Cryptology ePrint Archive: Report 2011/229

Routing Protocol Based Shared and Session Key Exchange Protocol for Wireless Mobile Ad-hoc Network

Md. Golam Kaosar

Abstract: Mobile Ad-hoc Network (MANET) is a transitory and infrastructureless network supported by no fixed trusted infrastructure. To achieve security goals like: authentication, integrity, non-repudiation, privacy, a secret key (or session key) is necessary to be shared between the sender and receiver. Because of the nature of MANET, it is unrealistic in many circumstances to implement Certification Authority (CA) concept. Some popular key exchange protocols also have some demerits in case of MANET which are due to mainly the requirement of high computational capability. In this key exchange protocol we propose an algorithm to exchange shared and session key between the sender and destination even during the route creation in various routing protocols.

Category / Keywords: secret-key cryptography / Key Exchange, MANET routing.

Publication Info: Not published

Date: received 9 May 2011

Contact author: golam kaosar at vu edu au