DOI https://doi.org/10.36059/978-966-397-491-0-39

ПРОГРАМНА МОДЕЛЬ ТРАФІКУ СТАНДАРТУ STANAG-4677 В АВТОМАТИЗОВАНИХ СИСТЕМАХ УПРАВЛІННЯ

Стрелковська І. В.
доктор технічних наук, професор
Міжнародний гуманітарний університет
м. Одеса, Україна

Золотухін Р. В.
аспірант за спеціальністю 121 Інженерія програмного забезпечення
Міжнародний гуманітарний університет
м. Одеса, Україна

Стрелковська Ю. О.
кандидат юридичних наук, доцент
Вортінгський коледж
Вортінг, Велика Британія

Автоматизовані системи управління (АСУ) державного рівня низової ланки управління, що працюють у мережах зв'язку на базі ультракороткохвильових (УКХ) радіостанцій з активним переміщенням користувачів, широко використовують спеціалізований протокол JDSS стандарту STANAG 4677 [1, 2]. Протокол JDSS стандарту STANAG 4677 використовується в УКХ радіомережах з низькою швидкістю та великою затримкою передачі даних, великим джитером затримки передачі даних, великою ймовірністю втрати даних в радіоканалі [3].

В процесі планування мереж зв'язку для АСУ використовуються математичні та програмні моделі трафіку для оцінки якості обслуговування користувачів, але на сьогоднішній день відсутні моделі трафіку протоколу JDSS щодо розрахунку показників якості обслуговування в низькошвидкісних мереж зв'язку. В роботі [1] розроблено програмне забезпечення для моделювання телекомунікаційних компонентів АСУ державного рівня низової ланки управління з активним переміщенням користувачів з використання мови програмування C# та фреймворку .NET, отримано показники трафіку щодо стандарту STANAG 4677 та визначено, що щільність розподілу проміжку часу між моментами надходження пакетів на обслуговування відповідає розподілу Вейбула. В роботі [4] запропоновано алгоритм роботи імітаційного моделювання радіомереж АСУ з використанням недетермінованих генераторів випадкової величини «random_device» бібліотеки boost для генерації інтервалів між вимогами на обслуговування.

Метою роботи є реалізація програмної моделі трафіку стандарту STANAG 4677 в автоматизованих системах управління, що дозволить отримати показники функціонування низькошвидкісної радіомережі ще на проектування та планування системи зв'язку АСУ.

Відповідно до роботи [1] щільність розподілу проміжків часу між моментами надходження пакетів на обслуговування підпорядковується розподілу Вейбула:

$$f(x) = \frac{k}{\lambda}(\frac{x}{\lambda})^{k-1}e^{-(\frac{x}{\lambda})^k}, x \geq 0, \quad (1)$$

де k – параметр форми кривої,

λ – параметр масштабу,

x – проміжок часу між вимогами на обслуговування.

Функція розподілу Вейбула описується формулою [13, 14]:

$$F(x) = 1 - e^{-(\frac{x}{\lambda})^k}, x \geq 0. \quad (2)$$

Отримані в роботі [1] дані показують, що параметр форми кривої k ≈ 0,43, а параметр розподілу випадкової величини $\lambda \approx 0{,}34$. Використовуючи формули (1),(2) та параметри розподілу отримуємо:

$$f(x) \approx 0{,}68x^{-0{,}57}e^{-1{,}59x^{0{,}43}}, x \geq 0, \quad (3)$$

$$F(x) = 1 - e^{-1{,}59x^{0{,}43}}, x \geq 0. \quad (4)$$

Використовуючи формулу (3) та недетермінований генератор випадкової випадкової величини «random_device» бібліотеки boost можливо реалізувати програмну модель трафіку протоколу JDSS стандарту STANAG 4677. Реалізація генератору проміжків часу між моментами надходження пакетів на обслуговування на основі бібліотеки boost передбачає використання мови програмування C++. В якості фреймворку застосуємо QT Creator версії 15.0.0. Використаємо програмний код, що показано на рис.1, в результаті отримуємо генератор випадкових проміжків часу, що підпорядковується розподілу Вейбула та має k ≈ 0,43 і $\lambda \approx 0{,}34$.

```cpp
#include "mainwindow.h"
#include "ui_mainwindow.h"
#include <boost/random.hpp>
#include <boost/random/normal_distribution.hpp>
#include <boost/random/weibull_distribution.hpp>
#include <boost/random/random_device.hpp>

MainWindow::MainWindow(QWidget *parent): QMainWindow(parent), ui(new Ui::MainWindow)
{
    ui->setupUi(this);
    QVector<double> quantity(32), relativeFrequency(32), histogramHeights(32),
        probabilityFunction(32), realFrequency(32), realProbabilityFunction(32), realQuantity(32), x(32);
    for(int i = 0; i < 32; i++){
        x[i] = 0.25*i;
    }
    int countOfCicles = 10000;
    double criteriaPirson = 0.0;
    boost::random_device rngDevice;
    boost::random::weibull_distribution<> weibullDist(0.43, 0.34);
    double mysumm = 0.0;
    for(int i = 0; i < countOfCicles; ++i)
    {
        double randomNumber = weibullDist(rngDevice);
        mysumm+=randomNumber;
        if(randomNumber < 7.75){
            quantity[int(randomNumber/0.25)]++;
        }else if (randomNumber <= 8.0){
            quantity[31]++;
        }
    }
    for(int i = 0; i < 32; i++){
        relativeFrequency[i] = quantity[i]/countOfCicles;
        histogramHeights[i] = relativeFrequency[i]/(x[1] - x[0]);
    }
    for(int i = 0; i < 32; i++){
        if(i == 0){
            probabilityFunction[i] = 0;
        }else{
            for(int j = 0; j < i; j++){
                probabilityFunction[i]+= relativeFrequency[j];
            }
        }
    }
    for(int i = 0; i < 32; i++){
        realProbabilityFunction[i] = 1 - exp(-1*pow(x[i]/0.34, 0.43));
    }
    for(int i = 0; i < 31; i++){
        realFrequency[i] = realProbabilityFunction[i+1] - realProbabilityFunction[i];
    }
    realFrequency[31] = 1 - exp(-1*pow(8.0/0.34, 0.43)) - realProbabilityFunction[31];
    for(int i = 0; i < 32; i++){
        realQuantity[i] = countOfCicles*realFrequency[i];
    }
    for(int i = 0; i < 32; i++){
        criteriaPirson+=pow(quantity[i]-realQuantity[i],2)/realQuantity[i];
```

