УДК 004.056.55; 004.051

Р.А. Бурачок, Гуськов П.О., Р.І. Бак
Національний університет “Львівська політехніка”

ВИКОРИСТАННЯ СИМЕТРИЧНИХ АЛГОРИТМІВ ШИФРУВАННЯ ПРИ ПЕРЕДАВАННІ МУЛЬТИМЕДІЙНИХ ДАНИХ

Проаналізовано можливості передавання мультимедійних даних, представлених у різних форматах, через мережу зв’язку з використанням деяких видів симетричних алгоритмів шифрування.

Ключові слова: криптографічний алгоритм, мультимедійний трафік, часові затримки, алгоритми: DES, 3DES, IDEA, AES, CAST-128, режими роботи алгоритму: ECB, CBC, OFB, CFB.

The analysis of the multimedia capabilities of data presented in various formats via the network communication when using some types of symmetric encryption algorithms.

Key words: cryptographic algorithm, multimedia traffic, time delay, algorithms: DES, 3DES, IDEA, AES, CAST-128, modes of encryption algorithm: ECB, CBC, OFB, CFB.

Вступ. Сучасна криптографія для забезпечення конфіденційного передавання інформації передбачає можливість використання значного розмаїття симетричних алгоритмів шифрування. До типових симетричних алгоритмів, призначених для шифрування інформації типу “дані”, можна зарахувати алгоритми DES, 3DES, IDEA, AES, Twofish, Blowfish, CAST-5 (CAST-128) та інші, які можуть бути використані як самостійно, так і у режимах типу ECB, CBC, OFB та CFB. Типовою областю застосування цих алгоритмів є передавання даних, які є нечутливими або малочутливими до часових затримок. Тому єдиною проблемою, яка виникає під час передавання такого типу інформації, є надійність алгоритму, яка визначається рядом критеріїв: довжиною ключа, кількістю раундів шифрування, довжиною блока даних відкритого тексту та математичною складністю реалізації раунду шифрування. Але в сучасних телекомунікаційних мережах щораз частіше виникає потреба передавати у захищеному вигляді дані іншого типу, зокрема зашифровані мультимедійні дані в реальному часі. І для передавання таких даних виникає суперечлива задача: з одного боку, необхідно забезпечити високу криптографічну надійність, яка, як правило, досягається за рахунок використання складних математичних операцій алгоритму, а з іншого боку – потрібно досягти високої швидкості передавання, а отже, і незначних часів затримок, які переважно обмежуються швидкістю криптографічних перетворень на сторонах передавання та приймання. Крім того, на аналіз цієї задачі накладається ще одне додаткове обмеження, а саме: криптографічні алгоритми реалізовуються у вигляді програмного або апаратного забезпечення і час затримки на обробку типового інформаційного блока сталий для вибраного алгоритму шифрування, вплинути на який неможливо. Тому єдиним розв’язанням цієї задачі є підбір алгоритму, режиму роботи та його відповідної реалізації – апаратної або програмної, яка б задовольняла вимоги стосовно конфіденційної надійності та часових затримок передавання. Також необхідно зауважити, що передавання і приймання мультимедійних даних відбувається, як правило, з використанням персональних комп’ютерів.

1. Спосіб визначення тривалості шифрування при передаванні мультимедійного трафіку. Отже, для розв’язання цієї задачі необхідно визначитися із максимально допустимими часовими затримками для типових мультимедійних послуг: передавання відеоданих різних форматів, враховуючи при цьому час перетворення первинного звуку та/або зображення у відповідний формат на сторонах передавання та приймання. При аналізі часових затримок для

