УДК 621.391

О.П. Трухан, Ю.Б. Паляниця, канд. техн. наук, доцент
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

МАТЕМАТИЧНА МОДЕЛЬ КЛЮЧІВ ШИФРУВАННЯ В МЕРЕЖАХ TETRA ДЛЯ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

O.P. Truhan, Y.B. Palaniza, PhD.

MATHEMATICAL MODEL OF ENCRYPTION KEYS IN TETRA NETWORKS FOR TELECOMMUNICATION SYSTEMS

У даній роботі досліджується методика впровадження математичної моделі ключів шифрування для забезпечення безпеки зв’язку в мережах TETRA. Зокрема, реалізується наскрізне шифрування (E2EE) з використанням механізму Over The Air Keying (OTAK), що дозволяє автоматизувати розподіл ключів без фізичного доступу до пристроїв. У межах проекту здійснено системне тестування, виявлення дефектів, а також оптимізацію параметрів передачі ключів у середовищі з високим навантаженням.

Запропоноване рішення найбільш оптимально інтегрується з системами, що використовують стандарт GMR (GEO Mobile Radio Interface). Воно може бути застосоване в мережах із геостаціонарними супутниками (GEO), що оперують у Ku- та Ka-діапазонах, оскільки вони забезпечують високу пропускну здатність для сигналізації OTAK.

Також система може працювати з іншими телекомунікаційними стандартами, наприклад, DVB-S2X для широкомовлення та VSAT для фіксованого зв’язку, що дозволяє адаптувати рішення до спеціалізованих потреб, таких як навігаційні системи або віддалені мережі.

Модуляції та методи передачі

Для забезпечення стійкості передачі використовуються сучасні схеми модуляції:

QPSK (Quadrature Phase Shift Keying) для базової надійності;

8PSK (8 Phase Shift Keying) для підвищеної пропускної здатності;

OFDM (Orthogonal Frequency Division Multiplexing) для зменшення інтерференції між каналами.

Для підвищення точності та надійності передачі даних у телекомунікаційних мережах з шумами можуть бути використані методи синфазного виявлення радіосигналів, що базуються на спеціалізованих алгоритмах та комп'ютерних інструментах [4].

Результати дослідження

Створено математичну модель розподілу ключів у мережах TETRA.

Виявлено та усунено понад 10 критичних дефектів у процесі інтеграції рішення OTAK.

Збільшено ефективність передачі ключів, що дозволило масштабувати мережу до тисяч активних користувачів.

Результати свідчать про доцільність впровадження механізму OTAK для захищеного зв’язку у великих мережах.

Література

1. Stallings, W., Brown, L. Computer Security: Principles and Practice. Pearson Education, 2008.
2. Airbus Defence and Space. Security features in TETRA systems. 2015.
3. ETSI. TETRA standardization documentation. 2016.
4. https://scholar.google.com.ua/citations?view_op=view_citation&hl=uk&user=_80WiBwAAAAJ&citation_for_view=_80WiBwAAAAJ:SeFeTyx0c_EC