Макоївець Д.В.
студент,
Науковий керівник: **Полторак В.П.**
Кандидат технічних наук, доцент,
Національний технічний університет України
«Київський політехнічний інститут»

ЗАХИСТ ВІДЕОДАНИХ В ПАКЕТНИХ МЕРЕЖАХ

Розглядаючи проблему захисту відеоданих в мережах передачі даних можна виділити два типи захисту. Перший – це захист від третіх осіб, тобто від несанкціонованого доступу до відеоданих. Для його забезпечення використовують алгоритми шифрування (криптографічний захист). Другий – це захист від спотворень (помилок), що можуть виникати в процесі передачі даних по каналу зв'язку. Захист від помилок можна реалізувати повторним пересиланням спотворених даних, або виправленням помилок на стороні приймача. Для виявлення і виправлення помилок приймаючою стороною застосовують коди, що виявляють і виправляють помилки (завадостійкі коди).

Метою завадостійкого кодування є підвищення достовірності доставки повідомлень, переданих по каналах зв'язку із завадами. Актуальними залишаються методи завадостійкого кодування, орієнтовані на доставку повідомлень без використання зворотного каналу повідомлень в пакетних мережах. Прикладами таких мереж є будь-яка комп'ютерна мережа та мережа Інтернет. Тема використання корекції завадостійкого кодування (FEC – Forward Error Correction) в таких мережах не нова. Однак за останні 5-6 років у цій галузі кодування народилося багато нових ідей. В результаті був створений новий клас потокових кодів, орієнтований на вирішення великого числа мережевих додатків, для яких в інтерактивності немає необхідності. Застосування кодування в таких додатках дозволяє різко зменшити обсяг трафіку в мережі. Ці ідеї вже знайшли практичне втілення в таких мережевих додатках як IP мовлення, IP Multicast-сервіс, одночасна передача даних з декількох сайтів в Інтернет і т.д.

Останнім часом все більшого поширення набуває цифрове телебачення форматів DVB-T та DVB-T2. Оскільки при трансляції телевізійного сигналу немає можливості і часу на повторну пересилку пошкодженого пакету, то для виправлення помилок, що виникають при передачі, застосовують завадостійке кодування. У цифрових телевізійних передавачах застосовується завадостійкий код з виправленням помилок на вході приймача FEC. Він складається з двох кодів: зовнішнього і внутрішнього. Це забезпечує отримання помилок в тракті передачі-прийому BER (bit error rate) рівна 10^{-11} (і навіть 10^{-13}) [1].

Для формату DVB-T застосовується кодування згортковим кодом та кодом Ріда-Соломона, у форматі DVB-T2 – LDPC код та код БЧХ. Застосовуючи БЧХ + LDPC, вдається отримати виграш у порівнянні з кодом Ріда-Соломона + згортковий приблизно в 5 дБ.

По своїй суті принципи захисту від помилок у системах відеоконференцзв'язку (ВКЗ) дуже схожі з системами захисту в цифровому телебаченні. Це все ті ж завадостійкі коди і перемішування пакетів. Однак тут дещо переважає застосування згорткових кодів із використанням декодування за алгоритмом Вітербі. Це частково пояснюється саме оптимізацією алгоритму декодування. Алгоритм оптимізований за рахунок використання особливостей структури конкретної решітки коду. Перевага декодування Вітербі порівняно з декодуванням за методом повного перебору полягає в тому, що складність декодера Вітербі не є функцією кількості символів в послідовності кодових слів.

Згорткові коди виправляють окремі бітові помилки. Блокові коди, у тому числі коди Ріда-Соломона, здатні виправляти пачки помилок в окремо взятому пакеті. Але у випадку втрати пакета цілком вони безсилі.

В даний час можна говорити про створення нового класу завадостійких кодів для каналів зі стиранням – стираючих кодів [2, с. 37]. Кодами з цього класу можна закодувати повідомлення скінченого розміру потенційно необмеженим потоком незалежних пакетів. Ця властивість нового класу кодів принципово відрізняє його від класичних блокових або згорткових завадостійких кодів із заданою швидкістю (fixed rate). Для кодів з нового класу з'явився термін «rateless» (нефіксованої швидкості). Їх називають також фонтанними кодами (Digital Fountain Codes). Історично першим і найбільш ідейно цікавим rateless кодом вважається LT код.

Найважливішою відмінністю стираючих кодів від блокових і згорткових кодів є можливість відновлення цілого пакету в разі його втрати.

Аналіз наявних на даний момент джерел показав, що є лише поодинокі спроби застосування стираючих кодів в IPTV. Говорити про більш-менш цілісну технологію IPTV із застосуванням стираючих кодів поки не доводиться. Можна виділити лише стандарт мобільного телемовлення DVB-H (Digital Video Broadcasting Handheld), який передбачає використання стираючих кодів Raptor, розроблених на основі кодів ЛТ з урахуванням специфіки мобільного телемовлення.

Основними властивостями ЛТ кодів є:

1. Кодові символи генеруються незалежно один від одного; це так звана «фонтанна» властивість ЛТ кодів – для відновлення вихідного повідомлення приймачем можуть бути використані будь-які отримані кодові символи.

2. Вихідні символи мають рівний пріоритет.

3. Довжина вихідних символів може бути будь-яка, але довжини всіх вихідних символів рівні. Довжини кодових символів також рівні довжині вихідних символів.

