computing@tanet.edu.te.ua
www.tanet.edu.te.ua/computing

ISSN 1727-6209
International Scientific
Journal of Computing

Синтез структур операційних пристроїв виконання криптографічних алгоритмів IPSEC оптимізованих для обробки медіа пакетів

Тимур Коркішко[1)], Руслан Шевчук[2)]

[1)] к.т.н., старший викладач кафедри комп'ютерних наук, tko@tanet.edu.te.ua
[2)] асистент кафедри комп'ютерних наук, rsh@tanet.edu.te.ua
Інститут комп'ютерних інформаційних технологій,
Тернопільська академія народного господарства,
вул. Львівська, 11, м. Тернопіль, 46004

Анотація: *У роботі досліджується операційний пристрій протоколу IPSec оптимізований для обробки медіа пакетів. Запропоновано аналітичні вирази, які описують час обробки медіа пакетів залежно від параметрів структури операційного пристрою, побудовано математичну модель операційного пристрою процесора IPSec. На основі математичної моделі, з метою зменшення затримки та джітера, що виникають при генеруванні медіа пакету, розроблено програмне забезпечення для оптимізації характеристик структур операційного пристрою процесора IPSec. Отримано ряд оптимізованих структур операційного пристрою для різних сервісів обробки даних IPSec за різних технологічних характеристик компонентного базису. Аналіз результатів дозволив встановити, що в більшості випадків, найменший час обробки медіа пакетів спостерігається при ітераційній та ітераційно-конвеєрній реалізації операційного пристрою IPSec.*

Ключові слова: *протокол IPSec, H.235, медіа пакет, операційний пристрій, оптимізація, алгоритми MD5, SHA-1, DES.*

1. ВСТУП

Захист інформації є однією із важливих задач у телекомунікаційних мережах. Бурхливий розвиток глобальних комп'ютерних мереж та їх поступова конвергенція дає змогу територіально віддаленим користувачам взаємодіяти між собою в реальному часі, використовуючи будь-які засоби зв'язку. Більшість додатків, які працюють на базі технологій IP-телефонії, мультимедіа конференцій, веб-конференцііЙ тощо взаємодіють згідно з протоколом H.323, який визначає набір рекомендацій прийнятих Міжнародним союзом електрозв'язку (ITU) та встановлює вимоги до мультимедійних комунікаційних систем, що не гарантують якості обслуговування [1, 2]. Зауважимо, що впровадження мультимедійних додатків, що взаємодіють по протоколу H.323 повинно проводитись із врахуванням можливих загроз, визначенні критично важливих ресурсів мережі та аналізу ризиків щодо втрати інформації. Для захисту мультимедіа пакетів, що генеруються та передаються згідно з протоколом H.323 використовується протокол H.235 [3], однак даних протокол має ряд недоліків. Зокрема, недосконалі механізми захисту передачі медіа пакетів від мобільних терміналів [4], не регламентовані механізми безпечної передачі пакетів згідно протоколів серії H.26X та серії T.12X [5]. Тому, для захисту медіа пакетів, пропонується використовувати протокол IPSec [6], який застосовується на транспортному рівні OSI, що дозволяє усунути деякі недоліки H.235. Використання захищених віртуальних каналів, створених згідно з протоколом IPSec, дозволяє терміналу-приймачу привілейовано опрацьовувати медіа пакети. Додатково, протокол IPSec є більш гнучкішим в адмініструванні.

2. ПОСТАНОВКА ЗАДАЧІ

Протокол IPSec [6] використовується для забезпечення цілісності, автентичності та конфіденційності даних, що передають незахищеними комп'ютерними мережами. Головною перевагою IPSec, яка зумовила його широке використання, є можливість шифрування і/або автентифікування всієї інформації, яка передається на рівні інтернет-протоколу. Однак, невисока продуктивність роботи програмованих

процесорів, ресурси яких використовуються для реалізації протоколу IPSec зменшують продуктивність мультимедійних додатків. Крім того додавання додаткових службових полів цим протоколом до результуючого медіа пакету значно збільшує розмір пакету. Тому постає задача створення спеціалізованих процесорів IPSec оптимізованих для обробки медіа пакетів.

Проведений аналіз протоколу IPSec показав що основним компонентом, який найбільше впливає на час обробки медіа пакету та його розмір є операційний пристрій спеціалізованого процесора IPSec, який реалізує криптографічні алгоритми [7]. В основу побудови цього операційного пристрою закладено принцип апаратного відображення структури виконуваного алгоритму на операційні пристрої тракту обробки даних [12]. Структури операційних пристроїв для виконання алгоритмів симетричного блокового шифрування досліджено у [8], а структури хешування у [9].

Тому в даній роботі досліджуються структури комплексних операційних пристроїв IPSec оптимізованих відповідно до часу обробки медіа пакетів різного розміру.

3. БАЗОВІ СТРУКТУРИ ТА ЧАСОВІ ХАРАКТЕРИСТИКИ ОПЕРАЦІЙНИХ ПРИСТРОЇВ IPSEC

Сервіси IPSec дозволяють системі вибрати необхідні протоколи захисту, визначити алгоритми для відповідного сервісу і встановити значення криптографічних ключів, що використовуються для встановленого сеансу. IPSec використовує два протоколи: протокол автентифікування – AH (Authentication Header) [10] та комбінований протокол автентифікування/шифрування – ESP (Encapsulating Security Payload) [11], що в комплексі забезпечують сервіси:

- керування доступом;
- цілісність без встановлення з'єднання;
- автентифікування джерела даних;
- захист від відтворення;
- конфіденційність і частковий захист від аналізу потоку даних.

Кожен з цих сервісів вносить додаткову затримку при обробці медіа пакету, оскільки додаються відповідні поля до результуючого пакету.

