9781118445112.stat08170>.
- [4] P.-J. Chuang, and Y.-J. Jiang, “Effective neural network-based node localisation scheme for wireless sensor networks”, *Wireless Sensor Systems, IET*, vol. 4, iss. 2, pp. 97-103, 2014, doi: <https://doi.org/10.1049/iet-wss.2013.0055>.
- [5] Cisco Annual Internet Report (2018–2023). [Online]. Available: <https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.pdf>. Accessed on: Jan. 15, 2022.
- [6] ITU-T Y.1541. [Online]. Available: <https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11462&lang>. Accessed on: Jan. 03, 2022.
- [7] ITU-T Y.1540. [Online]. Available: <https://www.itu.int/rec/T-REC-Y.1540> Accessed on: Jan. 05, 2022.
- [8] ITU-T Y.1221. [Online]. Available: <https://www.itu.int/rec/T-REC-Y.1221/en>. Accessed on: Jan. 27, 2022.
- [9] Summary of the Joint All-Domain Command and Control Strategy. Department of Defense USA, March 2022. [Online]. Available: <https://www.defense.gov/News/Releases/Release/Article/2970094/dod-announces-release-of-jadc2-implementation-plan>. Accessed on: Dec. 03, 2021.
- [10] S. Ali, and A. Ali, “Performance Analysis of AODV, DSR and OLSR in MANET”, Department of Electrical Engineering with emphasis on Telecommunication Blekinge Institute of Technology, Sweden 2009. [Online]. Available: <http://www.diva-portal.org/smash/get/diva2:833565/FULLTEXT01.pdf>. Accessed on: Jan. 11, 2022.
- [11] N. P. Bobade, and N. N. Mhala, “Performance evaluation of AODV and DSR on-demand routing protocols with varying MANET size”, *International Journal of Wireless & Mobile Networks (IJWMN)*, vol. 4, no. 1, February 2012, doi: <http://dx.doi.org/10.5121/ijwmn.2012.4113>.

YURIY GOLOVIN,
BOHDAN PASTUKH

EFFICIENCY ANALYSIS OF ROUTING PROTOCOLS IN WIRELESS MESH NETWORKS

An important direction in the administration of the state is the creation of a single information environment that will provide reliable feedback, timely planning and coordination of the actions of various units and structures of the state for the effective performance of assigned tasks. These issues are very relevant for the armed forces and other power structures of the state. JADC2 (Joint All-Domain Command and Control) technology was adopted in 2022 as an important strategy in the US armed forces and the armies of NATO countries. It is envisaged that JADC2 will cover all branches of the armed forces in order to combine the communications of various devices in the overall structure of command and control. To achieve success, a constant connection between a large number of domains, including sensors and control objects – Internet of Things in the military sector with the use

of artificial intelligence AI/ML (Artificial Intelligence/Machine learning) must be maintained. The communication between the elements of the JADC2 architecture at the respective levels should be provided by different telecommunication networks using different physical channels, such as KH and VHF radio links, satellite communication, fixed fiber optic lines, etc. At the same time, it is necessary to transfer large volumes of data through global networks in a timely manner without losing data integrity, so JADC2 networks must be ready for cyber attacks. To solve these problems, it is necessary to switch from existing conventional radio communication networks to high-speed broadband, including MANET mesh networks (Mobile Ad hoc Network). The main advantages of MANET networks are: deployment speed, low cost with high efficiency, the ability to transmit data over long distances without increasing the transmitter power, resistance to changes in the network infrastructure, the ability to quickly reconfigure in adverse interference conditions. Routing protocols in such networks are the most effective means of solving the problem of service quality. This work presents the results of evaluating the effectiveness of routing protocols in mesh networks in accordance with the requirements of the services provided.

Keywords: mesh network, service classes, routing protocols, QoS, JADC2, ITU-T recommendations.

Головін Юрій Олександрович, кандидат технічних наук, доцент, доцент кафедри спеціальних телекомунікаційних систем, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0000-0002-8361-0060, yrgol59@gmail.com.

Пастух Богдан Михайлович, фахівець сфери захисту інформації, Державна служба спеціального зв'язку та захисту інформації України, Київ, Україна, ORCID: 0000-0002-0248-522X, bohpast@gmail.com.

Golovin Yuriy, candidate of technical sciences, associate professor, associate professor of special telecommunication systems academic department, Institute of special communications and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kiev, Ukraine.

Pastukh Bohdan, specialist in the field of information protection, State Service of Special Communications and Information Protection of Ukraine, Kyiv, Ukraine.