Мрежова прозрачност и съвместно кодиране източник-канал в 4G мобилни мрежи

Григор Михайлов, Теодор Илиев, Георги Христов, Венцеслав Миланов

Network transparency and joint source-channel coding in 4G mobile networks: *Fourth generation of wireless mobile network (4G) is foreseen as a globally integrated communication network interconnecting, in a transparent way, a multitude of heterogeneous networks and systems. Optimal allocation of user and system resources may be effectively achieved with the joint source channel coding and decoding (JSCC/D), where the source coding, channel coding, modulation, and, possibly, network parameters are jointly determined to yield the best end-to-end system performance.*

Key words: *4G, Joint source-channel coding, network transparency.*

ВЪВЕДЕНИЕ

Следвайки посоката, поставена от GSM системите, внедрените в последствие UMTS системи доведоха до по-надеждни, интелигентни, сигурни, но също така и по-сложни безжични решения. С цел манипулиране на предаваната цифрова информация от различно естество (текст, глас, изображения, видео ...), която ще се използва в различни контексти и местоположения (дом, офис, в движение), тези системи разчитат на вътрешния софтуер, който да ги направи по-ефективни и по-лесни за употреба. Едно от ключовите предизвикателства за внедряване на 4G ще бъде определянето на гъвкаво реконфигуриране на мрежовата архитектура, която позволява едновременна оптимизация на честотната лента и управление на качеството на услугата (QoS). Предизвикателството на 21 век към проектантите на комуникационни системи е да се съсредоточат върху по-интегрирана стратегия [1].

МРЕЖОВА ПРОЗРАЧНОСТ

Мрежовата прозрачност е фундаментален аспект, който е и някак си абстрактна идея за превръщането на основната мрежова инфраструктура почти невидима за всички субекти и устройства, участващи в съвместното оптимизиране на (де)кодирането и (де)модулирането на информацията. Прозрачността е свързана с факта, че телекомуникационната мрежа, такава, каквато е в този вид, неминуемо оказва влияние върху цялата система, като например въвеждане на закъснение, загуба и различни видове грешки и то, без да общува с разположените в нея устройства, като по този начин няма гаранции за доставката на желаните от потребителя видео потоци, а също така не се постига необходимото качество на услугата (QoS) за крайните потребители.

Целта е да се постигне следното:

- Да се осъществи комуникационен обмен между различните устройства, които са разположени на различни места в мрежата (включително и крайните потребители).
- Да не се оказва негативно влияние на устройства, които не използват съвместното (де)кодиране източник-канал.

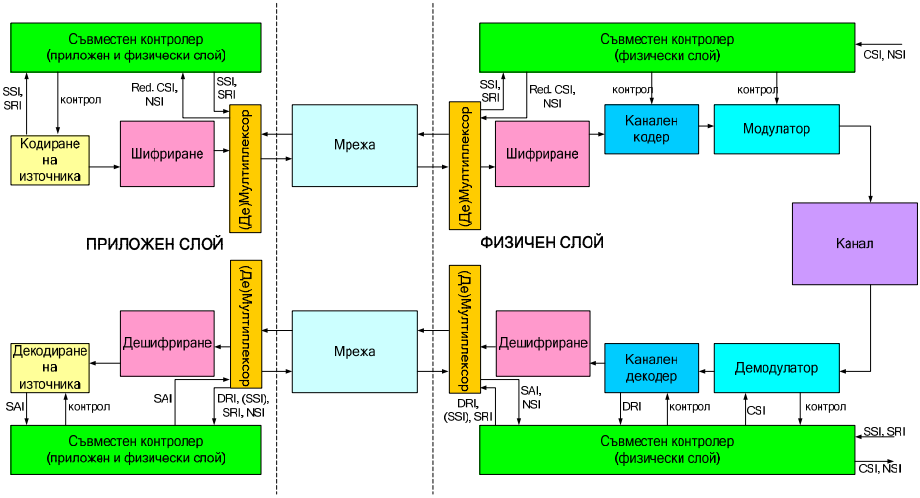
Първата цел се отнася за възможността за прехвърляне при нужда на сигнализация/контрол на информацията между различни възли и слоеве, по прозрачен начин, въпреки строгите правила на OSI модела, които налагат модулен и независим дизайн на всеки свързващ слой и съответно дефинираните интерфейси. Втората цел се стреми да гарантира възможно най-добра обратната съвместимост, не само със съществуващите стандарти, а и със съвременните системи, които тепърва навлизат масово и представляват мрежите от следващо поколение. Това дава възможност за плавна миграция към IPv6-съвместими устройства, използващи

функционалността на съвместното (де)кодиране източник-канал (СК/ДИ-К).

