УДК 621.391

І. В. Стрелковська
доктор технічних наук, професор,
декан факультету кібербезпеки, програмної інженерії та комп'ютерних наук
Міжнародний гуманітарний університет
м. Одеса, Україна
Р. В. Золотухін
начальник департаменту програмування ТОВ «Телекарт-прилад»
м. Одеса, Україна
Т. І. Григор'єва
кандидат технічних наук, доцент,
завідувач кафедри інформаційних технологій
Міжнародний гуманітарний університет
м. Одеса, Україна

ПОРІВНЯЛЬНИЙ АНАЛІЗ ПРОТОКОЛІВ ПЕРЕДАЧІ ДАНИХ АВТОМАТИЗОВАНИХ СИСТЕМ УПРАВЛІННЯ В НИЗЬКОШВИДКІСНИХ МЕРЕЖАХ ЗВ'ЯЗКУ

Анотація. *При створенні автоматизованих систем управління в низькошвидкісних мережах зв'язку критично важливою задачею є організація взаємодії та передачі інформації між вузлами системи. У мережах IoT для обміну даними в низькошвидкісних мережах широко застосовуються алгоритми та протоколи технології «publish-subscribe». Для роботи в мережах на базі УКХ радіостанцій було створено протокол JDSS стандарту STANAG 4677. В роботі проведено порівняльний аналіз протоколів JDSS, MQTT та DDS щодо їх використання для побудови автоматизованих систем управління з активним переміщенням користувачів низової ланки управління в низькошвидкісних мережах зв'язку на базі УКХ радіостанцій. Проведено аналіз можливості забезпечення автентифікації, шифрування, захисту даних, стискання даних та реалізації контролю доступу протоколів JDSS, MQTT та DDS.*

Ключові слова: *порівняльний аналіз, АСУ, JDSS, MQTT, DDS, УКХ, низькошвидкісні канали зв'язку.*

Вступ

Розвиток технологій стало поштовхом для створення та реалізації цифрових автоматизованих систем управління (АСУ). Сучасні АСУ широко використовуються при управлінні підприємствами, виробництвом, суспільними організаціями та в державному управлінні. Актуальною задачею в області АСУ є пошук рішень взаємодії та передачі інформації між вузлами системи [1–4]. В даній роботі розглядаються АСУ державного рівня низової ланки управління з активним переміщенням користувачів. Такі системи, в основному, працюють у мережах зв'язку на базі ультракоротко-хвильових (УКХ) радіостанцій [1,5]. Технології передачі інформації в таких АСУ повинні відповідати низці вимог [1]:

- підвищені вимоги до надійності;
- масштабованість системи в процесі експлуатації;
- можливість роботи в низькошвидкісних мережах зв'язку;
- захищеність та живучість.

Отримані в роботі [5] характеристики QoS показують, що використання стандартних протоколів для передачі даних в УКХ радіомережах неможливо через низьку швидкість та велику затримку передачі даних, великий джитер затримки передачі даних, велику ймовірність втрати даних в каналі. Для таких каналів зв'язку було створено ряд протоколів, одним з яких є протокол JDSS стандарту STANAG 4677 [6], який розроблено для обміну інформацією в низькошвидкісних мережах зв'язку в тактичній ланці управління військами при сумісних операціях різних країн НАТО. За допомогою цього стандарту можливо передавати текстові повідомлення, графічні позначки об'єктів на карті, геометричні зображення (точка, лінія, полігон), цілевказівки, спеціальні повідомлення радіаційної, біологічної та хімічної обстановки та медичної евакуації тощо.

В мережах Internet of Things (IoT) для реалізації технологій передачі інформації широко застосовуються алгоритми та протоколи моделі «publish-subscribe» [3; 7; 8]. Найпоширенішим прикладом

реалізації моделі «publish-subscribe» є протоколи Message Queuing Telemetry Transport (MQTT) [7] та Data Distribution Service (DDS) [8]. MQTT представляє собою відкритий та простий протокол, який має три варіанти реалізації QoS та застосовується в основному при «машино-машинній» взаємодії та в мережах IoT [3; 8]. DDS же навпаки більш складний протокол, який на сьогоднішній день має статус стандарту НАТО і широко застосовується при створенні державних автоматизованих систем управління [8]. Реалізації протоколів MQTT та DDS передбачають їх використання в низькошвидкісних мережах зв'язку.

