УДК 629.39

О.М. ОДАРУЩЕНКО, В.І. БОЖКО

Полтавський військовий інститут зв'язку, Україна

АНАЛІЗ МЕТОДІВ БОРОТЬБИ З ТУПИКОВИМИ СИТУАЦІЯМИ В КРИТИЧНИХ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Проведено аналіз основних методів боротьби з тупиковими ситуаціями в критичних телекомунікаційних системах, наведено варіант їх класифікації. На основі виявлених недоліків, визначені можливі шляхи підвищення коректності розглянутих методів.

критична телекомунікаційна система, deadlock, тупикова ситуація, clinch, функціональна стабільність, розподіл ресурсів

Постановка проблеми та її зв'язок з науково-практичними задачами

Одним з основних факторів, що приводить до різкого зниження функціональної стабільності критичних телекомунікаційних систем (КТС) [1], є виникнення тупикових ситуацій (deadlock, взаємоблокувань, критичних ситуацій, клинчів (clinch), надалі deadlock) на використання ресурсів процесами системи. Ресурсами в КТС є: сервіси, послуги, служби, додатки, обчислювальна потужність процесорів, балансувальники навантаження, різні види пам'яті (буферна мережних вузлів, диски і т.д.).

Deadlock виникає, коли декілька процесів виявляються в стані невизначеного взаємного чекання і кожний з них не може продовжуватися, оскільки деякий інший процес з цієї множини або не може звільнити хоча б один ресурс що запитується, або не може одержати якесь керуюче повідомлення (квитанцію, відгук). Загальною рисою deadlock в є те, що вони виникають при обставинах, що важко передбачити (а іноді і не можливо взагалі), або за думкою проектувальників є малоймовірними, через відсутність достатньої апріорної інформації про функціонування системи.

З deadlock можливо досить ефективно боротися, однак ціна подібних дій висока і відповідні зусилля повинні застосовуватися тільки в системах, де ігнорування deadlock приводить до катастрофічних наслідків, що є характерним для КТС.

В майбутніх КТС deadlock стануть ще критичнішим фактором для їх ефективного функціонування, тому що [2]:

– їх програмне забезпечення буде у більшому ступені орієнтовано на паралельну роботу;

– буде переважно реалізовуватися динамічний розподіл ресурсів.

Потенційно в КТС можливі наступні види deadlock (табл. 1, 2). Як класифікаційні ознаки обрано рівень моделі взаємодії відкритих систем (ВВС) та етапи життєвого циклу КТС на яких можливе виникнення deadlock.

Таблиця 1

Потенційно можливі види deadlock

Рівень моделі ВВС	Вид deadlock
канальний	– пряма і непряма deadlock передачі з проміжним збереженням; – додаткового навішення
мережний	– компоновочна deadlock; – deadlock при установленні віртуального каналу; – deadlock викликана пріоритетністю пакетів
транспортний	– статистична deadlock потоків; – deadlock, зв'язані з не доведенням повідомлень і темпом передачі
сеансовий, прикладний	– deadlock в банках даних

Таблиця 2

Причини виникнення deadlock на різних етапах

Етап виникнення deadlock	Причини виникнення deadlock
проектування та модернізації	– логічні помилки проектувальників; – недосконаліть алгоритмів керування розподілом ресурсів; – неможливість фізичної реалізації оптимальних рішень
функціонування	– вихід з ладу обчислювального обладнання; – вихід з ладу мережних пристроїв; – порушення процедур контролю за користувачем; – порушення угод по трафіку; – несанкціонований доступ до мережі; – зміни фізичної структури; – вплив різного роду перешкод; – апаратурні помилки та збої у програмному забезпеченні

Пряма deadlock передачі виникає в двох суміжних вузлах, коли буфер одного з них заповнений, повідомленнями призначеними для іншого. Непряма deadlock передачі виникає на ділянці мережі, що містить більш ніж два вузли і утворює логічний цикл, у якому повідомлення направляються вузлам адресатам, що знаходяться на відстані двох чи більш переприйомів. Коли всі буфери в вузла зайняті цими пакетами, передачі цілком блокуються.

Deadlock збірки повідомлення може виникнути, коли повідомлення розбивається на повідомленнями у вузлі-відправнику, а збирається у вузлі-адресаті. Deadlock настає, коли всі буфери збірки вузла-адресата зайняті незібраними повідомленнями і новий пакет не може бути приєднаний до жодного з них.

