面向两层 WSNs 的高效随机调制隐私保护最值查询协议

刘泓晖[1,2] 刘树波[1,2] 刘梦君[1,2] 蔡朝晖[1]
(武汉大学计算机学院 武汉 430072)[1]
(武汉大学空天信息安全与可信计算教育部重点实验室(B类) 武汉 430072)[2]

摘 要 无线传感器网络(WSNs)隐私保护一直是研究热点,其中包括对隐私保护最值查询的研究。针对隐私保护最值查询问题,首先利用随机数和数值变换,提出一种不泄露原始参数的数值比较方法,并通过该方法和密码理论,提出一种面向两层无线传感器网络的高效随机调制隐私保护最值查询协议(ERM-MQP)。传感节点使用随机数对采样数据进行调制产生隐私保护数据,在存储节点处查找隐私保护数据的最值,Sink 节点恢复隐私保护最值数据得到采样数据最值,完成最值查找。在整个查询过程中数据加密后传送。最后,对安全性和能耗进行了分析,并通过实验与现有的隐私保护最值查询协议进行能耗对比,证明了 ERM-MQP 协议是安全且高效的。

关键词 两层无线传感器网络,隐私保护,随机调制,最值查询
中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2014.12.021

Efficient Random Modulation Privacy-preserving MAX/MIN Query Protocol in Two-tiered Wireless Sensor Networks

LIU Hong-hui[1,2] LIU Shu-bo[1,2] LIU Meng-jun[1,2] CAI Zhao-hui[1]
(College of Computer, Wuhan University, Wuhan 430072, China)[1]
(Key Laboratory of Aerospace Information Security and Trusted Computing of Ministry of Education, Wuhan University, Wuhan 430072, China)[2]

Abstract Privacy preservation is always a hot research area in wireless sensor networks (WSNs), which includes the privacy-preserving MAX/MIN Query Protocol. This paper proposed a numeric comparison method that will not leak the raw value first to address the problem of pricacy-preserving MAX/MIN query, which is based on random number and numerical map. With this numeric comparison method and cryptography, we proposed an efficient random modulation privacy preserving MAX/MIN query protocol (ERM-MQP) in two-tiered wireless sensor networks. In ERM-MQP, sensors modulate the sampled data with random number to compute the privacy-preserving data and the storage nodes search the privacy-preserving MAX/MIN value. The Sink sensor recovers the privacy-preserving MAX/MIN data and gets the MAX/MIN value of sampled data in the end. All data is encrypted before transmission on query process. Finally according to the result of security analysis and energy analysis, and comparing with existing method by experiment on energy consumption, the ERM-MQP is secure and needs less energy.

Keywords Two-tiered wireless sensor networks, Privacy preserving, Random modulation, MAX/MIN query

1 引言

目前,无线传感器网络(WSNs)作为构成物联网的底层基础和信息收集的源头,已大量应用于军队、国防、日常生活等多个领域,它具有感知信息丰富、传输数据量大和节点资源有限的特点。由于无线传感器部署量大,同种信息采集过程存在大量的冗余数据,网络资源浪费严重。传统 WSNs 通过传感节点进行数据融合、查询等,以减少向上层节点传输的数据量。但传感节点资源非常有限,且还需要兼顾数据感知,这大大降低了网络的生命周期。同时传感器网络往往部署在远程或者恶劣的环境中,想要保证实时通信是很困难的。为解决这些难题,近年来国内外学者提出并研究了两层 WSNs[1,2],两层 WSNs 以介于 Sink 节点和传感节点之间的存储节点为中间层,传感节点感知的数据传送给存储节点暂时存储,然后根据 Sink 节点的需求以及网络状况,向 Sink 节点发送数据。存储节点具备良好的数据存储和计算能力,能有效地进行负载均衡的控制、数据融合以及查询操作。两层 WSNs 在实际中有广泛的应用。例如,在水环境和水资源监控中,需要利用 WSNs 大范围、实时地对水质、水文、开采水量等进行实时监测,这种网络由于部署的点多面广,多采用两

到稿日期:2013-12-11 返修日期:2014-03-29 本文受国家 973 计划项目(2011CB302306),中央高校基本科研业务费专项资金(211-274230),国家自然科学基金(41371402),水利部"948"项目(201044),湖北省水利厅农村饮用水水资源远程监控项目资助。
刘泓晖(1990—),男,硕士生,主要研究方向为无线传感器网络安全、嵌入式系统,E-mail:lhh410@126.com;刘树波(1970—),男,博士,教授,CCF 会员,主要研究方向为嵌入式系统、物联网及其安全,E-mail:liu.shubo@whu.edu.cn(通信作者);刘梦君(1988—),男,博士生,主要研究方向为无线网络安全;蔡朝晖(1968—),女,博士,副教授,主要研究方向为物联网技术。