В роботі [1] було проведено моделювання та аналіз протоколів JDSS, NFFI стандарту STANAG 4677 та отримано показники трафіку щодо цих протоколів. В роботі [3] було проведено моделювання та аналіз протоколів MQTT, MQTT-SN, DDS, визначено можливість їх використання в АСУ державного рівня низової ланки управління з активним переміщенням користувачів та отримано показники трафіку щодо цих протоколів. На основі проведених досліджень [1, 3, 5] протокол JDSS стандарту STANAG 4677 та протоколи шаблону «publish-subscribe» можливо використовувати в низькошвидкісних мережах зв'язку, які мають свої недоліки та переваги. Метою роботи є порівняльний аналіз протоколів передачі даних JDSS, MQTT та DDS в низькошвидкісних мережах зв'язку на базі УКХ радіостанцій щодо забезпечення максимальної кількості користувачів, автентифікації, шифрування, захисту даних, стискання даних, реалізації контролю доступу та визначення архітектури цих протоколів.

Порівняльний аналіз протоколів JDSS, MQTT, DDS

Метою створення стандарту STANAG 4677 є організація взаємодії військ різних країн НАТО для підвищення ситуаційної обізнаності на полі бою шляхом обміну тактичною інформацією між різними групами військ в низькошвидкісних каналах зв'язку на базі УКХ радіостанцій. Основним об'єктом застосування цього стандарту є система спішеного солдата в тактичній ланці управління.

Інформація, яка поступає від АСУ, трансформується в Joint Dismounted Soldier System Data Model (JDSSDM). Моделі даних JDSSDM описуються мовою XML, теги та структура якого чітко прописані у стандарті STANAG 4677 відповідно до типу повідомлення. JDSSDM інкапсулюються ще в одну структуру даних Joint Dismounted Soldier Information Exchange Mechanism (JDSSIEM). JDSSIEM реалізує механізм гарантованого обміну інформацією в мережі JDSS. Цей механізм призначений для використання в broadcast і multicast системах зв'язку. Тобто пакети, які відправляються у IP-мережу використовують мультикасні IP адреси. Рішення цього стандарту зображено на рис. 1 [6].

