

УДК 621.391

В.А. КАПТУР, Є.В. ДОБРОВОЛЬСЬКИЙ, О.О. ЯНІНА

Одеська національна академія зв'язку ім. О.С. Попова, Україна

## МЕТОД МІНІМІЗАЦІЇ СЛУЖБОВОЇ ІНФОРМАЦІЇ ПРИ ТУНЕЛЮВАННІ ІР-НАВАНТАЖЕННЯ

В роботі розглянуто базові принципи тунелювання голосового навантаження крізь ІР-мережу та запропоновано новий метод мінімізації надлишковості службової інформації при тунелюванні ІР-навантаження, який базується на принципах збереження контекстної інформації RTP-сесій, а також на мультиплексуванні корисного навантаження паралельних сесій. Розроблено алгоритми роботи компресора та декompresора, які можуть бути використані на протилежних кінцях тунелю. Запропоновано низку аналітичних виразів для оцінки ефективності запропонованого методу тунелювання голосового навантаження, а також надано рекомендації щодо сфери його застосування.

**Ключові слова:** пакетна мережа, тунель, стиснення голосового навантаження, ІР-телефонія, протокольна надлишковість.

Стрімкий розвиток інфокомунікаційних технологій, який викликав зростання обсягів ІР-навантаження, що циркулює в сучасних телекомунікаційних мережах, як ніколи гостро поставив перед науковцями проблему пошуку нових методів підвищення ефективності передавання цього навантаження. За таких умов особливо актуальним постає питання мінімізації обсягів службового навантаження (протокольної надлишковості).

Особливої актуальності це питання набуває при створенні корпоративних мереж, які складаються з декількох територіально рознесених сегментів, для поєднання яких використовуються орендовані ресурси операторів телекомунікацій. Це пояснюється тим, що найбільш розповсюдженим методом поєднання окремих сегментів до єдиної логічної мережі є організація єдиного адресного простору та прозорого транспортування ІР-пакетів між такими сегментами за допомогою тунелювання. При цьому орга-

нізація такого поєднання, як правило, лише збільшує обсяг інформації, що передається орендованими каналами за рахунок додаткової інкапсуляції, що найбільше позначається на пакетах невеликих розмірів (наприклад, медіа даних голосового навантаження).

Метою статті є розробка методу мінімізації протокольної надлишковості при тунелюванні медіа даних голосового навантаження.

Як відомо в основу процесу тунелювання (рис. 1) ІР-навантаження між двома сегментами пакетної мережі покладено принцип інкапсуляції блоків даних нижчих або рівних рівнів до блоків даних вищих або рівних рівнів моделі OSI (Open System Interconnection) [1]. За рахунок цього з'являється можливість використовувати єдину адресацію та механізми маршрутизації в межах всієї корпоративної мережі, не зважаючи на кількість сегментів, що входять до її складу.

