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

李 睿,林亚平,李晋国.两层传感器网络中一种高效的加密数据条件聚合协议研究[J].通信学报,2012,(12):58~68

两层传感器网络中一种高效的加密数据条件聚合协议研究

DOI：

中文关键词：

英文关键词：

基金项目：

作者	单位
李 睿	
林亚平	
李晋国	

中文摘要：

提出了一种隐私保护的条件聚合协议，使存储节点在不知道数据真实值的情况下对满足条件的数据进行聚合，防止存储节点对敏感信息的泄漏。为了保护数据和查询条件的隐私性，提出了一种基于前缀成员确认和布鲁姆过滤器相结合的编码方法对数据和查询条件进行编码，实现存储节点在不知道数据真实值和查询条件真实值的情况下进行查询处理；为了对查询结果中的数据进行聚合而不暴露数据真实值，采用同态加密技术对数据进行加密，使数据在不解密的情况下能进行聚合运算。进一步，根据传感器采集数据的特点，提出了一种基于代码表的数据压缩表示及传输方法，有效减小了传感器节点和存储节点之间的通信开销。分析和实验结果验证了所提方案的有效性。

英文摘要：