Розглянемо структуру операційного пристрою виконання базових криптографічних алгоритмів протоколу IPSec в режимі передавання (рис. 1) і приймання даних (рис. 2).

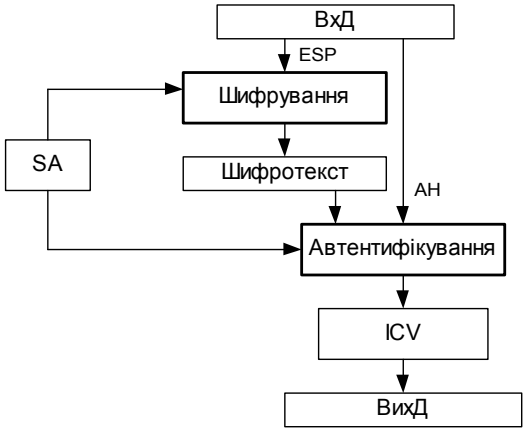

Рис. 1 – Структура операційного пристрою виконання базових криптографічних операцій IPSec в режимі передавання даних.

Вхідними даними операційного пристрою є медіа пакети, тому залежно від методу передавання даних (приймання/ передавання/суміщення) протоколу IPSec (AH/ ESP/AH+ESP) та режиму передачі даних на виході отримаємо захищені медіа пакети різного розміру. Часова затримка вихідних пакетів буде визначатися вихідними характеристиками операційного пристрою.

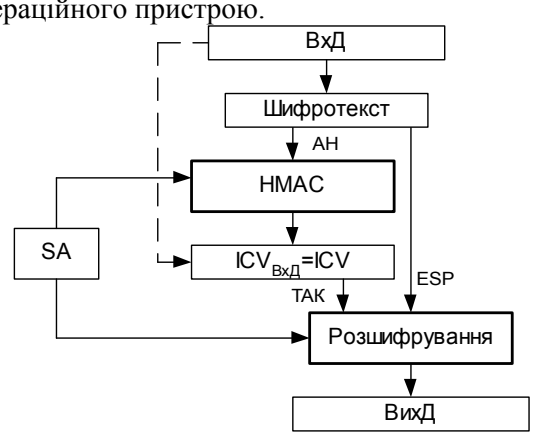

Рис. 2 – Структура операційного пристрою виконання базових криптографічних операцій IPSec в режимі приймання даних

Проведемо аналіз операційних пристроїв IPSec під час передавання/приймання даних різними протоколами в транспортному режимі з використанням IP пакетів стандарту IPv4. Для транспортного режиму AH, дані AH розміщуються безпосередньо після оригінального IP заголовку (рис. 3). Автентифікуванню підлягає весь пакет, за виключенням змінних полів в заголовку IPv4, які обнуляються для обчислення значення HMAC. Транспортний режим AH дозволяє ідентифікувати дані IP, а також окремі частини IP заголовку.

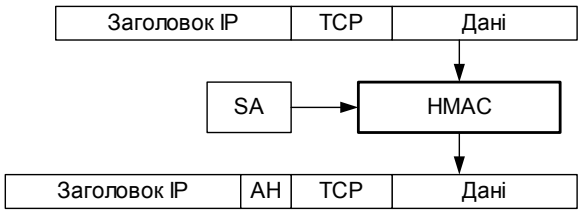

Рис. 3 – Використання протоколу AH для обробки IP пакету

Такт операційного пристрою виконання протоколу AH– t_{IPSec}, та час обробки пакету T_{IPSec} – складають відповідно:

$$t_{IPSec} = max(t_{SNx}, t_{SNx}^{1}), \quad (1)$$

$$T_{IPSec} = T_{SNx} + T_{SNx}^{1}. \quad (2)$$

де t_{SNx}, t_{SNx}^{1} – такти роботи операційних пристроїв функції автентифікування за якою обчислюється HMAC; T_{SNx}, T_{SNx}^{1} – часи роботи операційних пристроїв функції автентифікування за якою обчислюється HMAC [6,7].

Транспортний режим передачі даних ESP забезпечує шифрування даних. При цьому заголовок ESP розміщається безпосередньо перед заголовком транспортного рівня, а трейлер (містить поля заповнювача, довжини заповнювача і наступного заголовку) розміщується після пакета IP (рис. 4). Весь пакет транспортного рівня разом з трейлером шифруються.

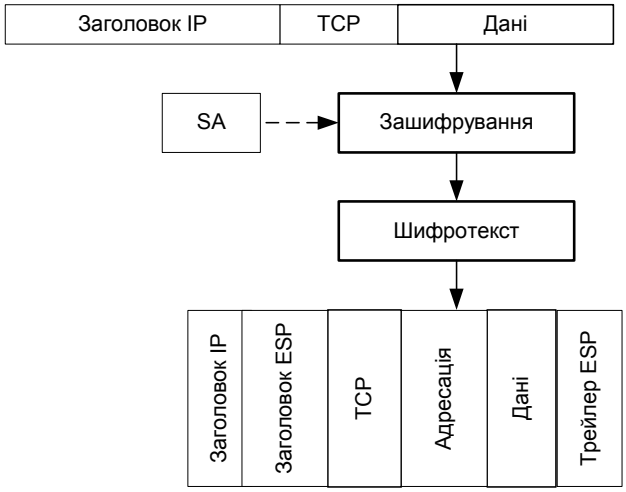

Рис. 4 – Використання протоколу ESP для обробки IP пакету

Такт роботи для виконання протоколу ESP у транспортному режимі – t_{IPSec}, та час обробки пакетів T_{IPSec} – складають відповідно:

$$t_{IPSec} = t_{SNш}, \quad (3)$$

$$Tt_{IPSec} = T_{SNш}. \quad (4)$$

де $t_{SNш}$ – такт роботи операційного пристою шифрування із структурою *SNш*, $T_{SNш}$ – час роботи операційного пристрою шифрування із структурою *SNш* [5,6].