层 WSNs 网络结构。水环境和水资源监测多数属于预警监测，感兴趣的是非正常数据，如水质监测中只需要监测某一区域的最大值，水文数据中关心最大水位值，水量开采中关心最大超采量等，因此为减轻网络数据传输的压力和延长网络寿命等，不感兴趣的小数据就可以不传输到 Sink 节点。其它有些 WSNs 两层网络的应用也是只对最值感兴趣，如山洪预警、火灾预警、军事上的震动监测等。

另外，与传统 WSNs 相同，两层 WSNs 也面临大量的安全威胁，而数据的隐私安全问题尤其突出。由于存储节点存储大量的数据，并执行上层的请求，因此其容易成为各种攻击的目标。此外，传感节点也容易被俘获并被用于获取网络中数据的工具。因此，两层 WSNs 的安全性和隐私保护问题的研究，对无线传感器网络以及物联网技术的应用，具有重大意义。

无线传感器网络中，获取特定区域最值是常见的操作，在数据融合和查询中应用较多[3]。在两层 WSNs 中，目前对隐私保护查询技术的研究集中在两个方面：1）范围查询[4-7]，2）最值查询[8-10]，本文针对最值查询开展研究。目前对于两层 WSNs 隐私保护最值查询的研究，主要采用的方法为：先对数据进行编码，并将编码和加密的数据传输到存储节点，存储节点通过对各数据的编码进行运算得到最值，并向 Sink 节点传输相应的加密数据。

文献[8] 提出了基于前缀编码的隐私保护最值查询协议（PMV-MQP），即采用前缀编码验证机制，在传感节点处对传感数据进行编码，得到数据所对应的所有前缀码集合。同时对该传感数据和可能的采样数据值的上限值（下限值）各取一个特定位数的前缀码，组成区间集合。完成编码后，计算两个集合中所有编码的哈希运算消息认证码（HMAC），同时对存储节点保密的密钥加密原始数据。传感节点将两个 HMAC 码集合和加密数据传输到存储节点，存储节点通过查找数据前缀码集合是否与其他节点的区间集合有交集，来查找出最值，这就实现了无需明文参与下的最值查询。然而，该协议需要对每个数据进行前缀编码，同时还需要对每一个前缀码进行 HMAC 计算，且对于原始数据还需要进行加密，产生的数据量大，计算和传输过程能量消耗大。

文献[9]提出基于 Z-O 编码的隐私保护最值查询协议（ZOMQP），采用 Z-O 编码（0-1 编码）[11,12]进行数据隐私化。在编码前先对数据进行填充，保证所有参与比较的数据位数相同。将填充后的数据进行 Z 编码和 O 编码，得到两个编码集合。与文献[8]相同，其对编码后集合中的每个元素进行 HMAC 计算，并对原始数据进行加密后，将两个 HMAC 码集合和加密数据传输到存储节点。存储节点通过查找该数据的 Z 编码集合与其他数据的 O 编码集合是否有交集来判断两个原始数据大小，实现隐私保护下的最值查询。相比于 PMV-MQP，ZOMQP 产生的编码数量较少，但仍需要同时传输编码集合和加密数据，数据传输量仍然较大。对于每个编码，依然需要进行 HMAC 计算。此外，由于 HMAC 后集合中每个元素的长度均相同，在两集合比较是否有交集时，比较的复杂度会达到 $O(n^2)$[11]。在数据量大且数值较大的情况下，ZOMQP 计算量和通信量同样较大。

文献[10]对文献[9]的方法进行了改进，利用模运算，对 HMAC 数据量进行优化，提出了一种高效的隐私保护最值查询协议（EMQP），能耗降低较多，但同时会产生少量的误码。

除了已经提出的隐私保护最值查询协议，安全多方计算的相关研究成果也可以用于最值查询。文献[11-17]使用同态加密研究了姚式百万富翁问题[18]的解决方案，并扩展到了安全多方排序。在排序结果中，可以进行最值查询。但上述文献多是重复运用提出的百万富翁问题解决方案，得出某一节点产生的数据在所有数据中的大小位置，需要大量的数据交换，这就大大增加了网络负载。同时，计算过程也比较复杂，对于资源比较有限的 WSNs 而言，是难以接受的。

本文首先提出一种不泄露原始数值的隐私保护数值比较方法。该方法利用随机数对原始参数进行数值变换，通过比较变换后的数值得出原始数值大小关系。结合该方法和密码理论，本文提出一种面向两层 WSNs 的高效随机调制隐私保护最值查询协议 ERM-MQP（Efficient Random Modulation Privacy Preserving Max/Min Query Process Protocol），并针对该协议，进行了安全分析和能耗分析，同时通过与文献[8，10]提出的 PMV-MQP 和 EMQP 进行对比实验。相比于 PMV-MQP 和 EMQP，本文提出的协议不需要先对数据进行编码，仅需要简单的数值变化和数据加解密，不会产生大量数据编码，有效地减少了节点资源的占用和能耗开销。