Deadlock, викликане пріоритетністю потоків, виникає, коли всі буфери вузла зайняті низькопріоритетними пакетами, що очікують інші низькопріоритетні повідомленнями для зборки чи повідомлень для витягу з них квитанцій і знищення копій пакетів. Але ці повідомленнями можуть бути блоковані в сусідніх вузлах високопріоритетними пакетами, що очікують передачі в даний вузол.

Варто зазначити, що найбільш ймовірними причинами виникнення deadlock бачаться ті, що пов'язані з особливостями їх функціонування (ризиками) такими як просторова розосередженість і рухливість елементів системи, нестаціонарність і функціональна залежність потоків повідомлень, імовірнісний та агресивний вплив середовища функціонування [1]. Найбільш характерними з них будуть: вихід з ладу мережного обладнання, несанкціонований доступ, вплив різного роду перешкод. Зазначені особливості виникнення deadlock потребують застосування методів боротьби з ними, які дозволять гарантувати необхідну функціональну стабільність КТС.

Проведемо аналіз основних методів боротьби з deadlock в різних прикладних областях, та визначимо їх обмеження при застосуванні в КТС.

Класифікація методів боротьби з тупиковими ситуаціями в КТС

Відомі наступні стратегії (підходи) боротьби з deadlock [2 – 7]: ігнорування, визначення, попередження й уникнення тупикових ситуацій. Усі вони, при деякий умовах, можуть тією чи іншою мірою бути використані в КТС.

Методи стратегій визначення, попередження й уникнення deadlock базуються на перевірці наступних чотирьох умов [2]:

1. Умова взаємовиключення (Mutual exclusion).
2. Умова очікування ресурсів (Hold and wait).
3. Умова неперерозподілу (No preemtion).
4. Умова кругового очікування (Circular wait).

Для deadlock необхідне виконання всіх умов.

Більшість з відомих методів боротьби з deadlock засновані на графових моделях доступу процесів до ресурсів системи (WFG).

Порівняння методів боротьби з deadlock проводять за наступними основними параметрами: кіль-

кість процесів беруть участь в deadlock; комунікативна затримка при взаємодії областей; період між двома модифікаціями WFG; діаметр WFG. Окремо визначають ймовірність появи deadlock, що залежить від багатьох факторів, таких як склад множини процесів, середнього числа об'єктів що використовуються процесами, часу використання ресурсів й т.п.

За способом використання інформації про функціонування процесів методи боротьби з deadlock можливо поділити на детерміновані та імовірнісні. При розгляданні детермінованих методів істотного значення набуває апріорна інформація про потреби процесів в ресурсах. При повній апріорній інформації використовуються методи попередження deadlock. При відсутності апріорної інформації використовується методи виявлення deadlock. Імовірнісні методи поки не одержали практичного використання в КТС через необхідність стабільної статистичної інформації, для одержання якої потрібен значний досвід експлуатації, що для КТС проблематично.

Найпростіша з визначених стратегій – ігнорування проблеми deadlock. Якщо deadlock зустрічається рідше аварійної зупинки системи через відмови устаткування чи помилки в програмному забезпеченні, то в деяких додатках (наприклад в ОС Unix) використання цієї стратегії може виправдовуватися. У КТС даний підхід не застосовують.

Методи виявлення deadlock не використовують апріорну інформацію про потреби процесів у ресурсах і базуються на необхідних і (чи) достатніх умовах існування (наявності) чи відсутності deadlock. З перерахованих у табл. 3 методів боротьби у КТС, у принципі, може бути використаний кожний. Але варто мати на увазі, що майже всі методи вимагають, щоб у кожному елементі системи при децентралізованому методі керування підтримувалася глобальна графова модель доступу всіх процесів до всіх ресурсів системи, що різко збільшує обсяги службової пам'яті і вимагає додаткового обміну службовими повідомленнями, що підвищує імовірність визначення фальшивої deadlock-ситуації.

