Cryptology ePrint Archive: Report 2011/259

Comments on a sensor network key redistribution technique of Cichon, Golebiewski and Kutylowski

Douglas R.~Stinson

Abstract: Cichon, Golebiewski and Kutylowski (\cite{CGK}) proposed a technique for ``key redistribution" in sensor networks. The idea is that long-term keys held by the sensor nodes are used to encrypt temporal keys that a base station then broadcasts to the network. The temporal keys are used as session keys by the nodes in the sensor network. It is argued that this provides increased connectivity and resilience as compared to a standard Eschenauer-Gligor key predistribution scheme, as well as providing some additional advantages.

In this paper, we provide some simpler proofs of some results from \cite{CGK}. As well, we give a precise analysis of the resilience of Cichon, Golebiewski and Kutylowski's scheme, and we discuss modifications of the scheme based on defining a suitable intersection threshold.

Category / Keywords: applications / key predistribution,sensor network

Publication Info: not yet submitted for publication

Date: received 25 May 2011

Contact author: douglas stinson at yahoo ca