УДК 621.395:004.056

Русляченко М.С., Гонсіоровський Д.М.
Русляченко М. С., Гонсиоровский Д. М.
Ruslyachenko M.S., Honsiorovskyi D.M.

ДОСЛІДЖЕННЯ ПАРАМЕТРІВ ЯКОСТІ ОБСЛУГОВУВАННЯ ТРАФІКА VOIP ПРИ ВИКОРИСТАННІ ПРОТОКОЛУ ЗАХИЩЕНОГО ПЕРЕДАВАННЯ IPSEC

ИСЛЕДОВАНИЕ ПАРАМЕТРОВ КАЧЕСТВА ОБСЛУЖИВАНИЯ ТРАФИКА VOIP ПРИ ИСПОЛЬЗОВАНИИИ ПРОТОКОЛА ЗАЩИЩЕННОЙ ПЕРЕДАЧИ IPSEC

RESEARCH OF THE QUALITY OF SERVICE PARAMETERS OF THE VOIP TRAFFIC WHILE USING SECURE TRANSMISSION PROTOCOL IPSEC

Анотація. Досліджено вплив протоколу IPSec, що застосовувався для забезпечення захищеного передавання даних, на параметри якості обслуговування голосових трафіків, таких як E-Model R-factor та MOS.

Анотация. Исследовано влияние протокола IPSec, используемого для обеспечения защищенной передачи данных, на параметры качества голосовых трафиков, таких как E-Model R-factor и MOS.

Summary. There was a research of the impact of the protocol IPSec which was used to secure data transmission on the quality of service parameters of the voice traffic, such as E-Model R-factor and MOS.

Для вирішення проблеми забезпечення захищеного передавання даних за технологією VoIP, яка не передбачає можливостей захисту передаваних даних, можна застосовувати протокол захищеного передавання IPSec. Недоліком цього методу є те, що протокол IPSec до кожного пакета додає свої заголовки, тим самим збільшуючи необхідну смугу пропускання і зменшуючи показники якості обслуговування. Проте наскільки погіршуються показники якості обслуговування при впливі протоколу IPSec в літературі відсутні.

Метою роботи є визначення параметрів якості обслуговування під час передавання голосового трафіка при використанні протоколу захисту IPSec.

Для дослідження використовувалася реалізація IPSec Openswan, тунельний режим роботи IPSec, методи шифрування AES з 128-бітовим ключем та 3DES з 192-бітовим ключем, кодеки G.711 A-law та G.729.

Експериментально отримані розміри заголовків пакетів IPSec. Зробивши серію тестових викликів між комп'ютерами Ubuntu121 і Ubuntu135 та проаналізувавши захоплені за допомогою програмного забезпечення Wireshark пакети, можна зробити висновок, що типовий розмір заголовка пакета IPSec є сталим. Отримані значення для досліджуваних кодеків та методів шифрування зведено до табл. 1.

Таблиця 1 – Довжина заголовка IPSec при різних кодеках та методах шифрування

Кодек	AES, 128 біт	3DES, 192 біта
G.711 A-law	64	56
G.729	60	52

Базовими етапами мовного оброблення на боці передавача є кодування й пакетування [1]. RTP пакети відправляються в певний час й інтервал між двома послідовними пакетами залежить від часової складової. Час, пов'язаний із процесом пакетування, визначається наступним базовим рівнянням

$$\Delta t = \frac{P_S}{S_R}, \quad (1)$$

де Δt [s] – відлік часу; P_S [bytes] – розмір корисного навантаження і C_R [bps] представляє швидкість кодека.

Для протоколу RTP, який має таймінг (час між відправленням двох послідовних пакетів) $\Delta t = 20$, кодеки G.711 A-law та G.729 мають наступні значення параметрів C_R та P_S:

– G.711 A-law: C_R = 64 кбіт/с; P_S = 160 байт;

– G.729: C_R = 8 кбіт/с; P_S = 20 байт.

Відлік часу може бути отриманий з змісту RTP пакетів як різниця двох послідовних позначок часу (*timestamp*), в наступному рівнянні (типове значення частоти дискретизації (*sampling_frequency*) 8 KHz)

$$\Delta t = \frac{timestamp_{(N+1)} - timestamp_{(N)}}{sampling\_frequency} . \quad (2)$$

Інтервал відліків для конфігурації VoIP дорівнює 20 мс.

