УДК 004.056.5

Саврацький В.В.
Яремчук Ю.Є.

АНАЛІЗ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ ПРИВАТНОСТІ В БАГАТОВУЗЛОВИХ МЕРЕЖАХ

Вінницький Національний Технічний Університет

Анотація
В даній роботі розглянуто аналіз методів забезпечення приватності в багатовузлових мережах. Наведено їх особливості, переваги та недоліки. Здійснено порівняння досліджуваних методів..
Ключові слова: Захист, приватність, багатовузлові мережі.

Abstract
This paper analyzes methods of ensuring privacy in multi-node networks. Their features, advantages and disadvantages are presented. A comparison of the studied methods is made.
Key words: Security, privacy, multi-node networks.

Вступ

Питання забезпечення приватності та анонімності в сучасних інформаційних мережах стає дедалі актуальнішим через збільшення кількості кіберзагроз і зростання обсягів конфіденційних даних, які передаються через цифрові канали. Багатовузлові мережі, як-от Tor, I2P та інші, пропонують потужні рішення для захисту приватності, інтегруючи різні методи анонімізації та захисту від аналізу трафіку. У цій статті здійснено аналіз основних методів, які застосовуються у багатовузлових мережах, із визначенням їхніх принципів дії, переваг, недоліків та прикладів використання.

Дослідження

Onion Routing (маршрутизація цибулевого типу) є одним із найбільш поширених методів забезпечення анонімності у багатовузлових мережах. Принцип його роботи базується на багатошаровому шифруванні, де повідомлення огортається кількома шарами шифрування, подібно до шарів цибулі. Кожен вузол у мережі видаляє лише один шар, використовуючи власний унікальний ключ, після чого передає повідомлення далі, розкриваючи наступний пункт маршруту. Завдяки такій структурі жоден із вузлів, окрім відправника і кінцевого отримувача, не має інформації про повний маршрут повідомлення, що забезпечує високий рівень анонімності.

Цей метод надає ефективний захист від аналізу трафіку, оскільки навіть у разі компрометації одного вузла сторонніми суб'єктами, отримати повну інформацію про маршрут стає практично неможливо. Onion Routing широко застосовується у мережі Tor, яка є однією з найвідоміших платформ для анонімного серфінгу в Інтернеті, обміну повідомленнями та передачі даних. Основною перевагою цього методу є його здатність забезпечувати захист конфіденційності шляхом шифрування кожного етапу передачі, що робить перехоплення ідентифікуючих даних неможливим.

Однак Onion Routing має і певні недоліки, серед яких ключовим є зниження швидкості передачі даних через необхідність багатошарового шифрування та обробки на кожному вузлі. Крім того, у разі компрометації значної кількості вузлів зростає ризик деканонімізації користувача. Незважаючи на це, Onion Routing залишається однією з найбільш ефективних і надійних технологій для забезпечення анонімності в умовах сучасних інформаційних мереж, що робить його незамінним інструментом для багатьох користувачів і організацій, які потребують захисту приватності.

Garlic Routing (маршрутизація часникового типу) є вдосконаленим методом забезпечення приватності та безпеки даних, що використовується у багатовузлових мережах. Принцип роботи цього методу базується на об'єднанні кількох повідомлень в один шифрований пакет, який передається через мережу. Кожне з повідомлень у цьому пакеті має індивідуальне шифрування та адресу доставки, що ускладнює аналіз трафіку і робить неможливим визначення вмісту окремих повідомлень сторонніми спостерігачами. Назва цього методу походить від аналогії з часником, де кілька зубців (повідомлень) захищені загальною оболонкою (пакетом).

Garlic Routing забезпечує підвищений рівень анонімності та захисту від аналізу трафіку, оскільки об'єднання повідомлень у один пакет приховує індивідуальні властивості кожного з них. Це ускладнює

ідентифікацію відправника, отримувача та характеру даних навіть у разі компрометації окремих вузлів мережі. Однією з головних переваг Garlic Routing є ефективне маскування структури трафіку, що робить цей метод надзвичайно стійким до спроб деканонімізації. Завдяки цій властивості Garlic Routing є ключовим елементом у роботі мережі I2P, яка спеціалізується на захищеній передачі даних і забезпеченні анонімності.

