Ph: 9585554590, 9585554599
Email: support@salemsmartreach.com
URL: www.salemsmartreach.com

Asymptotic Analysis on Secrecy Capacity in Large-Scale Wireless Networks

Abstract:

Since wireless channel is vulnerable to eavesdroppers, the secrecy during message delivery is a major concern in many applications such as commercial, governmental, and military networks. This paper investigates information-theoretic secrecy in large-scale networks and studies how capacity is affected by the secrecy constraint where the locations and channel state information (CSI) of eavesdroppers are both unknown. We consider two scenarios: 1) noncolluding case where eavesdroppers can only decode messages individually; and 2) colluding case where eavesdroppers can collude to decode a message. For the noncolluding case, we show that the network secrecy capacity is not affected in order-sense by the presence of eavesdroppers. For the colluding case, the per-node secrecy capacity of $\Theta([1/(\sqrt{n})])$ can be achieved when the eavesdropper density $\psi e(n)$ is $O(n^{-\beta})$, for any constant $\beta > 0$ and decreases monotonously as the density of eavesdroppers increases. The upper bounds onnetwork secrecy capacity are derived for both cases and shown to be achievable by our scheme when $\psi e(n)=O(n^{-\beta})$ or $\psi e(n)=\Omega(\log^{[(\alpha-2)/(\alpha)]}n)$, where α is the path-loss gain. We show that there is a clear tradeoff between the security constraints and the achievable capacity. Furthermore, we also investigate the impact of secrecy constraint on the capacity of dense network, the impact of active attacks and other traffic patterns, as well as mobility models in the context.