https://doi.org/10.31649/mccs2022.20

УДК 620.92:621.311.29

Л. М. Куперштейн[1]
М. Д. Кренцін[1]
А. В. Притула[1]

ЗАСТОСУВАННЯ ПІРИНГОВИХ МЕРЕЖ ДЛЯ ЗАХИЩЕНОЇ КОМУНІКАЦІЇ

[1]Вінницький національний технічний університет

Розглянуто особливості прикладного застосування піринговых мереж (кожен вузол є рівноправним, може бути і клієнтом, і сервером). Математично децентралізовану мережу можна представити у вигляді графа. Проаналізовано причини виникнення піринговых мереж (мала завантаженість клієнтського процесора, необхідність надання доступу до даних та спільна робота над даними). Також розглянуто класифікацію P2P мереж за трьома характеристиками (функції, ступінь централізації та спосіб з'єднання). Визначено актуальність і перспективність їх застосування для комунікації осіб, особливо для обміну даними всередині компанії (необхідна захищеність даних, відмовостійкість та незалежність від доступу до мережі Інтернет).

Запропоновано модель організації піринговой мережі, що передбачає підвищення захищеності даних (повідомлення, файли, аудіо, користувацькі налаштування тощо), надійну автентифікацію вузлів (на основі поєднання ручного розповсюдження ключів та принципів мережі довіри), масштабованість самої мережі та розширення її функціональних можливостей (надсилання тексту, файлів, підтримка аудіо, відео тощо). Програмна реалізація повинна працювати на більшості сучасних пристроїв та операційних систем (Android, IOS, Windows, MacOS). Створена модель дозволяє підвищити захищеність за рахунок поєднання різних криптографічних алгоритмів та протоколів обміну даними. За основу обміну даних взято протокол Tox, що передбачає використання розподілених хеш-таблиць, асиметричного шифрування. Транспорт даних за допомогою протоколу Tox організовано на основі TCP та UDP. Наведено графічне зображення вищеописаної моделі, а також схему обміну ключами між вузлами. Дані зберігаються у вузла також взахищеному вигляді, і прочитати їх можна лише за наявності ключа.

Ключові слова: пірингова мережа, розподілені хеш-таблиці, асиметричне шифрування, мережа довіри, автенифікація, граф.

Вступ

На сьогоднішній день більшість людей користуються різноманітними програмами та сервісами для комунікації між собою. Зазвичай такі платформи є загальнодоступними та передбачають наявність центрального сервера, що є основою всієї комунікації. Такий підхід має ряд недоліків [1]. По-перше, обмін даними не є повністю захищеним, адже маючи доступ до сервера – можна отримати будь-які дані користувачів (або ж сама платформа може надавати третім особам дані користувачів). По-друге, у разі відсутності доступу сервера до мережі Інтернет чи якоїсь атаки на нього – обмін даними між користувачами унеможливлюється. Вищеперераховані проблеми є перешкодою для комунікації осіб всередині компанії (чи тих, що працюють над одним проектом), адже за відсутності комунікації значно знижується швидкість та якість виконуваної роботи. Допомогти у вирішенні подібного роду проблем можуть пірингові (однорангові, децентралізовані) мережі, суть яких полягає у тому, що відсутній центральний сервер, а комунікація відбувається безпосередньо між учасниками мережі [2]. Тому актуальною є задача підвищення захищеності комунікації за допомогою піринговых мереж.

Постановка задачі

Відома загальна характеристика систем для комунікації осіб. Необхідно створити модель піринговой мережі для комунікації, яка повинна передбачати підвищення захищеності даних, надійну автентифікацію вузлів, масштабованість та розширення функціональних можливостей.

Результати дослідження

Пірингова мережа – це технологія, яка реалізує об'єднання однорангових вузлів рівного статусу. Кожен такий вузол надає та отримує послуги (дані). Такі вузли можуть обмінюватись інформацією безпосередньо (без центрального сервера). Такий тип мереж використовується тоді, коли необхідно забезпечити конфіденційність, анонімність, масштабованість, високий ступінь доступності інформації та відмовостійкість [3].