ESP з автентифікуванням використовують для того, щоб забезпечити конфіденційність і автентифікування пакету. У транспортному режимі передавання даних, сервіси автентифікування і конфіденційності застосовуються до даних IP, не захищаючи при цьому заголовок IP (рис. 5). В цьому режимі після трейлера додається поле даних автентифікування ESP, автентифікується весь шифрований текст і заголовок ESP.

Такт роботи операційного пристрою для виконання протоколу ESP і AH у транспортному режимі – t_{IPSec}, та час обробки пакету T_{IPSec} – складають відповідно:

$$t_{IPSec} = max(t_{SNш}, t_{SNx}, t_{SNx}^{1}), \quad (5)$$

$$T_{IPSec} = T_{SNш} + (T_{SNx+} T_{SNx}^{1}). \quad (6)$$

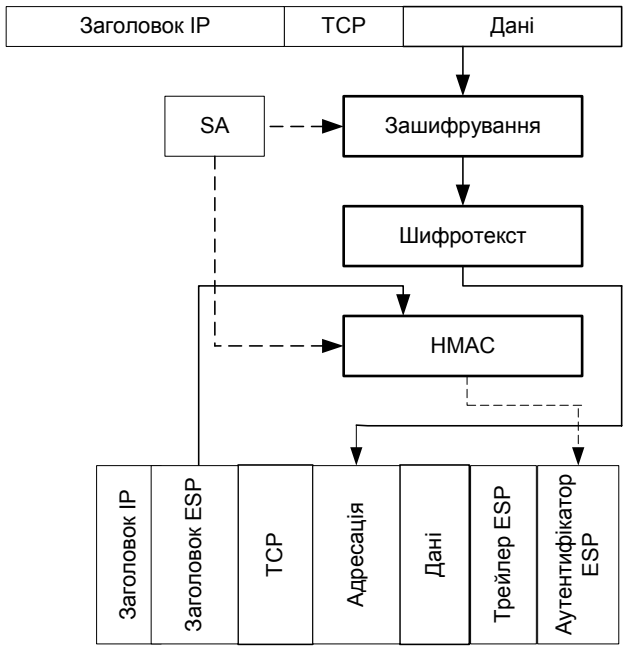

Рис. 5 – Використання протоколу AH і ESP для обробки IP пакету

Проведені дослідження структур операційних пристроїв виконання алгоритмів хешування і шифрування, параметрів протоколу IPSec, дозволяють побудувати математичну модель структури операційного пристрою IPSec.

Вхідними параметрами для побудови структури операційного пристрою процесора IPSec є:

- криптографічні алгоритми процесора IPSec: алгоритм хешування, алгоритм шифрування;

- сервіси протоколу IPSec: AH, ESP, ESP+AH;
- розмір медіа пакету;
- часові характеристики операційних пристроїв
- виконання криптографічних алгоритмів IPSec.

Шуканими параметрами моделі операційного пристрою процесора IPSec є такі параметри структур операційних пристроїв шифрування і хешування, які при заданих алгоритмах обробки, сервісах IPSec, розмірах медіа пакетів і технологічних умов реалізації процесора приймають найменші значення.

Для побудови моделі ОП пристрою процесора IPSec спочатку визначимо вектори характеристик його складових операційних пристроїв. Характеристики операційного пристрою шифрування опишемо множиною:

$$P_{Ш}=\{P_{Шi} \mid P_{Шi}=[T_{Шi}, t_{Шi}]\}. \quad (7)$$

де $P_{Шi}$ – вектор характеристик операційних пристроїв шифрування *i*-ої структури, $T_{Шi}$ – час обробки одного пакету, $t_{Шi}$ – такт роботи операційного пристрою.

Структура операційного пристрою шифрування задається параметрами: $Npp_ш$ - кількість конвеєрних регістрів алгоритму шифрування, $Nksr_ш$ - кількість комбінаційних схем алгоритму шифрування, $Nr_ш$ - кількість послідовно з'єднаних комбінаційних схем, що реалізують відповідні раунди алгоритму шифрування. Ці параметри разом з технологічними умовами виготовлення операційного пристрою визначають часові характеристики цього операційного пристрою. До технологічних умов належать часи: $Tk_ш$ – час обробки даних в комутаторі даних алгоритму шифрування, $Ткс_ш$ – час обробки даних в комбінаційній схемі алгоритму шифрування, $Трг_ш$ – час запису даних у вихідний регістр алгоритму шифрування.

Виходячи з цього та виразів запропонованих в [8], які описують часові характеристики пристроїв шифрування залежно від структури (ітераційна, конвеєрна, ітераційно-конвеєрна) операційного пристрою, представимо $t_{Шi}$ і $T_{Шi}$ у вигляді:

$$t_{Шi}(Npp_ш,Nksr_ш,Nr_ш)=\begin{cases} T_k+T_{KC}*(Ct_1*Ct_1^{ОШ}+...+Ct_{Nksr}*Ct_{Nksr}^{ОШ})+T_{Рг}, & якщо\ SN_ш - ітераційна \\ T_{KC}*(Ct_1^{ОШ}+...+Ct_{Nr}^{ОШ})/Npp+T_{Рг}, & якщо\ SN_ш - конвеєрна \\ T_k+T_{KC}*(Ct_1*Ct_1^{ОШ}+...+Ct_{Nksr}*Ct_{Nksr}^{ОШ})/Npp+T_{Рг}, & якщо\ SN_ш - ітераційно\text{-}конвеєрна \end{cases} \quad (8)$$

$$T_{Шi}(Npp_ш,Nksr_ш,Nr_ш)=\begin{cases} t_{Шi}*(Nr/Nksr), & якщо\ SN_ш - ітераційна \\ t_{Шi}*Npp, & якщо\ SN_ш - конвеєрна \\ t_{Шi}*(Nr/(Nksr*Npp)), & якщо\ SN_ш - ітераційно\text{-}конвеєрна \end{cases} \quad (9)$$