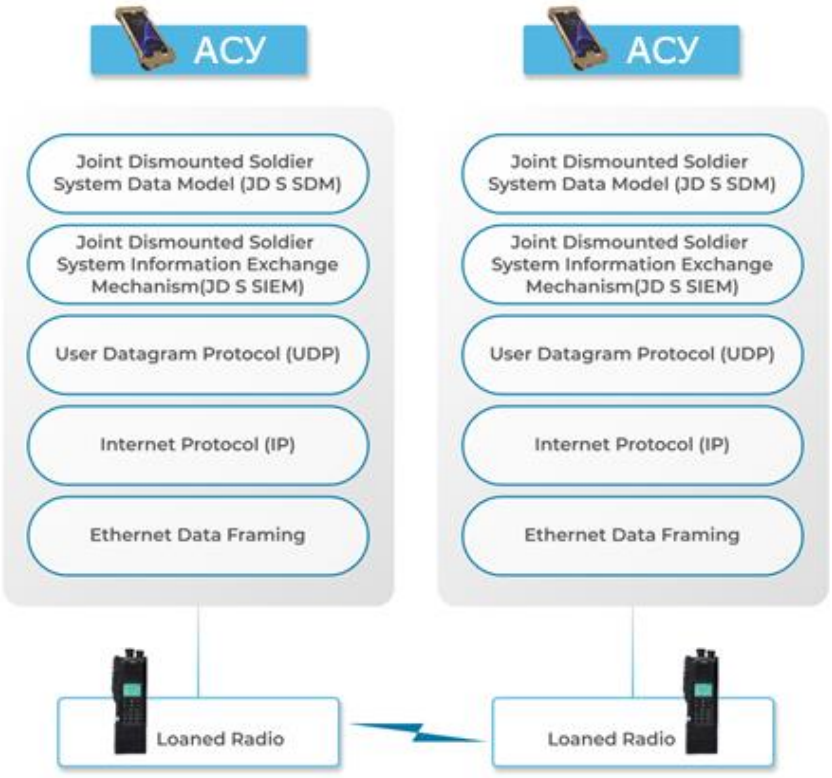

Рис. 1. Структура стадарту STANAG 4677

Передача даних відбувається за допомогою стандартного протоколу UDP та IP в мультикастній мережі зв'язку. JDSSDM використовується як XML повідомлення. NATO Friendly Force Information (NFFI) – це 16-байтовий бінарний заголовок, який використовується для маркування даних при їх фрагментації, для адресації даних між різними АСУ, вказує на наявність стискання даних та алгоритм стискання, а також вказані пріоритети пакетів. JDSSIEM представляє собою, як і JDSSDM, XML повідомлення, відповідає за синхронізацію пропущених повідомленнь та стискання даних. Стек протоколів STANAG 4677 показано на рис.2[6].

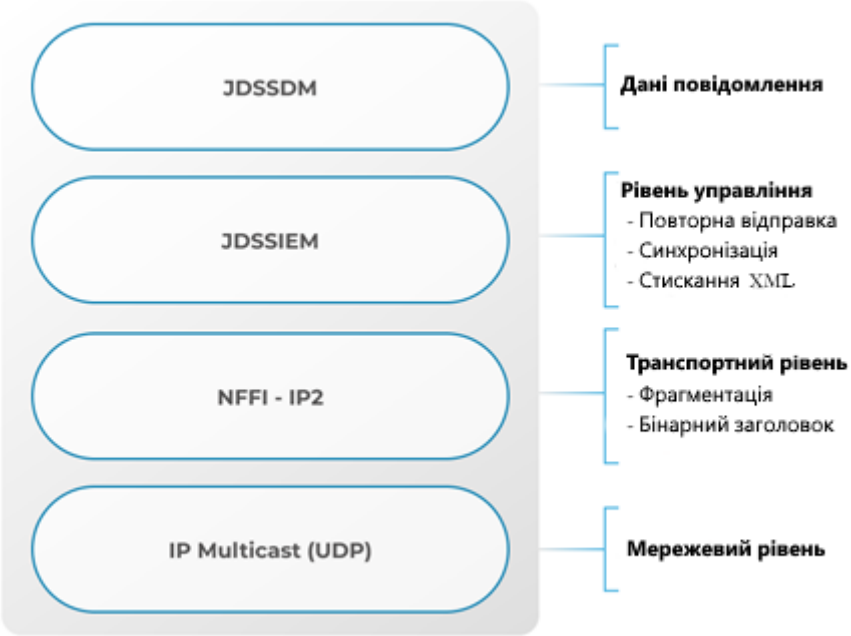

Рис. 2. Стек протоколів STANAG 4677

Механізм гарантованої передачі даних в стандарті STANAG 4677 має унікальну властивість, адже на відміну від стандартних протоколів стеку TCP/IP JDSS використовує спеціальний механізм синхронізації пропущених повідомлень. Для реалізації цього механізму використовується декілька службових повідомлень: "HeartBeat", "MessageSyncRequest", "MessageSyncReply", "FullSyncRequest", "FullSyncReply".

