3.3. ПІДСЕКЦІЯ - КІБЕРБЕЗПЕКА ТА МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ

УДК 004.056.5

МОДЕЛЬ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ КОМП'ЮТЕРНОЇ МЕРЕЖІ НА ОСНОВІ ТЕСТУВАННЯ НАВАНТАЖЕННЯ

Титаренко М. С., студ. гр. КБ-161
Науковий керівник: **Базилевич В. М.,** к.е.н., доцент
Національний університет «Чернігівська політехніка»

Поява хмарних обчислень і очікування доступності даних і послуг в будь-який момент часу для користувача висунули проблему стійкості мереж на передній план досліджень в області комп'ютерної науки. Сучасні мережі передачі даних можуть бути величезними за розміром і складатися з сотень тисяч серверів і мільйонів віртуальних кінцевих вузлів. При таких масштабах і складності, проблеми масштабованості, ефективності, доступності та відмовостійкості мережі стають все більш актуальнами для дослідження.

Метою даної роботи є дослідження основних проблем стійкості та надійності комп'ютерних мереж.

Більшість додатків звязку, такі як месенджер, телеграм або наприклад "whats up", або ж просто телефонні розмови чи транзакції кредитною карткою, припускають наявність надійної відмовостійкої мережі. На цьому этапі очікується, що дані циркулюватимуть в мережі та надходитимуть до місця призначення. З іншої сторони фізичні компоненти мережі стикаються з широким спектром проблем, починаючи від спотворення сигналу і закінчуючи збоями самих компонентів. Аналогічно програмне забезпечення з семантичним інтерфейсом високого рівня нерідко містить невідомі помилки та інші приховані проблеми з надійністю. Надмірність - є основою для всіх підходів відмовостійкості.

Надмірність приймає дві форми просторову та часову. Просторова надмірність здійснює реплікацію компонентів або даних в системі. Прикладом її є передача даних декількома шляхами мережі та використання кодів з виправленням помилок. Часова надмірність є основою для алгоритмів повторного запиту (ARQ), таких як абстракція змінного вікна, який використовується для надійної передачі даних в протоколі TCP. Надійна мережа зазвичай забезпечую як просторову так і часову надмірність, що дозволяє витримати збої з різною часовою стійкістю. Просторова надмірність необхідна для протистояння постійним збоям в фізичних компонентах, в той час як часова надмірність, вимагає менше ресурсів, і завдяки цьому є біль пріоритетною при роботі з тимчасовими помилками [1].

Розробляючи будь-яку систему, спочатку необхідно обрати модель помилок – набір можливих сценаріїв вімов, беручи до уваги частоту, тривалість та вплив кожного сценарію. Проста модель включає тільки набір несправностей, які необхідно враховувати; рішення про включення до набору приймається на основі комбінації частоти, що очікується, впливу на систему та вартості забезпечення захисту. Найбільш надійні ж конструкції мережі усувають збої будь-якого окремого компонента. А деякі конструкції іноді допускають множинні збої. Але мало хто намагається протистояти умовам, що можуть виникнути при терористичному акті, і катастрофічні атаки майже ніколи не розглядаються в масштабі, що перевищує місто. (Напротив, мало кто пытается справиться с противоборствующими условиями, которые могут возникнуть при террористической атаке, и катастрофические события почти никогда не рассматриваются в любом масштабе, превышающем город.)

Усі збої комп'ютерних мереж можна класифікувати за часовою характеристикою як постійні, преривчасті та перехідні [1]. Наприклад, збої, що перешкоджають функціонуванню компонента при його ремонті або заміні, такі як пошкодження мережевого волокна екскаватором є постійними. Відмови, що все ж дозволяють компоненту функціонувати належним чином називають преривчасті. Це можуть бути пошкодження електричних компонентів, що працюють справно до тих пір, поки механічні або температурні коливання не стануть причиною збою, і не відновляться до повернення показників у норму. Остання категорія – перехідні несправності, яка оброблюються найлегше. Вони варіюються від змін вмісту компютерної памяті через космічні промені до бітових помилок через теплові шуми в демодуляторі, що, як правило, є нечастими й непередбачуваними. Різниця між преривчастими та перехідними несправнотсями заключається тільки в частоті; для перехідних несправностей, комбінація кодів з виправленням помилок і повторною передачею даних зазвичай забезпечує непоганий захист.

Окрім вибора моделі несправностей, при проектуванні відмовостійкої мережі система повинна мати можливість ізолювати її від частини системи, що функціонує таким чином, щоб це запобігало поширенню некоректної поведінки. Так як механізм виявлення несправностей, може виявити більше, ніж одну можливу несправність, система також повинна враховувати процес діагностики або локалізаціїї, який звужує набір можливих несправностей і дозволяє застосовувати більш ефективні методи ізоляції. Помилки, які ідентифікувала система, не обовязково повинні бути звужені до одної, але менший набір можливостей зазвичай дозволяє використовувати більш ефективну стратегію відновлення.

Границі ізоляції відмов, як правило, призначені для забезпечення режиму аварійної зупинки. Термін аварійної зупинки передбачає, що некоректна поведінка не поширюється по всій границі ізоляції відмов; навпаки компоненти, що мають несправну поведінку припиняють видавати будь-які сигнали. Та слід зазначити, що аварійна зупинка не передбачає самодіагностику але компоненти суміжні з несправними, можуть діагностувати відмову и навмисно ігнорувати будь-які сигнали, що надходять від пошкодженого компонента і фізична конструкція системи має допускати таке рішення. В маршрутизаторі наприклад, в зєднанні між картами, повинна бути передбачена електрична ізоляція для підтримки відмовостійкості несправних карт. Міжкомпонентне зєднання на основі шини не допускає аварійної зупинки, так як ніщо не може запобігти неспавній карті некоректно керувати лініями шини. В сучасних високопродуктивних мережах шинні зєднання були замінені на комутативні для забезпечення такої ізоляції. Викорінення аналогічних явищ при переході від загальних до комутованих Ethernet в середині 1990-х років було одним з основних адміністративних переваг цієї зміни, оскільки хости, що відмовили з набагато меншою ймовірністю можуть зробити комутативну мережу непридатною для використання через її безперервну передачу трафіку.

