

АЛГОРИТМІЧНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ АНАЛІЗУ СТАНУ ТА ФУНКЦІОНУВАННЯ РОЗПОДІЛЕНОЇ ГЕТЕРОГЕННОЇ МЕРЕЖІ

Проблема аналізу стану та функціонування розподіленої гетерогенної мережі вимагає від спеціалістів розробки алгоритмічного програмного забезпечення, що забезпечує моніторинг та оптимізацію роботи мережі. У цьому контексті, програмне забезпечення, яке розробляється за технічним завданням, повинно вирішувати ряд актуальних завдань:

Забезпечення постійного моніторингу розподіленої гетерогенної мережі для виявлення можливих проблем, спричинених аномаліями або зовнішніми вторгненнями [1].

- Реалізація алгоритмів для аналізу трафіку мережі, що дозволяє виявляти кореляційні, структурні та інваріантні ознаки, характерні для нормального функціонування мережі та можливих загроз.

- Розробка модульної архітектури програмного забезпечення, що дозволяє легко інтегрувати нові компоненти для моніторингу та аналізу різних аспектів функціонування мережі.

- Створення інтуїтивного інтерфейсу користувача, що допомагає адміністраторам мережі швидко отримати доступ до потрібної інформації про стан та функціонування гетерогенної мережі.

- Розробка системи резервного копіювання та контролю версій для забезпечення надійності програмного забезпечення та зберегання історії змін у параметрах мережі.

- Інтеграція з існуючими системами моніторингу і керування мережею, що дозволить спеціалістам ефективно використовувати програмне забезпечення в різних мережевих середовищах.

- Реалізація механізмів автоматичного адаптування алгоритмів програмного забезпечення до змін у мережі та нових видів загроз, що полегшує процес моніторингу та аналізу стану мережі.

Забезпечення можливості масштабування програмного забезпечення для використання в мережах різних розмірів та конфігурацій, враховуючи специфіку гетерогенних мереж.

- Розробка засобів для підтримки різних протоколів зв'язку і стандартів мережевого обладнання, що гарантує широку сумісність програмного забезпечення з різноманітним мережевим обладнанням.

- Проведення експериментів та випробувань програмного забезпечення в реальних мережевих середовищах для перевірки ефективності алгоритмів та виявлення можливих проблем.

Автори [2] пропонують метод виявлення аномалій у мережі, заснований на інваріантах подоби, який передбачає порівняння значень інваріантів реальних обчислювальних процесів з еталонними значеннями. Це дозволяє розробити автоматичний алгоритм виявлення аномалій. Виявлення аномалій здійснюється за допомогою дворівневої класифікації мережевої активності, яка включає класифікатори та метод опорних векторів для визначення класів атак [2].

Використання тензорної методології для аналізу мережевого трафіку дозволяє отримати додаткові знання про власні вектори та топологічну структуру тензорного поля [3]. Графічні відображення тензор-трафіку і їх векторні аналоги демонструють високу ефективність використання векторних аналогів тензор-трафіку для ідентифікації аномальних режимів мережі.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. L. Gorjan, M. Vojkovic, and B. Jerman-Blazic, "A framework for the analysis and management of heterogeneous IoT-enabled network infrastructure," in *2018 IEEE/ACM 26th International Symposium on Quality of Service (IWQoS)*, 2018, pp. 1-6.

2. J. Fan, Q. Chen, H. Du, Y. Liu, and W. Li, "An Efficient and Privacy-Preserving Distributed Network Traffic Classification," in *2019 IEEE Global Communications Conference (GLOBECOM)*, 2019, pp. 1-6.

3. L. R. Rodrigues, S. Kundu, F. A. Silva, A. M. Alberti, and M. C. R. Melo, "Adaptive network monitoring and management through intelligent data aggregation," in *2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*, 2019, pp. 104-112.