УДК 004.056.5

ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ АЛГОРИТМІВ ЗАХИЩЕНИХ ГРУПОВИХ КОМУНІКАЦІЙ

А. К. Новокшонов[1, a]

[1] *Київський національний університет імені Тараса Шевченка, факультет кібернетики*

Анотація

У роботі представлені результати реалізації протоколів захищених групових комунікацій, а також проведене порівняння ефективності даних протоколів при роботі на персональних комп'ютерах та мобільних пристроях. Особливістю даного дослідження є: 1) реалізація не тільки стандартних алгоритмів захищених групових комунікацій, а й їх оптимізованих версій з метою ефективного виконання масових групових операцій; 2) здійснення порівняння ефективності алгоритмів на малопотужних пристроях на базі операційної системи Android.

Ключові слова: захищені групові комунікації, груповий протокол Діффі-Хеллмана на основі дерева, мобільні пристрої

Вступ

Захищені групові комунікації представляють собою сценарій, в якому сукупність довірених суб'єктів приймає участь у групових комунікаціях і потребує захисту важливих даних, що передаються. Захист цих даних ґрунтується на володінні спільними криптографічними параметрами (наприклад, знання спільного ключа шифрування). При цьому зовнішні спостерігачі, які не є учасниками групи, не мають змоги розшифрувати зміст групових повідомлень, навіть якщо вони мають можливість перехоплювати зашифровані повідомлення.

Метою алгоритмів захищених групових комунікацій є створення технології для обміну криптографічними ключами між учасниками групи, які потребують утворення спільного для них секретного ключа. Далі такий ключ може бути використаний для шифрування всіх повідомлень між учасниками групи за допомогою деякого швидкого алгоритму симетричного шифрування. Особливістю даного сценарію взаємодії є використання для комунікацій відкритих каналів зв'язку, щоправда необхідні механізми автентифікації всіх учасників для захисту від атак типу «людина посередині».

Основна складність таких групових протоколів полягає у тому, що при будь-якій зміні складу учасників групи (приєднання нових учасників, вихід старих) необхідно обчислювати новий спільний груповий ключ. Дана вимога присутня з тією метою, щоб нові учасники групи не мали доступу до попередніх зашифрованих групових повідомлень, а старі учасники, що вийшли зі складу групи, відповідно, не могли прочитати наступні повідомлення, що будуть надсилатися новим складом групи. Крім того, спільний груповий ключ необхідно періодично оновлювати і при відсутності зміни складу групи, щоб мінімізувати ризик компрометації поточних групових повідомлень.

Безпека групових комунікацій є вкрай важливою для розподілених додатків та застосувань зі спільним доступом, які функціонують у динамічних мережевих середовищах та здійснюють обмін інформації через незахищені мережі, такі, як Інтернет.

Прикладом сфер застосування захищених групових комунікацій є проведення телеконференцій, інформаційні сервіси реального часу (зокрема, потокове відео), телемедицина, інтерактивні ігри, VPN (virtual private networks), розподілені інтерактивні симулятори, системи онлайн-голосування, розподілені обчислення та реплікація даних, банківські застосування, системи спільної роботи над документами.

1. Методика дослідження

В якості основи реалізованих алгоритмів використовується *груповий протокол Діффі-Хеллмана на основі дерева* [1]. Детальне порівняння даного алгоритму з аналогами наведено у [2]. Принцип побудови дерева наступний. Для кожного учасника маємо ідентичне бінарне дерево, у листових вузлах якого знаходяться публічні ключі. У вузлах дерева на вищих рівнях розташовані відповідні приватні та публічні ключі, спільні для їх нащадків. Відповідно, у кореневому вузлі розташований спільний секретний груповий ключ, отримання якого є основною метою вибраного протоколу.