2 问题描述和相关知识

2.1 问题描述

在两层 WSNs 中，数据由传感节点采集，再经过存储节点向上层传输。存储节点存储大量的数据，可以方便网络负载控制和数据融合，一旦被俘获，大量的数据就会暴露[9]。又由于传感节点的数据通信具有广播特性，在一跳范围内的任何节点都可以收到数据，被俘获的存储节点很可能被敌手用来截获网络中其他节点的数据。通过对采集的原始数据进行加密传输，可以达到数据隐私保护的目的，但加密数据无法在存储节点完成基于进行数值比较的数据融合、数据查询等操作。

在一些预报、预警的应用环境中，传输最大或最小的最值数据比传输所有传感数据的意义大得多。最值查询的目的就是为了获得某区域内传感数据的最大值或者最小值。最值查询的数值比较是在存储节点中进行的，一旦存储节点被监听，如何在不泄露隐私的情况下仍旧能比较出数据大小，是本文面临的主要问题。在保证存储节点正确查找最值的情况下，本文的安全目标为：

1）传感节点除了自身采集的数据外，无法获取到其他节点采集的原始数据。

2）存储节点无法获取到任何节点的原始数据。

2.2 隐私保护数值比较方法

我们首先证明一种不泄露原始传感数据的隐私保护数值比较方法，定理及证明如下。

定理 1 设 $X_1=\theta\cdot v_1+\delta_1$，$X_2=\theta\cdot v_2+\delta_2$，满足 $\theta\in R^*$，$\delta_1,\delta_2\in(0,\theta)$，$v_1,v_2\in Z$（$R^*$ 为非零正实数集，Z 为整数集）；若 $X_1-X_2\leqslant 0$，则 $v_1\leqslant v_2$；若 $X_1-X_2>0$，则 $v_1\geqslant v_2$。

证明：$X_1-X_2=(\theta\cdot v_1+\delta_1)-(\theta\cdot v_2+\delta_2)$

$=\theta\cdot(v_1-v_2)+(\delta_1-\delta_2)$

$v_1,v_2\in Z$，$v_1\neq v_2$ 时，有：

$v_1-v_2\in\{x\mid x\in(-\infty,-1]\cup[1,+\infty)\wedge x\in Z\}$，则

$\theta\cdot(v_1-v_2)\in\{x|x\in(-\infty,-\theta]\cup[\theta,+\infty)\wedge x\in Z\}$；

$v_1=v_2$ 时，$\theta\cdot(v_1-v_2)=0$。

当 $X_1-X_2\leqslant 0$ 时，即 $\theta\cdot(v_1-v_2)+(\delta_1-\delta_2)\leqslant 0$，此时，对于 $\delta_1-\delta_2$，有 $\delta_1-\delta_2\in(0,\theta)$ 和 $\delta_1-\delta_2\in(-\theta,0]$ 两种情况分类讨论：

1)若 $\delta_1-\delta_2\in(0,\theta)$，结合 v_1-v_2 取值范围，当且仅当 $v_1-v_2\in(-\infty,-1]$ 时，即 $\theta\cdot(v_1-v_2)<-\theta$ 时，$\theta\cdot(v_1-v_2)+(\delta_1-\delta_2)<0$ 成立，因此 $v_1<v_2$。

2)若 $\delta_1-\delta_2\in(-\theta,0]$，结合 v_1-v_2 取值范围，当且仅当 $v_1-v_2\in(-\infty,-1]$ 或 $v_1-v_2=0$ 时，即 $\theta\cdot(v_1-v_2)\leqslant 0$ 时，$\theta\cdot(v_1-v_2)+(\delta_1-\delta_2)\leqslant 0$ 成立，因此 $v_1\leqslant v_2$。综上所述，当 $X_1-X_2\leqslant 0$ 时，$v_1\leqslant v_2$。

同理，当 $X_1-X_2>0$ 时，可以得出 $v_1\geqslant v_2$。

定理 1 推论：对于 n 个节点情况，$X_1=\theta\cdot v_1+\delta_1$，$X_2=\theta\cdot v_2+\delta_2$，…，$X_n=\theta\cdot v_n+\delta_n$，由定理 1 可知，$\{X_1,X_2,\cdots,X_n\}$ 的最大值 $X_{\max}$/最小值 $X_{\min}$ 对应的 v_i 即为 $v_{\max}/v_{\min}$。

定理 2 对于定理 1 中 $X_1=\theta\cdot v_1+\delta_1$，$X_1$ 除以 θ 所得的整数部分即为传感器传感数据 v_1。

证明：$X_1/\theta=v_1+\delta_1/\theta$，$\delta_1/\theta$ 为大于 0 小于 1 的小数，故整数部分即为传感器传感数据 v_1。

3 隐私保护最值查询协议

3.1 网络模型

图 1 所示为一个两层 WSNs 网络模型，其每个存储节点和若干个传感节点组成一个查询单元，记为 $qc_s=(W,\{s_1,s_2,\cdots,s_n\})$，Sink 节点通过存储节点来获取传感节点的传感数据[11]。为方便讨论，做如下说明：