передавання різних мультимедійних даних вважатимемо, що перепускні здатності мережі є достатніми і на якість сприйняття відео- та аудіоданих при їх передаванні у відкритому вигляді не впливають. У зв'язку з цим при передаванні аудіо- та відеоданих накладаються певні обмеження стосовно часових затримок, а відповідно і якість суб'єктивного сприйняття цих послуг (див. табл. 1). Отже, часові затримки, наведені у табл. 1, враховують затримку передавання по мережі від передавача до приймача $T_{з\,пер}$ та представлення відео/аудіоданих у відповідному форматі $T_{з\,пер} = T_{з\,пр}$. Аналогічне значення часових затримок зберігатиметься і у випадку, якщо на сторонах передавання та приймання використано симетричні алгоритми шифрування, тобто для цього випадку часові затримки складатимуться з часів затримок представлення відео- та аудіоданих у відповідному форматі, передавання по мережі від передавача до приймача та шифрування/дешифрування на сторонах передавання/приймання $T_{з\,ш} = T_{з\,дш}$ (див. рисунок).

Таблиця 1

Допустимі часові затримки під час передавання мультимедійних даних

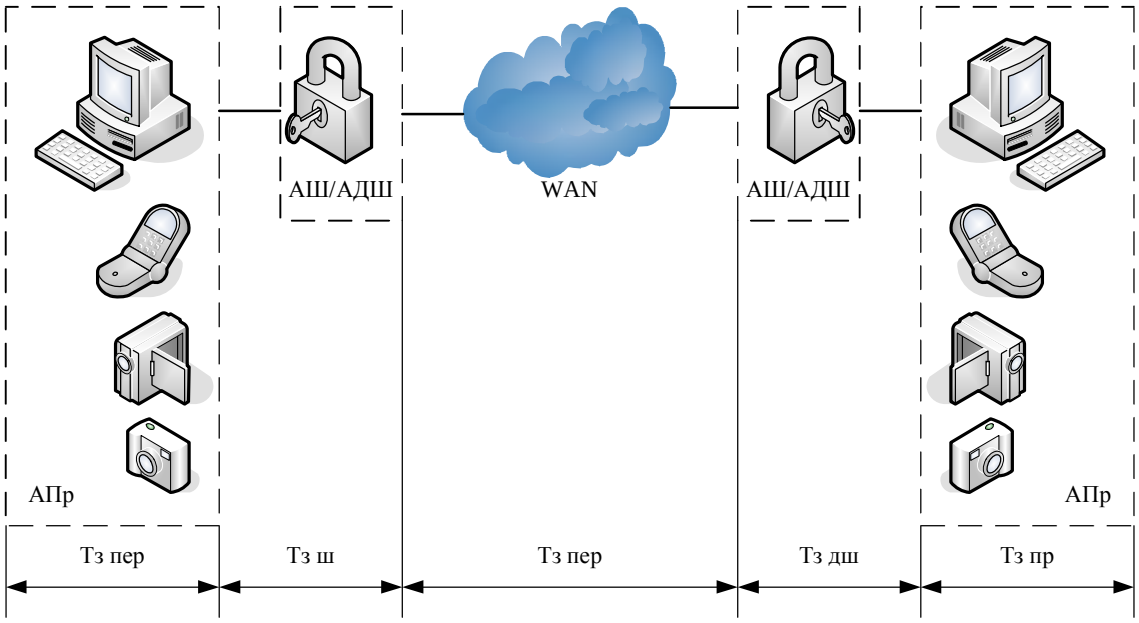
Затримка передавання, мс	Для аудіоданих	Для відеоданих
600 і більше	Передавання неможливе	Передавання неможливе
	Якість послуги згідно з MOS оцінкою, нижчою за 2	
250	Значна затримка, необхідність пристосовуватися для отримання послуги	Передавання неможливе або суттєво ускладнене (залежно від формату послуги)
	Якість послуги згідно з MOS оцінкою не вище за 3	
150	Задовільно	Значна затримка, помітні істотні затримки під час приймання кадрів
	Якість послуги згідно з MOS оцінкою лежить в межах від 3 до 3,5	
100	Затримка несуттєва, практично чистий зв'язок. Якість послуги згідно з MOS оцінкою лежить в межах від 3,5 до 4	Незначні, але помітні затримки при прийманні кадрів. Якість послуги згідно з MOS оцінкою лежить в межах від 3,5 до 3,8
50	Часова затримка не сприймається. Якість послуги згідно з MOS оцінкою лежить в межах від 4 до 4,8	Затримка не сприймається. Якість послуги згідно з MOS оцінкою лежить в межах від 3,8 до 4,8