Решението за мрежова прозрачност трябва да заеме място при механизмите за сигурност, осигурявайки функции на криптиране и идентификация, дори при едновременна работа на различни слоеве, например при приложния и каналния слой.

МЕХАНИЗМИ ЗА ВНЕДРЯВАНЕ НА МРЕЖОВАТА ПРОЗРАЧНОСТ

- *IP пакети* – IPv6 пакетите могат да пренесат максималното количество от информацията, в зависимост от максималната преносна единица (MTU) на телекомуникационната инфраструктура. Това обикновено е транспортна единица за обслужващата информация (SDU), която съдържа информация за приложенията. Ако данните за приложението за по-големи от MTU, те се разделят на по-малки части в приемната страна, посредством процесите на мрежовия слой, и след това се предават в няколко независими един от друг IP пакета [6].
- *IPv6 разширителни заглавни части* – При IPv6 има задължителна заглавна част и няколко допълнителни разширителни заглавни части. Допълнителната заглавна част се използва за пренос на допълнителна информация, която се разглежда от всеки възел по продължение на пътя за предаване. Вместо това може да се използва допълнителната заглавна част за местоположението (Destination Options header), която се използва за пренос на допълнителна информация, която се разглежда само от възела, за който е предназначена пренасяната информация.
- *ICMPv6* – ICMPv6 е протокол, който разчита директно на IPv6. Използва се от IPv6 възлите за докладване на грешки, които са се появили при обработката на пакетите и за предприемане на други интернет функции. ICMPv6 е неразделна част от IPv6 и трябва непременно да се интегрира във всеки IPv6 възел. ICMPv6 съобщенията се разделят на две групи – съобщения за грешки и информационни съобщения. Съобщенията за грешки са еднопосочни, обикновено за информация на състоянието, докато информационните съобщения са двупосочни и се използват за запитвания и извличане на информация [6].
- *Ad-hoc протоколи за сигнализация* – Този подход е базиран на вече съществуващи протоколи за контрол и сигнализация, които са проектирани за оптималното и ефективно транспортиране на необходимата информация за съвместното (де)кодиране източник-канал [8]. При този подход стриктно се определят структурата и транспортните функции на протокола, докато съдържанието на данните за доставка на по-горен слой може да бъде определен както и да е (въпреки това може да е необходимо ниво на адаптация).
- *Директна комуникация сокет-към-сокет (socket-by-socket)* – Този вид комуникация се отнася за комуникации от край до край, при които сокетите на операционната система са отворени за специфични протоколи и употреба. Например, когато се използва TCP/IP протокола, сокетите на системно ниво могат да бъдат запазени за TCP и UDP и предаването на информацията се осъществява през въпросните запазени сокети. Като допълнително решение за предаване на сигналната информация при съвместното (де)кодиране източник-канал може да се разгледа и допълнителна комуникация сокет-към-сокет.



Фиг. 1. Комуникационна система от край-докрай, реализирана на IP базирана мрежа

СХЕМИ ЗА КОДИРАНЕ НА ИЗТОЧНИКА

Защитата от грешка (UEP) може да бъде разгледана като специфичен вид на комбинацията между кодирането на източника и каналното кодиране [2]. По-специално каналния кодер използва информацията за битови грешки, а също така и информацията за състоянието на канала (CSI). В същото време кодерът на източника освобождава малки части от глобалната вероятност за поява на грешки, в случай на адаптивно добавяне на съкращения. Следователно UEP е полезно да се използва всеки път, когато пренасяната информация има различен приоритет или различна устойчивост на шум.