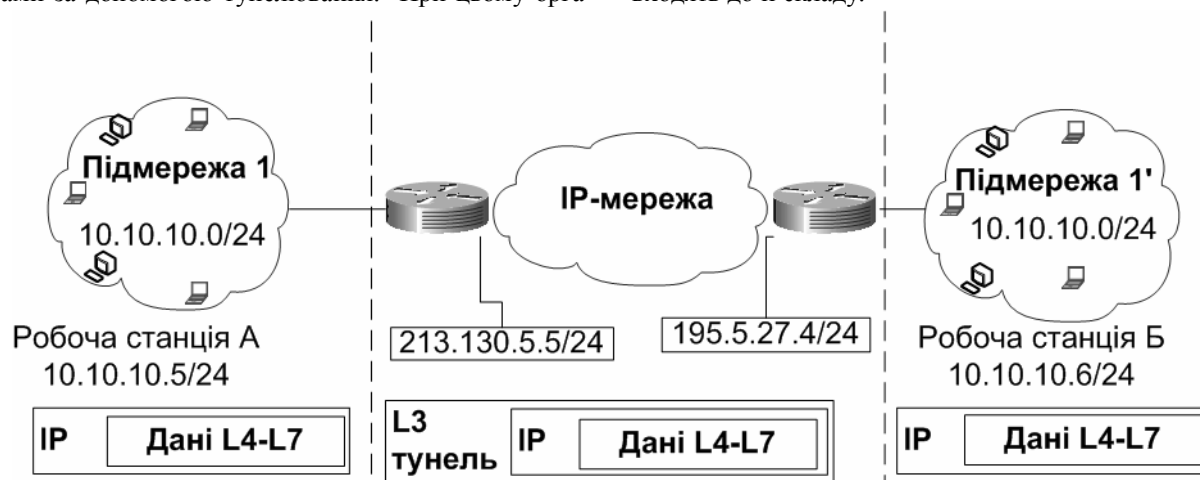


Рис. 1. Процес тунелювання ІР-навантаження

На рис. 1 наведено приклад поєднання двох незалежних сегментів корпоративної мережі крізь IP-мережу за допомогою двох маршрутизаторів. Слід зазначити, що адресація вузлів в обох зображених на рисунку підмережах (1 та 1') здійснюється в межах однієї логічної підмережі. Таким чином, для обміну інформацією між робочою станцією А та робочою станцією Б використовуються ті самі механізми, що й для обміну інформацією в межах одного фізичного сегменту. Такий ефект досягається за рахунок прозорого тунелювання навантаження між двома маршрутизаторами, яке полягає в додатковій інкапсуляції ще одного заголовку до надісланих на внутрішні інтерфейси маршрутизаторів пакетів (рис. 2). При цьому у разі, якщо пакет спрямований від робочої станції А до робочої станції Б (для наведеного вище прикладу) адресою призначення зовнішнього заголовку буде IP-адреса 195.5.27.4, а адресою відправника 213.130.5.5.

Обсяг службової інформації, який додатково додається до кожного IP-пакету при тунелюванні IP-навантаження, залежить від конкретної реалізації тунелю. Так, наприклад, при використанні тунелів типу «IP-GRE», розроблених компанією Cisco Systems [2], крім додавання ще одного IP-заголовку до кожного IP-пакету додається також спеціальний заголовок формату GRE (Generic Routing Encapsulation), який може мати розмір від 4 до 20 байт.

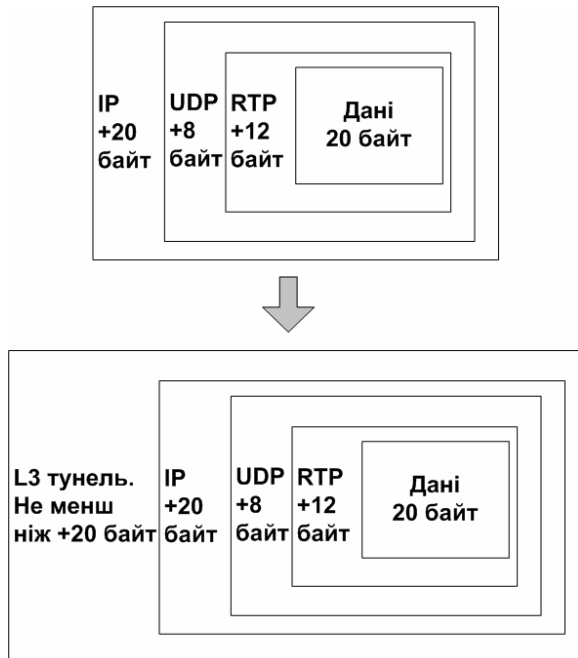


Рис. 2. Процедура додаткової інкапсуляції

В свою чергу тунелювання типу «IP-IP», розроблене компанією IBM [3], передбачає додавання до базового пакету лише одного IP-заголовку розміром 20 байт. Зрозуміло, що саме цей тип тунелю є

найменш витратним з точки зору протокольної надлишковості. Очевидно, що додаткова інкапсуляція 20-ти байт до кожного пакету практично не впливає на передавання пакетів великих розмірів, однак призводить до небажаних наслідків при тунелюванні навантаження IP-телефонії, при якому корисна голосова інформація передається пакетами невеликих розмірів. При цьому збільшення розміру кожного такого пакету, що передається каналами зв'язку, на 20 байт автоматично призводить до необхідності збільшення достатньої для передавання навантаження [4] пропускної спроможності каналу зв'язку приблизно на 30%. Зазначена проблема особливо гостро постає у разі організації віртуальних тунелів між двома мережними об'єктами, що виконують роль комутаторів з'єднань IP-телефонії (Softswitch, IP-PBX тощо). В цьому випадку для кожного віртуального з'єднання з метою передавання голосової інформації між двома вузлами мережі пересилається значна кількість пакетів невеликих розмірів, до кожного з яких застосовується процедура додаткової інкапсуляції.

Орієнтовний розмір пропускної спроможності  $v_{\text{тун}}$  каналу зв'язку необхідної для одночасного передавання  $C_{\text{з'єднань}}$  телефонних з'єднань крізь тунель між двома комутаційними вузлами можна визначити за формулою:

$$v_{\text{тун}} = \frac{C_{\text{з'єднань}} (L_{\text{PL}} + L_{\text{RTP}} + L_{\text{UDP}} + L_{\text{IP}} + L_{\text{tun}})}{t_{\text{PL}}}, \quad (1)$$

де  $L_{\text{PL}}$  – розмір корисного навантаження, необхідного для передавання одного голосового кадру, біт;

$L_{\text{RTP}}$  – розмір RTP-заголовку, біт;

$L_{\text{UDP}}$  – розмір заголовку UDP-датаграми, біт;

$L_{\text{IP}}$  – розмір заголовку IP-пакету, біт;

$L_{\text{tun}}$  – розмір заголовку, який визначається типом тунелю, біт;

$t_{\text{PL}}$  – тривалість одного голосового кадру, с.

