УДК 621.391

Г.Л. Антонюк[1]
О.С. Полуденко[1]
А.О. Юрченко[1]

СИСТЕМА ДОСТУПУ З КВАНТОВИМ КАНАЛОМ

[1] Вінницький національний технічний університет;

Анотація

Досліджено інтегруввання,сучасних пристроїв QKD втелекомунікаційні системи та мережі GPON та EPON, що засновані на TDM, а також WDM-PON.

Ключові слова: квант, криптографія, точка-точка,секретний ключ, AWG,WDM-PON, телекомунікаційна мережа.

Abstract

The integration of modern QKD devices into telecommunication systems and GPON and EPON networks based on TDM, as well as WDM-PON has been studied.

Keywords:quantum, cryptography, point-to-point, secret key, AWG, WDM-PON, telecommunication network.

Вступ

На відміну від перших схем інформаційного захисту, сучасна криптографія не приховує алгоритму, шифрування та розшифровки інформаційних потоків. Безпека процедури залежить від ключа повідомлень, ймовірності витоку інформації та обчислювальної стійкості до порушення алгоритму інформаційного захисту. Окрім традиційних рішень, таких як контрольні повідомлення та фізичний обмін пулами ключів, додатковий інформаційний захист може забезпечуватися за допомогою криптографії асиметричних ключів на основі односторонніх функцій (наприклад, RSA, Dif fi e Hellman) [1].

Альтернативний більш високий рівень інформаційної безпеки з'явилася з відкриттям квантової механіки. Першою пропозицією квантової криптографії був розподіл квантового ключа (QKD), протокол, який створює секретний ключ між двома частинами каналу передавання з інформаційно-теоретичною безпекою. На відміну від звичайних рішень, вказаний протокол захищений від зловмисника з необмеженими ресурсами (за рахунок використання квантового комп'ютера).

Мета даної роботи є обґрунтування використання квантових сигналів у найбільш вживаних мережевих стандартах (GPON, EPON), не змінюючи режиму роботи, звичайних користувачів та не вимагаючи занадто великих змін від телекомунікаційної компанії.

Результати дослідження

Було розглянуто кілька варіантів мереж QKD. Більшість із них належать до категорії надійних ретрансляторів із виділеними каналами.

До переваг QKD можна віднести покращення відстані, ключової швидкості та перевіркастабільності у довгостроковому сценарії. Тим не менше, щоб отримати комерційне впровадження, послуга повинна бути конкурентоспроможною. Відповідно до цього, інтеграція QKD у стандартні телекомунікаційні мережі останнім часом привертає велику увагу[2].

Інтеграція квантових каналів у мережу доступу на основі WDM простіша, ніж у TDM-PON. Як і у випадку з TWDM-PON, навіть незважаючи на те, що використовуються більш звичайні канали (зазвичай один або два на ONU), вони використовують сітку DWDM і знаходяться в діапазоні C оптичного спектру. Таке розташування залишає значну частину спектра вільним для використання квантових каналів у будь-який час без будь-якої синхронізації та подальшої обробки[3].

Мережа доступу, заснована на пасивних оптичних компонентах є, по суті, ідеальним сценарієм інтеграції QKD, коли забезпечується можливість контролювати перехресні перешкоди за допомогою потужних звичайних сигналів. Незважаючи на обмежене охоплення та кількість користувачів, запропоновані системи є наступним кроком в розвитку мереж QKD [4].

Крім того, пропоновані рішення є перспективними, оскільки схеми сумісні зі стандартами PON наступного покоління та другого наступного покоління (поки технологія QKD постійно вдосконалюється) [5].

Головна перевага полягає в тому, що інтеграція є простою та прозорою для решти мережі.

Квантові інформаційні технології відкривають новий спектр можливостей у телекомунікаціях, особливо в галузі безпеки. Наприклад, QKD дозволяє двом користувачам створити секретний ключ між собою за допомогою інформаційно-теоретичної безпеки, таким чином вирішуючи проблему розподілу ключів звичайної криптографії. Практичні системи QKD комерціалізуються, і дослідження показали її довгострокову стабільність[4].

Зокрема, існуючі телекомунікаційні мережі, засновані на оптичних волокнах є ідеальним середовищем завдяки своїй поширеності, охоплюючи майже всіх потенційних користувачів. Поширюючи запропоновану технологію, вартість використання QKD різко зменшиться, а кількість можливих сценаріїв зросте. Технологія стане дешевшою та кориснішою.

