УДК 621.396

М. В. ВАСИЛЬКІВСЬКИЙ
В. К. СКОЩУК

ЗАХИСТ ІНФОРМАЦІЇ В МУЛЬТИСЕРВІСНИХ МЕРЕЖАХ ЗВ'ЯЗКУ

Вінницький національний технічний університет

Анотація

Виконано дослідження нових методів маршрутизації, здатних вирішувати завдання захисту інформації з підтримкою QoS додатків мультисервісної мережі зв'язку.

Ключові слова: *мультисервісні мережі, захист інформації, QoS додатки.*

Abstract

New routing methods capable of solving information security tasks with support of QoS applications of multiservice communication network have been performed.

Keywords: *multiservice networks, information security, QoS applications.*

Вступ

В останнє десятиліття ведуться активні дослідження можливості забезпечення конфіденційності інформації в мобільних мережах за рахунок механізмів мережевого рівня моделі взаємозв'язку відкритих систем [2, 4]. Даний підхід має ряд переваг. По-перше, чим масштабніше мережа зв'язку, тим більше її ресурсів можна задіяти для забезпечення конфіденційності інформації користувачів. По-друге, користувач не обов'язково повинен мати додаткове спеціальне програмно-апаратне забезпечення.

Використання територіально-розподілених ресурсів мультисервісної мережі зв’язку ММЗ (баз даних, криптографічних програмно-апаратних комплексів, каналів зв'язку і так далі) є одним із шляхів забезпечення цілісності, доступності та конфіденційності інформації. В цьому випадку користувачеві досить визначити свій профіль захисту інформації – кількісні або якісні оцінки параметрів інформаційної безпеки. Система управління, провівши моніторинг вільних ресурсів ММЗ, реалізує не тільки з'єднання, що підтримує QoS для обраної програми, але і заявлений користувачем профіль захисту інформації.

Наукова проблема, вирішенню якої присвячена ця робота полягає в дослідженні застосування технологій мережевого рівня (протоколів маршрутизації і сигналізації) ММЗ для захисту інформації.

Актуальність даної проблематики підтверджується тим фактом, що вона зачіпає технології, які мають важливе соціально-економічне значення та важливе значення для оборони країни і безпеки держави.

Основна частина

Базовими параметрами захисту інформації прийнято вважати конфіденційність, цілісність і доступність.

Гібридна система шифрування (асиметричні алгоритми використовуються для організації закритого каналу зв'язку, а симетричні безпосередньо для шифрування інформації) є цілком прийнятною для ММЗ. Для користувачів є можливість скористатися високошвидкісними додатками, що функціонують в реальному масштабі часу з забезпеченням конфіденційності.

Недоліки гібридної системи шифрування: користувачі повинні володіти знаннями в області захисту інформації; мати в своєму розпорядженні спеціальне криптографічне програмно-апаратне забезпечення.

Метод багатолінійної маршрутизації з пороговою схемою поділу повідомлення дозволяє забезпечити конфіденційність інформації, збільшити пропускну здатність мережі, зменшити ризик

перевантажень мережі, що позитивно впливає на QoS додатків ММЗ.

Недоліком використання методу багатоколійної маршрутизації з пороговою схемою поділу повідомлення є чутливість до модифікації частин секретного повідомлення і необхідність організації незалежних маршрутів, що володіють однаковими ймовірнісно-часовими характеристиками (швидкість передачі інформації, час затримки, ймовірність помилкового прийому на пакет).

На рисунку 1 наведені основні підходи, що забезпечують цілісність інформації – криптографічні методи з дублюванням інформації та методи, які використовують резервування інформації.

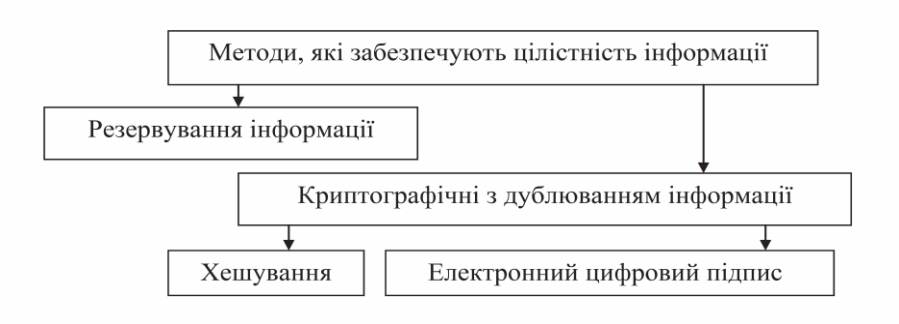

Рисунок 1 – Основні методи забезпечення цілісності інформації в телекомунікаційних системах

Криптографічний метод (змішування, електронний цифровий підпис) [3] полягає у введенні в передане повідомлення надлишковості – перевірочної комбінації, яка обчислюється за певними алгоритмами і є «індикатором» порушення цілісності інформації.

В результаті можна зробити висновок, що криптографічний метод тільки контролює цілісність інформації. У разі її модифікації джерелу необхідно зробити повторну передачу повідомлення. Дана процедура буде повторюватися до тих пір, поки цілісність інформації не буде забезпечена. І тут між віддаленими користувачами необхідно організувати канал зворотного зв'язку [4] і канал для повторної передачі повідомлення, тобто виконати багаторазове дублювання інформації, що значно впливає на час затримки. Таким чином, застосування в ММЗ криптографічного методу з дублюванням інформації з метою забезпечення цілісності обмежено для високошвидкісних додатків, що функціонують в реальному масштабі часу.

