通信学报
Journal on Communications
主管单位：中国科学技术协会
主办单位：中国通信学会

钟晓睿1,马春光1,2.基于动态累加器的异构传感网认证组密钥管理方案[J].通信学报,2014,(3):124~134

基于动态累加器的异构传感网认证组密钥管理方案

Dynamic accumulators-based authenticated group keymanagement scheme for heterogeneous wireless sensor network

投稿时间： 2012-11-09

DOI：10.3969/j.issn.1000-436x.2014.3.014

中文关键词：无线传感器网络 密钥管理 组密钥 动态累加器 认证

英文关键词：wireless sensor network key management group key dynamic accumulators authentication

基金项目：国家自然科学基金资助项目(61170241)；黑龙江省自然科学基金资助项目(F201229)

作者	单位
钟晓睿1，马春光1,2	1. 哈尔滨工程大学 计算机科学与技术学院，黑龙江 哈尔滨 150001；2. 哈尔滨工程大学 国家保密学院，黑龙江 哈尔滨 150001

摘要点击次数：**66**

全文下载次数：**15**

中文摘要：

利用动态累加器的证人能够证明特定累加项是否参与累加的特性，实现了组成员身份认证，提出了一种新的支持节点动态增加和撤销的组密钥管理方案DAAG。在需要建立组密钥时，所有成员节点提供自己持有的累加项，参与累加计算。DAAG方案在保证成员节点证人机密性的基础上，通过绑定证人与组密钥更新计算，限制了非成员节点对新密钥的计算能力。安全性和性能分析表明，DAAG方案虽比FM方案消耗更多的通信代价，但能够抵抗伪造、重放和共谋等恶意攻击，提供前后向安全性。

英文摘要：

Witnesses of a dynamic accumulator (DA) can ensure whether an object has been accumulated. On the basis of this, node membership in a cluster was verified and a novel authenticated group key management protocol was proposed, which supports node revocation and addition. In order to establish a group key for a cluster, each member provides their assigned number to join accumulation. DAAG can not only guarantee the confidentiality of witnesses, but also keep non-members from calculating novel group keys by binding witness with group key update. The security and performance analyses show that DAAG is resistant against replay attack, forgery attack and collusion attack, and can provide forward security and backward security.

查看全文 查看/发表评论 下载PDF阅读器

关闭

版权所有：《通信学报》
地址：北京市丰台区成寿寺路11号邮电出版大厦8层 电话：010-81055478，81055479
81055480，81055482 电子邮件：xuebao@ptpress.com.cn
技术支持：北京勤云科技发展有限公司