Для аналізу часових затримок у мережі від передавача до приймача можна скористатися або середньостатистичними даними, отриманими під час відповідних замірів тривалості передавання мультимедійного трафіку на мережі, або визначити, використовуючи теорію систем масового обслуговування, подавши набір вузлів та ліній між передавачем та приймачем як набір відповідних систем масового обслуговування з відповідними структурами вузлів та інтенсивностями надходження і обслуговування пакетів.

Часові затримки представлення відео- та аудіоданих у відповідних форматах – MPEG-1, MPEG-2, MPEG-4, H.264/MPEG-4 AVC та MiniDV є типовими і насамперед залежать від швидкодії апаратного або програмного забезпечення абонентів на приймальній або передавальній сторонах. Залежно від типового обладнання та форматів подання відеоданих цей час лежить в межах 3–25 мс та аудіоданих – 1–5 мс. Використання спеціалізованого апаратного забезпечення дає змогу отримувати нижчі значення часової затримки.

Час затримки шифрування та дешифрування, аналогічно, як і представлення відео- та аудіоданих у відповідних форматах, залежать передусім від швидкодії апаратного або/і програмного забезпечення абонентів на приймальній або передавальній сторонах, а також від виду використовуваного абонентами симетричного алгоритму шифрування та режиму його застосування, що відображається у кількості операцій, які виконують для отримання закритих даних. Істотно вливає

на час затримки при шифруванні й дешифруванні й обсяг інформації, яку необхідно зашифрувати та передати, – ця вимога відображається через формат подання відео- та аудіоданих.



Складові часової затримки при конфіденційному передаванні мультимедійних даних: АПр – абонентський пристрій; АШ/ДШ – алгоритм шифрування/дешифрування на сторонах передавання/приймання; WAN – глобальна мережа

2. Дослідження тривалості затримки для симетричних алгоритмів шифрування під час передавання мультимедійного трафіку. Для визначення часів затримок під час шифрування та дешифрування відео- та аудіоданих у різних форматах пропонується застосовувати алгоритми шифрування DES, 3DES, IDEA, AES та CAST-128 у режимах ECB, CBC, OFB та CFB при їх програмній та апаратній реалізації. Ці алгоритми шифрування є блочними, характеризуються різною довжиною ключа та блоком відкритої та зашифрованої інформації. Отримані відношення значення часів затримок без шифрування та з шифруванням даних, представлених у разах як відношення $K = \frac{T_{з\,ш}}{T_{з\,бш}}$, де $T_{з\,бш}$, $T_{з\,ш}$ – затримка у разі відсутності та наявності алгоритму шифрування відповідно, для різних алгоритмів та режимів шифрування при застосуванні апаратної та програмної реалізації наведено у табл. 2. Час тривалості шифрування визначається для блока відкритого тексту, в випадку мультимедійних даних, загальною довжиною 50 Мбайт. Час затримки при шифруванні визначається як: $T_{з\,ш} = T_{з\,ш} + T_{п\,ш}$, де $T_{з\,ш}$ та $T_{п\,ш}$ – момент часу покидання останнім бітом – зашифрованим 50 Мбайтного блока даних апаратної або програмної реалізації алгоритму та момент часу надходження першим бітом – відкритим 50 Мбайтного блока даних в апаратній або програмній реалізації алгоритму.

