УДК 004.7

Корнійчук В.В., здобувач
Державний університет «Житомирська політехніка»

ПРОБЛЕМИ ТА МЕТОДИ ПРОЄКТУВАННЯ МЕРЕЖЕВИХ ПРОТОКОЛІВ

У сучасних комп'ютерних мережах питання безпечного обміну даними набуває особливої актуальності у зв'язку зі зростанням обсягів інформації, кількості мережевих загроз та вимог до продуктивності мережевих систем. Оскільки основним призначенням комп'ютерних мереж є передача даних, потрібно визначитись, як будуть надсилатися ці дані між користувачами, враховуючи певні обмеження у плані швидкості та надійності. Для цього існує мережевий протокол – набір правил про те, як повідомлення та дані будуть формуватися та оброблятися[1]. Існуючі стандартизовані мережеві протоколи не завжди відповідають вимогам спеціалізованих клієнт-серверних чи однорангових систем, що обумовлює необхідність дослідження альтернативних підходів до проєктування захищених мережевих протоколів.

Питання безпеки мережевого обміну даними широко висвітлюється у наукових дослідженнях та практичних реалізаціях, зокрема в межах протоколів транспортного рівня стеку TCP/IP[3]. Проте більшість наявних рішень орієнтовані на універсальне застосування і не завжди оптимальні для систем із підвищеними вимогами до затримок, масштабованості, контролю над протокольною логікою та насамперед – швидкості[2]. У практиці розробки програмного забезпечення часто виникає потреба створення власних протоколів, що зумовлює необхідність глибшого наукового обґрунтування принципів їх захисту та оптимізації[3].

Мета дослідження полягає у застосуванні системного підходу до проєктування захищеного мережевого протоколу, який поєднує сучасні криптографічні механізми з оптимізованими схемами обміну даними. У межах роботи обґрунтовано доцільність вибору легковагових механізмів захисту та структурної організації протоколу з урахуванням вимог сумісності, надійності та продуктивності. Зроблено висновок, що раціональне поєднання засобів захисту та архітектурних рішень дозволяє зменшити негативний вплив безпеки на швидкодію мережевого обміну.

У результаті дослідження запропоновано архітектуру захищеного мережевого протоколу для обміну даними, що забезпечує

автентифікацію, конфіденційність, продуктивність у мережі та контроль цілісності інформації. Також представлено можливість налаштування передачі даних перед формуванням протоколу під час виконання та власну реалізацію фрагментації протоколу для більшої передачі даних (2048 кб).

Отримані результати мають практичне значення для розробки клієнт-серверних систем, мережевих сервісів та спеціалізованих програмних рішень, які потребують безпечного та продуктивного обміну даними, насамперед в програмах та системах реального часу. Подальші дослідження у цьому напрямі дозволять розробити ефективні архітектурні рішення, здатні забезпечити безпечний та продуктивний обмін даними в сучасних комп’ютерних мережах.

Список використаних джерел

1. Б.Ю. Жураковський, І.О. Зенів, «РОЗРОБКА ТА РЕАЛІЗАЦІЯ МЕРЕЖНИХ ПРОТОКОЛІВ НАВЧАЛЬНИЙ ПОСІБНИК», Київ: КПІ ім. Ігоря Сікорського, 2020 – 462 с.

2. Andrew Tanenbaum, David Wetherall, «Computer Networks 5th edition», New Jersey, 2012 – 960 с.

3. Douglas E. Comer, «Internetworking With TCP/IP Vol I: Principles, Protocols, and Architecture Sixth Edition», 2013 – 733 с.