З математичної точки зору пірингова мережа може бути представлена графом невизначеного виду: немає будь-якої стандартної архітектури мережі (наприклад, зірки або кільця). Більше того, цей граф - динамічний, так як окремі користувачі включаються в мережу і виходять з її складу в довільні моменти часу. Будь-який користувач, який грає роль сервера, в будь-який момент часу може перетворитися на клієнта на певний відрізок часу. Але може і перебувати одночасно в положенні і сервера і клієнта.

Виникнення такого роду мереж пов'язане з трьома факторами:

1. Процесор клієнтського пристрою мало завантажений, особливо в офісах. Тому ці обчислювальні потужності можна використати в корисних цілях.
2. Багато користувачів зберігають на своїх пристроях різноманітні дані, які можуть бути корисними іншим користувачам. Але при цьому власники цих даних не можуть зробити свій пристрій повноцінним загальнодоступним сервером.
3. Певна користувачів спільно працює над якимось проектом/документом. Але така робота (наприклад, всередині приватної компанії) повинна передбачати захищеність даних, аби ніякий зловмисник не зміг отримати доступ до приватних даних.

Пірингові мережі можна класифікувати за функціями, ступенем централізації та способом з'єднання. За функціями зазвичай виділяють такі: розподілені обчислення, файлообмін та співпраця. За способами з'єднання P2P мережі є двох типів: структуровані (використовується єдиний алгоритм, щоб гарантувати ефективну передачу даних) та неструктуровані (дані передаються довільно, без якогось алгоритму). За ступенем централізації є трьох типів: чисті (повністю децентралізовані), гібридні (використовують сервер для пошуку вузлів), федеративні (взаємодія між вузлами відбувається всередині попередньо визначених доменів). Для вирішення поставленої задачі слід використати чисту архітектуру однорангових мереж. Це дозволить не залежати від доступу до глобальної мережі, легко організувати масштабованість, підвищити швидкість обміну даними тощо.

Системи для комунікації передбачають такі можливості, як миттєвий обмін повідомленнями та файлами, організацію групових чатів та відеоконференцій, спільну роботу над документом (проектом) тощо. Всі ці речі передбачають використання певних протоколів обміну даними та захисту даних.

Для забезпечення з'єднання учасників мережі та розповсюдження інформації про інших учасників використовуються розподілені хеш-таблиці (distributed hash tables, DHT) [4]. DHT-зберігання ідентифікаторів організовано так, що користувачі не бачать IP-адреси один одного, доки не додадуть один одного у свої контакт-листи; тільки після цього у них з'являється можливість здійснювати комунікацію. Такий підхід і буде використовуватись для вирішення поставленої задачі. Для забезпечення захищеного обміну даними слід використовувати криптографічні алгоритми. У сучасних піринговых мережах зазвичай використовується асиметричне шифрування, а саме алгоритм RSA (для кодування повідомлень, наприклад). Саме тому, було прийнято рішення взяти за основу протокол Tox [5], що передбачає використання DHT та асиметричного шифрування. Для обміну ключами використовується Curve25519 [6]. Реалізація цього протоколу є у відкритому доступі та закріплена ліцензією GNU GPL-3.0 [7]. Протокол також використовує наскрізне шифрування. Спільні ключі детерміновано отримують за допомогою методу Діффі-Хеллмана, тому ключі ніколи не передаються через мережу [8]. Транспорт даних організований на основі стандартних протоколів TCP та UDP.

Для того, аби мережа була захищена від зловмисників, необхідно передбачити автентифікацію вузлів, унеможливити під'єднання до мережі стороннього учасника. Пірингові мережі за своєю суттю не передбачають звичної у всьому світі автентифікації, адже немає єдиного джерела (центрального сервера), яке може надати достовірну інформацію про вузол. Для децентралізованих мереж існує два підходи автентифікації:

1. Завчасно визначені ідентифікатори. Можуть видаватись в ручному режимі, або надіслані стороннім програмним забезпеченням. Такий підхід забезпечує дуже високу надійність до тих пір, поки ідентифікатор не потрапить у руки зловмисника.

2. Мережа довіри (web of trust). Концепція мережі довіри була вперше висунута творцем Філом Ціммерманом у 1992 році [9]. Ґрунтується на принципі транзитивності, а саме на тому, що якщо вузол А довіряє вузлу Б, а вузол Б довіряє вузлу В, то вузол А може довіряти вузлу В (і, відповідно, встановлювати з ним з'єднання).

