Анотація

Продемонстровано найбільш популярні протоколи автентифікації та шифрування Wi-Fi мереж, виявлено їх вплив на пропускну здатність, на екологію і які алгоритми шифрування необхідно використовувати в різних мережах. Було продемонстровано реальні дослідження пропускної здатності та висновки до них.

Ключові слова: Wi-Fi, Безпека, Пропускна здатність, Екологія, Автентифікація, Шифрування, Потужність передавача.

Аннотация

Продемонстрированы наиболее популярные протоколы аутентификации и шифрования Wi-Fi сетей, выявлено их влияние на пропускную способность, на экологию и какие алгоритмы шифрования необходимо использовать в различных сетях. Были продемонстрированы реальные исследования пропускной способности и выводы к ним.

Ключевые слова: Wi-Fi, Безопасность, Пропускная способность, Экология, Аутентификация, Шифрование Мощность передатчика.

Abstract

Showcased the most popular authentication protocols and encryption Wi-Fi networks revealed their influence on the bandwidth on the environment and which encryption algorithms to be used in different networks. There were pro-demonstrate real research capacity and outputs to them.

Keywords: Wi-Fi, Security, Capacity, Ecology, Authentication, Encryption transmitter power.

СИНТЕЗ МОДЕЛІ ДІЯЛНКИ МЕРЕЖІ З ПЕРЕВАНТАЖЕННЯМ

Варваров П.О., ст. гр. ТКСз-14м, mr_orange91@mail.ru
ДонНТУ, Красноармейск, Украина

Проблема перевантаження в мережах TCP/IP виникає у разі, коли кількість переданих даних починає наближатися до значення допустимої пропускної спроможності мережі або навіть перевищувати його. Результатом перевантажень у комп'ютерній мережі є високий рівень втрати пакетів, суттєве збільшення часу їх доставки від відправника до одержувача і навіть тимчасова недоступність мережевих ресурсів і сервісів [1].

Одним з місць виникнення перевантаження є вузькі місця мережі, а саме, черги маршрутизатора, що обмежені об’ємом його буферу, та виникають під час суттєвого збільшення обсягу передачі даних по одному мережному каналу (часто через одночасну роботу декількох користувачів) [2].

Є деяка множина комп'ютерів-хостів, що об’єднані локальною високошвидкісною мережею. Вони підключаються до маршрутизатора, що з однієї сторони з'єднаний з локальною мережею, а з іншої – до низькошвидкісного каналу зв'язку.

Для створення навантаження на низькошвидкісний канал усі комп'ютери передають дані на віддалений сервер. Маршрут передачі пакету с даними буде виглядати наступним чином: хост відправника – високошвидкісний сегмент мережі – маршрутизатор – низькошвидкісний сегмент мережі – маршрутизатор – високошвидкісний сегмент мережі – сервер-отримувач. Пакет, що підтверджує отримання пакету, проходить той же путь в зворотному порядку. Розмір такого пакету звичайно становить близько 64 байт. Це TCP-пакет, інкапсульований у IP-пакет з порожнім полем даних. Завдяки малому розміру цього пакету можно вважати, що перевантаження ліній зв'язку у зворотному напрямку малоймовірне та розмір черги маршрутизатора, що встановлений зі сторони серверів, завжди близький до нуля. Також таке підключення дозволяє уникнути перевантажень маршрутизатора на переході з низько швидкісної мережі до високошвидкісної на стороні серверів. Таким чином, у мережі з такою топологією буде лише одна черга.

Топологія ділянки мережі на рис. 1.

Ділянка мережі представлена наступними вузлами: 100 джерел (node1-node100), сервер-отримувач (Server) та 2 маршрутизатори (Router1, Router2), що створюють вузьке місце мережі. Параметри каналів, що з'єднують вузли з маршрутизаторами, а саме затримка розповсюдження a_i та пропускна здатність C, становлять 10Мбіт/с та 1мс відповідно. Канали мережі є повно дуплексними. Канал між маршрутизаторами, що моделює вузьке місце мережі, тобто канал з невеликою пропускною здатністю, ресурси якого розділяються між великою кількістю потоків, має пропускну здатність $C = 80\ Мбіт/с$ з $a_i = 20\ мс$.