Де Ct_1 – коефіцієнт зростання часу спрацювання *i*-тої комбінаційної схеми, що реалізує проекцію раундів алгоритму шифрування; $Ct_1^{ОШ}$ – коефіцієнт зростання часу спрацювання *i*-тої комбінаційної схеми при виконанні різних операцій шифрування. Діапазон значень *i* для алгоритму DES складає 15 структур операційних пристроїв [7].

$$t_{Xj}^{A}(Npp_x,Nksr_x,Nr_x)=\begin{cases} Nksr*T_{KC1}+T_k+T_{Рг}, & якщо\ SN_x - ітераційна \\ Nksr*T_{KC1}+T_{Рг}, & якщо\ SN_x - конвеєрна \\ Nksr*T_{KC1}+T_k+T_{Рг}, , & якщо\ SN_x - ітераційно\text{-}конвеєрна \end{cases} \quad (11)$$

$$T_{Xj}^{A}(Npp_x,Nksr_x,Nr_x)=\begin{cases} (Nr-1)*t_{Xj}^{A}/Nksr+T_{KCNr}+T_{Рг}, & якщо\ SN_x - ітераційна \\ Npp*t_{Xj}^{A}+T_{KCNr}+T_{Рг}, & якщо\ SN_x - конвеєрна \\ (Nr-1)*t_{Ai}^{A}/Npp+T_{KCNr}+T_{Рг}, & якщо\ SN_x - ітераційно\text{-}конвеєрна \end{cases} \quad (12)$$

Характеристики операційного пристрою для обчислення HMAC визначається характеристиками двох операційних пристроїв хешування, з однаковими структурами операційних пристроїв, які входять до його складу.

Характеристики операційних пристроїв хешування опишемо множиною:

$$P_X^A=\{P_{Xj}^A \mid P_{Xj}^A=[T_{Xj}^A, t_{Xi}^A]\}. \quad (10)$$

де P_{Xj}^A – вектор характеристик операційних пристроїв хешування *j*-ої структури для виконання алгоритму хешування $A=\{A_M \mid A_M=[SHA\text{-}1, MD\text{-}5]\}$, $m=1,2.$, T_{Xj}^A – час виконання хешування, згідно з алгоритмом A, t_{Xi}^A – такт роботи операційного пристрою хешування згідно з алгоритмом A.

Структура операційного пристрою хешування задається алгоритмом *A,* та параметрами: Npp_X - кількість конвеєрних регістрів алгоритму хешування, $Nksr_X$ - кількість комбінаційних схем алгоритму хешування, Nr_X - кількість послідовно з'єднаних комбінаційних схем, що реалізують відповідні раунди алгоритму хешування. До технологічних умов належать часи: Tk_X^A– час обробки даних в комутаторі даних алгоритму хешування *A,* $Tкс_X^A$ - час обробки даних в комбінаційній схемі алгоритму хешування A, $Tрг_X^A$ – час запису даних у вихідний регістр алгоритму хешування A, $Tкс_{NrX}^A$ $Tкс_X^A$ - час обробки даних в Nr-тій комбінаційній схемі алгоритму хешування A.

Виходячи з цього, та виразів запропонованих в [9], які описують часові характеристики операційних пристроїв хешування залежно від структури (ітераційна, конвеєрна, ітераційно-конвеєрна) пристрою представимо, t_{XAj} та T_{XAj} у вигляді:

Характеристики операційного пристрою виконання алгоритму HMAC (A) визначається відповідними часовими характеристиками операційних пристроїв хешування, згідно з цим же алгоритмом. Враховуючи, що перший операційний пристрій обробляє повідомлення довільної довжини, а другий лише один буфер, отримаємо такі вирази:

$$T_{HMAC}^A(Npp_x,Nksr_x,Nr_x)=N^* T_{Xj1}^A(Npp_x,Nksr_x,Nr_x)+ T_{Xj2}^A(Npp_x,Nksr_x,Nr_x), \quad (13)$$

$$t_{HMAC}^A(Npp_x,Nksr_x,Nr_x)=max(t_{Xj1}^A(Npp_x,Nksr_x,Nr_x), t_{Xj2}^A(Npp_x,Nksr_x,Nr_x)). \quad (14)$$

де N – кількість буферів для обробки повідомлення.

Враховуючи, що перший і другий операційний пристрій хешування можуть мати різні структури, введемо розподілення індексів *j1, j2*. За кількістю структур операційних пристроїв HMAC для SHA-1 є 55, а для MD5 – 28 [7].

Отримавши вирази для оцінки характеристик операційних пристроїв хешування, шифрування і обчислення HMAC, побудуємо вирази для обчислення характеристик операційного пристрою процесора IPSec. При цьому врахуємо варіанти сервісів протоколу IPSec, які включають сервіси AH, ESP і AH+ESP.

Для сервісу AH з використанням алгоритму хешування A і алгоритму шифрування DES отримаємо такі вирази:

$$T_{IPSec}^{AH,A}= T_{HMAC}^A(Npp_x,Nksr_x,Nr_x). \quad (15)$$

Для сервісу ESP з використанням алгоритму шифрування DES отримаємо:

$$T_{IPSec}^{ESP,DES}= T_{Ш}(Npp_ш,Nksr_ш,16). \quad (16)$$

Для сервісу AH+ESP при передачі та приймання даних з використанням алгоритму A отримаємо:

$$T_{IPSec}^{ESP+AH}= T_{Ш}(Npp_ш,Nksr_ш,16)+T_{IPSec}^{AH,A} \quad (17)$$

4. СИНТЕЗ СТРУКТУР ОПЕРАЦІЙНИХ ПРИСТРОЇВ ВИКОНАННЯ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ IPSEC ОПТИМІЗОВАНИХ ДЛЯ ОБРОБКИ МЕДІА ПАКЕТІВ

Вхідною інформацією для синтезу структур операційних пристроїв процесорів IPSec є:

- алгоритм шифрування і хешування;
- перелік сервісів, які повинен забезпечувати процесор;
- параметри компонентного базису, в якому буде реалізовано процесор;
- розмір медіа пакетів.