Повідомлення "HeartBeat" відправляється кожним шлюзом JDSS через однакові інтервали часу (зазвичай 60 секунд), в якому вказується кількість надісланих повідомлень кожної категорії цим вузлом. Інші шлюзи JDSS при отриманні цього повідомлення перевіряють це значення з фактично прийнятою кількістю повідомлень від цього шлюза. В залежності від кількості пропущених повідомлень будуть відправлятись "MessageSyncRequest" для запиту одиничних повідомлень або "FullSyncRequest" для запиту усіх актуальних даних. У відповідь будуть надсилатись "MessageSyncReply" та "FullSyncReply" відповідно до запиту. При чому, якщо запит відправляється на адресу певного шлюзу, то відповідь адресується на всі вузли мультикастним пакетом для запобігання повторних запитів та можливих втрат інших вузлів. Окрім цього, необхідно зазначити, що не усі повідомлення повторно перезапрошуються, так як інформація в деяких повідомленнях застаріває швидше одного інтервалу відправки "HeartBeat". До повідомлень, що не перезапрошуються відносяться: "PresenceMsg", "HeartBeat, "MessageSyncRequest", "MessageSyncReply", "FullSyncRequest", "FullSyncReply".

Необхідно зазначити, що для зменшення навантаження на мережу зв'язку та отримання лише актуальної інформації стандарт передбачає максимальну кількість повідомлень для кожного типу моделі даних, які можливо запросити повторно. На основі проведеного аналізу можна виділити основні аспекти стандарту STANAG 4677:

1. Протокол JDSS представляє собою моделі даних для різних повідомлень – JDSSDM та механізму передачі цих повідомлень – JDSSIEM.
2. Протокол NFFI використовується як бінарний заголовок та відповідає за фрагментацію, адресацію та вказує на стискання даних.

3. Стандарт STANAG 4677 створено для організації взаємодії існуючих цифрових АСУ країн НАТО.

4. Кожне повідомлення відправляється у мультикастну групу, що дозволяє отримати дані декільком абонентам одночасно.

5. Стандарт створено спеціально для прийому та відправки даних в низькошвидкісних радіомережах зв'язку.

6. Механізм інформаційного обміну JDSS використовує синхронізацію повідомлень на відміну від стандартних квитувань на запити.

Протокол MQTT створювався для організації взаємодії в мережах з низькою пропускною здатністю, недетермінованою затримкою передачі даних та нестабільним каналом зв'язку. Простота цього протоколу дозволила на сьогоднішній день використовувати його для передачі інформації між пристроями з обмеженою потужністю процесора та часом автономної роботи. Реалізація протоколу MQTT передбачає використання централізованого підходу до мережевої топології. Система зв'язку, яка побудована на основі MQTT, складається з «видавця», «брокеру» та «підписника». «Видавець» не потребує налаштувань по кількості чи місцезнаходженню своїх «підписників», а лише відправляє повідомлення за необхідними «темами». «Підписники» також не потребують налаштувань на конкретних «видавців», вони лише повідомляють «брокеру» за якими темами хочуть отримувати повідомлення. Брокер представляє собою центральний вузол MQTT, який забезпечує взаємодію між «видавцями» і «підписниками». Обмін даними між клієнтами відбувається тільки через брокера. Його основними задачами є отримання даних від клієнтів, обробка та контроль за доставкою повідомлень. Кількість «підписників», «видавців» та «брокерів» у мережі необмежена. Архітектура протоколу MQTT показана на рис.3[7].