Так, наприклад, при використанні голосових кадрів тривалістю 20 мс, кожен з яких представлено у вигляді корисного навантаження розміром 20 байт, а також за умов використання мінімальних розмірів заголовків протоколів RTP (Real-time Transport Protocol), UDP (User Datagram Protocol) та IP (12, 8 та 20 байт відповідно) при передаванні одночасно більш ніж 100 голосових з'єднань орієнтовний розмір необхідної пропускної спроможності каналу зв'язку складе 2,4 Мбіт/с без використання тунелювання IP-навантаження та 3,2 Мбіт/с при використанні тунелю типу «IP-IP».

Одним з найбільш відомих шляхів мінімізації необхідної пропускної спроможності каналів зв'язку при передаванні мультимедійного IP-навантаження

є застосування протоколу сRTP (Compressed RTP) [5, 6], який передбачає стиснення заголовків IP/UDP/RTP для передавання в межах низькошвидкісних каналів зв'язку побудованих за принципом «точка-точка». Базовим принципом протоколу сRTP є збереження на обох кінцях каналу зв'язку (компресорі та декомпресорі) контекстів RTP-сесій, які включають опис типової для сесії структури службових заголовків IP/UDP/RTP, із подальшим передаванням між компресором та декомпресором лише тієї частини заголовків, які змінилися в супереч очікуванням компресора.

Всі поля в структурі заголовків трьох вищезазначених протоколів (IP, UDP та RTP) при передаванні пакетів в межах однієї RTP-сесії можна умовно поділити на три класи: статичні поля, відновлювальні поля, змінні поля.

Статичні поля – це поля, значення яких не змінюються під час передавання інформації в межах RTP-сесії. Таким чином, достатньо на початку RTP-сесії передати від компресора до декомпресора значення цих полів, і вони можуть бути відновлені на іншому кінці каналу зв'язку для кожного пакету, що надійшов від компресора. До таких полів належить весь заголовок IP-пакету, більша частина UDP-заголовку (крім поля контрольна сума), а також всі поля RTP-заголовку крім «чергового номеру» та «мітки часу».

Відновлювальні поля – це поля, алгоритм відтворення яких заздалегідь відомий, що дозволяє не передавати їх значення крізь канал зв'язку, а просто вилучати їх на стороні компресора та відтворювати на іншому. Прикладом відновлювального поля може бути поле «контрольна сума» UDP-заголовку.

Змінні поля можуть або приймати певну завершену кількість значень, що дозволяє закодувати це поле кодовою послідовністю значно меншого розміру, або їх стиснення взагалі недоцільне. В типовому пакеті, який містить голосові фрейми, як правило, є лише два змінних поля, які розміщуються в межах RTP-заголовку – «черговий номер» та «мітка часу». Слід однак зазначити, що поле «черговий номер» має чітко оговорений алгоритм змінення від одного пакету до іншого, та можливі відхилення від цього алгоритму є виключенням з правил та частіш за все пояснюються проблемами при передаванні голосової інформації, що потребує оновлення контекстів RTP-сесій на обох кінцях каналу зв'язку.

Зважаючи на те, що при тунелюванні IP-навантаження утворюється віртуальний канал зв'язку, побудований за принципом «точка-точка», принцип стиснення заголовків IP/UDP/RTP, розглянутий в специфікації протоколу сRTP, може бути використаний і в цьому випадку. Однак, зважаючи на те, що протокол сRTP було розроблено для низь-

кошвидкісних каналів зв'язку (наприклад, dial-up з'єднання) він має декілька суттєвих недоліків. Так, наприклад, цей протокол не дозволяє використовувати частину незадіяних полів IP-заголовку верхнього рівня для мінімізації відносного збільшення обсягу службової інформації, а також не має механізмів поєднання корисної інформації від різних RTP-сесій в межах одного пакету. Необхідність в реалізації такого функціоналу особливо гостро постає при організації взаємоз'єднань між двома серверами IP-телефонії за умов одночасного передавання великої кількості RTP-сесій. В цьому випадку заголовки IP/UDP/RTP з паралельних RTP-сесій також містять велику кількість схожих за значеннями полів, що дозволяє застосувати цю властивість для більш ефективного стиснення службової інформації, ніж для випадку незалежної компресії RTP-сесій.

Вирішенням цих проблем може стати запропонований механізм мінімізації службової інформації при тунелюванні IP-навантаження. В основу запропонованого методу покладено принцип, зображений на рис. 3.