Метод синтезу спеціалізованих комп'ютерних систем [12] складається з двох етапів. На першому етапі виконується представлення криптографічних алгоритмів IPSec у вигляді проекцій конкретизованих потокових графів, що реалізується заданим компонентним базисом, проводиться оцінка отриманих структур в частині часу обробки заданого числа пакетів і такту роботи для різних сервісів протоколу. Результатом виконання цього етапу є набір операційних пристроїв та відповідних їм множин параметрів, згідно з виразами (7, 10).

На другому етапі на основі результатів отриманих на першому етапі синтезуються структури операційних пристроїв процесора IPSec, оцінюються їх параметри згідно з (15 – 17) та вибирається така структура, яка забезпечує найменший час обробки медіа пакетів відповідного розміру.

На основі проведених обчислень будуються графіки залежності часу обробки медіа пакетів від структур операційних пристроїв шифрування, хешування та їх комбінації (рис. 6).

Для ідентифікації структур операційних пристроїв на рисунку 6 було використано умовне позначення запропоноване в [9]: *SN*(*Nksr*, *Npp*), де *SN* – код назви структури операційного пристрою ("і" – ітераційний граф-алгоритмічний операційний пристрій, "к" – конвеєрний граф-алгоритмічний операційний пристрій, "ік" – ітераційно-конвеєрний граф-алгоритмічний операційний пристрій), *Nksr*, *Npp* – параметри структур операційних пристроїв: кількість

реалізованих комбінаційних схем і конвеєрних регістрів відповідно.

Відомо [13], що затримку та джітер можна зменшити за рахунок обмеження максимально

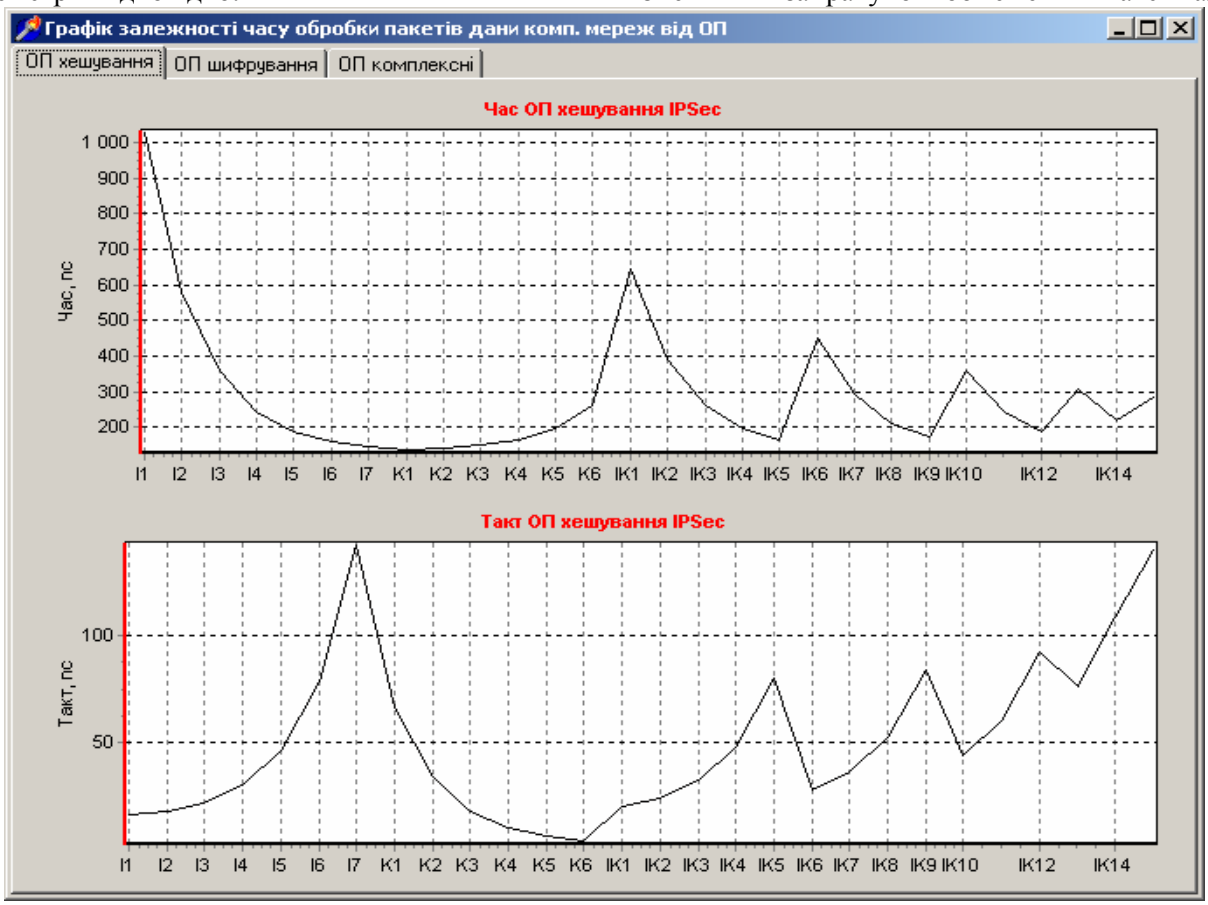

Рис. 6 – Графік залежності часу обробки медіа пакетів від структур операційних пристрої базових криптографічних алгоритмів IPSec

Аналіз графіків показує, що вибір структури оптимального операційного пристрою IPSec залежить від розміру медіа пакету та сервісів протоколу IPSec. Встановлено, що для забезпечення сервісів протоколу AH доцільно використовувати ітераційні структури операційних пристроїв, для забезпечення сервісів протоколу ESP – ітераційно-конвеєрні, а для комбінованого протоколу шифрування/автентифікування – ітераційно-конвеєрні для ESP та ітераційні для AH.