Для вирішення поставленої задачі було прийнято рішення об'єднати ці два підходи. Нехай є перший учасник мережі, A. Він надає ключі доступу в ручному режимі N особам. В свою чергу кожна із N осіб $n_i, i \in [0; N]$ може видати ключ доступу ще M особам. Але при цьому на основі концепції мережі довіри A може комунікувати як з n_i, так і з $m_j, j \in [0; M]$. Відповідно кожен n_i може здійснювати обмін даними з кожним m_j. На рис. 1 наведено схему передачі ключів користувачами.

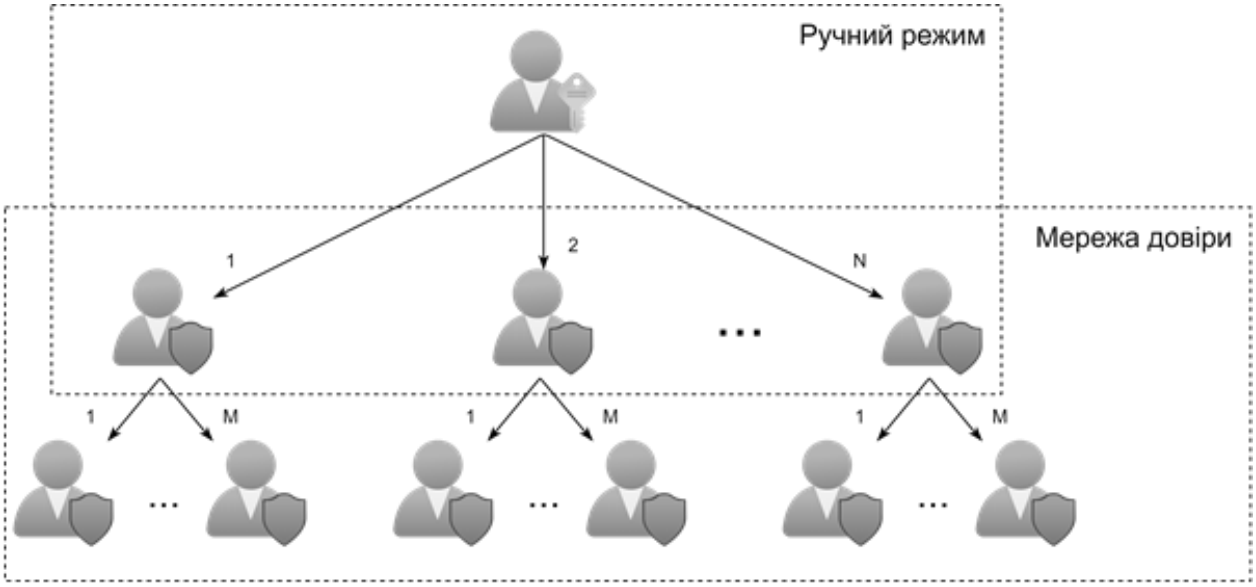

Рис. 1. Схема передачі ключів користувачами

Також для вирішення поставлено задачі необхідно певним чином передбачити розширення функціональних можливостей. Сьогодні це може бути простий обмін повідомленнями, а завтра вже спільна робота над проектом. Також модель повинна передбачати різноманіття кінцевих користувачів мережі та інформації, з якою вони працюють. Мережа повинна вміти працювати з текстовими даними, файлами, потоковим аудіо та відео тощо. Тому для вирішення поставленої задачі необхідно будувати мережу модульною. Наприклад, є модуль, що відповідає за обмін повідомленнями, за відеозв'язок тощо. При цьому обмін даними має бути уніфікованим, що дозволить під'єднувати до мережі нові додаткові модулі без змін структури мережі та протоколу обміну. Ще одним критерієм при побудові мережі має бути те, що програмна реалізація має бути доступною для більшості сучасних пристроїв (мобільні телефони та планшети з операційними системами Android та IOS, а також стаціонарні комп'ютери та ноутбуки з операційними системами Windows та MacOS). Така універсальність необхідна аби максимально легко масштабувати мережу та сфери її використання.

Запропонована модель пірингової мережі для підвищення захищеності комунікації зображена на рисунку 2.