Для оцінки пропускної здатності, надійності, відмовостійкості та інших характеристик мережі необхідне проведення її діагностики та тестування. Під діагностикою мережі розуміють вимірювання її характеристика під час її експлуатації.

Тестування можна умовно класифікувати на декілька видів в залежності від цілі. Це тестування кабельної системи мережі на відповідність стандартам; стресове тестування, ціллю якого є перевірка стійкості компонентів мережі при різних рівнях навантаження та різних типах трафіку; тестування ПЗ, для визначення його вимого до пропускної здатності мережевих ресурсів; стресове тестування конкретних мережевих конфігурація для виявлення прихованих дефектів в обладнанні та слабких місць в архітектурі мережі, а також для визначення порогових значень трафіку, що допускається в мережі; тестування навантаження, що перевіряє як швидко працює мережа при різних навантаженнях; тестування стабільності, що розглядає надійність мережі на довгому інтервалі часу; тестування відмовостійкості – перевірка наскільки швидко система справляється зі збоями; тестування обємів, аналіз поведінки системі після збільшення обємів; тестування масштабованості, що показує як збільшить навантаження на компоненти системи при збільшенні числа користувачів; тестування потенціальних можливостей – ціль якого є розрахунок користувачів, що можуть працювати в системі.

Використання можливих методів тестування та діагностики мереж, дозволить своєчасно виявити та виправити якомога швидше підвищити ефективність та збільшити експлуатаційних термін мережі.

Для побудови моделі забезпечення стійкості компютерної мережі було обрано найбільш відомий та використовуваний метод тестування мережі - метод тестування навантаження.

Даний тип тестування дозволить в повній мірі оцінити поведінку системи при зростаючому навантаженні. Його ціль – визначення максимального навантаження, яке може витримати система. За навантаження може сприйматися як кількість користувачів, так і кількість операцій.

Отже, було проаналізовано та виділено основні проблеми надійності та відмовостійкості комп'ютерних мереж. Цілі стійкості комп'ютерної мережі можна розділити на три категорії: запобігання, виявлення та реагування. Виявлення вторгнень відіграє критичну роль в безпеці більшості систем, так як методи встановлення паролів та контроль доступу часто можуть бути скомпроментовані. Тож при управлінні мережею необхідно включати додаткові механізми виявлення вторгнень. Не менш важливим є і аналіз виявлених вторгнень, що дозволить скорегувати або заблокувати загрозу. Та реагування, що дозволить залишити мережу доступною. До того ж розглянуто класифікацію методів тестування мережі та обрано найоптимальніший – метод тестування навантаження. Отримані дані будуть використані в подальших дослідженнях у цьому напрямку для розробки моделі забезпечення стійкості комп'ютерних мереж.

Список використаних джерел

1. Muriel Médard, Steven S. Lumetta. Network Reliability and Fault Tolerance March 2003 [Электронный ресурс] / Muriel Médard, Steven S. Lumetta - Режим доступу до ресурсу: https://www.researchgate.net/publication/2884965_Network_Reliability_and_Fault_Tolerance.
2. Paul Rubens. Understanding Fault Tolerance: Securing Your System [Электронный ресурс] / Paul Rubens - Режим доступу до ресурсу: https://www.enterprisestorageforum.com/storage-management/fault-tolerance.html.
3. Нагрузочной тестирование [Электронный ресурс] - Режим доступа до ресурсу: https://www.performance-lab.ru/blog/load-testing/testirovanie-proizvoditelnosti.
4. В. Олифер. "Компьютерные сети. Принципы, технологии, протоколы. Учебник" / В. Олифер, Н. Олифер., 2016. - (5).
5. А. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник. КОМП'ЮТЕРНІ МЕРЕЖІ / А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник. - Львів: Магнолія 2006, 2013 - 253 с.

УДК 004.056

МЕТОДИКА ОЦІНКИ ЕФЕКТИВНОСТІ ПРОТИДІЇ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИМ ВПЛИВАМ

Тимошенко Є. М., студ. гр. КБ-161
Науковий керівник: **Гур'єв В. І.,** к.т.н., доцент
Національний університет «Чернігівська політехніка»

Цінність інформації можуть визначити лише і виключно суб'єкти захисту інформації люди та/або соціальні групи. Більш того: саме поняття цінності інформації носить суб'єктивний характер: різні люди (соціальні групи) цілком можуть надати різну цінність для однієї й тієї ж самої інформації. Крім того, цінність інформації є різною для різної діяльності людини та/або соціальної групи. Таким чином, і тут наявність моделі для опису діяльності людини та соціальної групи є фактором, який здатний підвищити захищеність інформації.

Наведемо аналіз основних існуючих формальних моделей інформаційної безпеки. Розглянуто лише ті складові моделей та методів, які описують суб'єктну складову, так як саме врахування «не ідеальності» суб'єктів та суб'єкт-суб'єктних відношень є сьогодні одним із головних джерел зниження рівня захищеності людини та соціальної групи.

Моделі забезпечення конфіденційності.