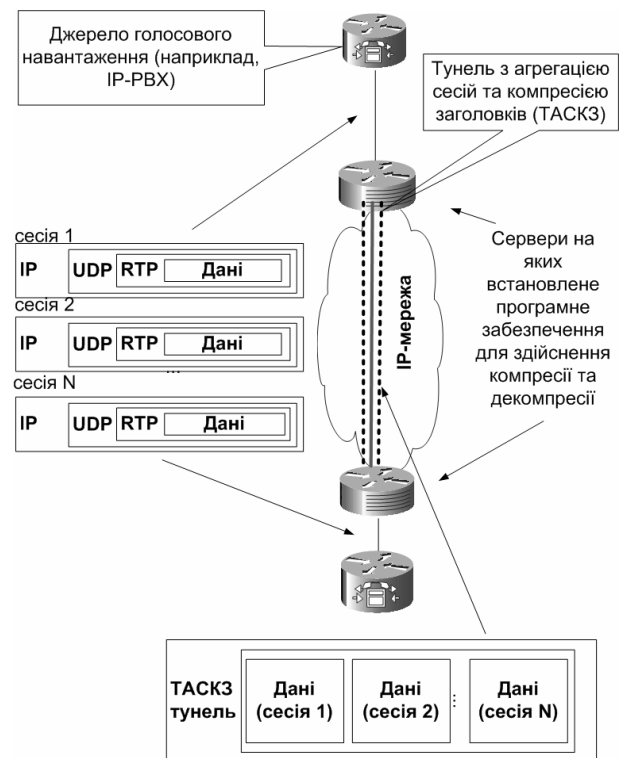


Рис. 3. Пропонований принцип роботи тунелю

Як зображено на рис. 3, на кожній зі сторін IP тунелю окрім звичайних засобів тунелювання, що передбачають включення до кожного пакету додаткового IP-заголовку, реалізовано компресор та декомпресор. Як компресори, так і декомпресори оперують спеціальними таблицями контекстів RTP-сесій. За допомогою інформації, яка зберігається в зазначених таблицях, компресори (за аналогією з

протоколом sRTP) можуть не передавати всю службову інформацію для кожного голосового кадру, а попередньо забезпечити передавання першого з пакетів в межах RTP-сесії декомпресору і в подальшому передавати лише унікальний ідентифікатор контексту та спеціальні інформаційні повідомлення у разі відхилення службової інформації в наступному пакеті тієї самої RTP-сесії від очікуваних значень. Такий підхід дозволяє зменшити розмір службової інформації, що передається із кожним голосовим кадром з 40 байт до 2-4 байт на кожен пакет [5].

Додаткового зменшення обсягу службової інформації можна досягти за рахунок агрегації пакетів з різних RTP-сесій, що надходять до компресора на протязі періоду часу меншого за середню різницю в часі між надходженням двох пакетів з однієї RTP-сесії. Така агрегація дозволяє збільшити швидкість передавання корисного навантаження за рахунок зменшення сукупного обсягу службового навантаження, що передається із кожним голосовим фреймом. Можливість агрегації RTP-сесій передбачена в протоколі IAX2 (Inter-Asterisk eXchange protocol) [7], який використовується сумісно із IP-PBX Asterisk та в протоколі TCRTCP (Tunneling Multiplexed Compressed RTP) [8], який запропонований компанією Cisco Systems. Однак зважаючи за низку суттєвих недоліків: в специфікації обох протоколів не визначається реалізація механізмів агрегації, а лише констатується її можливість; обидва протоколи мають обмежене застосування (в межах окремої платформи або виключно із певним типом протоколу каналного рівня) – жоден з цих протоколів не може використовуватися для вирішення проблем в комплексі.

На рис. 4 зображено узагальнений алгоритм роботи компресора, який крім процедур, характерних для протоколу sRTP, використовує механізм агрегації голосових фреймів, які належать різним RTP-сесіям між одними і тими самими вузлами.

Після надходження до компресору нового IP-пакету (рис. 4) в першу чергу здійснюється перевірка на наявність в цьому пакеті голосових даних, що передаються в межах типової RTP-сесії (перевіряється тип протоколів у відповідних полях заголовків, розмір пакету тощо). У разі, якщо до тунелю надійшов пакет із голосовою інформацією, проводиться аналіз IP-адрес відправника та одержувача, а також номерів портів протоколу UDP та за допомогою цієї інформації здійснюється пошук контексту RTP-сесії в таблиці контекстів. Якщо контекст знайдено, компресором здійснюється перевірка на додержання очікуваних змін по відношенню до останнього збереженого стану контексту і у випадку, коли надійшов пакет, змінні поля службових заголовків якого набули очікуваних змін, здійснюється формування пакету із зменшеним обсягом заголовку,

який обов'язково містить ідентифікатор контексту, порядковий номер пакету в межах сесії тощо. У разі, якщо контекст не було знайдено або до компресора надійшов пакет із не очікуваними змінами, здійснюється створення нового контексту в таблиці або оновлення існуючого із подальшим пересиланням пакету із всіма службовими заголовками та додаванням ідентифікатора контексту.

Після формування пакету (рис. 4) він зберігається до проміжного буфера. У разі, якщо до цього в буфері інших пакетів не було, лічильник часу агрегації встановлюється в нульове значення. Додавання значень до лічильника здійснюється із надходженням до компресора штучних пакетів синхронізації. Одержані пакети зберігаються до проміжного буфера та не надсилаються до іншої сторони тунелю до того часу, доки лічильник часу агрегації не перевищить заданого значення  $T_{max}$ . Після цього всі збережені в проміжному буфері пакети (як повні так і зменшені) збираються до одного агрегованого пакету та пересилаються на інший бік тунелю до декомпресора. В свою чергу всі інші пакети (в яких не міститься голосова інформація) відразу пересилаються на інший бік тунелю.