допустимого розміру медіа пакету. В цьому випадку пакети великої довжини не затримують відправку інших медіа пакетів. Цього ефекту можна досягти засобами сегментації всіх вихідних пакетів, які перевищують відповідну довжину на пристроях генерування медіа пакетів. Враховуючи рекомендації компанії Micom, в яких пов'язано максимальний розміру

Таблиця 1 – Структури операційних пристроїв виконання криптографічних алгоритмів IPSEC оптимізовані для обробки медіа пакетів

Розмір медіа пакету, біт	Швидкість поступлення медіа пакетів, Кбіт/с	Сервіси IPSec				
		AH (MD5)	AH (SHA-1)	ESP (DES)	AH+ ESP (MD5, DES)	AH+ ESP (SHA-1, DES)
256	64	i(64;1)	i(80;1)	ik(2;8)	i(64;1), ik(8;2)	i(80;1), ik(8;2)
512	128	i(64;1)	i(80;1)	ik(8;8)	i(64;1), ik(8;2)	i(64;1), ik(8;2)
2048	512	i(64;1)	i(80;1)	ik(2;8)	i(64;1), ik(8;2)	i(64;1), ik(8;2)
6144	1576	i(64;1)	i(80;1)	ik(8;8)	i(64;1), ik(16;8)	i(64;1), ik(16;2)

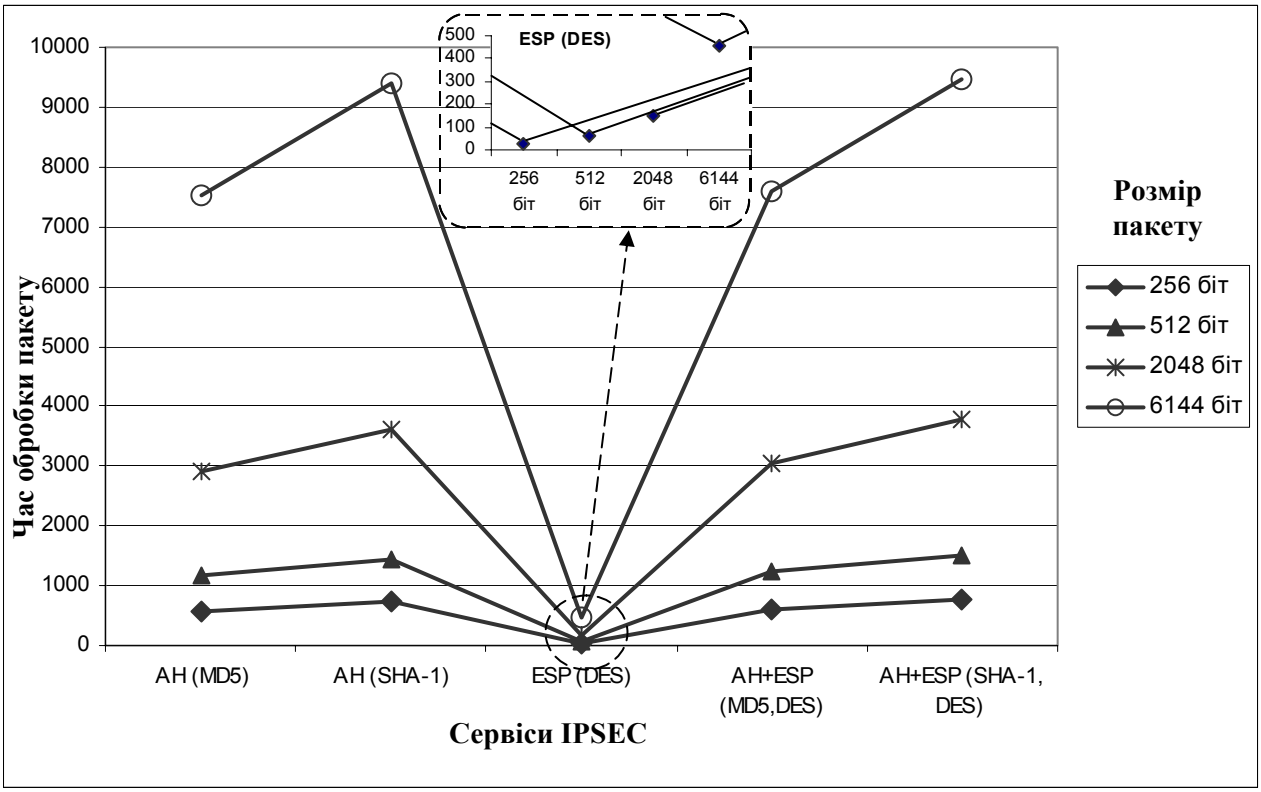

Рис. 7 – Графіки залежності часу обробки медіа пакетів різного розміру від сервісів IPSec

каналів зв'язку [13], та використовуючи розроблене програмне забезпечення для оптимізації характеристик структур операційних пристроїв процесора IPSec ми знайшли оптимізовані структури операційних пристроїв IPSec для медіа пакетів різного розміру при різних сервісах протоколу (таблиця 1).

