A Novel Key Chain-Based En-route Filtering Protocol For Wireless Sensor Networks

Zhiming Zhang[1], Xiaoyong Xiong[1], Jiangang Deng[2]

[1]School. of Software,

[2]Science and technology research place,

Jiangxi Normal University, Jiangxi, Nanchang, China.

Emails: zzm_9650@163.com

Submitted: Apr. 20, 2013 ***Accepted: July 26, 2013*** ***Published: Sep.05, 2013***

Abstract- Sensor nodes may be deployed in hostile environments. An adversary may compromise the sensor nodes and inject false data into the network, which wastes scarce energy resources of the forwarding nodes. Existing schemes can effectively resist false data injection, but most of them do not consider the identifiers (IDs) attack, the en-route nodes check only the Message Authentication Codes (MACs) and do not verify the nodes identifiers (IDs) of the endorsing reports. In this paper, we propose a novel security routing protocol (KCEFP) based on one-way key chain. The proposed protocol can resist false data injection, replay and IDs attacks, and if the endorsement report is modified, the forwarding nodes can verify the endorsement report by the key chain, and filters out the fabricated packet right now. The security and performance analysis shows that our scheme provides a high security level and the energy savings significantly increasing with the number of fabricated report packet increasing.

Index terms*:* Wireless Sensor Networks, key chain, false data injection attack, different operation, fabricated packet.