1)所有节点已知其他节点的身份标识号；

2)Sink 节点和传感节点在网络部署时需要设定采集数据的精度(即数据保留的小数点后位数)。在协议执行过程中，需要根据设定的精度对数据进行整数化。

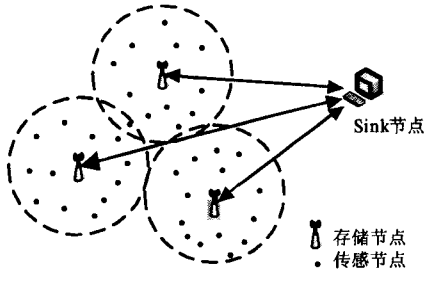


图 1 两层 WSNs 网络模型

存储节点收到数据后，根据发送数据的传感节点编号和收到的时间进行存储。存储消息的格式如下：

SN:…，$\{ID_{S_{i-1}},t,X_{i-1}\}$，$\{ID_{S_i},t,X_i\}$，$\{ID_{S_{i+1}},t,X_{i+1}\}$，…

ID_{S_i} 为传感节点身份标识号，X_i 为传感节点 s_i 传送的隐私保护数据，t 为采样时间。

3.2 保密通信信道建立

本文讨论的协议需要建立两条保密通信信道：1)Sink 节点和一个查询单元内所有传感节点需要一个用于参数传递的保密通信信道；2)每个传感节点和存储节点之间需要一个用于数据传输的保密通信信道。

保密信道的建立通过密钥分配和管理技术实现。目前关于 WSNs 密钥分配和密钥管理的研究成果较多，如文献[19，20]均提出了较好的解决方案。同时，基于公钥密码的方案[21]也很好地解决了 WSNs 的保密通信问题。本文采用文献[19]所述基于身份加密的密钥分配方案，利用基于身份标识的加密算法(IBE)建立所需的两条通信信道。两条信道建立过程如下：

在网络部署时，利用 Boneh-Franklin(BBF)算法[22]中的 Setup 函数，计算参与 IBE 算法的所需参数和主密钥，并内置于各节点之中。

对于信道 1)的建立，需要 Sink 节点和存储单元内的传感节点进行群密钥协商。主要步骤如下：

(a)传感节点 s_i 计算参数 Y_i：

随机选取 $Z_i<q$。

计算 $Y_i=\eta^{Z_i} \bmod q$。

其中 q、η 为网络部署时内置于节点中的参数，q 为素数。

Sink 节点计算参数 Y_{Sink}：

随机选取 $Z_{Sink}<q$。

计算 $Y_{Sink}=\eta^{Z_{Sink}} \bmod q$。

(b)传感节点 s_i 应用 Boneh-Franklin(BBF)算法中的 Encrypt 函数，分别使用存储单元内其他节点的 id 或 Sink 节点的 id 和内置的密钥对 Y_i 进行加密，并将密文消息发送至对应的存储单元中其他传感节点以及 Sink 节点。

Sink 同样应用 Boneh-Franklin，BBF 算法中的 Encrypt 函数，分别使用存储单元内节点 id 和内置的密钥对 Y_{Sink} 进行加密，并将密文消息发送至对应的存储单元中的传感节点。

(c)传感节点 s_i 应用 Boneh-Franklin(BBF)算法中的 Decrypt 函数对存储单元内其他节点和 Sink 节点发送的密文消息进行解密，得到 $\{Y_1,Y_2,\cdots,Y_{i-1},Y_{i+1},\cdots,Y_n,Y_{Sink}\}$，进行计算并保存群会话密钥：

$K_1=(Y_1\cdot\cdots\cdot Y_{i-1}\cdot Y_{i+1}\cdot\cdots\cdot Y_n\cdot Y_{Sink})^{Z_i} \bmod q$。

Sink 节点应用 Boneh-Franklin(BBF)算法中的 Decrypt 函数对存储单元内所有节点的密文消息进行解密，得到 $\{Y_1,Y_2,\cdots,Y_n\}$，进行计算并保存群会话密钥：

$K_1=(Y_1\cdot\cdots\cdot Y_n)^{Z_{Sink}} \bmod q$

至此，保密通信信道 1)建立完成。

信道 2)的建立与信道 1)类似，不同之处在于密钥分配过程只需要建立每个传感节点和存储节点之间存在的单独的会话密钥，即传感节点 s_i 计算并保存会话密钥 $K_{s_i\leftrightarrow SN}=(Y'_{SN})^{Z_i'} \bmod q$，存储节点 SN 计算并保存会话密钥 $K_{s_i\leftrightarrow SN}=(Y_i')^{Z_{SN}} \bmod q$。

保密信道建立后，Sink 节点和一个查询单元内所有传感节点存在一个参数传递保密信道，拥有一个共享密钥，密钥对存储节点保密。使用共享密钥加密操作记为 E_P；同时，每个传感节点和存储节点之间存在单独的会话密钥，传感节点 s_i 与存储节点(Storage Node，SN)之间通信加密记为 $E_{s_i\to SN}$。