Декомпресор, алгоритм роботи якого зображено на рис. 5, після одержання чергового пакету, насамперед, здійснює деінкапсуляцію інформації, одержаної з іншого боку тунелю.

Після виділення цієї інформації здійснюється перевірка типу пакету (агрегований або ні). У разі, якщо до декомпресора надійшов агрегований пакет, декомпресор організує цикл обробки всіх пакетів, що входять до його складу. Першим кроком такої обробки є перевірка на повноту пакету. У разі, якщо пакет містить повні заголовки протоколів IP/UDP та RTP здійснюється створення нового контексту або оновлення існуючого в таблиці контекстів RTP-сесій декомпресора. В свою чергу, якщо пакет містить лише ідентифікатор контексту та порядковий номер пакету, здійснюється пошук контексту в таблиці та або відновлення пакету з контексту із подальшим його передаванням до верхніх рівнів стеку або формування та надсилання до іншого боку тунелю повідомлення про пошкодження контексту.

В свою чергу, якщо до декомпресора надійшов не агрегований пакет, то в цьому випадку насамперед здійснюється перевірка на одержання повідомлення про пошкодження контексту. Така перевірка необхідна для обробки повідомлень від декомпресора на іншому боці тунелю. У разі одержання такого повідомлення здійснюється знищення пошкодженого контексту з таблиць контекстів RTP-сесій компресора та декомпресора та вихід з процедури без передавання пакету далі (рис. 5). У всіх інших випадках пакет передається до верхніх рівнів стеку.

