Cryptology ePrint Archive: Report 2011/103

Cryptographically Sound Security Proof for On-Demand Source Routing Protocol EndairA

István Vajda

Abstract: We present the first cryptographically sound security proof of a routing protocol for mobile ad-hoc networks. More precisely, we show that the route discovery protocol does not output a non-existing path under arbitrary active attacks, where on a non-existing path there exists at least one pair of neighboring nodes without communication connection during the run of the route discovery protocol. The proof relies on the Dolev-Yao-style model of Backes, Pfitzmann and Waidner, which allows for mapping results obtained symbolically within this model to cryptographically sound proofs if certain assumptions are met.

Category / Keywords: cryptographic protocols /

Publication Info: cryptanalysis

Date: received 2 Mar 2011

Contact author: vajda at hit bme hu