Необхідно надати розмір пакетів на прикладному рівні, що може бути визначений наступним виразом

$$S_{ApL} = H_{RTP} + P_S , \quad (3)$$

де S_{ApL} [bytes] – очікуваний розмір пакетів на прикладному рівні, що складається із суми RTP заголовка (12 Bytes), H_{RTP} [bytes] і розміру корисного навантаження, P_S [bytes].

Сумарна смуга пропускання $BW(N)$ [kbps] може бути визначена наступним виразом [2]

$$BW(N) = N \cdot C_R \cdot (1 + \frac{H_{RTP} + H_{TrL} + H_{NwL} + H_{DLL}}{P_S}) . \quad (4)$$

Для розрахунку смуги пропускання при роботі сценарію IPsec у тунельному режимі у рівнянні (4) необхідно змінити розміри заголовка пакета на мережному рівні.

Розрахунок необхідної смуги пропускання для сценарію, коли IPSec працює у туннельному режимі може бути проведений за формулою

$$BW(N) = N \cdot C_R \cdot (1 + \frac{H_{RTP} + H_{TrL} + H_{NwL} + H_{IPSec} + H_{DLL}}{P_S}) , \quad (5)$$

де $BW(N)$ – полоса пропускання, кбіт/с; N – кількість одночасних викликів; C_R – швидкість кодека, кбіт/с; H_{RTP} – довжина заголовка протокола RTP, байт (12 байт); H_{TrL} – довжина заголовка транспортного рівня, байт (8 байт); H_{NwL} – довжина заголовка мережного рівня, байт (20 байт); – довжина заголовка IPSec (див. табл. 1); – довжина заголовка канального рівня, байт (26 байт); P_S – розмір навантаження кодека, байт.

Виконавши розрахунки за формулою (4) і (5), зведемо отримані результати до табл. 2.

Таблиця 2 – Значення необхідної полоси пропускання для одного виклику за різних методів захисту трафіка

Кодек	Δt, мс	Незахищений трафік, кбіт/с	З шифруванням 128-бітовим AES, кбіт/с	З шифруванням 192-бітовим 3DES, кбіт/с
G.711 A-law	20	90,4	116	112,8
G.729	20	34,4	58,4	55,2

З табл. 2. видно, що при використанні шифрування зростає необхідна для передчі смуга пропускання, а тому зменшується кількість викликів, які можуть бути зроблені при використанні каналу з обмеженою смугою пропускання. В табл. 3 наведемо максимальну теоретичну кількість успішних викликів для з'єднання зі смугою пропускання 2048 кбіт/с.

Таблиця 3 – Максимальна кількість успішних викликів для з'єднання зі смугою пропускання 2048 кбіт/с

Кодек	Полоса пропускання, кбіт/с	Незахищений трафік, кбіт/с	З шифруванням 128-бітовим AES, кбіт/с	З шифруванням 192-бітовим 3DES, кбіт/с
G.711 A-law	2048	22	17	18
G.729	2048	59	35	37

Розрахунок ITU-T E-Model R-factor

R-factor можна розрахувати за наступною формулою [3]

$$R = R_0 - I_S - I_d - I_{e,eff} + A \ , \tag{6}$$

де – значення R-factor; – описує якість мовлення через базове відношення сигнал/шум, яке залежить від рівнів мовлення та рівнів різних джерел шуму; – фактор одночасного погіршення; – фактор погіршення через затримки; – ефективний фактор погіршення за рахунок обладнання; A – фактор корисності.

Якщо знехтувати впливом відношення сигнал/шум (SNR – Signal-to-Noise Ratio) та затуханням сигналу через луну, тоді розрахунок значення R-factor можна спростити згідно з рекомендацією ITU-T Recommendation G.107 [3]. В цьому разі у формулу (6) можна підставити значення $R_0 = 93{,}3553$, $I_S = 1{,}41136$ та $A = 0$.