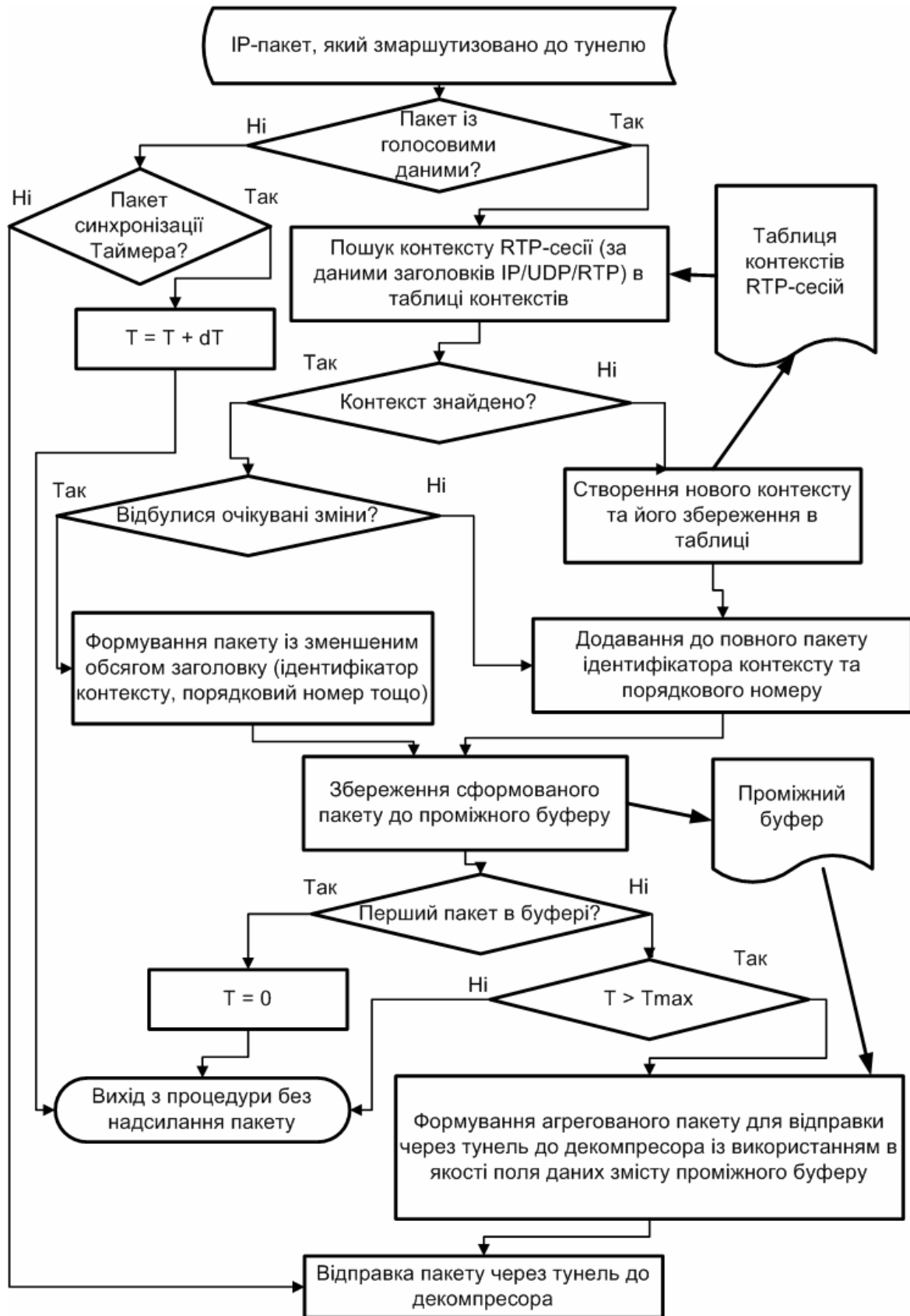


Рис. 4. Алгоритм роботи компресора

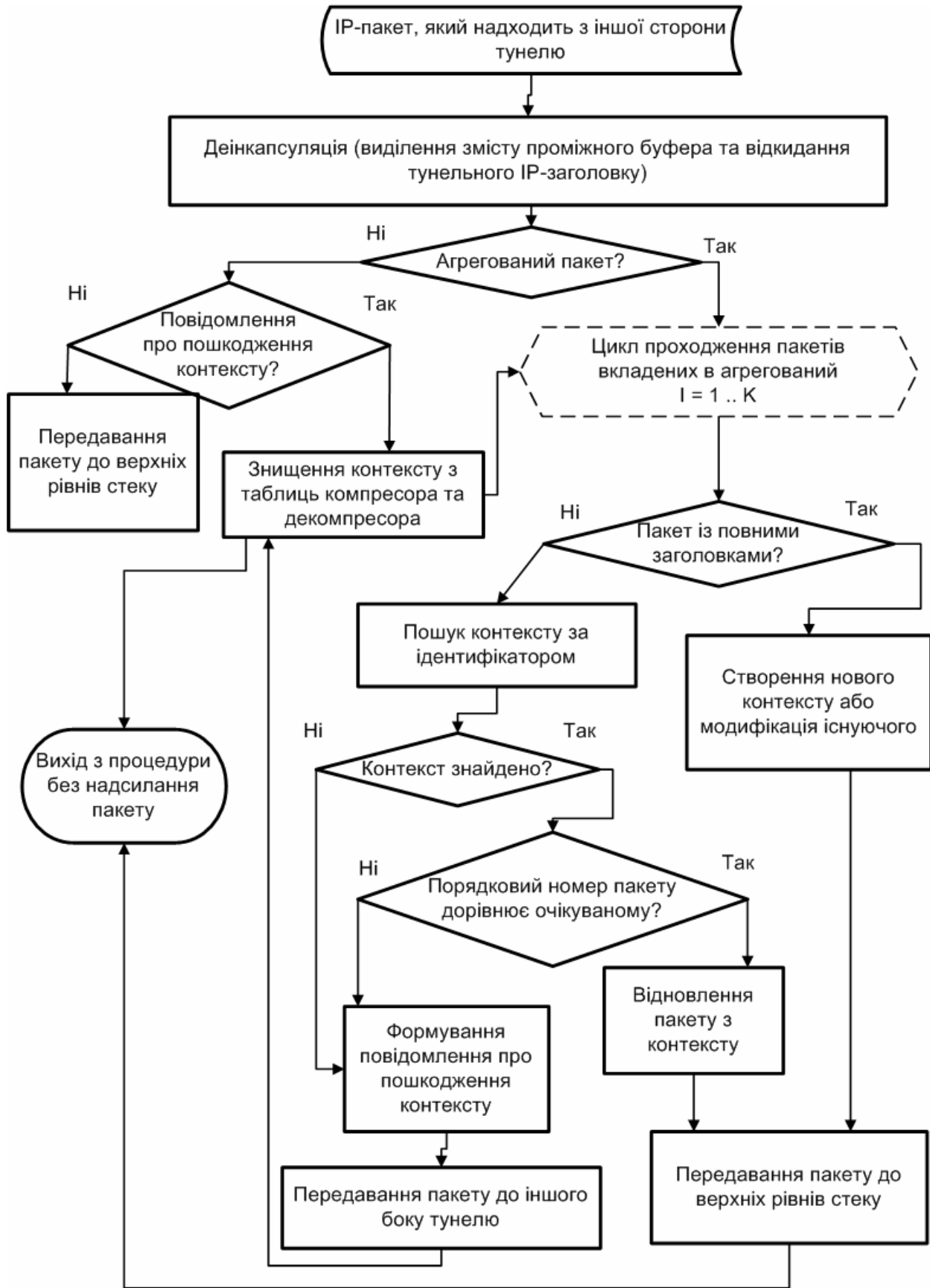


Рис. 5. Алгоритм роботи декомпресора

З рис. 4 та 5 зрозуміло, що спосіб агрегації голосової інформації від різних RTP-сесій дозволяє зменшити загальний обсяг інформації, що передається каналом зв'язку за рахунок зменшення обсягів службової інформації, що передається із кожним голосовим пакетом. Така мінімізація, в свою чергу, зменшує необхідну для передавання однієї RTP-сесії пропускну спроможність. Орієнтовний розмір пропускної спроможності  $v_{\text{TACK3}}$  каналу зв'язку, необхідної для одночасного передавання  $C_{\text{з'єднань}}$  телефонних з'єднань крізь тунель з агрегацією сесій та компресією заголовків («TACK3») між двома комутаційними вузлами, можна визначити за формулою:

$$v_{\text{TACK3}} = (L_{\text{IP}} + L_{\text{TACK3}} + C_{\text{з'єднань}}(L_{\text{PL}} + L_{\text{TACK3\_PL}})) / t_{\text{PL}}, \quad (2)$$

