Summary: Consider a stochastic process being controlled across a communication channel. The control signal that is transmitted across the control channel can be replaced by a malicious attacker. The controller is allowed to implement any arbitrary detection algorithm to detect if an attacker is present. This work characterizes some fundamental limitations of when such an attack can be detected, and quantifies the performance degradation that an attacker that seeks to be undetected or stealthy can introduce.

MSC:

- 93E03  Stochastic systems in control theory (general)
- 90B18  Communication networks in operations research
- 68M99  Computer system organization

Keywords:

cyber-physical system security; networked control systems; stochastic systems

Full Text: DOI arXiv

References:


[22] Liu, Y.; Ning, P.; Reiter, M. K., False data injection attacks against state estimation in electric power grids, ACM Transactions on Information and System Security, 14, 1, 13, (2011)


[34] Richards, G., Hackers vs slackers, Engineering & Technology, 3, 19, 40-43, (2008)


This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.