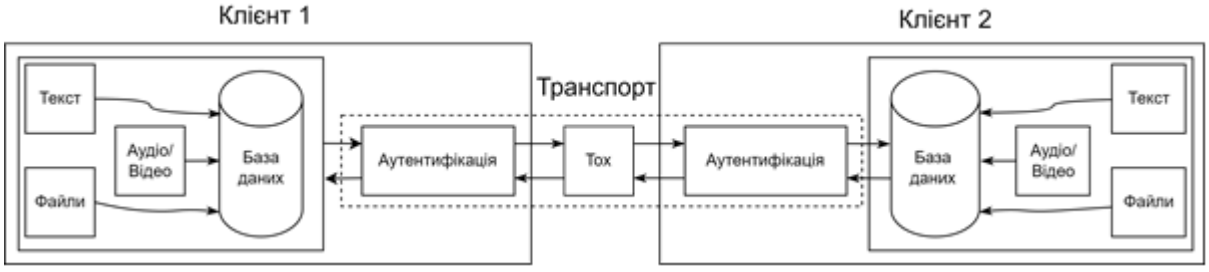

Рис. 2. Запропонована модель пірингової мережі

Запропонована модель зображує взаємодію двох вузлів. Кожен клієнт місить модуль роботи з даними (текст, база даних тощо) та модуль автентифікації. Вузли взаємодіють між собою через модуль транспорту даних, в основі якого лежить Tox. Модуль автентифікації є елементом, що поєднує модуль даних вузла та загальний транспорт даних. Дані всередині кожного вузла також є зашифрованими і можуть бути прочитані лише у разі наявності ключа.

Висновки

Запропонована модель пірингової мережі дозволяє підвищити захищеність комунікації. Модель передбачає захищеність обмінюваних даних, надійну автентифікацію вузлів, масштабованість та розширення функціональних можливостей. Підвищення захищеності відбувається за рахунок поєднання різних криптографічних алгоритмів та протоколів обміну даними.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Кренцін М. Д., Куперштейн Л. М. Аналіз тенденцій розвитку піринговых мереж. *Вісник Хмельницького національного університету. Технічні науки.* 2021. Т. 4, № 299. С. 25–29. URL: http://journals.khnu.km.ua/vestnik/wp-content/uploads/2021/11/299-text_2021_4_t.pdf (дата звернення: 07.11.2022).

[2] Hauben M. The social forces behind the development of usenet. *Columbia University in the City of New York*. URL: http://www.columbia.edu/~hauben/book/ch106.x03 (дата звернення: 07.11.2022).

[3] Аналіз проблем безпеки піринговых мереж / М. Д. Кренцін та ін. *Інформаційні технології та комп'ютерна інженерія*. 2022. Т. 54, № 2. С. 5–14. URL: https://doi.org/10.31649/1999-9941-2022-54-2-5-14.

[4] What is a distributed hash table?. *Educative: Interactive Courses for Software Developers.* URL: https://www.educative.io/answers/what-is-a-distributed-hash-table (дата звернення: 08.11.2022).

[5] Tox documentation. *Welcome to the tox automation project*. URL: https://tox.wiki/en/latest/ (дата звернення: 08.11.2022).

[6] Curve25519: high-speed elliptic-curve cryptography. *cr.yp.to*. URL: https://cr.yp.to/ecdh.html (дата звернення: 08.11.2022).

[7] The GNU General Public License v3.0 - GNU Project - Free Software Foundation. URL: https://www.gnu.org/licenses/gpl-3.0.en.html (дата звернення: 08.11.2022).

[8] The TokTok project – Protocol. URL: https://toktok.ltd/spec.html (дата звернення: 06.11.22).

[9] Anonymous and Distributed Authentication for Peer-to-Peer Networks / P. Tennakoon та ін. URL: https://eprint.iacr.org/2021/838.pdf (дата звернення: 08.11.2022).

REFERENCES

[1] Krentsin M. D., Kupershtein L. M. Analiz tendencii rozvitku pirinhovih merezh. *Visnuk Khmenlytskogo natsionalnogo universitetu. Tekhnichni nayku.* 2021. T. 4, № 299. S. 25–29. URL: http://journals.khnu.km.ua/vestnik/wp-content/uploads/2021/11/299-text_2021_4_t.pdf (accessed on: 07.11.2022).