Таблиця 3

Методи боротьби с deadlock у КТС

Стратегія боротьби	Методи боротьби
Ігнорування deadlock	– алгоритм „страуса”
Виявлення deadlock	*Централізованого керування:* – однофазний і двохфазний Ho-Ramamoorhy-алгоритми; – ієрархічні мережі Петрі; – графова модель Холта; – графова модель Ислора й Марсланда; – використання методів теорії категорій та логіки присутності. *Розподіленого й ієрархічного керування*: – алгоритми проштовхування шляхів (Path-pushing): Obermarck's, Menasce-Muntz, Badal- алгоритм; – алгоритми прогону (Edge-chasing): Mitchell-Meritt, Chandy-Misra-Haas- алгоритм; – дифузійні алгоритми, Chandy-Misra-Haas, Hermann- Chandy – алгоритм; – використання багаторівневих нейронних моделей з ансамблевою організацією
Попередження та уникання deadlock	– за рахунок ретельного розподілу ресурсів (алгоритм Дейкстри); – порушення однієї з умов виникнення deadlock (стратегія Хавендера); – графовая модель Кинга
Відновлення після deadlock	– через перерозподіл ресурсів; – через відкат назад; – через ліквідацію одного із процесів

У КТС із централізованим методом керування повинна формуватися і підтримуватися тільки одна глобальна графова модель, коли за виявлення deadlock відповідає один керуючий елемент. Але цей підхід прийнятний тільки для локальних систем, тому що в територіально розподілених системах виникають труднощі в зборі інформації з усіх елементів системи. Варто зазначити, що виявлення deadlock ще не приводить до їхньої ліквідації, тому необхідно приймати відповідні міри для їх усунення

через перерозподіл ресурсів, відкат назад чи ліквідацію одного із заблокованих процесів.

Методи попередження та уникання deadlock можна розділити на два види: запит усіх необхідних ресурсів одночасно й їх перерозподіл. Вони широко використовується в більшості сучасних операційних системам. Застосування їх в КТС обмежене через неефективне використання і значний час чекання звільнення ресурсів. Відбувається обмеження можливих послідовностей запитів на ресурси.

Таким чином, у КТС попередження та уникання deadlock здійснюється або за допомогою глобального резервування усіх ресурсів, необхідних процесу, або шляхом упорядкування виконання конфліктуючих процесів. Основні недоліки методів попередження deadlock: неефективне використання ресурсів і необхідність мати повну апріорну інформацію про потреби процесів у ресурсах, порядок запитів або в накладенні обмежень на структуру телекомунікаційних ресурсів.

Висновки і перспективи подальших досліджень

Проведені дослідження показують, що незважаючи на використання значної кількості методів боротьби з deadlock в КТС, залишається реальністю їх низька коректність. У зв'язку з цим, можливо зробити наступні висновки:

– незважаючи на витрати у виді додаткових ресурсів, попередження deadlock може виявитися настільки неефективним, що вигідніше допускати їхнє виникнення з метою подальшого виявлення і ліквідації;

– у КТС, коли не представляється можливим заздалегідь спланувати розподілені ресурси, а користувачі працюють в системі в режимі реального часу, ініціюючи процеси випадковим образом, виявлення й усунення deadlock можуть виявитися єдиними методами боротьби з deadlock, що забезпечують підвищення функціональної стабільності системи;

– одним з можливих підходів в підвищенні функціональної стабільності КТС може стати використання нетрадиційних методів боротьби з КТС та їх комплексування на основі апарату теорії надійності апаратних та програмних засобів.

Література

1. Талалаєв В.О. Методологія наукового супроводу впровадження сучасних цифрових технологій в польових телекомунікаційних мережах критичного застосування // Зб. доповідей ІІ НПК “Пріоритетні напрямки розвитку телекомунікаційних систем спеціального призначення”. – К.: ВІТІ НТУУ “КПІ”, 2005. – С. 45-51.

2. Гарви М., Дейтел Г. Введение в операционные системы. – М.: Мир, 1987. – 620 с.

3. Сундеев П.В. Автоматизация анализа функциональной стабильности критичных информационных систем // Научный электронный журнал КубГАУ № 3 (5). – Краснодар: Краснодарский государственный аграрный университет. – 2004. – [Электрон. ресурс]. – Режим доступа: http://ej2.kubagro.ru/2004/03/05/p05.htm.

4. Андрюхин А.И., Ковалева Т.В. Анализ и проблемы алгоритмов диагностирования блокировок в распределенных системах // Донецк: ДонНТУ, 2005. – [Электрон. ресурс]. – Режим доступа: http://www.uran.donetsk.ua/~masters/2005/fvti/kovalyova.

5. Охорзин В.М., Титов В.С. Сети передачи данных и методы обмена данными. – Л.: ВАС, 1985. – 82 с.

6. Menasce D.A., Muntz R.R. Locking and deadlock detection in distributed data bases // IEEE Trans.Software Eng. – 1979. – 5 (3). – С.195-202.

Надійшла до редакції 1.02.2006

Рецензент: канд. техн. наук, доцент О.Ю. Стрюк, Полтавський військовий інститут зв’язку, Полтава.