Об'єктом дослідження є процес забезпечення QoS в мережах наступного покоління. Предмет дослідження – методи й алгоритми розрахунків показників QoS в мережах наступного покоління.

Проведені дослідження базуються на теорії ймовірностей, теорії масового обслуговування, теорії фрактальних процесів і методах імітаційного моделювання.

Список літератури

1. McDysan. “QoS and Traffic Management in IP and ATM Networks”. McGraw-Hill.2000.
2. Е.А. Кучерявый. Управление трафиком и качество обслуживания в Интернет. СПб, Наука и Техника. 2004.
3. Р. Кох, ГГ. Яновский. “Эволюция и конвергенция в электросвязи”. М., Радио и связь. 2001.
4. МСЕ-т Recommendation Y.1541. “Network Performance Objectives for IP-Based Services”. May 2002.
5. Лагутин В.С. Оценка характеристик пропускной способности мультисервісних пакетных сетей при реализации технологии разделения типов нагрузки. “Электросвязь”, №3, 2003.
6. Gunnar Ronneberg and Olav Lysne. ”An OPNET-based Simulation Model of SCI-nodes”.
7. Debasis Mitra, K. G. Ramakrishnan,”Techniques for traffic engineering of multiservice, multipriority networks”. BLTJ. - 2001. - Vol.1.- №1.
8. Лихтциндер Б.Я., Попов П.М. Инжиниринг трафіку в мультисервісних сетях. «Электросвязь», №7, 2005.

УДК 004.4

Ф.О. Семенов
Науковий керівник – Якименко Н.М., канд. фіз.-мат. наук, доцент
Кіровоградський національний технічний університет

Розробка програмного забезпечення методу виявлення аномалій телекомунікаційного трафіку на основі спектрально-часового аналізу

Активне використання на сучасний час розподілених комп’ютерних систем та мереж приводить до необхідності приділяти увагу питанням безпеки.

Особливе місце в реалізації політики безпеки організації займають системи виявлення вторгнень (подій з безпекою) (СВВ), які можуть як виконувати функцію зворотного зв'язка, контролюючи ефективність компонентів системи безпеки, тобто бути, як доповненням до існуючого комплексу засобів захисту, так і являти собою самостійний продукт.

Впровадження багатьох СВВ, як і комплексних систем безпеки, стримує ряд факторів, таких як одноразові капіталовкладення, необхідність компетентної установки, настроювання, підтримки й т.д. У таких компаніях, як правило, функція спостереження за роботою мережі покладається на адміністратора. У такому випадку результат залежить від людського фактора, що включає досвід, інтуїцію, відповідальність, працездатність і т.п. Слід зазначити, що практично в кожній компанії, що має в розпорядженні розподілену мережу, установлені засоби збору статистичних даних про завантаження інтерфейсів мережного встаткування. Таким чином, закономірним кроком до автоматизації процесу виявлення позаштатних ситуацій, є впровадження доступного й, можна сказати, універсального засобу, що аналізує інтенсивності потоків даних у пошуку незвичайних і підозрілих подій або тенденцій, яке можна віднести до підкласу СВВ.

При цьому може використовуватися як сигнатурний метод, так і метод описової статистики. Математично обґрунтованими видами аналізу часових рядів є дослідження

сигналу на основі часових, спектральних і спектрально-часових алгоритмів, які інтенсивно розвиваються останнє з невеликим десятиліття.

Аналіз у часовій області ґрунтується на методах математичної статистики і його можливості досить великі. Але слід зазначити, що досліджуваному телекомунікаційному сигналу властиво «виражене коливальне поводження» через його особливості його формування. Хоча в методах часового аналізу існують підходи для опису такого роду сигналів, найбільш підходящими для дослідження коливального процесу є методи спектрального й спектрально-часового аналізу. Частотні подання є більше інформативними й дозволяють розширити можливості існуючих систем виявлення аномалій, але вимагають більших розмірностей для подання результатів і мають більшу обчислювальну складність алгоритмів, що стримує їхнє застосування й розвиток у прикладних завданнях. Отже, є актуальною розробка методу виявлення аномалій в інтенсивностях потоків даних на основі алгоритмів аналізу частотних складових, оптимізованих по обчислювальному навантаженню.

Метою роботи є розробка підвищуючого безпеку функціонування мережі методу виявлення аномалій у даних про завантаження інтерфейсів телекомунікаційного встаткування, на основі аналізу частотних характеристик; оптимізація по обчислювальному навантаженню формуючих метод зсувних спектральних і спектрально-часових алгоритмів з одержанням математичних моделей оптимізації й дослідження особливостей і обмежень використання частотного подання в розглянутому додатку.

Завдання досліджень включають: дослідження спектральних і спектрально-часових алгоритмів аналізу й подання часових рядів, у тому числі визначення особливостей і обмежень їхнього використання в області застосування; дослідження алгоритмів спектрального розкладання, у тому числі з урахуванням зрушень аналізованої послідовності, із пропозицією математичної моделі оптимізації обчислень; дослідження формування областей впливу й вірогідності картини вейвлет-коефіцієнтів при реалізації алгоритмів спектрально-часового аналізу.

Пропозиція математичної моделі оптимізації алгоритмів спектрально-часового розкладання, у тому числі з урахуванням зрушень аналізованої послідовності й області вірогідності коефіцієнтів розкладання.

Пропозиція способу зменшення області невірогідності за рахунок введення в аналіз так званого довірчого простору вейвлет-коефіцієнтів.

Формування теоретичної й практичної бази для методу виявлення аномалій у результаті дослідження впливу особливостей сигналу на вейвлет-коефіцієнти.

Розробка методу виявлення аномалій у даних про завантаження інтерфейсів мережного устаткування на основі аналізу частотних характеристик.

Об'єктом дослідження є процес виявлення аномалій телекомунікаційного трафіку. Предмет дослідження – методи виявлення аномалій телекомунікаційного трафіку на основі спектрально-часового аналізу. Методи дослідження базуються на теорії ймовірностей і математичної статистики, теорії розпізнавання образів, теорії обчислювальних систем і мереж.

Список літератури

1. Будько М.Б., Будько М.Ю. Отслеживание изменений в структуре сети и решение задач повышения безопасности на основе анализа потоков данных // Научно-технический вестник Санкт-петербургского гос. унив. информац. технол., механики и оптики. №59. – СПб.: СПбГУ ИТМО. – 2009. – С. 78-82.
2. Будько М.Б. Определение источника широковещательного шторма на основе данных протокола SNMP // Сборник трудов конф. мол. ученых. № 6. Информац. технолог.–СПб.: СПбГУ ИТМО.–2009.–С.153-157
3. Будько М.Б., Будько М.Ю., Гирик А.В. Применение авторегрессионного интегрированного скользящего среднего в алгоритмах управления перегрузками протоколов передачи потоковых данных // Научно-технический вестник СПбГУ ИТМО. – 2007. – № 39. – С. 319-323.