[2] Hauben M. The social forces behind the development of usenet. *Columbia University in the City of New York*. URL: http://www.columbia.edu/~hauben/book/ch106.x03 (accessed on: 07.11.2022).

[3] Analiz problem pirinhovih merezh / M. D. Krencin ta in. Informacinii tekhnologii ta komputerna inzheneriia. 2022. T. 54, № 2. s. 5–14. URL: https://doi.org/10.31649/1999-9941-2022-54-2-5-14.

[4] What is a distributed hash table?. *Educative: Interactive Courses for Software Developers.* URL: https://www.educative.io/answers/what-is-a-distributed-hash-table (data zvernennia: 08.11.2022).

[5] Tox documentation. *Welcome to the tox automation project.* URL: https://tox.wiki/en/latest/ (accessed on: 08.11.2022).

[6] Curve25519: high-speed elliptic-curve cryptography. *cr.yp.to*. URL: https://cr.yp.to/ecdh.html (accessed on: 08.11.2022).

[7] The GNU General Public License v3.0 - GNU Project - Free Software Foundation. URL: https://www.gnu.org/licenses/gpl-3.0.en.html (accesses on: 08.11.2022).

[8] The TokTok project – Protocol. URL: https://toktok.ltd/spec.html (accessed on: 06.11.22).

[9] Anonymous and Distributed Authentication for Peer-to-Peer Networks / P. Tennakoon ta in. URL: https://eprint.iacr.org/2021/838.pdf (accessed on: 08.11.2022).

Купершейн Леонід Михайлович – к.т.н., доцент кафедри захисту інформації, e-mail: kupershtein.lm@gmail.com; ORCID: https://orcid.org/0000-0001-6737-7134

Кренцін Михайло Дмитрович – аспірант кафедри захисту інформації, e-mail: mishatron98@gmail.com; ORCID: https://orcid.org/ 0000-0002-1792-9401

Притула Андрій Вікторович – магістр кафедри захисту інформації, e-mail: andrik.pritula@gmail.com

Вінницький національний технічний університет

L. M. Kupershtein[1]
M. D. Krentsin[1]
A. V. Prytula[1]

USE OF PEER-TO-PEER NETWORKS FOR SECURED COMMUNICATION

[1]Vinnytsia national technical university

Peculiarities of the applied application of peering networks are considered (every node is equal; it can be both a client and a server). Mathematically, a decentralized network can be represented as a graph. The reasons for the emergence of peering networks are analyzed (low load on the client processor, the need to provide access to data and joint work on data). The classification of P2P networks according to three characteristics (functions, degree of centralization and method of connection) is also considered. The relevance and perspective of their application for personal communication, especially for data exchange within the company (required data security, fault tolerance and independence from Internet access) are determined.

A peering network organization model is proposed, which provides for increased data security (messages, files, audio, user settings, etc.), reliable authentication of nodes (based on a combination of manual key distribution and trust network principles), scalability of the network itself and expansion of its functional capabilities (sending text, files, support for audio, video, etc.). The software implementation should work on most modern devices and operating systems (Android, IOS, Windows, MacOS). The created model makes it possible to increase security due to the combination of various cryptographic algorithms and data exchange protocols. Data exchange is based on the Tox protocol, which involves the use of distributed hash tables and asymmetric encryption. Data transport using the Tox protocol is organized based on TCP and UDP. A graphic representation of the above-described model is given, as well as a key exchange scheme between nodes. The data is also stored at the node in a protected form, and it can be read only if the key is present.

Keywords: peer-to-peer network, distributed hash tables, asymmetric encryption, web of trust, authentication, graph.

Kupershtein Leonid M. – Ph.D., associate professor of the department of information protection, e-mail: kupershtein.lm@gmail.com; ORCID: https://orcid.org/0000-0001-6737-7134

Krentsin Mykhailo D. – PhD student of the department of information protection, e-mail: mishatron98@gmail.com; ORCID: https://orcid.org/0000-0002-1792-9401

Prytula Andrii V. – master of information protection department, e-mail: andrik.pritula@gmail.com

Vinnytsia National Technical University