Camouflage Traffic: Minimizing Message Delay for Smart Grid Applications under Jamming

Title	Camouflage Traffic: Minimizing Message Delay for Smart Grid Applications under Jamming
Publication Type	Journal Article
Year of Publication	2015
Authors	Zhuo Lu, Wenye Wang, Wang, C.
Journal	Dependable and Secure Computing, IEEE Transactions on
Volume	12
Pagination	31-44
Date Published	Jan
ISSN	1545-5971
Keywords	camouflage traffic, code channel, Communication system security, control messages, cyber-physical system, delay performance guarantee, delays, existing attack model, generic jamming process, information exchange, information technologies, jamming, jamming attack, jamming attacks, jamming resilience, latency guarantee, message delay minimization, multiple-frequency channel, network load balance, network traffic load, Power distibution, power infrastructures, power system security, primary security threat, probability , radio interference broadcast, radio networks, radiofrequency interference, Receivers, Smart grid, smart grid application, smart grid communication, Smart grids, smart power grids, spread spectrum systems, TACT, telecommunication security, telecommunication traffic, transmitting adaptive camouflage traffic, U-shaped function, well-adopted attack model, wireless communication security , wireless network deployment, wireless networks, worst-case message delay

Abstract

Smart grid is a cyber-physical system that integrates power infrastructures with information technologies. To facilitate efficient information exchange, wireless networks have been proposed to be widely used in the smart grid. However, the jamming attack that constantly broadcasts radio interference is a primary security threat to prevent the deployment of wireless networks in the smart grid. Hence, spread spectrum systems, which provide jamming resilience via multiple frequency and code channels, must be adapted to the smart grid for secure wireless communications, while at the same time providing latency guarantee for control messages. An open question is how to minimize message delay for timely smart grid communication under any potential jamming attack. To address this issue, we provide a paradigm shift from the case-by-case methodology, which is widely used in existing works to investigate well-adopted attack models, to the worst-case methodology, which offers delay performance guarantee for smart grid applications under any attack. We first define a generic jamming process that characterizes a wide range of existing attack models. Then, we show that in all strategies under the generic process, the worst-case message delay is a U-shaped function of network traffic load. This indicates that, interestingly, increasing a fair amount of traffic can in fact improve the worst-case delay performance. As a result, we demonstrate a lightweight yet promising system, transmitting adaptive camouflage traffic (TACT), to combat jamming attacks. TACT minimizes the message delay by generating extra traffic called camouflage to balance the network load at the optimum. Experiments show that TACT can decrease the probability that a message is not delivered on time in order of magnitude.

DOI 10.1109/TDSC.2014.2316795

Citation Key 6786992

camouflage traffic, code channel, Communication system security, control messages, cyber-physical system, delay performance guarantee, delays, existing attack model, generic jamming process, information exchange, information technologies, Jamming, jamming attack, jamming attacks, jamming resilience, latency guarantee, message delay minimization, multiple-frequency channel, network load balance, network traffic load, Power distibution, power infrastructures, power system security, primary security threat, probability, radio interference broadcast, radio networks, radiofrequency interference, Receivers, Smart Grid, smart grid application, smart grid communication, Smart Grids, smart power grids, spread spectrum systems, TACT, telecommunication security, telecommunication traffic, transmitting adaptive camouflage traffic, U-shaped function, well-adopted attack model, wireless communication security, wireless network deployment, wireless networks, worst-case message delay