3.3 隐私保护最值查询协议设计

如 2.1 节所述，对于普通的数据传输，将原始数据进行加密，可以达到隐私保护的目的。最值查询需要在存储节点上进行，但存储节点无法通过密文来进行数值比较，无法完成隐私保护最值查询。本节将设计隐私保护最值查询协议，通过随机数对原始数据进行调制，存储节点通过比较调制后的数据完成最值查询，同时达到了隐私保护的目的。

协议分为 4 个阶段。第一阶段为随机调制参数传递，主要目的是使得传感节点获得 2.2 节中提到的 θ 值。第二阶段为隐私数据收集，传感节点将采集的数据进行变换后，传送到存储节点。第三阶段为存储节点内最值查询处理。第四阶段为 Sink 节点内最值数据还原，Sink 节点通过计算可恢复原始传感数据值。

3.3.1 随机调制参数传递

如定理 1，要对传感数据进行数值变换，必须知道 θ 和 δ_i，其中 θ 需要各传感节点共有。

θ 可以使用 Sink 节点产生和传感节点共享协商两种方法来获得。考虑到协商方法传感节点需要大量的能耗开销，本文通过 Sink 节点随机产生 θ，并通过 3.2 节建立的参数传递保密信道，经由存储节点广播给传感节点。

存储节点收到 Sink 发送的消息，验证 Sink 节点身份标识 ID_{Sink} 后，将 ID_{Sink} 替换为存储节点 SN 的身份标识符 ID_{SN} 后，在查询单元内广播。传感节点收到后，验证标识符 ID_{SN} 后解密 $E_P(\theta)$，即可得到 θ。

3.3.2 隐私数据收集

传感节点 s_i 在 t 时间进行采样，得到传感数据 d_i。首先将 d_i 整数化，即按照预先设定的精度放大 10^n 倍后得到整数 v_i，n 为传感数据的小数点位数，同时产生一个随机数 δ_i，$\delta_i \in (0,\theta)$。然后对数据 v_i 数值变换，得 $X_i=\theta \cdot v_i+\delta_i$，并使用存储节点间的通信密钥进行加密后传送给存储节点。

3.3.3 存储节点内最值查询处理

存储节点收到查询单元内节点发送的加密数据后，解密得到 t 采样时刻的隐私数据集 $\{X_1, X_2, \cdots, X_n\}$，通过数值比较找出最值 $X_{max/min}$。存储节点得出最值 $X_{max/min}$ 后，使用 Sink 节点的公钥进行加密后传送给 Sink 节点。

3.3.4 Sink 节点内最值数据还原

Sink 节点收到存储单元发送的消息包后，解密得到 $X_{max/min}$。根据 2.2 节的定理 2，将 $X_{max/min}$ 除以 θ 后得到的整数部分按照设定精度缩小 10^n，得到该查询单元内 t 时刻采样数据最值 $d_{max/min}$。

协议详细过程如下所示，协议数据交换如图 2 所示。

面向两层 WSNs 的高效随机调制隐私保护最值查询协议：

1）Sink 节点产生一定范围内的随机数 θ，使用与传感节点之间的共享密钥加密，然后和 Sink 节点的身份标识号组成消息包，发送给存储节点 SN：$Sink \rightarrow SN: \langle ID_{Sink}, E_P(\theta)\rangle$。存储节点 SN 收到 Sink 节点发送的消息包后，将节点的身份标识符 ID_{Sink} 与说明 1）中已经存储在节点中的身份标识符进行对比验证，确定是 Sink 节点发送的消息包后，将密文 $E_P(\theta)$ 和 SN 的身份标识符组成消息包，向所在查询单元内节点广播：$SN \rightarrow Sensor: \langle ID_{SN}, E_P(\theta)\rangle$。

2）收到消息包 $\langle ID_{SN}, E_P(\theta)\rangle$ 后，传感节点 s_i 与说明 1）中已经存储在节点中的身份标识符进行对比验证，并将 $E_P(\theta)$ 解密后得到 θ。然后产生随机数 δ_i，$\delta_i \in (0,\theta)$。t 时刻的采样数据 d_i 放大 10^n 倍后得到整数 v_i，再进行数值变换得到 $X_i=\theta \cdot v_i+\delta_i$，最后加密 X_i 并和节点编号组成消息包，向存储节点传送：$s_i \rightarrow SN: \langle ID_{s_i}, t, E_{s_i \rightarrow SN}(X_i)\rangle$。

3）存储节点收到传感节点发送的消息包后，验证节点编号，然后对 $E_{s_i \rightarrow SN}(X_i)$ 解密得到 X_i 并根据 ID_{s_i} 和 t 进行存储。对于各节点 t 采样时刻的隐私数据集 $\{X_1, X_2, \cdots, X_n\}$，通过数值比较找出最值 $X_{max/min}$。查找完成后，使用 Sink 节点的公钥加密 $X_{max/min}$，并与查询类型 φ 以及存储节点编号 ID_{SN} 组成消息包传送给 Sink 节点：

