Cryptology ePrint Archive: Report 2011/555

On the Role of Expander Graphs in Key Predistribution Schemes for Wireless Sensor Networks

Michelle Kendall and Keith Martin

Abstract: Providing security for a wireless sensor network composed of small sensor nodes with limited battery power and memory can be a non-trivial task. A variety of key predistribution schemes have been proposed which allocate symmetric keys to the sensor nodes before deployment. In this paper we examine the role of expander graphs in key predistribution schemes for wireless sensor networks. Roughly speaking, a graph has good expansion if every `small' subset of vertices has a `large' neighbourhood, and intuitively, expansion is a desirable property for graphs of networks. It has been claimed that good expansion in the product graph is necessary for `optimal' networks. We demonstrate flaws in this claim, argue instead that good expansion is desirable in the intersection graph, and discuss how this can be achieved. We then consider key predistribution schemes based on expander graph constructions and compare them to other schemes in the literature. Finally, we propose the use of expansion and other graph-theoretical techniques as metrics for assessing key predistribution schemes and their resulting wireless sensor networks.

Category / Keywords: cryptographic protocols / Wireless sensor networks, key management, key predistribution, expander graphs

Publication Info: Submitted to WEWoRC 2011 post-proceedings

Date: received 7 Oct 2011

Contact author: michelle kendall 2009 at rhul ac uk