Tradeoff Between Reliability and Security in Multiple Access Relay Networks Under Falsified Data Injection Attack

Taha A. Khalaf, Member, Sang Wu Kim, Senior Member, and Alaa E. Abdel-Hakim, Member,

Abstract:

We consider a multiple access relay network where multiple sources send independent data to a single destination through multiple relays, which may inject falsified data into the network. To detect the malicious relays and discard (erase) data from them, tracing bits are embedded in the information data at each source node. In addition, parity bits are added to correct the errors caused by fading and noise. When the total amount of redundancy, tracing bits plus parity bits, is fixed, an increase in parity bits to increase the reliability requires a decrease in tracing bits, which leads to a less accurate detection of malicious behavior of relays, and vice versa. We investigate the tradeoff between the tracing bits and the parity bits in minimizing the probability of decoding error and maximizing the throughput in multisource, multirelay networks under falsified data injection attacks. The energy and throughput gains provided by the optimal allocation of redundancy and the tradeoff between reliability and security are analyzed.

Keywords:

Multiple access relay network, tradeoff between reliability and security, falsified data injection, forward error correction.

Published In:

IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 3,