$SN \rightarrow Sink: \langle ID_{SN}, \varphi, t, E_{Sink}(X_{max/min})\rangle$

其中，$\varphi \in \{0,1\}$，0、1 分别为最小值和最大值查询。

4）Sink 节点收到存储节点发送的消息包，验证存储节点编号后，使用私钥对 $E_{Sink}(X_{max/min})$ 解密得到 $X_{max/min}$。通过计算 $X_{max/min}/\theta$，得出整数部分即为整数化后的传感数据，根据 2.2 节定理 1 推论，该传感数据即为整数化后的最值数据 $v_{max/min}$。再将 $v_{max/min}$ 按照预先设定的数据精度进行还原，得出该查询单元内 t 时刻采样数据的 $d_{max/min}$。Sink 节点根据 φ 即可知道查询的是最大值还是最小值。

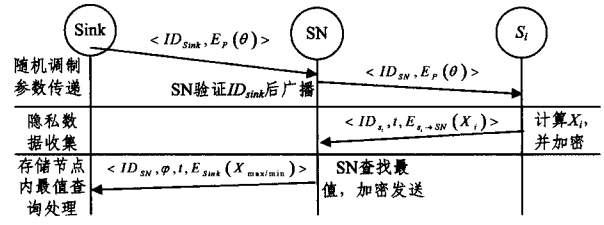


图 2 协议的数据交换

4 协议分析

4.1 隐私保护安全性分析

本文采用基于身份加密的密钥分配算法以及数据加密算法，相关文献已进行了较完整的安全性分析，验证了其具备较好的安全性。故我们认为采用的密钥分配算法和数据加密算法是安全的。

本文提出的协议安全性目标是防止窃听攻击，即在最值查询过程中，存储节点和非源节点的传感节点无法获取传感数据的数值。由 2.2 节定理 2 可知，获取数值 v_i 需要同时知道 X_i 和 θ，二者通过除法即可算出 v_i。

传感节点 s_i 当被监听时，可以被监听者用来进行窃听攻击以获取数据。对于获取到的密文 $E_{s_j \rightarrow SN}(X_j)$，$s_i$ 无法获取 s_j 的会话密钥。s_i 在无密钥的情况获取 X_j 的复杂度与破解加密算法相同，从而保证了传感节点无法获取路径中其他节点的明文数据。即使在已知 θ 的情况下，也无法得到源传感节点的 v_i 数值。

当存储节点 SN 被监听时，存储节点上的数据集 $\{X_1, \cdots, X_n\}$ 均会被监听。但存储节点上所有参与最值查询的数据均是经过随机数调制的隐私保护数据，而随机调制参数 θ, δ_i 对 SN 保密。存储节点需要获得数值 v_i，只能通过穷举攻击。对穷举攻击的分析如下：

对于 $X_i=\theta \cdot v_i+\delta_i$，使用任何小于 X_i 的 θ 去除 X_i 所得的整数部分，都是一个“合理”的数据，并无法判断原始数值是哪一个。例如，$X_i=24$，假设 $\theta=10$，得出 $v_i=2$，若假设 $\theta=5$，计算的 $v_i=4$，所以无法判断原始数据是 2 还是 4。

而在存储节点上有大量的 X_i，找出 X_{min} 便可大范围减小 θ 可能的取值范围。然而，由 $\theta \in R^*$，有 $X_{min} \in R^*$，在可获取 X_{min} 数据长度的情况下，区间 $(0, X_{min})$ 中 θ 的可能取值范围仍然很大。以 X_{min} 数据长度为 8 位，且 X_{min} 整数部分长度为 4 位为例，存储节点无法获知 θ 长度。由于 θ 的整数部分长度可能为 1 至 4 位，有超过 4×10^8 种取值可能，因此，无法通过

穷举攻击获取明文。

通过以上分析，本文提出的 ERM-MQP 具有良好的隐私保护能力，能够保护数据的隐私安全。

4.2 能耗分析

本文提出的 ERM-MQP，除了加密外，无较复杂的计算。文献[9,10]中的能耗分析方法，对 ERM-MQP 进行能耗分析。由于两层 WSNs 中，存储节点具有充足的存储空间和能量储备，网络的生命周期主要受传感节点影响，故仅对传感节点进行能耗分析。

由于保密通信信道构建于 WSNs 建立初期，不要求实时进行密钥更新，仅在较长时间使用后利用网络空闲即可完成密钥更新，对网络性能影响较小，因此仅对隐私保护最值查询过程进行能耗分析。