При побудові табл. 1 ми скористались результатами синтезу операційних пристроїв хешування [9] та операційних пристроїв шифрування [8] на програмовану логічну інтегральну схему ALTERA EPF10K50-3, які дозволили визначити технологічні характеристики для знаходження параметрів оптимізованої структури процесора IPSec: $Tk_ш$=1,2 нс, $Tкс_ш$=14,3 нс, $Tрг_ш$=0,9 нс, Tk_x=0,7 нс, $Tкс_x$=9 нс, $Tрг_x$=0,3 нс, $Tкс_{Nгх}$=2,1 нс.

На рисунку 7 представлено графіки залежності часу обробки медіа пакетів різного розміру від сервісів IPSec.

Аналіз графіків дозволяє зробити висновок, що найменша тривалість обробки медіа пакетів спостерігається при використанні сервісу ESP (DES). Із збільшенням розміру пакету, значення часу його обробки зростає прямопропорційно. Найбільший час обробки медіа пакетів спостерігається при автентифікуванні згідно алгоритму SHA-1 та суміщенні сервісів протоколу IPSec (AH+ESP).

5. ВИСНОВКИ

У роботі проведено дослідження базових структур операційних пристроїв процесора IPSec, що дозволило побудувати аналітичні вирази, які описують час обробки медіа пакетів залежно від параметрів структури операційного пристрою. На основі побудованих аналітичних виразів запропоновано математичну модель операційного пристрою процесора IPSec, параметрами якої є спосіб апаратного відображення потокових графів базових криптографічних алгоритмів, вхідними змінними є алгоритми обробки даних, технологічні характеристики компонентного базису реалізації, перелік сервісів IPSec. З метою зменшення затримки та джітера що виникають при генеруванні медіа пакету розроблено програмне забезпечення для оптимізації характеристик структур операційного пристрою процесора IPSec, що дало змогу отримати ряд оптимізованих структур цього операційного пристрою для різних сервісів обробки даних за різних технологічних характеристик компонентного базису. Аналіз результатів дозволив встановити, що в більшості випадків, найменший час обробки медіа пакетів досягається при ітераційній та ітераційно-конвеєрній реалізації операційного пристрою IPSec.

6. ЛІТЕРАТУРА

[1] International Telecommunication Union, "*Packet based multimedia communication systems*", Recommendation H.323 / Telecommunication Standardization Sector of ITU, Geneva, Switzerland, Feb., 1998.
[2] Zheng Wang, "*Internet QoS, Architecture and Mechanism for Quality of Service*", Morgan Kaufmann Publishers, 340, Pine Street, San Francisco, CA 94104-3205, USA, 2001.
[3] ITU-T H.323: *Packet-based multimedia communications systems*, 9.1999. http://www.imtc.org/h323.htm.
[4] www.wave-conferencing.com/seminarb/
[5] Study Group 15. *Security and Encryption for H-Series (H.323 and other H.245-Based) Multimedia Terminal*s. Telecommunication Standardization Sector, ITU-T, November 2000.
[6] S. Kent , R. Atkinson. *Security Architecture for the Internet Protocol* // Internet-Draft, May 1998.
[7] Шевчук Р.П.. *Оптимізація програмно-апаратних засобів реалізації IPSec*. Маг. Роб., Тернопіль: , 2003. – 121 с.
[8] Коркішко Т.А., Мельник А.О. *Методика проектування багатоканальних процесорів симетричного блокового шифрування* // Вісник Тернопільського державного технічного університету. – Тернопіль, 2002. – Т.7, № 2. – С. 100 – 109.
[9] Т. Коркішко, Л. Коркішко, Р. Шевчук. *Базові структури операційних пристроїв хешування для процесорів підтримки протоколу IPSEC* // Комп'ютинг. – 2003. – Том 2. - №1. – С. 41-47.
[10] Kent S, Atkinson R. *IP Authentication Header* // RFC 2402, November 1998.
[11] Kent S, Atkinson R. *IP Encapsulating Security Payload* // RFC 2406, 1998.
[12] Мельник А.О. *Спеціалізовані комп'ютерні системи реального часу*. –Львів, 1996.
[13] http://www.micom.com

***Тимур Коркішко**, закінчив Державний університет "Львівська політехніка" за спеціальністю "Комп'ютерні та інтелектуальні системи і мережі" у 1997 році. У 2003 році отримав науковий ступінь кандидата технічних наук. З 2002 року працює старшим викладачем кафедри комп'ютерних наук Тернопільської академії народного господарства. Викладає курси: мови програмування, основи автоматизованого проектування засобів обчислювальної техніки. Області наукових інтересів: високошвидкісна криптографія, методологія розробки криптографічних процесорів і акселераторів, мови програмування. Автор більш як 25 наукових праць.*

***Руслан Шевчук**, з 1998 року студент інституту комп'ютерних інформаційних технологій Тернопільської академії народного господарства. З 2001 року працює інженером в спеціалізованій лабораторії програмного забезпечення кафедри комп'ютерних наук. Області наукових інтересів: процесори протоколу IPSec, криптографія, апаратна реалізація криптографічних алгоритмів.*

SYNTHESIS OF STRUCTURES OF OPERATING DEVICES IMPLEMENTATION CRYPTOGRAPHIC ALGORITHMS IPSEC OF OPTIMIZED FOR MEDIA PACKAGES PROCESSING

Tymoor Korkishko[1], Ruslan Shevchuk[2]

1) Chief lecturer of Computer Science department , tko@tanet.edu.te.ua
2) Assistant of Computer Science department, rsh@tanet.edu.te.ua
Institute of Computer Information Technologies
Ternopil Academy of National Economy
Peremoga Square 3, Ternopil 46004, Ukraine

Abstract: *In the paper the operating device of IPSec protocol optimized for treatment media of packages is investigated. Analytical expressions which describe time of media packages processing depending on the parameters of operating device structure are offered, the mathematical model of operating device of IPSec processor is developed. On the basis of mathematical model, with the purpose of reduction of delay and jitter, which rise up during the generation of media package, software is developed for optimization of structures descriptions of processor IPSec operating device. The row of the optimized structures of operating device is got for different services of given IPSec treatment at different technological descriptions of component base. The analysis of results allowed to set that in most cases, the least time of treatment media of packages is observed at iterative and iterative-conveyer realization of IPSec operating device.*

