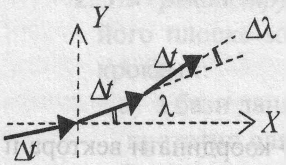

Рис.2. Утворення кривої за системою параметричних рівнянь

обмеженого розміру обробляючого поля. За допомогою програмного управління можна також досягти представлення зображень живої природи в динаміці. І нарешті, оптико-електронна техніка найкраще пристосована до голографічної реалізації викладених уявлень. Зрозуміло, що такий апарат має більше переваг, ніж дисплей, навіть якщо не враховувати естетичні уявлення.

1. Джордан Айян, 10 способов освободить ваш творческий гений. – Спб., Питер, 1997. – 340с.
2. Завьялов Ю.С., Леус В.А., Скороспелов В.А. Сплайны в инженерной геометрии. – М.: Машиностроение, 1985. – 220 с.
3. OpenGL Programming Guide, 353 p. Internet resources (PDF), opengl.miem.edu.ru

К. Обельовська
Національний університет "Львівська політехніка"

УДК 681.324

ДОСТОВІРНІСТЬ ПЕРЕДАЧІ ІНФОРМАЦІЇ В СИСТЕМІ СИГНАЛІЗАЦІЇ *SS7*

Проаналізовано помилки, що не виявляються в підсистемі передачі повідомлень рівня 2 системи сигналізації SS7. Запропоновано спосіб зменшення їх кількості в два рази.

The SS7 signaling system level 2 message transfer part undetected error analysis was carried out. The technique to reduce their amount twice is proposed.

У цифрових мережах інтегрального обслуговування (*Integrated Services Digital Network*, *ISDN*) обмін управляючою інформацією здійснюється у межах системи сигналізації N7 (*Signaling System 7*, *SS7*). Другий рівень архітектури *SS7* реалізовано за допомогою підсистеми передачі повідомлень рівня 2 (*Message Transfer Part 2*, *MTP2*) [1]. Для обміну даними в *MTP2* використовуються сигнальні одиниці, а оскільки вони

містять управляючу інформацію, то забезпечення достовірності їх передачі має важливе значення.

Формат значущої сигнальної одиниці та алгоритм забезпечення достовірності

Формат значущої сигнальної одиниці показано на рисунку, де числа вказують розмір відповідних полів в двійкових розрядах [2].

Значуща сигнальна одиниця починається і закінчується полем П (прапор).

Для нумерації сигнальних одиниць, що передаються, використовується семирозрядне поле ППН (прямий порядковий номер). Номери кадрів, що підтверджуються, записуються в семирозрядному полі ЗПН (зворотний порядковий номер). Це означає, що в системі сигналізації *N7* для нумерації кадрів використовуються порядкові номери від 0 до 127.

Додатне або від'ємне підтвердження значущих сигнальних одиниць здійснюються за допомогою поля ЗПН та зв'язаного з ним поля зворотного біту індикації (ЗБІ). Від'ємне підтвердження формується шляхом інверсії символу ЗБІ, інвертоване значення ЗБІ залишається доти, поки не буде виявлено новий спотворений кадр. При додатньому підтвердженні біт ЗБІ залишається незмінним.

Інверсія символу ПБІ означає повторну передачу значущої сигнальної одиниці. Інвертоване значення ПБІ залишається доти, поки знову не буде здійснюватись повторна передача значущої сигнальної одиниці.

П	ЗПН	ЗБІ	ППН	ПБІ	ВТіД	Р	БСІ	ПСІ	ППК	П
8	7	1	7	1	6	2	8	Ціле число байт	16	8

Формат значущої сигнальної одиниці системи сигналізації *SS7*

Поле сигнальної інформації (ПСІ) несе повідомлення користувача і містить адреси та іншу інформацію сигналізації. Воно має змінну довжину, значення якої вказується в шестирозр'ядному полі ВТіД (вказівник типу сигнальної одиниці і довжини). Після поля ВТіД у форматі значущої сигнальної одиниці є резервне поле (Р) довжиною два біти. Для розпізнавання національних і міжнародних повідомлень, визначення підсистеми користувача використовується восьмирозрядне поле байт-сервісної інформації (БСІ). Прикладами підсистеми користувача є підсистема телефонного абонента – *TUP*, підсистема користувача *ISDN-ISUP*.

У полі ППК (перевірочна послідовність кадру) знаходиться 16 надлишкових символів циклічного коду, які використовуються для виявлення помилок. Для виправлення помилок використовується протокол з *N*-поверненнями. В каналах з часом розповсюдження сигналу в один бік 15 Мс і більше (супутникових, міжконтинентальних) застосовується модифікований протокол з *N*-поверненнями – протокол з попереджувальним циклічним повторенням. При цьому методі при відсутності нової значущої сигнальної одиниці циклічно повторюється (без очікування на підтвердження) передача раніше переданих значущих сигнальних одиниць.

Якщо значущі сигнальні одиниці відсутні, замість них передаються заповнюючі сигнальні одиниці. Заповнюючі сигнальні одиниці служать для передачі додатних та від'ємних підтверджень.