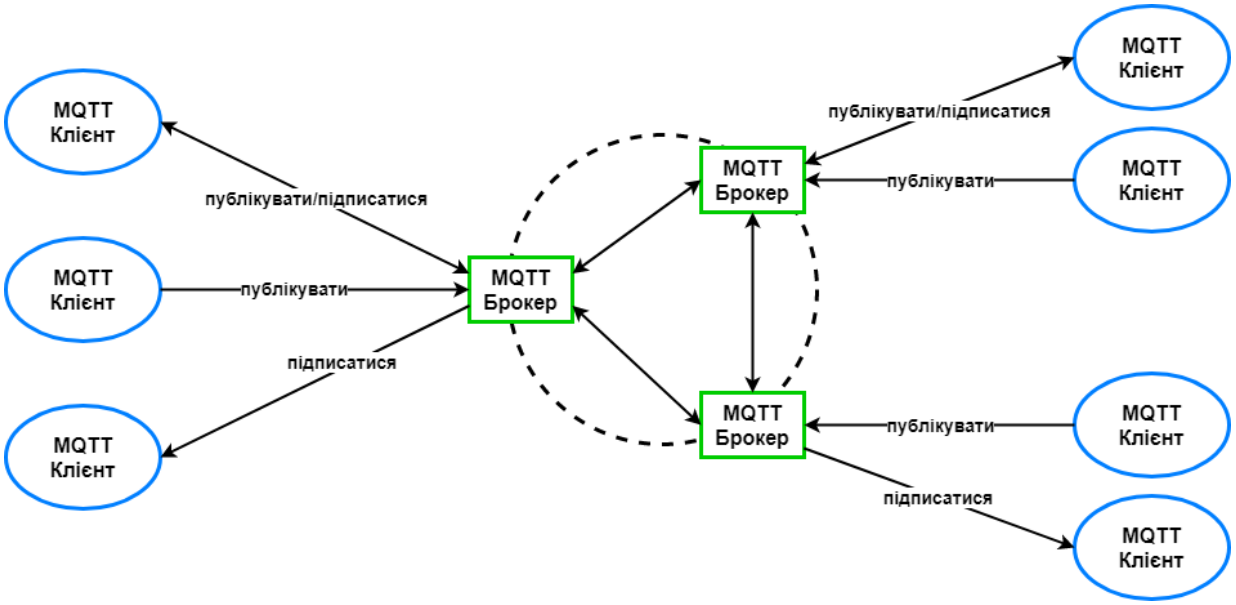

Рис. 3. Архітектура протоколу MQTT

Протокол MQTT займає 7-ий рівень в моделі OSI та в якості транспортного протоколу використовує TCP/IP. Протоколи MQTT підтримують три рівні QoS [7]: рівень 0 (At most once delivery), рівень 1 (At least once delivery), рівень 2 (Exactly once delivery). Протокол MQTT підтримує автентифікацію користувачів та надає спеціальні поля для відправки ім'я користувача та паролю в службовому повідомленні. Протокол MQTT не підтримують жодних алгоритмів та механізмів організації контролю доступу [3; 7]. Деякі реалізації брокеру протоколу MQTT, наприклад Mosquitto, дозволяють не тільки авторизувати користувачів, а й формувати Access Control List (ACL) для розмежування доступу користувачів до публікацій та підписок в різних темах. Перевірка цілісності даних не передбачено.

Протокол DDS – це протокол для передачі інформації за допомогою моделі «видавець-підписник», який орієнтоване на дані та призначене для високо динамічних розподілених систем. Він стандартизований Object Management Group (OMG). Повідомлення публікуються в домені DDS, а інформаційний пакет описує структуру даних, відправника та отримувача інформації. Клієнти можуть публікувати

та отримувати повідомлення лише в своєму домені та мають свої сертифікати для авторизації. Протокол DDS є одним із багатьох протоколів, що використовуються в таких галузях промисловості, як залізничні мережі, управління повітряним рухом, інтелектуальна енергетика, медичне обслуговування, військова, аерокосмічна промисловість та промислова автоматизація [3; 8].

Передача даних в протоколі DDS здійснюється за допомогою транспортного фреймворку, який підтримує одразу декілька протоколів передачі: TCP, UDP unicast, UDP multicast, shared memory та Real-time Publish-Subscribe (RTPS) wire protocol. DDS, на відміну від MQTT, підтримує як централізовану топологію побудови системи зв'язку, так і децентралізовану.

Централізований підхід будується за допомогою «Information Repository», який представляє собою сервер з інформацією про клієнтів домену, але не бере участі в передачі даних. Принцип взаємодії програмного забезпечення за допомогою вищевказаного підходу показано на рис.4.