де  $L_{\text{TACK3}}$  – розмір службового заголовку, який додається до кожного агрегованого пакету, біт;

$L_{\text{TACK3\_PL}}$  – розмір службового заголовку, який додається до кожного голосового фрейму (при необхідності), біт.

Значення  $L_{\text{IP}}$ ,  $L_{\text{PL}}$  та  $t_{\text{PL}}$  мають той самий сенс, що й для формули (1).

Приблизну оцінку ефективності застосування запропонованого методу можна зробити шляхом обчислення коефіцієнту ефективності

$$K_{\text{ефект}} = \frac{v_{\text{тун-IP}}}{v_{\text{TACK3}}} \quad (v_{\text{тун-IP}} - \text{пропускна спроможність, визначена за допомогою формули (1) при } L_{\text{тун}}=20 \text{ байт), який наглядним чином демонструє, в скільки разів можна зменшити необхідну пропускну спроможність каналу зв'язку при застосуванні запропонованого в роботі тунелю «TACK3» замість класичного «IP-IP».$$

На рис. 6 зображено графік залежності коефіцієнту від кількості одночасних з'єднань при розмірі службових заголовків  $L_{\text{TACK3}}$  та  $L_{\text{TACK3\_VF}} = 4$  та 2 байти відповідно, для голосових кадрів тривалістю 20 мс при стандартних розмірах заголовків IP, UDP та RTP (20, 8 та 12 байт відповідно).

Як видно з графіку (рис. 6), вже при 5-ти одночасних RTP-сесіях при застосуванні запропонованого методу обсяг інформації, що передається крізь канал зв'язку, зменшується втричі у порівнянні із використанням класичних методів тунелювання навантаження.

В свою чергу, кількість одночасних з'єднань, корисне навантаження яких може бути агреговане за допомогою запропонованого методу, досить сильно залежить від розміру інтервалу агрегації. Таким чином, очевидно, що чим більше розмір інтервалу аг-

регації, тим більшим буде значення коефіцієнту ефективності.

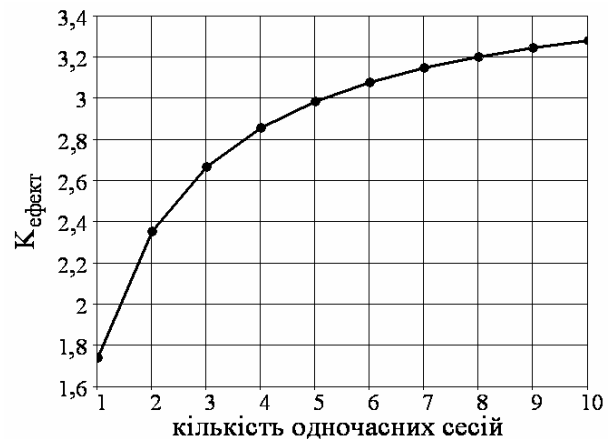


Рис. 6. Оцінка ефективності застосування запропонованого методу

Одним з найбільш важливих напрямів подальшого розвитку запропонованого методу є розробка математичних та імітаційних моделей, які дозволять одержати більш точні показники ефективності для різних випадків, розробити рекомендації щодо оптимального розміру часу агрегації та оцінити вплив запропонованого методу на реальне навантаження (зміни розміру затримки та джиттера тощо). Крім того, важливим аспектом є практична реалізація запропонованого методу, якому має передувати розробка логічних та процедурних характеристик протоколу взаємодії компресора та декомпресора.

## Висновки та результати

1. Існуючі схеми інкапсуляції голосового навантаження значно зменшують ефективність використання каналів зв'язку за рахунок протокольної надлишковості, особливо при застосуванні механізмів тунелювання.

2. Додаткова інкапсуляція, на якій базується тунелювання IP-навантаження, збільшує розмір кожного пакета, що містить голосове навантаження, приблизно на 30%, що призводить до пропорційного збільшення необхідної пропускної спроможності каналів зв'язку.

3. Запропонований метод, який базується на принципах збереження інформації про чинні контексти RTP-сесій із застосуванням процедури агрегації пакетів з паралельних RTP-сесій, дозволяє зменшити загальний обсяг навантаження, що передається крізь канал зв'язку при тунелюванні, в 1,5–3,5 рази в залежності від кількості одночасних RTP-сесій і таким чином зменшити вимоги до пропускної спроможності каналу зв'язку.