Попри численні переваги, Garlic Routing має і свої обмеження. Основним недоліком є висока обчислювальна складність, пов'язана з багатошаровим шифруванням кожного повідомлення та управлінням великими пакетами даних. Це може призводити до збільшення затримок під час передачі та потребує значних ресурсів для роботи мережі. Крім того, складність реалізації цього методу робить його менш придатним для застосування в умовах із обмеженими ресурсами.

Загалом Garlic Routing є ефективним інструментом для забезпечення приватності та безпеки даних у багатовузлових мережах. Його унікальний підхід до структурування і захисту трафіку дозволяє значно підвищити рівень анонімності, що робить його важливим рішенням для користувачів і систем, які потребують високого рівня конфіденційності.

Мікс-мережі є одним із провідних методів забезпечення приватності в багатовузлових мережах, який базується на принципі випадкового перемішування повідомлень на кожному вузлі мережі. Цей метод був розроблений для мінімізації ризику аналізу трафіку, забезпечуючи анонімність користувачів шляхом приховування взаємозв'язків між відправниками та отримувачами. У мікс-мережах кожне повідомлення шифрується за допомогою багатошарового шифрування, і, проходячи через вузли мережі, піддається процесу "змішування". Це означає, що порядок отримання повідомлень на вході вузла відрізняється від порядку передачі повідомлень на виході, що ускладнює ідентифікацію відправника.

Основною перевагою мікс-мереж є їхня здатність ефективно протистояти аналізу трафіку, навіть у разі тривалого моніторингу мережі. Завдяки випадковому перемішуванню повідомлень і багатошаровому шифруванню, сторонній спостерігач не може визначити відповідності між початковим відправником і кінцевим отримувачем. Цей підхід робить мікс-мережі ідеальними для використання у випадках, коли необхідна висока анонімність, таких як системи електронної пошти, обмін повідомленнями чи забезпечення безпеки в корпоративних середовищах.

Однак мікс-мережі мають свої недоліки. Основним із них є зниження швидкості передачі даних, оскільки процес перемішування потребує часу для накопичення достатньої кількості повідомлень і їхньої обробки. Крім того, високий рівень захисту вимагає значних ресурсів для виконання криптографічних операцій і управління трафіком. Це може обмежувати їхнє застосування у системах, де критичними є низькі затримки або обмежені обчислювальні ресурси.

Загалом мікс-мережі залишаються потужним інструментом для забезпечення анонімності у мережах, де приватність даних є ключовим пріоритетом. Їхній принцип дії дозволяє значно ускладнити аналіз трафіку, що робить цей метод особливо актуальним для використання у високозахищених середовищах і в сценаріях, які вимагають захисту від спостереження за комунікаціями.

Шумові протоколи є методом забезпечення приватності в багатовузлових мережах, який базується на додаванні випадкових даних (шуму) до реальних повідомлень. Основною метою цього підходу є ускладнення аналізу трафіку, оскільки сторонньому спостерігачу стає важко відрізнити справжні дані від штучно доданих. У таких протоколах кожен вузол у мережі може генерувати випадкові пакети або додавати шум до існуючих, створюючи ефект "захаращення" трафіку, що унеможливлює або значно ускладнює аналіз патернів передачі даних.

Головною перевагою шумових протоколів є їхня здатність ефективно протидіяти спробам сторонніх суб'єктів відстежити взаємозв'язок між відправником і отримувачем повідомлення. Додавання шуму не тільки маскує реальні дані, а й збільшує невизначеність у поведінці мережі, що робить її менш вразливою до атак аналізу трафіку. Цей підхід використовується в деяких анонімних мережах, зокрема в Tor, для додаткового захисту трафіку.

Проте шумові протоколи мають низку недоліків, серед яких основним є значне збільшення обсягу даних, що передаються через мережу. Це може створювати додаткове навантаження на мережеву інфраструктуру та призводити до зниження швидкості передачі даних. Крім того, рівень анонімності, який забезпечують шумові протоколи, є обмеженим, оскільки сам по собі доданий шум не гарантує повної конфіденційності, якщо використовується без інших методів захисту, таких як шифрування чи маршрутизація.

Незважаючи на ці обмеження, шумові протоколи залишаються важливим компонентом систем забезпечення приватності, особливо в умовах, де необхідно зменшити ймовірність успішного аналізу трафіку. Вони добре працюють у поєднанні з іншими методами, такими як Onion Routing або Garlic Routing, доповнюючи їх та створюючи додатковий рівень захисту. Це робить шумові протоколи корисним інструментом у боротьбі з загрозами, пов'язаними з моніторингом і аналізом трафіку в інформаційних мережах.