Когато са известни различните устойчивости на грешки на всички битови позиции в генерирания информационен поток, какъвто е случая на по-голямата част от аудио-видео кодирането, на теория каналния кодер лесно може да бъде съпоставен с източника [4,5].

В резултат основните съвременни стандарти за видео кодиране (MPEG-2, MPEG-4, H.263 и H.26L) предлагат два инструмента, които позволяват йерархично представяне на информационния [7]:

- *Мащабиране*, то е част от кодирането на източника, позволяващо декодирането на подходящите подмножества, за да може да се генерират цялостни изображения (време/пространствени) на редуцираната резолюция и/или качество, което съответства на част от декодирания информационен поток.
- *Разделяне на информацията*, което е йерархично представяне, при което по-важните части от информационния поток (заглавните части, векторите за движение и др.) се разделят от по-маловажните части (коефициентите на директното косинусово преобразуване и др.).

СХЕМИ ЗА КАНАЛНО КОДИРАНЕ И МОДУЛАЦИЯ

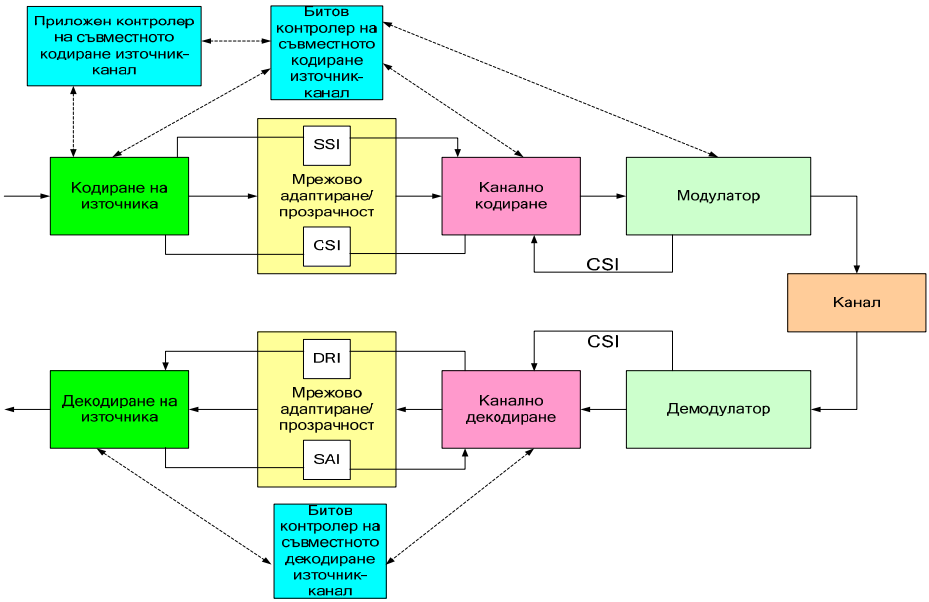
Широко използвано в света на безжичните комуникации, каналното кодиране осигурява задоволително минимално ниво на грешки, чрез добавяне на излишък към потока от информация, с цел предпазване от шума и затихващите ефекти. Дизайнът на кода за защита от грешки обикновено се състои от избирането на фиксиран код с възможности за защита, необходими според изискванията при пренасянето на

информацията и адаптирани към условията на канала [3]. Ако обаче информационния поток има различни изисквания за устойчивост на грешки и се предава през променлив във времето канал е необходима по-голяма гъвкавост на кодиращите схеми. Поради тази причина е необходимо степента на кода да може да се променя, така че коригиращата сила на кода да може да се адаптира към нуждите на източника и канала. RCPC кодовете отговарят на тези изисквания, тъй като те позволяват увеличение на излишъка в схемите за автоматично искане за повторение/прогресивна корекция на грешката (ARQ/FEC) и продължително изменение на степента на кода по цялото продължение на рамката от данни.

СХЕМИ НА СЪВМЕСТНО КОДИРАНЕ ИЗТОЧНИК-КАНАЛ

Теоремата на Шенон доказва, че при идеални условия, кодирането на източника и каналното кодиране могат, асимптотично с дължината на информацията от източника, да се разглеждат отделно, без никакви загуби на производителност за цялата система. Въпреки това, повечето широко използвани приложения (например аудио- видео потоците) не отговарят на тази идеална хипотеза. Поради тази причина те имат някои ограничения при предаването на информация в реално време, а също така устойчивостта им към грешки на кодираната от източника информация се променя значително.

