RANDOM KEY PRE-DISTRIBUTION SCHEME BASED ON KEY UPDATING

ZHU Ling-Zhi[1], HE Rui[1] and ZHANG Jun-Ling[2*]

[1]Department of Computer and Information Science, Hunan Institute of Technology, Hengyang, 421002, Hunan, China

[2]Department of Cities and Tourism, Hengyang Normal University, Hengyang 421002, Hunan, China

Emails: lingzhi0825@163.com, 932900931@qq.com*

Submitted: Jan. 21, 2016 ***Accepted: Apr. 10, 2016*** ***Published: June 1, 2016***

Abstract-A random key pre-distribution scheme based on key updating (RKKU) was proposed, which is effective in wireless sensor networks. Firstly, the base station will randomly distribute some keys, a hash function and some code slices to each node. Furthermore, the RKKU scheme compares with the information of some random key to find the same key, and computes the communication key between two sensor nodes with one-way hash function. Since the one-way hash function can ensure that the attacker cannot use the obtained communication key to decipher the source key, it affects only two nodes communicate with each other. To assure the communication security, the key updating was designed based on code segment. The analysis shows that the proposed scheme can meet the security requirement of key management, and it also has less computation cost and storage cost than the existing schemes.

Index terms*: wireless sensor networks; code slices; pre-distribution; key updating, one-way hash function.*