按照文献[9,10]的方法，传感节点的总能耗为：

$E_{total}=E_{comp}+E_{comm}$

E_{comm} 表示传感节点接收和发送数据产生的通信能耗，E_{comp} 表示传感节点进行加解密计算所带来的能耗。

本文采用与文献[9]相同的符号来表示各个参数。设 WSNs 中查询单元中的传感节点总数量为 n。传感数据的二进制编码长度都为 w，节点编号长度为 l_{id}，l_t 为时间参数长度，参数 θ 长度为 l_θ，θ 加密后长度为 l_θ'，加密数据长度为 l_D；加密/解密计算的单位能耗为 e_d，接收和发送 1 个字节的平均能耗分别为 e_r 和 e_s；传感节点到存储节点的平均路径长度(跳数)为 L，存储节点具有较强通信能力，其到节点跳数设为 1。

在 ERM-MQP 中，随机调制参数传递阶段每个节点需要进行一次解密计算；在最值查询处理阶段，每个传感节点进行一次加密计算。因此，计算总能耗为：

$E_{comp}=n\cdot e_d\cdot l_\theta+n\cdot e_d\cdot l_D$

通信量方面，Sink 节点通过秘密信道向每个传感节点传送参数 θ，每个传感节点需要进行一次接收；每个节点发送一次加密后的数据，每经过一跳，传感节点增加一次发送和接收。因此，通信总能耗为：

$E_{comm}=n\cdot(l_\theta'+l_{id})\cdot e_r+n\cdot(l_D+l_t+l_{id})\cdot(L\cdot e_s+(L-1)\cdot e_r)$

故总能耗 E_{total} 最终公式为：

$$E_{total}=n\cdot e_d\cdot l_\theta+n\cdot e_d\cdot l_D+n\cdot(l_\theta'+l_{id})\cdot e_r+n\cdot(l_D+l_t+l_{id})\cdot(L\cdot e_s+(L-1)\cdot e_r)$$

从以上分析可知，整个过程需要进行的计算和通信并不复杂。与文献[9]提出的基于 Z-O 编码的隐私保护最值查询处理协议(ZOPPM)以及文献[10]的高效隐私保护最值协议(EMQP)相比，虽然加解密计算的次数略有上升，但不需要进行 HMAC 计算，而 ZOPPM 中，HMAC 数据量与原数据二进制编码长度 w 相同；EMQP 针对 HMAC 数据量进行了优化，但仍会有大量的 HMAC 数据。在下一节，将对 ERM-MQP 与文献[8]提出的基于前缀码隐私保护最值查询协议(PMV-MQP)以及文献[10]提出的高效隐私保护最值协议(EMQP)进行能耗对比实验。

5 实验分析

本文参照文献[9,10]的实验方法，在 Matlab 下进行仿真实验，对本文提出的 ERM-MQP、文献[8]提出的 PMV-MQP 和文献[10]提出的 EMQP 进行能耗对比。为了更好地进行实验结果分析，和文献[9,10]一样，本文做了通信和计算能耗的对比实验。

本文采用的能耗计算方法与文献[10]相同，在相同参数的环境下进行实验对比：无线通信电路发送和接收 1bit 的能量消耗公式为 $e_s=\alpha+\gamma\times d^k$ 和 $e_r=\beta$，其中，α、β 分别为通信发送电路和接收电路消耗的能量，γ 为传输放大器消耗的能量，d 为传输距离，k 为路径损失因子。采用文献[9,10,23]的参数，有：$\alpha=45$nJ/bit，$\beta=135$nJ/bit，$\gamma=10$pJ/bit/m^2，$k=2$。传感数据长度初始设置为 10bit，加密计算的初始能耗采用文献[23]给出的在 TelosB 中利用 RC4 对 10 bit 数据进行加密的能耗数据 8.92μJ。而 RC4 是以 8bit 为分组进行计算的，10bit 原始数据需要填充到 16bit 进行加密[23]。θ 取 8bit，由 4.1 分析可知，参数 θ 在取值较小的情况下，安全性仍然有保证，对于 10 bit 原始数据，已经能够较好地保证安全性。而对 θ 进行 RC4 加解密的能耗小于 8.92μJ，为方便计算，随机调制参数传递阶段传感节点解密的功耗采用 8.92μJ。而在最值查询处理阶段，传感数据与 θ 相乘后，数据长度最多会增加 8bit，因此这一步的加密功耗取其 2 倍(实际上功耗是低于 2 倍)，即 17.84μJ。同时，RC4 加密后长度与明文长度相同，即 $l_\theta=l_\theta'$，故 ERM-MQP 密文数据长度设置比 EMQP 中的密文长 8bit。其他参数的设置与文献[10]均相同，如表 1 所列。

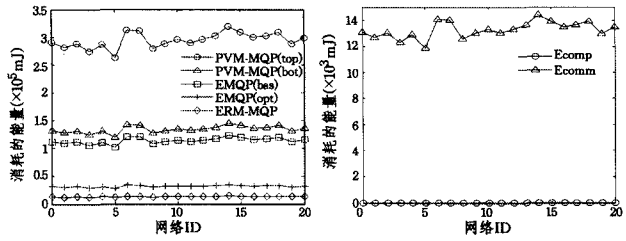
表 1 实验参数

网络覆盖区域	100×100m^2	实验次数	20
节点通信半径	10m	密文数据消息	136bits
传感节点分布	随机分布	节点编号长度	32bits
时间参数长度	32bits	传感节点数量	480