Ето защо, за да се избегне намаляване на производителността, (де)кодирането на източника и канала трябва да се проектират да работят съвместно, което означава, че те трябва да могат да обменят и използват информация за взаимните настройки на техните параметри.



Фиг. 2. Обмяна на информация между (де)кодирането на източника и каналното (де)кодиране/(де)модулация

Схемите за кодиране на източника трябва да се преразгледат, за да се определи тяхната надеждност при внедряването им в съвместното (де)кодиране на източник-канал. Наистина не е ясно, дали широко използваните в последно време схеми за кодиране (MPEG-2, MPEG-4, H.26L) са подходящи за употребата им при

СК/ДИ-К. Схемите за канално кодиране трябва бързо да се приспособяват към условията на канала, от гледна точка на честотната лента. Това ще гарантира, че няколко дефектни бита няма да доведат до загуба на информация или нейното качество. За да може каналния кодер да се приспособи постепенно към устойчивостта на битови грешки, трябва да се разработи йерархично представяне на информацията (мащабируемо видео кодиране и техники за разделяне на данните) без да се жертва в голяма степен производителността. Това включва ефективни описания на информацията от съответната страна. Трябва да бъдат разработени и внедрени UEP схеми, които постепенно да адаптират мощните канални кодери към променливата устойчивост на битова грешка.

ЗАКЛЮЧЕНИЕ

Подхода при съвместното (де)кодиране на източник-канал е мощно решение за всички видове мрежи, при които е необходимо подобрение на честотната лента и качеството на услугата. От голяма полза ще е по-нататъшното развитие на мрежовата архитектура при СК/ДИ-К технологията и симулирането на по-сложни схеми и сценарии, с цел оптимизиране на мултимедийното предаване и мрежовата прозрачност в 4G безжичните мобилни мрежи.

БЛАГОДАРНОСТИ

Публикуваните резултати са получени при работата по договор № ДМУ-02/13-2009 на Фонд „Научни изследвания” към Министерството на образованието, младежта и науката.

ЛИТЕРАТУРА

[1] М. Илиев, Илиев Т., Христов Г., Захариев П.. Безжични мрежи за предаване на данни, Русе, ИК „Парнас”, 2010

[2] C. E. Shannon, "A Mathematical Theory of Communication", Bell System Technical Journal, vol. 27, 1948

[3] J. Hagenauer, T. Stockhammer, "Channel Coding and Transmission Aspects for Wireless Multimedia", Proceedings of the IEEE, vol. 87, no. 10, October 1999

[4] J.L. Massey, "Joint source and channel coding," Commun. Systems and Random Process Theory, NATO Adv. Studies, 1978

[5] M.G. Martini and M. Chiani, "Joint source-channel error detection with standard compatibility for wireless video transmission," Proc. IEEE IVCN'02, Orlando, USA, 2002

[6] S. Deering et al., “Internet Protocol, Version 6 (IPv6) Specification,” RFC 2460, December 1998

[7] S. M´erigeault and C.Lamy, “Concepts for exchanging extra information between protocol layers transparently for the standard protocol stack,” in Proceedings of IEEE ICT’03, Tahiti, French Polynesia, Feb – Mar, 2003

[8] PHOENIX: FP6 IST European project http://www.ist-phoenix.org/

За контакти:

маг. инж. Григор Михайлов, Катедра “Комуникационна техника и технологии”, Русенски университет “Ангел Кънчев”, тел.: 082/888 836, e-mail: gmihaylov@uni-ruse.bg

доц. д-р Теодор Илиев, Катедра “Комуникационна техника и технологии”, Русенски университет “Ангел Кънчев”, тел.: 082/888 663, e-mail: tiliev@ecs.uni-ruse.bg

гл. ас. д-р Георги Христов, Катедра “Комуникационна техника и технологии”, Русенски университет “Ангел Кънчев”, тел.: 082/888 663, e-mail: ghristov@uni-ruse.bg

Докладът е рецензиран.