Аналіз помилок, що не виявляються в MTP2 системи *SS7*

Будь-який надлишковий код, в тому числі і цей, що використовується в *MTP2* системи *SS7*, містить як дозволені, так і заборонені кодові комбінації. Для передачі використовуються тільки дозволені кодові комбінації.

При відсутності завад в каналі зв'язку прийомною станцією буде прийнята та ж дозволена комбінація, що і передавалась. Циклічний код ідентифікує цю передачу як правильну, і прийомна станція за допомогою полів ЗПН та ЗБІ відправить додатне підтвердження.

Якщо передається спотворена сигнальна одиниця, то це спотворення переведе комбінацію, що передавалась, у заборонену, циклічний код виявить помилку. Вона буде виправлена засобами протоколу з *N*-поверненням.

Якщо передається спотворена сигнальна одиниця, коли одна дозволена комбінація буде переведена в іншу дозволену, циклічний код таку помилку не виявить. Проаналізуємо два випадки з цієї ситуації. Перший – спотворені символи не захопили поля ППН та ЗПН, що відповідають за нумерацію сигнальних одиниць, другий - спотворені символи захопили поля ППН та ЗПН.

У першому випадку підсистема забезпечення достовірності *MTP2* буде продовжувати працювати в режимі передачі, тобто спотворена сигнальна одиниця буде підтверджена як правильно прийнята, а повідомлення, яке містить помилку, буде передано підсистемі передачі повідомлень третього рівня *MTP3*. Помилка в спотвореному повідомленні залежно від місць її розташування може бути виявлена одним з протоколів верхніх рівнів, проте чим вищий рівень, на якому помилка виправляється, тим більше часу потрібно затратити на її виправлення.

У другому випадку, коли спотворені символи потрапили на поля ППН та ЗПН, можливі два варіанти.

1. Незважаючи на те, що прийнята спотвореною сигнальна одиниця є дозволеною кодовою комбінацією і циклічний код не виявив помилку, помилка може бути виявлена, якщо порушені правила протоколу з *N*-поверненнями. Помилка такого типу може бути виправлена підсистемою *MTP2*.
2. Розглядається випадок, коли додатне підтвердження відсилається не на кожну сигнальну одиницю. Віддалена сторона *SS7*, прийнявши без помилок декілька сигнальних одиниць, порядкові номери яких ідуть один за одним, може підтвердити безпомилковий прийом цієї групи одиниць, записавши в поле ЗПН однієї з сигнальних одиниць, що передаюься в зворотньому напрямку, значення ППН останньої правильно прийнятої сигнальної одиниці [3]. Можливий випадок, коли при передачі такого підтвердження буде мати місце помилка, що не виявляється циклічним кодом, і в результаті спотворення замість номера ЗПН буде прийнято номер ЗПН+*i*, що лежить в границях номерів, на які очікується підтвердження. Такий варіант передбачає можливість витирання з буфера передаючого пристрою станції-джерела всієї групи сигнальних одиниць. Якщо ж при передачі сигнальних одиниць з номерами від ЗПН+1 до ЗПН+*i* буде мати місце спотворення, яке виявиться циклічним кодом і буде перепитано, буфер канального рівня станції-джерела вже не буде мати

інформації, яку треба повторити. Перенесення виправлення цієї помилки на верхні рівні збільшує час на її усунення.

Спосіб зменшення кількості помилок, що не виявляються в MTP2 системи *SS7*

У форматі значущої сгнальної одиниці є резервне поле довжиною в два двійкових розряди, що не використовується. Якщо це поле використати для додаткової контрольної перевірки сигнальної одиниці на достовірність, а саме перевірки на парність, то в результаті 50 % всіх помилок, що не виявлялись, буде виявлено. При цьому буде використано один розряд резервного поля. Таке рішення дасть змогу підвищити достовірність передачі даних в компоненті MTP2 та зменшити час на обробку тих помилок, які виправляються протоколами більш високих рівнів.

1. Орлов С. IP поверх *SS7*. LAN, N9, 2002. http://www.osp.ru/lan/2002/09/030.htm#vr.
2. ITU-T Q-Series Recommendation. Q.703. Message transfer part. Signalling link.
3. Битнер В.И. Общеканальная система сигнализации N7. http://center.neic.nsk.su/page_rus/htm/UCH_MAT/course2/index.

А.Ковальчук
Національний університет"Львівська політехніка"

УДК 511.217

ПРОСТІ ЧИСЛА ФЕРМА І МЕРСЕННА В СИСТЕМІ RSA

Встановлено нескінченність множини простих чисел Ферма і Мерсенна за умови, що існує хоч би два відповідні прості числа.

The infinity of a set of prime numbers Fermat and Mersenne is established provided that there are even two appropriate prime numbers

У системі *RSA*, як відомо, при шифруванні інформації для досягення високої стійкості шифру використовуються великі прості числа. Такі прості числа можна вибирати, зокрема, в нескінченних підмножинах чисел Ферма і Мерсенна.

Надалі використовуватимо таке твердження.

Аксіома нескінченного зменшення (АНЗ): якщо з твердження, за яким задане додатнє ціле число має задану множину властивостей, випливає, що існує менше до-