1. Key Challenges in Video Transmission
The behavior of video consumers has evolved tremendously in the past five years. Traditional television delivery mechanisms, based on content that is acquired and distributed to a single end device under the control of a single operator, is in upheaval and moving from classical broadcast to web based platforms. DVDs are already in the process of being replaced by streaming services. The ubiquitous TV set is becoming a much more personal multi-device ecosystem. Video consumption is now geo-localized and shifted in time and place. Furthermore, video streaming is now used in combination with Web 2.0 messaging and widgets. Television content is consumed more and more in a social way over multi-screens and heterogeneous environments.

Clearly, novel networking approaches are needed to provide the quality video experience demanded by today’s users over any network in and out of the home. At the same time, the demands of content providers and consumers for secure and private mechanisms to procure and protect video content must be met in a convincing manner. Since the main content is often combined with ancillary features inserted anywhere in the network, traditional end-to-end architectures result in inefficient implementations.

On the other hand, the challenges of video-rich data distribution over wireless are growing with the uncompromising demand for mobile content. Missed opportunities for video transmission over wireless are mainly due to the multitude and limitations of devices and networks.

It is our contention that the solution to surviving this video glut is not to add more resources to the silos. The key is to use the available networks and rendering devices opportunistically and cooperatively. This includes (a) improving the reliability of the connected information nodes, (b) adding content protection where needed, and (c) minimizing access to core elements over expensive wireless access networks. In essence, the goal is to create a truly “video centric wireless network” with “streamware” that can be adapted to local transmission and existing requirements in terms of privacy and content protection.

The purpose of this overview paper is thus to summarize recent research in network coding (NC) for multi-network collaborative communication systems and multiscreen content. NC is paving new ground for novel services in particular as it applies to video streaming with high quality of experience and security guarantees in a social viewing environment.

2. Network Coding in a Nutshell
NC views digital traffic not merely as groups of bits but rather as algebraic entities. NC adds functionality to networking elements beyond the usual forwarding of data units from one interface to another. It assumes that added functionality inside the network can be provided with simple finite field arithmetic: packets can be multiplied by coefficients and combined additively. NC transforms the usual data stream into a set of linearly combined entities that can be recovered with simple equation solving algorithms.

Having been a very active topic of research in the last 10 years, NC is now moving into the real world, particularly in streaming and storage applications. This aligns it to emerging content-centric architectures for future Internet.

Since network codes do not need to be end to end, NC allows for the tailoring of coding strategies to the dynamics and topology of the network, as well as to the features of the receiver ecosystem. This is very beneficial when streaming video traffic over heterogeneous networks to a variety of end devices. NC allows content to be modified and/or stored in the network nodes without tight controls. Protection can be added only where needed, thus freeing vital resources and enabling peer-to-peer distribution with local features. This is particularly of interest for “social distribution” over small community networks. With network coded video there is no need to know
IEEE COMSOC MMTC E-Letter

exactly where a piece of video is located: to regenerate a file there is only a need to gather “useful” combinations of content until enough degrees of freedom have been accumulated to allow for perfect decoding. There is a small trade-off between using a complex implementation, which requires state information to be kept in network nodes, and the added acquisition and decoding delay of NC. Our research has shown that there exist coded approaches, particularly quasi-systematic coding, that can provide the required streams within the acceptable completion requirement of video delivery networks and indeed improve over approaches requiring state information.

3. New Strategies for Secure Dissemination of Video Streams

There are now major incentives to address delivery mechanisms beyond traditional client-server architectures. Because of the scarcity of wireless resources, we observe a growing requirement for content to be shared locally without wasting bottleneck resources for digital rights management (DRM), retransmission of lost segments and other non-revenue generating traffic. Peer to peer and distributed storage as well as quality of experience (QoE) with device augmentation have emerged as key enablers for layered content protection, which socializes viewing over the device ecosystem. However, without network coding the complexity of distributed approaches increase rapidly and lead to inefficient implementations and reduced scalability. NC creates the underlying network infrastructure that will deliver the next generation of streaming protocols.

It is important to stress that getting the information to its destination is not sufficient for the business success of any strategy: the intellectual property rights of content generated commercially or by private users must be protected, whereas user privacy cannot be compromised. Traditional encryption and DRM approaches need to be updated to meet the bandwidth constraints of wireless networks, the delay requirements of user applications and the need to separate business models from content protection. Commercially produced content shared among devices and “friends” that gets annotated and enhanced in this exchange is not suitable for traditional DRM. Key exchanges necessitating numerous cross-network round trips are inappropriately using precious wireless bandwidth and affecting QoE through excessive delay. Encryption and decryption of large packets stress the capabilities of end-devices by generating added delays, wasting bottleneck resources and compromising end-to-end delay budgets.

We propose an approach for distributed content verification without the need to contact a centralized trusted authority. This relies on constructing homomorphic encryption. The encryption remains decryptable under coding, without the need to perform decoding, even at a single packet level for peer-to-peer system with untrusted nodes. Our system uses standard schemes based on verifying if the received instance belongs to a subspace generated by the data itself. The power of this approach is that it allows us to consider distributed verification of data, whether it originates from a single source or is provided in a distributed fashion. The original content will be a subspace of the content with additional user-generated content. The original content can be seen as consisting of the total possible space with the portions allotted to users’ content as having been set to having zero coefficients. Thus, even in the presence of user content, the original content may be verified. Note that original content may be reduced (in effect setting some portions of the contributions to be nil) but not modified. A modification of the original content will lead to rejection of the homomorphic signature for any packet. We may also deal with modifications through corrections. The goal is to take content that was modified and either restore it to its original state or discard it without the need to resort to techniques such as hash value computation and exchanges with trusted authorities.

