



TWO DISTRIBUTIVE KEY MANAGEMENT SCHEMES IN MOBILE AD HOC NETWORKS

MOHAMMAD AL-SHURMAN¹, SEONG-MOO YOO²,
BONAM KIM^{3*}, SEUNGJIN PARK⁴

¹*Computer Engineering Department
Jordan University of Science and Technology
Jordan*

²*Electrical and Computer Engineering Department
The University of Alabama in Huntsville
USA*

³*School of Electrical and Computer Engineering
Chungbuk National University
Korea*

⁴*Department of Management, Management Information Systems, and Computer Science
University of Southern Indiana
USA*

ABSTRACT—Today's ever smaller computing systems are increasingly spreading in our ubiquitous environment. Being available ubiquitously in the devices and appliances that we use everyday and everywhere, these embedded computing systems are accessible to mobile users via hand-held devices connected over wireless networks. A mobile ad hoc network (MANET) is one of the important wireless networks. In a MANET a reliable key management system is required to generate and distribute symmetric encryption/decryption keys. The key management schemes proposed in MANETs so far have used trusted third parties (TTP) which have limitations because of the mobility of nodes. A Distributed Key Pre-distribution Scheme was proposed based on a probabilistic method without relying on any TTP but with results identical to TTP-based schemes. The scheme utilized cover-free family (CFF) properties. However, the precondition of the probabilistic method was claimed to be falsely deduced.

In this paper, we propose two distributive key management schemes using maximum distance separable codes (MDS). First, we will construct a practical $(n, t + 1)$ -threshold key management system. Second, we propose a key pre-distribution scheme achieving CFF properties. We use a global MDS code instead of the probabilistic method to generate node keys. The scheme is secure enough against malicious nodes' fraud and tapping. The effects of block size and network parameters are also studied.