Для знаходження параметра I_d слід скористатись наступною формулою [5]:

$$I_d = \begin{cases} 0{,}0267 \cdot d, & d < 125 \text{ мс} \\ 0{,}1194 \cdot d - 15{,}876, & 175 мс \le \text{d} \le 400 \text{ мс} \end{cases}, \tag{7}$$

де d – значення затримки при розповсюдженні даних в один кінець, мс. Даний параметр можна розрахувати за допомогою формули [5]

$$d = \frac{RTD}{2} + ESD(A) + ESD(B) \ , \tag{8}$$

де RTD – середній час проходження пакета в обидва кінці, мс; $ESD(A)$ – затримка кінцевої системи-відправника, тобто затримка кодера та час на пакетизацію, мс; $ESD(B)$ – затримка кінцевої системи-одержувача, складається з довжини деджитерного буфера, що становить 40 мс (довжина двох речових датаграм), та часу на депакетизацію, що становить $0{,}1 \cdot ESD(A)$, мс. Значення $ESD(A)$ для кодеків G.711 A-law та G.729 становлять 20 мс та 25 мс відповідно.

Використовуючи формули (7) та (8), розрахуємо значення параметра I_d для досліджуваних кодеків:

Кодек G.711 A-law: $I_d = 0.0267 \cdot \left(\frac{2{,}603}{2} + 20 + 40 + 0{,}1 \cdot 20 \right) = 1{,}690$.

Кодек G.729: $I_d = 0{,}0267 \cdot \left(\frac{2{,}603}{2} + 25 + 40 + 0{,}1 \cdot 25 \right) = 1{,}837$.

Згідно з рекомендацією ITU-T Recommendation G.113 [6], величина ефективного фактора погіршення за рахунок обладнання для досліджуваних кодеків становить:

Кодек G.711 A-law: $I_{e,eff} = 0$.

Кодек G.729:

Використовуючи формулу (6), проведемо розрахунок значення R-factor для кодеків G.711 A-law та G.729:

Кодек G.711 A-law: $R = 90.25394$.

Кодек G.729: $R = 79.10694$.

Розрахунок MOS (Mean Opinion Score)

Значення MOS може бути розраховано з значення R-factor, згідно з рекомендацією ITU-T Recommendation G.107 [3], за формулою

$$\text{MOS} = \begin{cases} 1, & R \le 0, \\ 1 - \frac{7}{1000} \cdot R + \frac{1}{6250} \cdot R^2 - \frac{7}{1000000} \cdot R^3, & 0 < R < 100 \\ 4{,}5, & R \ge 100 \end{cases}. \tag{9}$$

Використовуючи формулу (9), наведемо отримані значення R-factor до значень MOS.

Кодек G.711 A-law: MOS = 4,3776;

Кодек G.729: MOS = 4,0430.

Дослідження показників якості обслуговування

Використовуючи теоретичні розрахунки кількості одночасних викликів, проведемо низку тестів для одного VoIP-з'єднання та кількості з'єднань з максимальними втратами для канала з полосою пропускання 2048 кбіт/с. Результати тестів для кожного кодека занесемо до табл. 4.

В табл. 4 показано, що при досягненні максимальної теоретичної кількості одночасних викликів для незахищеного з'єднання при використанні вищезазначених механізмів захисту затримка розповсюдження в один кінець та джитер збільшуються, а також з'являються втрати (до 58 %). При зменшенні кількості з'єднань до теоретично розрахованої максимальної кількості викликів для захищених з'єднань можна помітити зменшення часу розповсюдження пакетів, менший джитер та відсутність втрат.

Порівняння результатів

Для порівняння результатів для незахищеного та захищених з'єднань у якості еталона виберемо максимальну теоретичну кількість успішних з'єднань VoIP для заданої смуги пропускання 2048 кбіт/с.

На рис. 1 та 2 зобразимо порівняльні діаграми значень R-factor для одного з'єднання та максимальної кількості з'єднань з табл. 3 для кодеків G.711 A-law та G.729 відповідно, а на рис. 3 та 4 зобразимо порівняльні діаграми значень MOS для тих самих параметрів.