Метод резервування інформації для забезпечення цілісності полягає в одночасній паралельній передачі інформації по декількох маршрутах і прийняття рішення про цілісність інформації на приймальному боці [3]. Тим самим зменшується час затримки передачі інформації і забезпечується QoS високошвидкісних додатків, що функціонують в реальному масштабі часу.

Основними методами забезпечення доступності інформації є: дублювання інформації, до якої здійснюється доступ; резервування каналів зв'язку.

Таким чином, доступ до інформації зводиться до завдань забезпечення живучості та надійності мереж зв'язку [2].

Аналіз основних підходів щодо забезпечення базових параметрів захисту інформації (цілісність, доступність і конфіденційність) в ММЗ виявив такі проблеми.

1. Для забезпечення конфіденційності, доступності та цілісності інформації користувачі ММЗ повинні мати в своєму розпорядженні спеціалізоване актуальне програмно-апаратне забезпечення і володіти знаннями в області захисту інформації.

2. Обмежене застосування основних підходів захисту інформації в ММЗ. Це пов'язано зі збільшенням часу затримки передачі інформації, що є критичним для додатків мультисервісної мережі, що функціонують на великих швидкостях і в реальному масштабі часу.

Перераховані проблеми вирішуються за рахунок залучення ресурсів ММЗ (криптографічних, канальних та інших) під кожну заявку користувачів для передачі захищеної інформації. У зв'язку з цим виникає необхідність в розробці, дослідженні нових методів, способів і алгоритмів, що дозволяють вирішувати завдання забезпечення базових параметрів захисту інформації (цілісність, доступність і конфіденційність) з підтримкою QoS додатків ММЗ.

Висновки

Багаторазове асиметричне шифрування ключами меншої довжини забезпечує конфіденційність інформації при меншому часі її шифрування.

Паралельні з'єднання між вузлом-джерелом і вузлом-одержувачем, що враховують ймовірнісно-вартісні параметри, дозволяють за сукупністю паралельно прийнятих символів відновити передану інформацію, тим самим забезпечити її цілісність і зменшити час затримки передачі інформації (в порівнянні з відомими методами, які використовують контроль модифікації переданої інформації і запит на її повторну передачу).

Формування паралельних незалежних з'єднань відповідно до критерію вибору мережевих ресурсів, що враховує ймовірнісно-вартісні параметри з'єднань, забезпечує доступність і цілісність інформації в ММЗ.

Застосування методу інформаційного резервування і резервування елементів інфраструктури дозволяє забезпечити захист інформації з QoS.

Процедури, які беруть участь у моніторингу інфраструктури ММЗ, виборі оптимального маршруту і встановлення з'єднань, дозволяють забезпечити не тільки QoS додатків, але і необхідний рівень інформаційної безпеки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Новиков С. Н. Имитационное моделирование мультисервисной сети связи в условиях внешних, деструктивных воздействий / С. Н. Новиков, Д. А. Тахтараков // Современныеипроблемы телекоммуникаций : материалы Российской науч. - техн. конференции. - Новосибирск, 2015. – С. 602–608.

2. Новиков С. Н. Исследование влияния внешних деструктивных воздействий на элементы мультисервисной сети связи / С. Н. Новиков, С. А. Петров // Вестник СибГУТИ. – 2016. – № 1. – С. 108–117.

3. Новиков С. Н. Методология защиты пользовательской информации на основе технологий сетевого уровня мультисервисных сетей связи / С. Н. Новиков ; под ред. В. П. Шувалова. – М. : Горячая линия - Телеком, 2015. - 128 с.

4. Шувалов В. П. Обеспечение показателей надежности телекоммуникационных систем и сетей / В. П. Шувалов, М. М. Егунов, Е. А. Минина. – М. : Горячая линия-Телеком, 2015. – 168 с.

Васильківський Микола Володимирович – канд. техн. наук, доцент кафедри телекомунікаційних систем та телебачення, Вінницький національний технічний університет, Вінниця, e-mail: mvasylkivskyi@gmail.com.

Скощук Валентин Костянтинович – студент групи ТКР-16б, факультет інфокомунікацій, радіоелектроніки та наносистем, Вінницький національний технічний університет, Вінниця, e-mail: skoschuk999@gmail.com.

Науковий керівник: ***Кононов Сергій Павлович –*** к.т.н., доцент кафедри телекомунікаційних систем та телебачення, Вінницький національний технічний університет, Вінниця, e-mail: knnvknnv@ukr.net.

Vasylkivskyi Mikola V. – Phd, Assistant Professor of Telecommunication Systems and Television, Vinnytsia National Technical University, Vinnytsia, e-mail: mvasylkivskyi@gmail.com.

Skoshchuk Valentin K. – student of the TKR-16b group, Faculty of Infocommunications, Radioelectronics and Nanosystems, Vinnytsia National Technical University, Vinnytsia, e-mail: skoschuk999@gmail.com.

Supervisor: ***Kononov Sergiy P.*** – Phd, Assistant Professor of Telecommunication Systems and Television, Vinnytsia National Technical University, Vinnytsia, e-mail: knnvknnv@ukr.net.