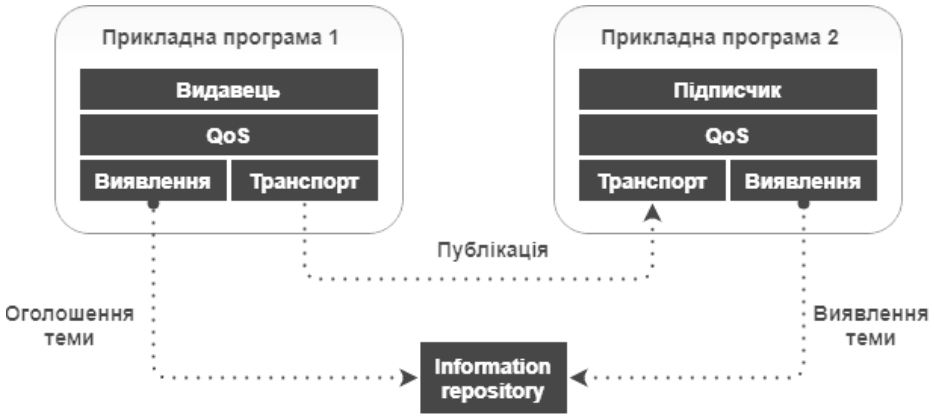

Рис. 4. Централізована взаємодія прикладних програм з DDS

Таким чином, «Information Repository» отримує від «видавців» та «підписників» назви тем, на які вони публікуються та підписуються відповідно. Передача даних відбувається безпосередньо між «видавцем» і «підписником». Окрім того, клієнти DDS можуть виступати «видавцем» і «підписником» одночасно.

Децентралізований підхід передбачає, що «підписники» та «видавці» виявляють один одного за допомогою протоколу RTPS (рис.5). Тобто кожен «видавець» виявляє сам своїх «підписників» та зберігає інформацію про них.

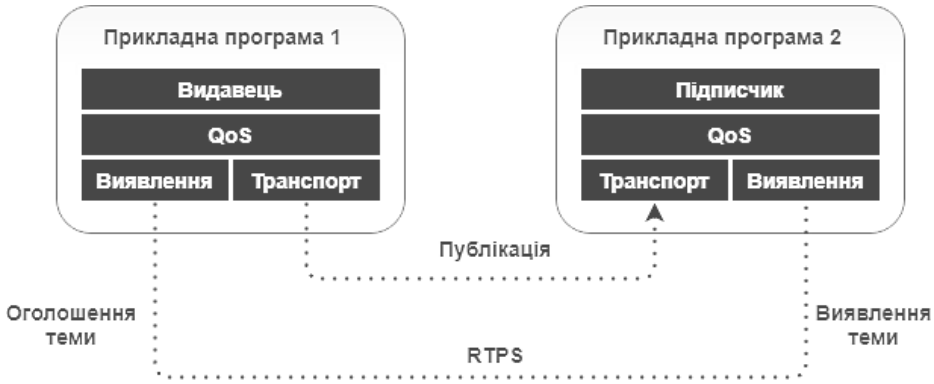

Рис. 5. Децентралізована взаємодія прикладних програм з DDS

Передача повідомлень може здійснюватись за допомогою мережевих протоколів TCP, UDP та на основі shared memory. На відміну від MQTT, DDS може передавати дані за допомогою одноадресної та багатоадресної адресацій. Протокол DDS має 22 можливі політики QoS. Дані політики можуть призначатися відповідно теми, «підписника» та «видавця». Політики QoS розподіляються за наступними критеріями: проміжок часу, між якими передаються службові повідомлення; кількість доступних ресурсів для роботи програмного забезпечення; необхідність та час на підтвердження отримання повідомлень; час на відправку повідомлень; пріоритети типів транспортних протоколів; максимально можлива затримка; гарантована доставка повідомлень; максимально допустима кількість повідомлень для повторного

перезапиту; необхідність зберігання повідомлень. Протокол DDS, на відміну від протоколів MQTT, підтримує модель безпеки (Security Model) для реалізації механізмів захисту та шифрування інформації, авторизації користувачів та розмежування прав доступу [3; 8]. Модель безпеки (Security Model) визначає принципи безпеки користувачів системи, об'єкти, які захищаються, і операції з об'єктами, які мають бути обмежені. Модель безпеки (Security Model) протоколу DDS реалізує наступні функції: конфіденційність даних, цілісність даних і повідомлень, автентифікація, авторизація підписників і видавців, автентифікація повідомлень та даних. Результати аналізу протоколів JDSS, MQTT, DDS представлено в табл.1.