Таблиця 4 – Результати тестів VoIP-генератора для кодеків G.711 A-law та G.729 з використанням різних механізмів захисту

Кодек	Шифрування	Кількість одночасних викликів	Середнє значення MOS	Середнє значення R-factor	Середня затримка розповсюдження в один кінець, мс	Втрати, %	Джитер, мс
G.711 A-law	немає	1	4,37	91,49	1	0	0
G.711 A-law	128AES	1	4,37	91,47	1	0	0
G.711 A-law	192Triple-DES	1	4,37	91,47	1	0	0
G.729	немає	1	4,03	80,16	1	0	0
G.729	128AES	1	4,03	80,15	1	0	0
G.729	192Triple-DES	1	4,03	80,16	1	0	0
G.711 A-law	немає	22	4,37	91,44	2	0	0,742
G.711 A-law	128AES	22	1,99	30,80	3	28,7	1,080
G.711 A-law	192Triple-DES	22	2,14	34,43	3	25,8	1,178
G.711 A-law	128AES	17	4,27	88,96	2	0	0,800
G.711 A-law	192Triple-DES	18	4,34	90,68	2	0	0,448
G.729	немає	59	4,01	79,56	4	0	0,628
G.729	128AES	59	1,01	0,55	9	57,7	5,814
G.729	192Triple-DES	59	1,06	2,40	4	50,1	2,612
G.729	128AES	35	4,01	79,78	2	0	0,448
G.729	192Triple-DES	37	4,02	79,90	2	0	0,405