У таблиці 1 здійснено порівняння проаналізованих методів.

Таблиця 1 – Порівняння методів забезпечення приватності в багатовузлових мережах

Метод	Принцип дії	Переваги	Недоліки	Приклад застосування
Onion Routing	Багатошарове шифрування і передача через вузли	Високий рівень анонімності, захист від перехоплення	Зниження швидкості, вразливість до деканонімізації	Tor
Garlic Routing	Пакування кількох повідомлень у один пакет	Підвищена безпека, захист від аналізу трафіку	Потребує більше ресурсів	I2P
Мікс-мережі	Випадкове перемішування повідомлень	Високий захист від аналізу трафіку	Зниження швидкості, потреба у значних ресурсах	Системи електронної пошти
Шумові протоколи	Додавання випадкового шуму до реальних повідомлень	Ефективний захист від аналізу трафіку	Збільшення обсягу даних, обмежена анонімність	Tor та інші анонімні мережі

Усі розглянуті методи мають свою специфічну сферу застосування та забезпечують захист за допомогою різних методів, тобто кожен з них адаптований для вирішення певної задачі.

Висновки

У ході дослідження було проведено аналіз методів забезпечення приватності в багатовузлових мережах, що включає Onion Routing, Garlic Routing, мікс-мережі та шумові протоколи. Визначено їхні принципи дії, переваги, недоліки та приклади застосування. Результати дослідження показали, що кожен із розглянутих методів відіграє важливу роль у забезпеченні анонімності та приватності користувачів в інформаційних мережах, але має свої обмеження та специфіку використання.

Onion Routing забезпечує високий рівень анонімності завдяки багатошаровому шифруванню, що унеможливлює визначення маршруту передачі даних, проте його продуктивність може знижуватися через високу складність обробки. Garlic Routing, у свою чергу, пропонує підвищену безпеку через пакування кількох повідомлень у один пакет, що ускладнює аналіз трафіку, але потребує більше ресурсів для реалізації. Мікс-мережі, завдяки перемішуванню повідомлень, забезпечують надійний захист від аналізу трафіку, проте їхній недолік полягає у зниженні швидкості передачі даних. Шумові протоколи ефективно приховують реальні дані, додаючи випадковий шум, але при цьому збільшують обсяг переданих даних і мають обмежену анонімність у відсутності додаткових заходів захисту.

Загальний висновок полягає в тому, що жоден з методів не є універсальним і оптимальним для всіх сценаріїв. Вибір конкретного методу або їх комбінації залежить від вимог до анонімності, швидкості передачі даних, обчислювальних ресурсів та рівня загроз. Подальші дослідження повинні бути спрямовані на розробку комбінованих підходів, які поєднуватимуть переваги цих методів та мінімізуватимуть їхні недоліки. Це дозволить створити більш ефективні системи захисту приватності в умовах сучасних інформаційних мереж і підвищених кіберзагроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. GOLDSMITH A. Exploring Onion Routing: Principles and Applications [Електронний ресурс] / ALAN GOLDSMITH. – 2023. – Режим доступу до ресурсу: https://www.cyberdefensemagazine.com/onion-routing-basics/.

2. Garlic Routing in Anonymous Networks [Електронний ресурс]. – 2023. – Режим доступу до ресурсу: https://i2p.docs.org/garlic-routing-overview.
3. SECURITY LAB. Mix Networks: Ensuring Privacy in Data Transmission [Електронний ресурс]. – 2023. – Режим доступу до ресурсу: https://www.securitylab.com/articles/mix-networks-explained.
4. Noise Protocol Framework for Secure Communication [Електронний ресурс]. – 2022. – Режим доступу до ресурсу: https://noiseprotocol.org/specifications/latest/.

Савpацький Вячеслав Володимирович– студент групи КІТС-23М, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця.

Науковий керівник: ***Яремчук Юрій Євгенович***– доктор технічних наук, професор, директор Центру інформаційних технологій і захисту інформації, голова секції «Управління інформаційною безпекою» та професор кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця, e-mail: yurevyar@vntu.edu.ua

Savratsky Vyacheslav. – student of KITS-23M group, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia.

Supervisor: ***Yurii Yaremchuk.*** – Doctor of Technical Sciences, Professor, Director of the Center for Information Technology and Information Protection, Head of the Section “Information Security Management” and Professor of the Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: yurevyar@vntu.edu.ua