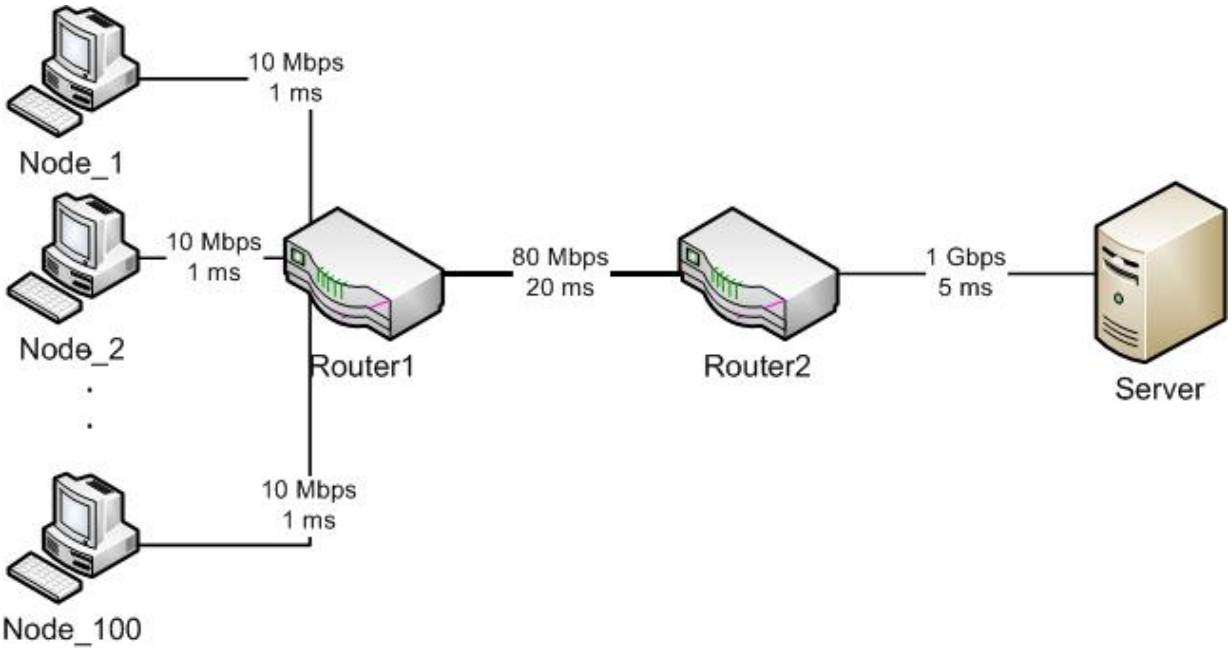

Рисунок 1. Ділянка мережі з перевантаженням

Черга буде створюватися на маршрутизаторі R1 у напрямку передачі від вузлів n1-n100 до сервера, що представлений вузлом S.

У якості додатку, який генерує потоки даних, що будуть створювати навантаження на низькошвидкісний сегмент мережі, оберемо протокол, що діє на базі протоколу транспортного рівня TCP, а саме FTP. По-перше, у процентному відношенні кількість пакетів та потоків TCP, що передається в сучасних мережах, становить близько 80% від загального об'єму переданих даних. По-друге, обрана у попередньому підрозділі гідродинамічна модель, як засіб проведення моделювання та дослідження роботи алгоритмів управління чергою, описує динаміку саме TCP протоколу, і не може бути застосована для моделювання, наприклад, UDP і відповідно протоколів, що діють на його основі.

FTP-потоки представлені наступним чином:

– розмір TCP-вікна $W = 8000$ пакетів;

– використовується реалізація протоколу TCP Reno;

– час початку дій потоків розподілено рівномірно у межах від 0 до 15 мс.

