

Joseph, John Felix Charles; Das, Amitabha; Lee, Bu-Sung; Seet, Boon-Chong

CARRADS: cross layer based adaptive real-time routing attack detection system for MANETS. (English) [Zbl 1202.68031](#)

[Comput. Netw.](#) 54, No. 7, 1126-1141 (2010).

Summary: Routing behavior in ad hoc networks is highly transient. Thus, dynamically adapting the routing attack detection system at real-time to new attacks and changing network conditions is critical in ad hoc networks. Conventional incremental learning methods are computationally expensive for resource-constrained nodes in ad hoc networks. In this paper, we propose CARRADS, a computationally efficient methodology for adapting the intrusion detection model at real-time. The adaptation process consists of two major stages. In the first stage, the main task is to identify occurrence of new patterns in the routing control traffic and prioritize them based on their information content. The second stage of adaptation is to incrementally update the detection model using the new patterns with minimum computational overhead. CARRADS uses SVM algorithm for its superior detection abilities. However, using some innovative techniques the computational overhead of incremental update is reduced by a factor of 20 to 30 times at the cost of a negligible decrease in detection accuracy. This makes CARRADS a viable approach for real-time IDS in ad hoc networks.

MSC:

[68M10](#) Network design and communication in computer systems

Keywords:

[intrusion detection](#); [routing security](#); [ad hoc networks](#); [cross layer system](#); [adaptive intrusion detection](#); [statistical classification](#)

Software:

[CARRADS](#)

Full Text: [DOI](#)