Keywords: *IPSec-protocol, H.235, MD5 algorithm, media packet, optimization, SHA-1, DES*

1 INTRODUCTION

Security of information is one of important tasks in communications networks. Development of global computer networks and their gradual convergence enables to the territorial remote users to co-operate between itself in the real time, using any communication means. Most programs of IP-telephony, multimedia conferences, web-conferences and others use protocol H.323. Protocol H.323 determines the set of recommendations accepted by the International telecommunication union (ITU) and sets the requirements to the multimedia communication systems that do not guarantee quality of service [1, 2]. Development of multimedia programs that use H.323 must be conducted with consideration of possible threats, determination critically of important resources of network and analysis of risks in relation to the loss of information. For security of multimedia packages, that are generated and transmission with H.323, protocol H.235 is used [3]. However, protocol H.235 has the some imperfection. Current system shortcomings of security for transmission media packages from mobile terminals [4]. There are no mechanisms of secure transmission of packages with protocols H.26X and T.12X [5]. Therefore, for security media packages, suggested to use protocol IPSec [6]. IPSec used on transport level OSI and allows remove some imperfection H.235. The use of the security virtual circuits created by IPSec, allows privileged processing media packages in terminal-receiver. Additionally, protocol IPSec is more flexible in administration.

Protocol IPSec [6] is used for providing of integrity, authentication and confidentiality of data that transmission by insecurity computer networks. Primary advantage IPSec there is possibility of coding and/or authentication all information which transmission by internet protocol. However, low productivity of programmable processors, the resources of which are used for realization of IPSec diminishes productivity of multimedia program. Adding additional fields by this protocol to the resulting media package considerably multiplies the size of package. Therefore the task of creation of the specialized processors IPSec of optimized for processing media packages is actual.

The conducted analysis of protocol IPSec showed that basic component, which most influences in a time of processing media package and his size is operating device of the specialized processor IPSec, which will realize cryptographic algorithms [7]. Basic principle of construction this operating device is vehicle reflection structure of executable algorithm to tracts of data processing operating devices [12]. The structures of operating devices for implementation algorithms of symmetric block encryption are research in [8], and structures of hash in [9].

Therefore in this work the structures of complex operating devices IPSec of optimized according to time of processing media packages of a different size are explored.

Media packages are entrance data of operating device, therefore depending on the method of data (receive/ transmit /combination) of protocol IPSec (AH/ ESP/AH+ESP) and mode of data communication on an output we will get the protected media packages of a different size. Time delay of output packages will be determined by output descriptions of operating device.

In work the conducted analysis of operating devices IPSec during transmit/receive by different protocols in the transport mode with the use of IPv4, that allowed to build analytical expressions, which describe time of processing media packages depending on the parameters of structure operating device. For the transport mode AH, the given AH take place directly after original to the IP header. Autentification is subject all package after the exception of the variable fields in a header IPv4, which set to zero for the calculation of value HMAC. The transport mode AH allows identifying given IP, and also separating parts to the IP header. The transport mode of transmission of given ESP provides encrypting of data. Thus a header ESP takes place immediately in front of header transport level, and trailer (contains the fields of filler, lengths of filler and following to the header) takes place after a package IP. All package of transport level together with trailer are encrypting.

On the basis of the built analytical expressions the mathematical model of operating device of processor IPSec, the parameters of which the method of vehicle reflection of flow-graph of base cryptographic algorithms. Reduction of delay and jitter that arise up during the generation media package software is developed for optimization of descriptions structures of operating device processor IPSec. The analysis of results allowed that with the increase the size of package, the value of time of his processing grows linear.

REFERENCES

[1] International Telecommunication Union, "*Packet based multimedia communication systems*", Recommendation H.323 / Telecommunication Standardization Sector of ITU, Geneva, Switzerland, Feb., 1998.

[2] Zheng Wang, "*Internet QoS, Architecture and Mechanism for Quality of Service*", Morgan Kaufmann Publishers, 340, Pine Street, San Francisco, CA 94104-3205, USA, 2001.

[3] ITU-T H.323: *Packet-based multimedia communications systems*, 9.1999. http://www.imtc.org/h323.htm.

[4] www.wave-conferencing.com/seminarb/

[5] Study Group 15. *Security and Encryption for H-Series (H.323 and other H.245-Based) Multimedia Terminal*s. Telecommunication Standardization Sector, ITU-T, November 2000.

[6] S. Kent , R. Atkinson. *Security Architecture for the Internet Protocol* // Internet-Draft, May 1998.

[7] Шевчук Р.П.. *Оптимізація програмно-апаратних засобів реалізації IPSec*. Маг. Роб., Тернопіль: , 2003. – 121 с.

[8] Коркішко Т.А., Мельник А.О. *Методика проектування багатоканальних процесорів симетричного блокового шифрування* // Вісник Тернопільського державного технічного університету. – Тернопіль, 2002. – Т.7, № 2. – С. 100 – 109.

[9] Т. Коркішко, Л. Коркішко, Р. Шевчук. *Базові структури операційних пристроїв хешування для процесорів підтримки протоколу IPSEC* // Комп'ютинг. – 2003. – Том 2. - №1. – С. 41-47.

[10] Kent S, Atkinson R. *IP Authentication Header* // RFC 2402, November 1998.

[11] Kent S, Atkinson R. *IP Encapsulating Security Payload* // RFC 2406, 1998.

[12] Мельник А.О. *Спеціалізовані комп'ютерні системи реального часу*. –Львів, 1996.

[13] http://www.micom.com