4. Implementation

Our approach to content protection is currently being implemented on Android, iOS and Symbian based smart phones using a peer-to-peer NC dissemination system developed at the University of Aalborg. The use case is simple. Registered users have ready access to content that is self-verifying and distributed locally. For unregistered users the current implementation uses advertisements to carry the required keys and signature but other mechanisms could also be implemented. Additionally there can be a mode where some of the received packets at any node would need to be verified against the source (or its proxy) to add more protection. While this needs to go back to a centralized server the amount of exchanged information remains very small when compared to traditional approaches. Moreover, we have flexibility in which data is sent, and when it is sent, since any coded packet will adequately
represent the whole space from which it was generated.

Figure 1 - NC video stream rendered on the iPod Touch.

5. Conclusions
We have proposed to use network coding and the inherent peering of wireless nodes to provide a distributed video dissemination network with better use of scarce resources. This results in distributed content verification without the need for a trusted authority. Our techniques build upon our earlier work on constructing secure storage over unsecured networks. The encryption of the NC coefficients is very lightweight hence the decryption is significantly faster than traditional methods and allows us to add further functionality. Thus, we can define an approach where commercial content is signed in a centralized way and the ancillary content is signed within the viewer group. Although outside peers can help to disseminate the video content, they will not be able to decode it without the right signature or see the viewer comments without the author’s authorized signature.

This approach combines a number of elements: (a) proximity networking to take advantage of the availability of edge resources, (b) network coding to protect and secure the video content and (c) homomorphic signatures to allow the identification of multiple content sources in converged streaming applications.

Acknowledgements
The authors would like to thank Raluca Ada Popa of the MIT Computer Science and Artificial Intelligence Laboratory for her advice on the use of homomorphic signatures. NBC Universal, the Fundação para a Ciência e Tecnologia (MIT Portugal) and the European Commission are also acknowledged for their support to the research.

References
Dr. Montpetit received a Ph.D. in EECS from the Ecole Polytechnique in Montreal, Canada. She is a member of the IEEE Standing Committee on DSP. She was the recipient of the Motorola Innovation Prize in 2007 for the development of a multi-screen and multi-network video mobility system. Her work on converged video applications, social and multi-screen IPTV has gotten her many invited papers and keynote presentations as well as a MIT Technology Review TR10 in 2010. Dr. Montpetit is a Senior Member of the IEEE.

Muriel Médard is a Professor in the Electrical Engineering and Computer Science at MIT. Professor Médard received B.S. degrees in EECS and in Mathematics in 1989, a B.S. degree in Humanities in 1990, a M.S. degree in EE 1991, and a Sc D. degree in EE in 1995, all from the Massachusetts Institute of Technology (MIT), Cambridge. Professor Médard's research interests are in the areas of network coding and reliable communications, particularly for optical and wireless networks. She was awarded numerous prizes for her publications and was named a 2007 Gilbreth Lecturer by the National Academy of Engineering. Professor Médard is a Fellow of IEEE and member of the Board of Governors of the IEEE Information Theory Society.

João Barros is an Associate Professor of Electrical and Computer Engineering at the University of Porto and the Director of the Instituto de Telecomunicações in Porto, Portugal. Since 2008 he has had a visiting appointment with the Massachusetts Institute of Technology (MIT). In February 2009, Dr. Barros was appointed National Director of the Carnegie-Mellon University CMU-Portugal Program. In recent years, João Barros has been PI and Co-PI of numerous national, European and industry funded projects, publishing extensively in the fields of information theory, networking and security, with a special focus on network coding, physical-layer security, sensor networks, and intelligent transportation systems. Dr. Barros has received several awards, including the 2010 IEEE Communications Society Young Researcher Award for the Europe, Middle East and Africa region, the 2011 IEEE ComSoC and Information Theory Society Joint Paper Award, and a state-wide best teaching award by the Bavarian State Ministry of Sciences, Research and the Arts. He received his undergraduate education in Electrical and Computer Engineering from the Universidade do Porto (UP), Portugal and Universitaet Karlsruhe, Germany, and the Ph.D. degree in Electrical Engineering and Information Technology from the Technische Universitaet Muenchen (TUM), Germany.

Frank H. P. Fitzek is a Professor in the department of Electronic Systems, University of Aalborg, Denmark heading the Mobile Device group. He received his diploma (Dipl.-Ing.) degree in electrical engineering from the University of Technology - Rheinisch-Westfälische Technische Hochschule (RWTH) - Aachen, Germany, in 1997 and his Ph.D. (Dr.-Ing.) in Electrical Engineering from the Technical University Berlin, Germany in 2002 and became Adjunct Professor at the University of Ferrara, Italy in the same year. He co-founded the start-up company acticom GmbH in Berlin in 1999. He has visited various research institutes including Massachusetts Institute of Technology (MIT), VTT, and Arizona State University. In 2005 he won the YRP award for the work on MIMO MDC and received the Young Elite Researcher Award of Denmark. He was selected to receive the NOKIA Champion Award several times in a row from 2007 to 2011. In 2008 he was awarded the Nokia Achievement Award for his work on cooperative
networks. In 2011 he received the SAPERE AUDE research grant from the Danish government. His current research interests are in the areas of wireless and mobile communication networks, mobile phone programming, network coding, cross layer as well as energy efficient protocol design and cooperative networking.