RECENT RESULTS ON BROADCAST NETWORKS WITH LAYERED DECODING AND SECRECY: AN OVERVIEW

Shaofeng Zou[⋆] *Yingbin Liang* [⋆] *Lifeng Lai*[‡] *H. Vincent Poor* [†] *Shlomo Shamai (Shitz)* [♯]

[⋆] Syracuse University [‡] Worcester Poly Insistitute [†] Princeton University [♯] Technion
Email: szou02@syr.edu, yliang06@syr.edu, llai@wpi.edu, poor@princeton.edu, sshlomo@ee.technion.ac.il

ABSTRACT

Recent information theoretic results on a class of broadcast channels with layered decoding and/or layered secrecy are overviewed. Designs for different models are compared and applications of these results to fading wiretap channels and secret sharing are briefly discussed. An outlook, focusing on theoretical challenges concludes the overview.

1. INFORMATION THEORETIC MODELS

We briefly introduce four models all belonging to the class of degraded broadcast channels with layered decoding and/or layered secrecy. More details can be found in [1].

The first model is the degraded broadcast channel with layered decoding and non-layered secrecy, in which a transmitter sends K messages $W_1, \ldots, W_K$ to K receivers with each receiver k, decoding the first k messages, and the eavesdropper ignorant of all messages. The capacity achieving scheme superposes multiple layers together with each layer carrying one more message than its previous layer. Furthermore, each layer applies random binning to secure not only the message in this layer but also all higher-layer messages.

The second model is the degraded broadcast channel with non-layered decoding and layered secrecy, in which a transmitter sends K messages $W_1, \ldots, W_K$ to one legitimate receiver, and each eavesdropper k, needs to be kept ignorant of the messages $W_k, \ldots, W_K$, for $k = 1, \ldots, K$. The capacity achieving scheme encodes each codeword with multiple messages so that lower-layer messages can serve as a random source to protect higher-layer messages.

The third model is the degraded broadcast channel with layered decoding and layered secrecy, in which a transmitter sends K messages $W_1, \ldots, W_K$ to K receivers. Receiver k is required to decode the first k messages $W_1, \ldots, W_k$, and is kept ignorant of messages $W_{k+1}, \ldots, W_K$. The capacity achieving scheme is similar to that for the first model except that random binning within one layer only protects the message corresponding to the same layer.

The fourth model is the degraded broadcast channel with layered decoding and layered secrecy and with secrecy outside a bounded range. We focus on the case in which the transmitter has four messages $W_1, \ldots, W_4$ intended for the four receivers. Receiver k is required to decode the messages $W_1, \ldots, W_k$. Furthermore, W_3 needs to be kept secure from receiver 1, and W_4 needs to be kept secure from receivers 1 and 2. Hence, each message is secured from a receiver with two-level worse channel quality. The capacity achieving scheme applies the joint design of superposition, embedded coding, random binning, and rate splitting and sharing.

2. APPLICATIONS

We discuss two applications of the broadcast models described in Section 1. The first application is to the fading wiretap channel, in which the legitimate and eavesdropping channels are corrupted by multiplicative random fading gains. In the case that the transmitter does not know the fading gains, the legitimate and eavesdropping channels can be viewed as having multiple states. A layered transmission scheme can be designed so that more layers can be decoded if the legitimate channel has better quality, and more layers can be made secure if the eavesdropper channel has lower quality. Thus, such an approach naturally yields a degraded broadcast channel with layered decoding and secrecy requirements as discussed in Section 1, and the secrecy capacity results for such models can be applied.

The second application is to the secret sharing problem with multiple secrets, which can be shown to be equivalent to the broadcast channel with secrecy requirements. Namely, the groups of participants that are required to determine secrets should be viewed as legitimate receivers and the groups of participants that are required to be ignorant of secrets should be viewed as eavesdroppers.

3. REFERENCES

[1] S. Zou, Y. Liang, L. Lai, H. V. Poor, and S. Shamai, "Broadcast networks with layered decoding and layered secrecy: Theory and applications," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1841–1856, Oct 2015.

The work of S. Zou and Y. Liang was supported by a National Science Foundation CAREER Award under Grant CCF-10-26565 and by the National Science Foundation under Grant CNS-11-16932. The work of L. Lai was supported by the National Science Foundation under Grant CCF-1318980 and Grant CNS-1457076. The work of H. V. Poor was supported in part by the National Science Foundation under Grant CMMI-1435778 and Grant CNS-1456793. The work of S. Shamai (Shitz) was supported in part by the Israel Science Foundation (ISF).