4. З огляду на те, що в основі теорії кодів ЛТ лежить статистична задача про м'ячі і корзини, ефективність ЛТ кодів проявляється при достатньо великих значеннях параметра K (кількість вихідних символів). Винахідниками ЛТ кодів рекомендуються значення K близько 10000.

Перераховані властивості ЛТ кодів дуже цінні і дозволяють використовувати ЛТ коди на практиці для будь-яких типів переданих даних.

Важливим є властивість фонтанів кодів, особливо для завдання «багато – багатьом».

Однак, названих властивостей стираючих кодів недостатньо для успішного вирішення завдань передачі цифрових мультимедійних даних, і, в особливості, для систем online телемовлення. В першу чергу це пов'язано з неприйнятно довгою затримкою телевізійного сигналу між приймачем і передавачем, що викликана необхідністю буферизації великого числа вихідних пакетів, якщо мова йде про величини K порядку 10000. У разі завантаження медіафайлів у відкладеному режимі це не є проблемою, але в режимі реального часу це спричинить затримку в кілька десятків секунд.

Для вирішення проблем були запропоновані нові стираючі коди, названі «невипадкові стираючі коди» (НВСК) [2, с. 40]. Мотивацією до створення НВСК стало те, що при низьких значеннях K не працюють статистичні властивості, що становлять основу теорії ЛТ коду. Тому необхідно контролювати кількість входжень вихідних символів в кодові пакети, забезпечуючи більшу робастність і підвищуючи ефективність коду.

Код НВСК використовує Модифікований Робастний розподіл (Robust Soliton Distribution). Робастність модифікованого розподілу додатково підвищена шляхом збільшення числа пакетів зі ступенем 3 на 30% від числа пакетів зі ступенем 1 (виведено емпірично). У поточній реалізації НВСК кількість кодових символів обмежена конкретною величиною N, яка визначається виходячи з максимально дозволеного надлишку кодових пакетів щодо числа K вихідних символів як $N = K\beta$, де β – величина, трохи більше 1 (задається виходячи з особливостей каналу передачі).

До недоліків застосування НВСК в системах IPTV слід віднести неминучість буферизації щодо великого обсягу мультимедійних файлів як на передавачі, так і на приймачі, і, як наслідок, збільшену загальну затримку передачі даних в ланцюзі «передавач – приймач» в порівнянні з системою без НВСК [3, с. 45].

Тож застосування НВСК в системах IPTV можна вважати досить перспективним, з огляду на те, що в даних системах є можливість використання буферизації, так як затримка передачі тут не дуже суттєва, а якість сервісу може бути покращена. Проте для систем відеоконференцзв'язку фактор затримки дуже суттєвий, тому неможливість стираючих кодів і продовження застосування згорткових кодів тут досить обґрунтоване.

Список використаних джерел:

1. Помехоустойчивое кодирование для передачи цифрового телевидения по каналам связи [Електронний ресурс]: Режим доступу: http://broadcasting.ru/articles2/codobor/ pomehoystoichivoe-kodirovanie-dlya-peredachi/ – 2011.

2. Шинкаренко К. В., Кориков А. М. Помехоустойчивое кодирование мультимедиа данных в компьютерных сетях // Томськ: «Известия Томского политехнического университета», 2008. – № 5. – С. 37–41.

3. Шинкаренко К. В., Кориков А. М. Применение неслучайных стирающих кодов в IP телевещании // Томськ: «Известия Томского политехнического университета», 2008. – № 5. – С. 42–46.

Микосовський В.І.
студент,
Науковий керівник: **Полторак В.П.**
Кандидат технічних наук, доцент,
Національний технічний університет України
«Київський політехнічний інститут»

КРИПТОГРАФІЯ НА ЕЛІПТИЧНИХ КРИВИХ

Еліптична крива – набір точок, описаних рівнянням Вейерштрассе [1]:

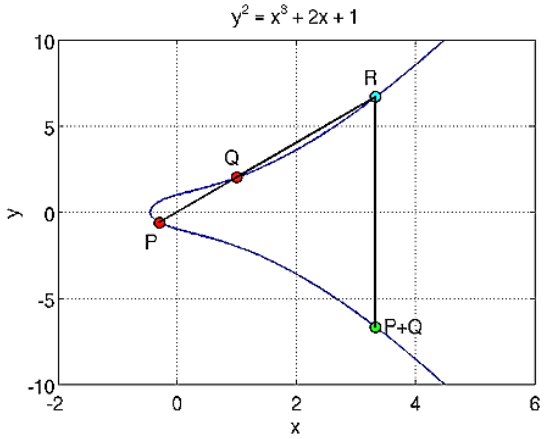
$$y^2 = x^3 + ax + b$$

Еліптичні криві поділяються на гладкі та сингулярні. Для гладких еліптичних кривих виконується наступна нерівність:

$$4a^3 + 27b^2 \neq 0$$

Тоді як для сингулярних кривих ця умова не виконується. В системах шифрування сингулярні криві зазвичай не використовуються, так як це значно знижує стійкість системи.

Арифметичні операції в еліптичній криптографії проводяться над точками кривої. Основною операцією являється «складання». Складання двох точок легко зобразити графічно:



Як видно з рисунка, для складання точок P і Q, необхідно провести між ними пряму лінію, котра обов'язково перетне криву в якій-небудь тертій точці R. Відобразимо точку R відносно горизонтальної осі координат і отримаємо шукану точку $P + Q$.

Алгебраїчне представлення «складання» запишемо складання двох точок в виді формули: $P + Q = -R$