Рис. 1. Лістинг програмного коду реалізації генератору проміжків часу

Використовуючи програмний код, що показано на рис.1, змоделюємо 10000 пакетів трафіку протоколу JDSS стандарту STANAG 4677. Побудуємо гістограму випадкової величини та графік функції розподілу випадкової величини (рис.2).

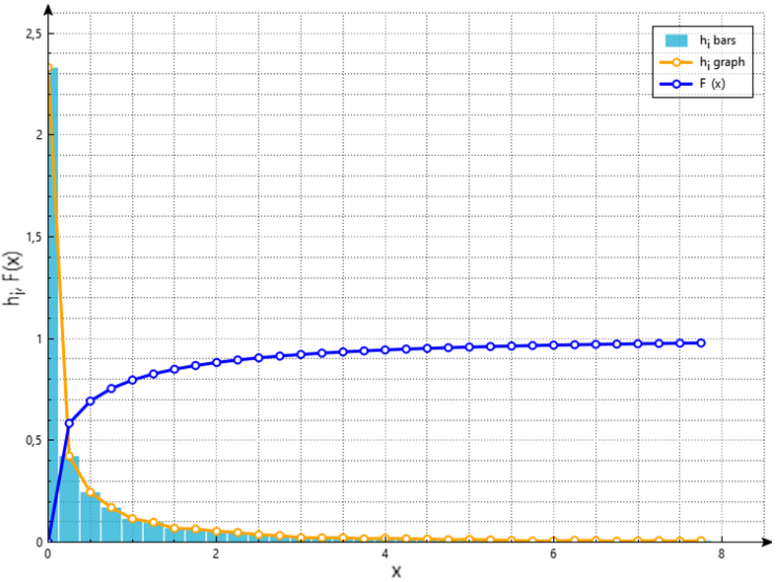

Рис. 2. Гістограма випадкової величини та її графік функції розподілу

За виглядом кривої (рис. 2) можна побачити, що випадкову величину розподілено за законом Вейбула.

В роботі реалізовано програмну модель трафіку протоколу JDSS стандарту STANAG-4677. Використання імітаційного моделювання за допомогою такої моделі дозволить розраховувати показники якості обслуговування мереж зв'язку для АСУ державного рівня низової ланки управління з активним переміщенням користувачів ще на етапі проектування та планування.

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, P 150-170.

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

3. Strelkovskaya I., Zolotukhin R. Research of low-bandwidth radionetworks QoS parameters // 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.

4. Strelkovskaya I.V., Zolotukhin R.V. « Simulation modeling algorithm of low-bandwidth radio network of automated control systems» / Springer Science + Business Media, 2025 (до друку).

DOI https://doi.org/10.36059/978-966-397-491-0-40

ЗБЕРЕЖЕННЯ КОНФІДЕНЦІЙНОСТІ ШЛЯХОМ МАСКУВАННЯ ПЕРЕДАЧІ ІНФОРМАЦІЇ

Тріль Д. Д.
здобувач
Міжнародний гуманітарний університет
м. Одеса, Україна

Збереження конфіденційності інформації набуває дедалі більшої значущості в умовах сучасного цифрового світу, де технологічний прогрес рухається стрімкими темпами. Цей розвиток супроводжується зростаючою кількістю загроз, включаючи витоки даних, кібернапади та незаконні способи збору персональної інформації. Враховуючи, що сьогодні майже кожна людина активно використовує інтернет у різних сферах життя – для спілкування, професійної діяльності, здійснення фінансових операцій – питання цифрової безпеки та захисту конфіденційності стає надзвичайно актуальним для широкого загалу [1].

Одним із дієвих способів зменшення ризиків втрати конфіденційності є використання технологій маскування передачі даних. Цей підхід дає змогу приховати як сам факт передачі інформації, так і її зміст, забезпечуючи захист від можливих спроб несанкціонованого доступу з боку зловмисників. У нинішніх реаліях, коли державні організації, великі корпорації та кіберзлочинці активно аналізують численні цифрові сліди, такі методи виступають важливим інструментом для збереження персональної безпеки.

Особливе значення маскування передачі даних має для тих, чия діяльність нерідко супроводжується ризиками витоку інформації чи її неправомірного використання. Це журналісти, котрі шукають правду у чутливих темах, правозахисники, що борються за свободу та права людини, підприємці, які прагнуть захистити інтелектуальну власність, а також