Таблиця 1

Результати аналізу протоколів JDSS, MQTT та DDS

Параметр	JDSS	MQTT	DDS
Архітектура	Децентралізована	Централізована	Децентралізована та централізована
Кількість користувачів	Необмежено	Необмежено	Необмежено
Автентифікація	Присутня	Присутня	Присутня
Захист даних	Присутнє (Loaned Radio)	Відсутнє	Присутнє
Шифрування	Присутнє (Loaned Radio)	Присутнє	Присутнє
Стискання даних	Присутнє	Відсутнє	Присутнє
Контроль доступу	Присутнє	Відсутнє	Присутнє

Побудова АСУ в низькошвидкісних каналах зв'язку на базі УКХ радіостанцій неможлива з використанням централізованої архітектури, так як такий підхід збільшить навантаження на центральний вузол мережі, що призведе до ще більшої втрати пакетів та збільшення затримки передачі даних [1-5]. А для виконання вимог щодо надійності та захищеності АСУ, протоколи передачі даних повинні підтримувати автентифікацію, захист даних, шифрування, стискання даних та реалізація контроль доступу. Таким чином, для побудови АСУ низової ланки управління з активним переміщенням користувачів в низькошвидкісних мережах зв'язку на базі УКХ радіостанцій доцільно використовувати протоколи JDSS та DDS. Згідно [1; 3; 5] отримано, що протокол DDS має надлишковість передачі службових даних та пакетів в порівнянні з протоколами MQTT та JDSS. Надлишковість службових даних призведе до зменшення пропускної здатності низькошвидкісних каналів зв'язку та збільшення ймовірності відмов на обслуговування. Таким чином, для побудови АСУ в низькошвидкісних мережах зв'язку раціонально використовувати протокол JDSS в порівнянні з протоколами MQTT та DDS.

Висновки

1. Проведено аналіз можливості використання протоколів JDSS, MQTT та DDS в АСУ державного рівня низової ланки управління з активним переміщенням користувачів в низькошвидкісних каналах звязку на базі УКХ радіостанцій.

2. Проведено порівняльний аналіз протоколів передачі даних JDSS, MQTT та DDS щодо забезпечення максимальної кількості користувачів, автентифікації, шифрування, захисту даних, стискання даних, реалізації контролю доступу та визначено архітектуру цих протоколів.

3. Визначено, що для побудови АСУ в низькошвидкісних мережах зв'язку доцільно використовувати протокол JDSS ніж протоколами MQTT та DDS.

ЛІТЕРАТУРА

1. Strelkovskaya I.V. Modeling of telecommunication components of automated control systems in low-bandwidth radio networks / I.V. Strelkovskaya, R.V. Zolotukhin, A.O. Makoganiuk. In: P. Vorobiyenko, M. Ilchenko, I. Strelkovska. Current Trends in Communication and Information Technologies. Lecture Notes in Networks and Systems, 2021,. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-76343-5_9.

2. Strelkovskaya I. Comparative analysis of file transfer protocols in low-bandwidth radionetworks / I.Strelkovskaya, R. Zolotukhin, J.Strelkovska. ICAIIT-2021, Vol. 9, Is. 1, Koethen, Germany, March, 16, 2017. *Anhalt University of Applied Sciences*. P. 27–32.

3. Strelkovskaya I.V., Zolotukhin R.V., (2022) Research of Automated Control Systems Development Based on "Publish-Subscribe" Technology Over Low-bandwidth Radio Networks (до друку).

