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. For "state-dependent Gaussian" wireless broadcast channels, by using insights from the deterministic problem, we propose an achievability scheme based on a multi-layer wiretap code. By using the wiretap code, we can mimic the phenomenon of converting the wireless channel to multiple independent erasure channels. Then, finding the best achievable secret key generation rate leads to solving a non-convex power allocation problem over these channels (layers). We show that using a dynamic programming algorithm, one can obtain the best power allocation for this problem. Moreover, we prove the optimality of the proposed achievability scheme for the regime of high-SNR and large-dynamic range over the channel states in the (generalized) degrees of freedom sense.

SHIELD TECHNOLOGIES,
2232, 3RD FLOOR, 16TH B CROSS, YELAHANKA NEW TOWN, BANGALORE-64
Mail us: shieldtechnoblr@gmail.com / manager@shieldtechno.com
Contact: 9972364704 / 8073744810

SHIELD TECHNOLOGIES,
2232, 3RD FLOOR, 16TH B CROSS, YELAHANKA NEW TOWN, BANGALORE-64
Mail us: shieldtechnoblr@gmail.com / manager@shieldtechno.com
Contact: 9972364704 / 8073744810