Апаратна реалізація алгоритму передбачає використання блока, реалізованого на спеціалізованій мікропроцесорній техніці. Програмні елементи при апаратній реалізації розміщуються у постійному запам'ятовуючому пристрої блока і при такій комбінованій реалізації дають змогу отримати нижчі тривалості затримок. Програмна реалізація алгоритму передбачає використання програмного забезпечення, яке реалізовує відповідний алгоритм і режим шифрування, а також при програмній реалізації використано процесор Intel Core i5-2500 з тактовою частотою 3,3 ГГц з реалізованими функцією прискорення обробки відео та функцією апаратного прискорення шифрування за стандартом AES.

Таблиця 2

Значення часу затримки для різних алгоритмів, режимів та методів реалізації симетричних алгоритмів шифрування під час передавання мультимедійних даних

Алгоритм і режим шифрування та метод реалізації			Формат представлення даних			
			MPEG-2	MPEG-4	H.264/MPEG-4 AVC	MiniDV
Алгоритм та режим шифрування	Апаратна реалізація	DES+ECB	1,172	1,1745	1,1851	1,3641
		DES+CBC	1,1721	1,1755	1,1862	1,3859
		DES+OFB	1,1978	1,1989	1,2101	1,4261
		DES+CFB	1,231	1,2412	1,3015	1,5314
		3DES	1,2461	1,2541	1,3657	1,5436
		IDEA+ECB	1,2173	1,2254	1,3617	1,5361
		IDEA+CBC	1,3241	1,345	1,4273	1,6318
		AES+ECB	1,2416	1,2434	1,3861	1,4327
		AES+CBC	1,2567	1,3071	1,4101	1,5102
		CAST-128+ECB	1,1894	1,2047	-	-
		CAST-128+CBC	1,243	1,2534	-	-
	Програмна реалізація	DES+ECB	1,2372	1,2561	1,2643	1,5679
		DES+CBC	1,238	1,2576	1,2761	1,6134
		DES+OFB	1,2597	1,2689	1,3011	1,6472
		DES+CFB	1,3965	1,4151	1,4383	1,8431
		3DES	1,4287	1,4842	1,5327	1,6239
		IDEA+ECB	1,3411	1,3521	-	-
		IDEA+CBC	1,3891	1,437	-	-
		AES+ECB	1,2371	1,2397	1,2537	1,2961
		AES+CBC	1,2467	1,2497	1,2579	1,2614
		CAST-128+ECB	1,5971	1,6437	-	-
		CAST-128+CBC	1,6733	1,7131	1,8341	-

Примітка: для симетричних алгоритмів шифрування, які допускають використання ключів змінної довжини, використано ключі мінімальної довжини.

Висновки. В результаті аналізу отриманих даних (табл. 2) можна зробити такі висновки.

Час затримки на шифрування/дешифрування для мультимедійних послуг різко зростає із ускладненням алгоритму шифрування та режиму роботи блочного шифру, що призводить до погіршення показника якості та суб'єктивного сприйняття послуги. Щоб уникнути погіршення показника якості послуги, можна виділити такі напрями вирішення проблеми: перший – це застосування порівняно простих алгоритмів шифрування та режимів роботи при використанні апаратної реалізації, таких як DES+ECB, DES+CBC, 3DES, AES+ECB, CAST-128+ECB; другий – це використання спеціалізованих апаратних засобів шифрування; третій – це використання комерційної версії алгоритму AES у програмній реалізації з використанням функції апаратного прискорення шифрування, реалізованої у процесорах серії Intel Core i5. Останній напрям вирішення проблеми погіршення показника якості можна вважати найоптимальнішим, оскільки, з одного боку, отримані затримки не є надто великими, з іншого – алгоритм AES забезпечує достатньо високий рівень криптографічної надійності.

Для покращення показника якості отримуваних мультимедійних послуг відносно часів затримок необхідно зменшити загальний час затримки передавання потоку відео/аудіо через мережу, оптимізувавши час затримок у вузлах зв'язку, введенням пріоритетності в обслуговуванні зашифрованих мультимедійних потоків даних, підвищенням пропускних здатностей ліній і усієї мережі та вибором оптимальних маршрутів передавання.