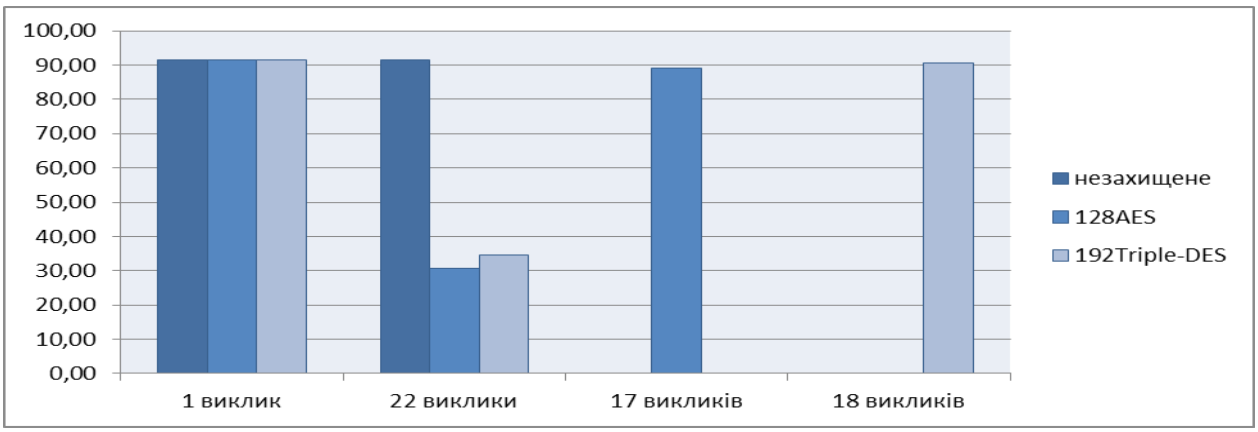

Рисунок 1 Порівняння значень R-factor для кодека G.711 A-law

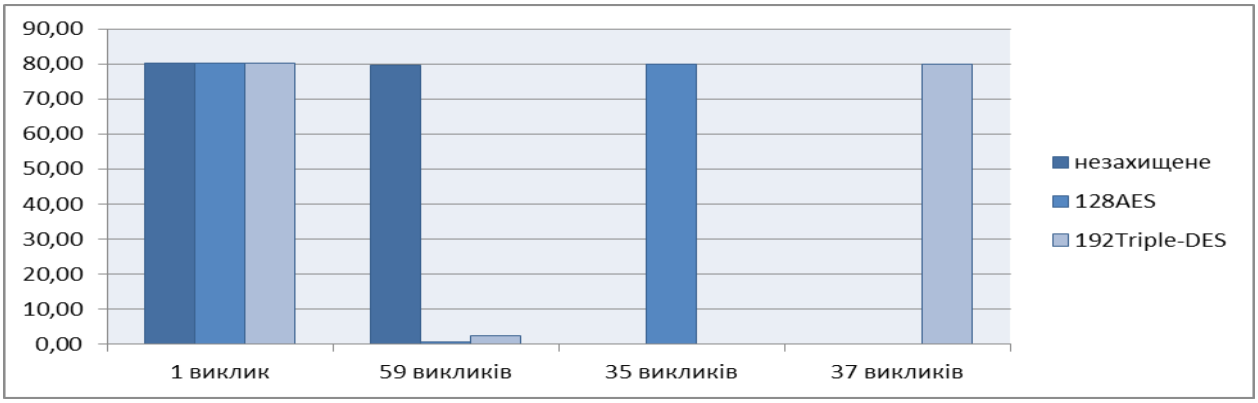

Рисунок 2 – Порівняння значень R-factor для кодека G.729

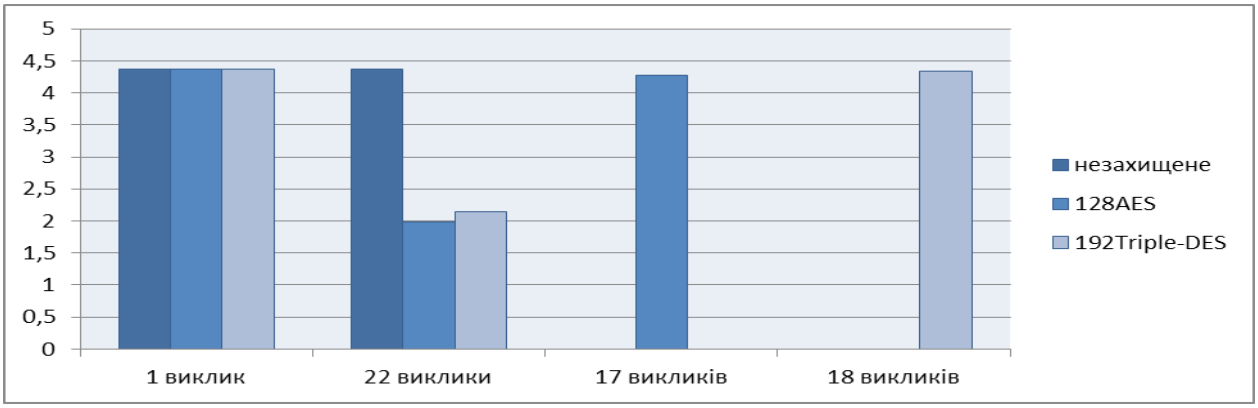

Рисунок 3 – Порівняння значень MOS для кодека G.711 A-law

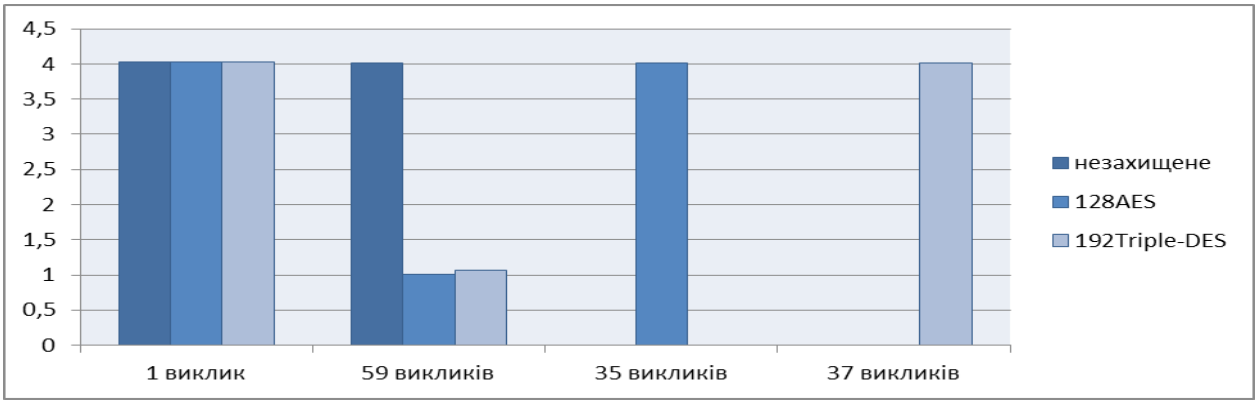

Рисунок 4 – Порівняння значень MOS для кодека G.729

Як видно з рис. 1…4, для одного виклику параметри якості обслуговування для обох кодеків та обох методів шифрування майже не змінюються.

