Multi-party secret key agreement over state-dependent wireless broadcast channels

ABSTRACT:

We consider a group of m trusted and authenticated nodes that aim to create a shared secret key K over a wireless channel in the presence of an eavesdropper Eve. We assume that there exists a state dependent wireless broadcast channel from one of the honest nodes to the rest of them including Eve. All of the trusted nodes can also discuss over a cost-free, noiseless and unlimited rate public channel which is also overheard by Eve. For this setup, we develop an information-theoretically secure secret key agreement protocol. We show the optimality of this protocol for "linear deterministic" wireless broadcast channels. This model generalizes the packet erasure model studied in literature for wireless broadcast channels. Here, the main idea is to convert a deterministic channel to multiple independent erasure channels by using superposition coding.

INTRODUCTION:

We consider the problem of generating a secret key K among m _ 2 honest (trusted and authenticated) nodes that communicate over a wireless channel in the presence of a passive eavesdropper Eve (for example consider a scenario where all people in a conference room aim to generate a common secret key in the presence of one or multiple adversaries behind the doors). We restrict our attention to the case where communication occurs either through a broadcast channel, where the received symbols are independent among all receivers of the broadcast transmissions including Eve (given that the transmitted symbols is known), or, through a no-cost noiseless public channel.