## Література

1. Таненбаум Э. Компьютерные сети / Э. Таненбаум. – СПб.: Питер, 2005. – 992 с.
2. Generic Routing Encapsulation over IPv4 networks. [Електронний ресурс] / S. Hanks, T. Li, D. Farinacci, P. Traina // RFC 1702. – Режим доступу до ресурсу: <http://www.faqs.org/rfcs/rfc1702.html>
3. Perkins C. IP Encapsulation within IP. [Електронний ресурс] / C. Perkins // RFC 2003. – Режим доступу до ресурсу: <http://www.faqs.org/rfcs/rfc2003.html>
4. Каптур В.А. Визначення достатньої пропускнув спроможності взаємопід'єднання мереж з комутацією пакетів / В.А. Каптур, Д.І. Сініна // Наукові праці Одеської національної академії зв'язку ім. О.С. Попова: збірник наукових праць Одеської національної академії зв'язку ім. О.С. Попова. – Одеса, 2008. – № 1. – С. 44-52.
5. Casner S. Compressing IP/UDP/RTP Headers for Low-Speed Serial Links. [Електронний ресурс] / S. Casner, V. Jacobson // RFC 2508. – Режим доступу до ресурсу: <http://www.faqs.org/rfcs/rfc2508.html>
6. Enhanced Compressed RTP (CRTP) for Links with High Delay, Packet Loss and Reordering. [Електронний ресурс] / T. Koren, S. Casner, J. Geeverghese, B. Thompson, P. Ruddy // RFC 3545 – Режим доступу до ресурсу: <http://www.faqs.org/rfcs/rfc3545.html>
7. IAX: Inter-Asterisk eXchange Version 2. [Електронний ресурс] / M. Spencer, B. Carouch, E. Guy, F. Miller, K. Shumard // RFC 5456. – Режим доступу до ресурсу: <http://www.rfc-editor.org/authors/rfc5456.txt>
8. Thompson B. Tunneling Multiplexed Compressed RTP (TCRTP). [Електронний ресурс] / B. Thompson, T. Koren, D. Wing // RFC 4170. – Режим доступу до ресурсу: <http://www.faqs.org/rfcs/rfc4170.html>

Надійшла до редакції 3.11.2009

**Рецензент:** д-р техн. наук, проф., зав. каф. ПЗМЗ Д.А. Зайцев, Одеська національна академія зв'язку ім. О.С. Попова, Одеса, Україна.

#### МЕТОД МИНИМИЗАЦИИ СЛУЖЕБНОЙ ИНФОРМАЦИИ ПРИ ТУНЕЛИРОВАНИИ IP-НАГРУЗКИ

*В.А. Каптур, Е.В. Добровольский, О.А. Янина*

В работе рассмотрены базовые принципы тунелирования голосовой нагрузки через IP-сеть и предложен новый метод минимизации избыточности служебной информации при тунелировании IP-трафика, который базируется на принципах сохранения контекстной информации RTP-сессий, а также на мультиплексировании полезной нагрузки параллельных сессий. Разработаны алгоритмы работы компрессора и декомпрессора, которые могут быть использованы на противоположных концах туннеля. Предложен ряд аналитических выражений для оценки эффективности предложенного метода тунелирования голосовой нагрузки, а также предоставлены рекомендации по сфере его применения.

**Ключевые слова:** пакетная сеть, туннель, сжатие голосовой нагрузки, IP-телефония, протокольная избыточность.

#### METHOD OF MINIMIZING SYSTEM INFORMATION FOR IP-TRAFFIC TUNNELING

*V.A. Kaptur, E.V. Dobrovolskiy, O.A. Yanina*

The paper discusses the basic principles of voice-traffic tunneling through IP-based network and a new method to minimize the redundancy of service information for tunneling of IP-traffic, which is based on the principles of RTP-sessions context information saving and on the aggregation of payloads of parallel sessions.. The algorithms of the compressor and decompressor, which can be used at opposite ends of the tunnel. A number of analytical expressions for evaluating the effectiveness of the proposed method of tunneling voice load, and provided recommendations on the scope of its application.

**Key words:** packet network, tunnel, voice compression, IP-telephony, protocol redundancy.

**Каптур Вадим Анатолійович** – канд. техн. наук, проректор з наукової роботи, Одеська національна академія зв'язку ім. О.С. Попова, Одеса, Україна, e-mail: [vadim.kaptur@onat.edu.ua](mailto:vadim.kaptur@onat.edu.ua).

**Добровольський Євген Валерійович** – канд. техн. наук, доцент каф. ТЕК, Одеська національна академія зв'язку ім. О.С. Попова, Одеса, Україна, e-mail: [reistlin@front.ru](mailto:reistlin@front.ru).

**Янина Ольга Олександрівна** – аспірант, Одеська національна академія зв'язку ім. О.С. Попова, Одеса, Україна, e-mail: [olga\\_yani@mail.ru](mailto:olga_yani@mail.ru).