При максимальній теоретичній кількості викликів без використання IPSec показники якості обслуговування знижуються. Наприклад, для кодека G.711 A-law значення R-factor зменшується в 3 рази для обох методів шифрування, а для кодека G.729 – в 30 … 145 разів, в залежності від методу шифрування. Таке погіршення є суттєвим, це призводить до того, що майже всі користувачі будуть не задоволені [3].

Також з рисунків видно, що теоретично розрахована максимальна кількість одночасних викликів при застосуванні IPSec підтверджується експериментальними даними: значення параметрів якості обслуговування для цих значень кількості одночасних викликів майже не відрізняються від значень відповідних параметрів при одному виклику.

Використовуючи дані табл.4 можна зробити висновок про те, наскільки при використанні IPSec треба зменшити кількість одночасних викликів порівняно із максимальною теоретичною кількістю викликів при використанні незахищеного з'єднання для отримання найбільших значень показників якості обслуговування. Результати цих розрахунків для обох кодеків та різних методів шифрування зведемо до табл. 5.

Таблиця 5 – Відносне зменшення максимальної кількості одночасних викликів для кодеків G.711 A-law та G.729 за різних методів шифрування

Кодек	Максимальна кількість одночасних викликів при незахищеному з'єднанні, од.	Відносне зменшення максимальної кількості викликів при використанні шифрування 128AES, %	Відносне зменшення максимальної кількості викликів при використанні шифрування 192Triple-DES, %
G.711 A-law	22	22,7	18,1
G.729	59	40,7	37,3

На закінчення зробимо висновки. У роботі визначені параметри якості обслуговування при передаванні голосового трафіка при використанні протокола захисту IPSec. Для одного виклику параметри якості обслуговування для обох кодеків та обох методів шифрування майже не змінюються. Теоретично розрахована максимальна кількість одночасних викликів при застосуванні IPSec підтверджується експериментальними даними: значення параметрів якості обслуговування для цих значень кількості одночасних викликів майже не відрізняються від значень відповідних параметрів при одному виклику. При максимальній теоретичній кількості викликів без використання IPSec показники якості обслуговування знижуються, для кодека G.711 A-law значення R-factor зменшується в 3 рази для обох методів шифрування, а для кодека G.729 — в 30 … 145 разів, в залежності від методу шифрування.

Література

1. Factors influencing voice quality in VoIP technology// 9th International Conference Informatics, 21-22 June 2007. - Bratislava, Slovakia / Edited by M. Halas, B. Kyrbashov, M. Voznak. – 2007 – P. 32–35.
2. Impact of security on speech quality. CESNET: Technical Report [Електронний ресурс] / Voznak M. // 2008 – 10 С. – Режим доступу до ресурсу: http://www.cesnet.cz/doc/techzpravy/2008/impact-of-network-security-on-speech-quality.
3. The E-model, a computational model for use in transmission planning: ITU-T Recommendation G.107 (Amendment 1) – [Чинний від 1.12.2011] – 26 С. – (Міжнародний стандарт).
4. Mathematical model of VoIP connection delay**:** Proceedings of the IADIS International Conference on Telecommunications// Networks and Systems, 3-8 July 2007, Lisbon, Portugal / Edited by Jörg Roth, Jairo Gutiérrez and Ajith P. Abraham. – IADIS Publications, 2007. – P. 95–99.
5. RTP Control Protocol Extended Reports (RTCP XR): IETF RFC 3611. – [Чинний від 1.11.2003]. – 55 с. – (Міжнародний стандарт).
6. Transmission impairments due to speech processing: ITU-T Recommendation G.113. – [Чинний від 1.11.2007]. – 26 С. – (Міжнародний стандарт).