Enhanced Security of Wireless Sensor Networks using Hybrid Secure Random Key Pre-distribution Scheme and A Modified NK Cryptosystem

Tamer Mohamed Abd El-Rahman, Dr. Nassar A M , Dr. Gody A M *

Cairo University
Giza, Egypt

Doctoral (PhD) Thesis, 2008

Abstract
In this thesis, a new random key pre-distribution scheme which named Hybrid Secure Random key Pre-distribution Scheme (HSRK scheme) is proposed. Security analysis of the HSRK scheme is presented to prove that our scheme has the highest resiliency and the best connectivity. Also, the Modified NK (MNK) cryptosystem is presented. Moreover, Security analysis of the MNK cryptosystem is presented which prove that the MNK cryptosystem is secure against all attacks that already applied on both RSA and the original NK cryptosystem. On the other hand, the energy analysis of the MNK cryptosystem is evaluated to show that the energy consumption due to the MNK cryptosystem is lower than that before.

Keywords
Wireless Sensor Networks, Key Management Protocol, Random Key Pre-Distribution Scheme,