Використовувати складні алгоритми шифрування (CAST-128 та 3DES) на основі їх програмної реалізації та режимів роботи OFB і CFB з використанням виключно програмної

реалізації для передавання мультимедійних даних із забезпеченням високого показника якості отримуваної послуги нині неможливо.

1. ISO/IEC 13818 Information technology / Generic coding of moving pictures and associated video. 2. ETS 300 468: "Digital Video Broadcasting (DVB); Specification for Service Information (SI) in DVB systems". 3. ETR 211: "Digital Video Broadcasting (DVB); Guidelines for the usage of Service Information (SI) in DVB systems". 4. ISO/IEC 13818–3 "Sound". 5. Biryukov, Alex and Khovratovich, Dmitry Related-key Cryptanalysis of the Full AES-192 and AES-256 (англ.) // Advances in Cryptology – ASIACRYPT 2009. – Springer Berlin / Heidelberg, 2009. – Т. 5912. – С. 1-18. 6. Federal Information Processing Standards Publication 197 November 26, 2001 Specification for the ADVANCED ENCRYPTION STANDARD (AES). 7. Столлингс В. Криптография и защита сетей. Принципы и практика. – М.–СПб.–К.: Изд. дом «Вильямс», 2001. – 672 с.

УДК 528.8+621.37+621.39

І.В. Горбатий
Національний університет “Львівська політехніка”

МЕТОД АДАПТИВНОГО ПЕРЕДАВАННЯ ДАНИХ У СИСТЕМАХ ДИСТАНЦІЙНОГО ЗОНДУВАННЯ ЗЕМЛІ, СУПУТНИКОВИХ СИСТЕМАХ ЗВ’ЯЗКУ, РАДІОРЕЛЕЙНИХ СИСТЕМАХ ПЕРЕДАВАННЯ ПРЯМОЇ ВИДИМОСТІ

Запропоновано метод адаптивного передавання даних у системах дистанційного зондування Землі (ДЗЗ), супутникових системах зв’язку, радіорелейних системах передавання прямої видимості та інших аналогічних системах із використанням амплітудної модуляції багатьох складових (АМБС). Показано можливість застосування такого методу для підвищення ефективності розглянутих систем.

Ключові слова: супутникові системи зв’язку, зондування Землі.

The method of adaptive data transmission in the remote sensing of Earth (RSE) systems, satellite telecommunication systems, radio-relay line-of-sight transmission systems and others similar systems with the use of amplitude modulation of many components (AMMC) was offered. The possibility of application of such method for the rise of efficiency of the consider systems was shown.

Key words: satellite telecommunication systems, remote sensing of Earth.

Вступ. Найсучасніша у світі система ДЗЗ компанії Digital Globe забезпечує передавання даних ДЗЗ радіоканалом із космічного апарата (КА) WorldView-2 на наземний інформаційний комплекс (НІК) зі швидкістю 800 Мбіт/с [1]. Однак провідні компанії світу працюють у напрямі покращення просторової розрізненності оптичних і радіочастотних засобів ДЗЗ для знімання поверхні Землі, що спонукає до необхідності в майбутньому забезпечити більші швидкості передавання даних ДЗЗ. Сьогодні у таких системах використовують переважно бінарну фазову маніпуляцію (БФМн) і квадратурну фазову маніпуляцію (КФМн) [2]. Актуальним залишається питання підвищення швидкості передавання даних у системах ДЗЗ, а також інших системах передавання даних і, зокрема супутникових системах зв’язку, радіорелейних системах передавання прямої видимості (РРСП ПВ) та інших аналогічних системах. Досягти подальшого підвищення швидкості передавання даних та підвищення ефективності таких систем можливо розробленням