ESKA: A Highly Reliable Authentication Protocol Based-on One-way Key Chain for WSN Broadcast

Qianping Wang, Ruoyu Li, Liangli Lai, Lei Kong
School of Computer
China University of Mining and Technology
Xuzhou 221116, China
Email: qpwang@cumt.edu.cn, vincentlry@126.com

Submitted: Mar. 30, 2013 *Accepted: July 15, 2013* *Published: Sep. 05, 2013*

Abstract- The authentication of broadcast sources is one of the most important research issues in the area of network security. To confirm that the control information received is from the genuine management nodes, the message broadcasted from management nodes must be verifiable for the working nodes. In this paper, a highly reliable WSN broadcast authentication protocol based-on one-way key chain, namely, the ESKA, is presented. For the purpose of comparison, a group of simulations are conducted. The results have demonstrated that compared with μTESLA, the presented method is of lower authentication delay and higher authentication rate in large broadcast data traffic transmission, meanwhile reducing considerable communication overheads in those applications.

Index terms: Broadcast Authentication Protocol, μTESLA, ESKA, High Reliability, One-way Key Chain.