4. Strelkovskaya I., Solovskaya I., Makoganiuk A., «Optimization of QoS chracteristics of self-similar traffic», 2017 4th PICS&T 2017, pp. 497–500. DOI: https://doi.org/10.1109/INFOCOMMST.2017.8246447.

5. Strelkovskaya I., Zolotukhin R., “Research of low-bandwidth radionetworks QoS parameters” in Information and Telecommunication Sciences, *International Research Journal*, Volume 11, Number 1(20), January-June 2020, DOI: https://doi.org/10.20535/2411-2976.12020.77-81.

6. STANAG 4677: 2014 Dismounted soldier systems standards and protocols for command, control, communications and computers (C4) interoperability / NATO 2014.

7. MQTT Version 3.1.1. Edited by A. Banks and R. Gupta. 2014. OASIS Standard.

8. OMG Data Distribution Service (DDS) Version 1.4. April 2015.

I. Strelkovskaya, R. Zolotukhin, T. Grigorieva. Comparative analysis of data transmission protocols of automated control systems in low-bandwidth communication networks. – Article.

Summary. *The organization of interaction and transmission of information between system nodes is a critical task, when creating automated control systems in low- bandwidth communication networks. In IoT networks, publish-subscribe algorithms and protocols are widely used for data exchange in low-bandwidth networks. The JDSS protocol of the STANAG 4677 standard was created for work in networks that basis on UHF\VHF radios. The paper presents comparative analysis of JDSS, MQTT and DDS protocols for construction of the automated control systems based on UHF\VHF radio stations. The analysis of the possibility to providing authentication, encryption, data protection, data compression and implementation of access control is carried out.*

Key words: *comparative analysis, ACS, JDSS, MQTT, DDS, UHF\VHF, low-bandwidth communication channels.*

И. В. Стрелковская, Р. В. Золотухин, Т. И. Григорьева. Сравнительный анализ протоколов передачи данных автоматизированных систем управления в низкоскоростных сетях связи. – Статья.

Аннотация. *При создании автоматизированных систем управления в низкоскоростных сетях связи критически важной задачей является организация взаимодействия и передачи информации между узлами системы. В сетях IoT для обмена данными в низкоскоростных сетях широко применяются алгоритмы и протоколы технологии publish-subscribe. Для работы в сетях на базе УКВ радиостанций был создан протокол JDSS стандарта STANAG 4677. В работе проведен сравнительный анализ протоколов JDSS, MQTT и DDS по их использованию для построения автоматизированных систем управления с активным перемещением пользователей низового звена управления в низкоскоростных сетях связи на базе УКВ радиостанций. Проведен анализ возможности обеспечения проверки подлинности, шифрования, защиты данных, сжатия данных и реализации контроля доступа протоколов JDSS, MQTT и DDS.*

Ключові слова: *сравнительный анализ, АСУ, JDSS, MQTT, DDS, УКХ, низкоскоростные каналы связи.*

УДК 621.39:519.65

І. В. Стрелковська
доктор технічних наук, професор,
декан факультету кібербезпеки, програмної інженерії та комп’ютерних наук
Міжнародний гуманітарний університет
м. Одеса, Україна

І. М. Соловська
кандидат технічних наук, доцент,
звідувачка кафедри комп’ютерних наук
Міжнародний гуманітарний університет,
м. Одеса, Україна

IPS-ПОЗИЦІОНУВАННЯ В МЕРЕЖАХ РАДІОДОСТУПУ WI-FI НА БАЗІ КОМПЛЕКСНИХ ПЛОСКИХ СПЛАЙНІВ

Анотація. *Розглянуто основні методи IPS-позиціонування користувачів в мережах радіодоступу Wi-Fi, які засновано на різних принципах функціонування. Для позиціонування користувача запропоновано використання комплексних плоских сплайнів. Показано побудову комплексних плоских лінійних сплайнів. Встановлено, що використання комплексних плоских лінійних сплайнів дозволяє підвищити точність позиціонування.*

Ключові слова: *IPS-позиціонування, мережа радіодоступу Wi-Fi, комплексний плоский лінійний сплайн, похибка позиціонування.*