Security Aspects of Viterbi Decoding

Aman Chawla

June 9, 2024

Abstract

In this note, the authors propose to consider Viterbi trellises whose "nodes" are compromised and have turned rogue. A "network random refresh" style approach might assist in mitigating the deleterious effects of such rogues.

This work builds on the Network Random Refresh approach to security proposed in [1]. Codes on Tanner graphs [2] are a generalization of Viterbi-style convolutional codes and can be decoded using sum-product decoding. Suppose a rogue alters a specific a-posteriori probability (APP) of the decoding process, hoping that it results in maximum damage to the sum-product decoding process. We then do sum-product decoding for a slightly altered Tanner graph. We do this periodically, based on random coin tosses. If we make only slight alterations to the original graph while modifying it, we may still be able to decode approximately correctly on average. Importantly, however, the rogue is thwarted as it doesn't know which APP to really alter for inflicting maximum damage since the underlying Tanner graph has changed and keeps changing randomly. The caveat is that the rogue could also follow a randomized strategy. This should be analyzed in future work.

References

[1] Aman Chawla. Network random refresh.

[2] Tuvi Etzion, Ari Trachtenberg, and Alexander Vardy. Which codes have cycle-free tanner graphs? *IEEE Transactions on Information Theory*, 45(6):2173–2181, 1999.