В якості середовища для реалізації моделі обраний симулятор ns-. Основною частиною ns-2 є симулятор ns. Він здійснює імітаційне моделювання мереж на рівні пакетів, тобто, моделює генерацію пакетів и проходження їх по мережі. Можливе моделювання протоколів транспортного рівня UDP и різних реалізацій TCP, multicast-протоколів, різних протоколів маршрутизації, протоколів прикладного рівня FTP и Telnet, черг с дисциплінами обслуговування DropTail и RED. Крім того, моделюється деякі фактори, які відносяться фізичного рівню: затримка пакетів в каналах, поява помилок та ін. Результатом роботи симулятора є вихідні текстові файли, в яких реєструється хід моделювання (моменти отримання пакетів, стан черг, відкидання пакетів в чергах та ін.). Крім того, в модель можуть бути додані інструкції, які розраховують будь-які величини, значення яких потрібно в конкретній задачі (затримка пакетів, пропускна спроможність та т.п.). Значення цих величин в ході моделювання також можуть реєструватися в вихідних файлах [3].

Мережа в ns-2 створюється за моделлю ділянки мережі, що наведена на рис.1, з відповідною кількістю вузлів та параметрами каналів.

Отож, маємо такі вузли мережі, що представлені у симуляторі:

– S(1) – S(100) – 100 джерел;

– R(1) та R(2) – вузли-маршрутизатори;

– Server – вузол, що виконує функцію сервера.

Джерела S(1) – S(100) та Server з'єднані з маршрутизаторами R(1) та R(2) повно дуплексними каналами з пропускною здатністю у 10 Мбіт/с та затримкою розповсюдження 1 мс. Вузьке місце мережі між маршрутизаторами представлено повно дуплексним каналом у 80 Мбіт/с та затримкою 20 мс. Розмір черги між маршрутизаторами – 1000 пакетів.

На вузлах S(1) – S(100) знаходяться джерела трафіку FTP, що приєднані до TCP-агентів. Джерела починають роботу в різний час після початку моделювання. Час початку роботи потоків розподілено за рівномірним законом у межах від 0 до 15с. Час моделювання становить 50 с.

Агенти TCP мають наступні параметри:

– алгоритм TCP – Reno;

– розмір TCP-вікна – 8000 пакетів;

– розмір TCP-пакета – 552 байт.

Також для ведення статистики подій в мережі, яка моделюється, використовуються файли трасування, а саме out.tr, queuesize.tr, queuebw.tr, queuelost.tr, queue.tr, win.dat. У файлі out.tr записуються усі події, що мають місце у мережі. Файли queuesize.tr, queuebw.tr, queuelost.tr, queue.tr містять дані щодо розміру черги, її пропускної здатності, кількості втрат у черзі та загальну інформацію про події у черзі між вузлами R(1) та R(2). Файл win.dat веде моніторинг розміру TCP-вікна усіх потоків від джерел S(1) – S(100).

Розроблена модель буде використана для дослідження процесів управління чергою на маршрутизаторах та прикордонних мережних пристроях.

Література

1. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы/В.Г. Олифер, Н.А. Олифер – СПб, «Питер», 2001 – 672с

2. Столингс В. Современные компьютерные сети / В. Столингс – 2-ое издание – СПб, «Питер», 2003 – 782 с.

3. The network simulator ns-2. [електронний ресурс] – режим доступу: http://www.isi.edu/nsnam/ns/. Назва з екрану.

Анотація

В статті поставлена задача з моделювання ділянки мережі за умов перевантаження. В якості базової моделі використовується сегмент комп'ютерної мережі. Реалізована модель в пакеті ns-2. Розроблена модель забезпечує можливість дослідження роботи алгоритмів управління при різних величинах навантаження.

Ключові слова: алгоритм, навантаження, модель, передача даних.

Аннотация

В статье поставлена задача по моделированию участка сети в условиях перегрузки. В качестве базовой модели используется сегмент компьютерной сети. Реализована модель в пакете ns-2. Разработанная модель обеспечивает возможность исследования работы алгоритмов управления при различных величинах нагрузки.

Ключевые слова: алгоритм, нагрузка, модель, передача данных.

Abstract

In the article the task of modeling area network overload conditions. As the base model uses a computer network segment. Implemented model package ns-2. The model provides the possibility of studies of control algorithms for different values of the load.

Keywords: algorithm, load, model, data transmission.