У даній роботі обмежимося розглядом і порівнянням таких операцій (без зайвої деталізації):

- *обчислення спільного групового ключа одним учасникам* – означає, що даний учасник має актуальне дерево, у якому наявні всі необхідні публічні ключі, і він на основі власного приватного ключа обчислює спільний секретний груповий ключ;

[a] andrey.novokshonov@ukr.net

- *одиничне приєднання* – означає, що до групи приєднується новий учасник, у дереві додається новий листовий вузол (при необхідності й вузли вищих рівнів) та всіма учасниками групи здійснюється переобчислення нового спільного групового ключа;
- *одиничний вихід* – означає, що з групи вибуває один учасник, відповідний листовий вузол помічається як неактивний (при необхідності і вузли вищих рівнів) та всіма учасниками групи здійснюється переобчислення нового спільного групового ключа;
- *масове приєднання* – означає, що до групи умовно одночасно входить велика кількість учасників (можна вважати, що більше двох), але особливістю є те, що дану операцію можна ефективно оптимізувати (позбутися зайвих переобчислень після приєднання кожного нового учасника та використати «пакетний» алгоритм (англ. bursty algorithm) [3, стор. 54]);
- *масовий вихід* – означає, що з групи умовно одночасно виходить велика кількість учасників, і можна застосувати оптимізації, аналогічні тим, що використовуються у операції масового приєднання.

У процесі роботи були реалізовані такі версії системи захищених групових комунікацій:

- стандартна версія для персонального комп'ютера;
- версія для персонального комп'ютера з оптимізованими алгоритмами масового додавання учасників до групи та масового виходу учасників з групи;
- стандартна версія для мобільних пристроїв на базі ОС (операційної системи) Android;
- версія для мобільних пристроїв на базі ОС Android з оптимізованими алгоритмами масового додавання учасників до групи та масового виходу учасників з групи.

Для порівняння ефективності реалізованих алгоритмів за основу були взяті наступні параметри:

- швидкодія операції генерування ключа одним учасником;
- швидкодія одиничних операцій приєднання та виходу учасників з групи;
- швидкодія оптимізованих масових операцій приєднання та виходу учасників з групи;
- обсяг використовуваної оперативної пам'яті для зберігання структури бінарного дерева.

2. Результати дослідження

Реалізовані програмні системи були протестовані за допомогою персонального комп'ютера з процесором Intel Pentium Duo 2.3 ГГц, 4 Гб DDR3 оперативної пам'яті, ОС Ubuntu 12.04 LTS x64 та смартфона з процесором 720 МГц, 256 Мб оперативної пам'яті, ОС Android 2.3.7.

У табл. 1 та 2 наведено результати тестування обсягу використовуваної оперативної пам'яті на персональному комп'ютері та мобільному пристрої при

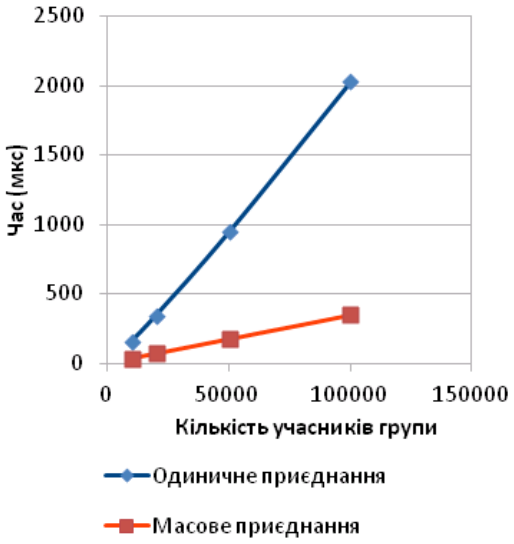

Рис. 1. Порівняння часу виконання одиничних та масових операцій приєднання учасників до групи (на персональному комп'ютері)

зберіганні структури бінарного дерева з відповідною кількістю учасників групи.