Висновок

У роботі розглянуто особливості інтеграції квантових комунікацій у телекомунікаційних мережах в так звану останню милю, яка підключається до кінцевих користувачів. Нашою метою було обґрунтувати використання квантових сигналів у найбільш задіяних сьогодні мережевих стандартах (GPON, EPON), не змінюючи режиму роботи та не впливаючи на звичайних користувачів або не вимагаючи занадто великих зусиль від телекомунікаційної компанії. Незалежно від можливості, рішення обмежені з точки зору охоплення, кількості користувачів та схеми підключення. Щоб вирішити ці проблеми, потрібно звільнитися від обмежень, накладених звичайними користувачами, їх сигналами та протоколами і перейти від простоїмодернізації існуючого мережевого стандарту до повнофункціональної квантової телекомунікаційної мережі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. N. Walenta, A. Burg, D. Caselunghe, J. Constantin, N. Gisin, O. Guinnard, R. Houlmann, P. Junod, B. Korzh, N. Kulesza, M. LegrÃ©, C. W. Lim, T. Lunghi, L. Monat, C. Portmann, M. Soucarros, R. T. Thew, P. Trinkler, G. Trolliet, F. Vannel, and H. Zbinden, "A fast and versatile quantum key distribution system with hardwarekey distillation and wavelength multiplexing, " New Journal of Physics, vol. 16, no. 1, p. 013047, 2014.

2. K. Patel, J. Dynes, M. Lucamarini, I. Choi, A. Sharpe, Z. Yuan, R. Penty, andA. Shields, "Quantum key distribution for 10 Gb/s dense wavelength divisionmultiplexing networks," Applied Physics Letter s, vol. 104, no. 5, pp. 051 123–051 123–4, 2014.

3. J. Qiu, "Quantum communications leap out of the lab," Nature, vol. 508, no. 7497, pp. 441–442, 2014.

4. K. Shimizu, T. Honjo, M. Fujiwara, T. Ito, K. Tamaki, S. Miki, T. Yamashita, H. Terai, Z. Wang, and M. Sasaki, "Performance of Long-Distance Quantum KeyDistribution Over 90-km Optical Links Installed in a Field Environment of TokyoMetropolitan Area," Lightwave Technology, Journal of, vol. 32, no. 1, pp. 141–151, 2014

5. Методи побудови високошвидкісних волоконно-оптичних трактів / М.В. Васильківський, Г.Л. Антонюк, О.С. Полуденко // Вимірювальна та обчислювальна техніка в технологічних процесах (ВОТ-ТП_17_2017) XVII міжнародної науково-технічної конференції, 8-13 червня 2017 р. – Матеріали – Одеса. – 2017 с. 187.

Антонюк Ганна Леонідівна— аспірант групи АС-20, кафедра ТКСТБ, Вінницький національний технічний університет, Вінниця, e-mail: annaantonuik@gmail.com

Полуденко Ольга Сергіївна - аспірант групи АС-19, кафедра ТКСТБ, Вінницький національний технічний університет, Вінниця, e-mail: rtt.poludenko@gmail.com

Юрченко Артем Олександрович – ст. гр. ТКС-19 м, кафедра ТКСТБ, Вінницький національний технічний університет, Вінниця, e-mail: rtt.poludenko@gmail.com

Науковий керівник:***Васильківський Микола Володимирович***— канд. техн. наук, доцент кафедри ТКСТБ, заступник декана факультету ІРЕН, Вінницький національний технічний університет

Antonuik Hanna L. — Department of Telecommunication system and television, Vinnytsia National Technical University, Vinnytsia, email :annaantonuik@gmail.com

PoludenkoOlha S. — Department of Telecommunication system and television, VinnytsiaNationalTechnicalUniversity, Vinnytsia, email :rtt.poludenko@gmail.com

YurchenkoArtem O. — student of department Telecommunication system and television, VinnytsiaNationalTechnicalUniversity, Vinnytsia, email :rtt.poludenko@gmail.com

Supervisor: ***VasylkivskyMykola V.***— Cand. Sc. (Eng), Assistant Professor of Telecommunication system and television, Vinnytsia National Technical University, Vinnytsia