Табл. 1. Обсяг використовуваної оперативної пам'яті для зберігання структури дерева (на персональному комп'ютері)

Кількість учасників групи	**Обсяг використання оперативної пам'яті (Мб)**
100	2,456
1000	3,248
10000	12,352
50000	51,660
100000	101,664

Табл. 2. Обсяг використовуваної оперативної пам'яті для зберігання структури дерева (на мобільному пристрої)

Кількість учасників групи	**Обсяг використання оперативної пам'яті (Мб)**
10	0,556
100	0,616
1000	0,972

Результати вимірювання швидкодії обчислення групового ключа одним учасником на персональному комп'ютері свідчать про те, що час обчислення змінюється від 4723 мкс для групи з 10 учасників і до 19849 мкс для групи з 100000 учасників.

Порівняльні графіки одиничних та оптимізованих масових версій операцій приєднання та виходу учасників з групи наведені на рис. 1, 2 (для персонального комп'ютера) та у табл. 3 (для мобільного пристрою).

Табл. 3. Швидкодія групових операцій залежно від кількості учасників групи (на мобільному пристрої)

Тип операції \ Розмір групи	**10 учасників**	**100 учасників**	**1000 учасників**
Створення групи одиничним приєднанням	0 с 17517 мкс	0 с 321625 мкс	6 с 866699 мкс
Створення групи масовим приєднанням	0 с 12391 мкс	0 с 129181 мкс	1 с 325195 мкс
Приєднання 1 учасника до існуючої групи	0 с 2167 мкс	0 с 3144 мкс	0 с 11994 мкс
Видалення 1 учасника з існуючої групи	0 с 122 мкс	0 с 488 мкс	0 с 6226 мкс
Приєднання 10 учасників до існуючої групи	0 с 13977 мкс	0 с 15046 мкс	0 с 17883 мкс
Видалення всієї групи (масовий вихід)	0 с 885 мкс	0 с 5158 мкс	0 с 17090 мкс
Обчислення групового ключа 1 учасником	0 с 1709 мкс	0 с 3051 мкс	0 с 4395 мкс

Рис. 2. Порівняння часу виконання одиничних та масових операцій виходу учасників з групи (на персональному комп'ютері)

Висновки

Підтримка групових комунікацій у динамічних групах з великою кількістю учасників створює серйозну проблему у сенсі обсягу необхідних обчислювальних ресурсів. Класичний підхід з обміном ключами між кожною парою учасників у такій ситуації стає і неефективним, і потребує наявності центрального сервера, що є потенційною точкою відмови всієї системи. Тому зараз на перший план виходять децентралізовані алгоритми захищених групових комунікацій, які володіють такими властивостями:

- дозволяють значно скоротити кількість обчислювальних операцій для отримання всіма учасниками групи спільного ключа шифрування;
- дозволяють значно зменшити кількість повідомлень, якими необхідно обмінятися учасникам групи, щоб узгодити спільний груповий ключ;
- дозволяють ефективно вирішувати проблему одночасного приєднання або виходу великої кількості учасників групи;
- дозволяють позбутися єдиної точки відмови (центрального сервера).

У свою чергу, такі оптимізації відкривають можливість ефективного використання захищених групових комунікацій у середовищі дуже поширених нині мобільних пристроїв, які характеризуються відносно невеликою обчислювальною потужністю та не завжди стабільним бездротовим доступом до мережі Інтернет. Відповідно, як показують результати проведеного дослідження, децентралізовані групові алгоритми узгодження ключа (у нашому випадку модифікації групового протоколу Діффі-Хеллмана на основі дерева) дозволяють ефективно (у розумінні швидкодії та обсягу використовуваних ресурсів) здійснювати підтримку захищених групових комунікацій на базі не тільки персональних комп'ютерів, а і на базі малопотужних мобільних пристроїв з популярною у наш час операційною системою Android.

Перелік використаних джерел

1. Kim Y., Perrig A., Tsudik G. Tree-based group key agreement. — ACM Transactions on Information and System Security, 7(1), 2004. — p. 60-96.
2. Amir Y., Kim Y., Nita-Rotaru C., Tsudik G. On the performance of group key agreement protocols. — ACM Transactions on Information and System Security, 7(3), 2004. — p. 457-488.
3. Zou X., Ramamurthy B., Magliveras S. Secure group communications over data networks. — Springer Science and Business Media, 2007. — 172 p.