而作为对比项，PMV-MQP 和 EMQP 的 HMAC 单位计算能耗 e_h 取与 RC4 加密能耗相同的值，即 $e_h=8.92$μJ，密文数据消息长度为 128 bits，HMAC 数据消息长度为 128 bits[10]。

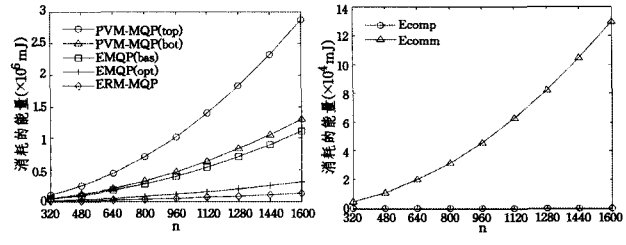
根据文献[10]，EMQP 中 HMAC 的数据量与原始数据长度 w 相同。此外，EMQP 进行 HMAC 数据优化的参数 μ 取值和文献[10]一样，取值为 24bits。而 PMV-MQP 需要进行 HMAC 的数据总量在区间[$w+2$,$3w-1$]之间，即能耗存在上限和下限。本文参照文献[10]的思路，做了 3 组对照实验。实验 1 为不同网络拓扑结构下的能耗对比，实验 2 为以传感节点数量 n 为自变量的能耗对比，实验 3 为以原始数据长度 w 为自变量的能耗对比，实验结果图分别对应图 3、图 4 和图 5。实验结果中，使用 PMV-MQP(top)和 PMV-MQP(bot)分别表示 PMV-MQP 的能耗上限和下限，EMQP(bas)和 EMQP(opt)分别表示优化前后的 EMQP 能耗。对具体的实验结果和分析如下：通信能耗方面，本文提出的 ERM-MQP，在隐私数据收集阶段只传递了节点编号、时间参数、查询类型和加密后的数据，而 PMV-MQP 和 EMQP 还需要传递大量的 HMAC 数据，这部分 HMAC 数据传输消耗的能量占据了通信能耗很大的一部分。而在随机调制参数传递阶段，每个节点需要接收一个包含 θ 加密后的消息包，但数据位数较少，对能耗的影响要远小于 PMV-MQP 和 EMQP 中大量 HMAC 数据传递的影响。计算能耗方面，ERM-MQP 每个节点需要多进行一次解密，而 PMV-MQP 和 EMQP 需要进行 HMAC 计算，从图 3(b)、图 4(b)和图 5(b)可以看出，相

比通信能耗，计算能耗所占比例很小，数量级相差较大，随着 n 和 w 变化，其增加的幅度也远小于通信能耗，对整个能耗对比影响较小。



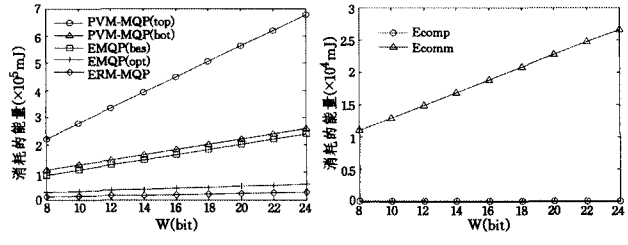
(a) 不同网络拓扑的能耗对比　　(b) ERM-MQP 计算能耗和通信能耗对比

图 3　不同网络拓扑下的能耗实验



(a) 不同网络拓扑的能耗对比　　(b) ERM-MQP 计算能耗和通信能耗对比

图 4　以节点数 n 为自变量的能耗实验



(a) 原始数据长度 w 变化的总能耗对比　　(b) ERM-MQP 计算能耗和通信能耗对比

图 5　以原始数据长度 w 为自变量的能耗实验

由以上分析得出，在本文的实验参数设置下，ERM-MQP 比文献[8]提出的 PMV-MQP 能耗下限减少约 80%，比文献[10]提出的优化后 EMQP 能耗减少了 50%。本文的协议能耗消耗优于 PMV-MQP 和 EMQP。

结束语　隐私保护问题是无线传感器网络中迫切需要解决的问题，在各应用领域都有较大需求。目前对于两层 WSNs 模型，针对隐私保护查询的研究主要集中在范围查询，对最值查询的研究处于起步阶段。本文提出一种面向两层 WSNs 的高效随机调制隐私保护最值保护协议 ERM-MQP，利用随机数和数值变化，并通过保密通信在不泄露原始数值的情况下进行最值查询。通过对协议进行分析和实验，证明了 ERM-MQP 具有较好的安全性和较低的能耗，适合无线传感器网络使用。

需要指出的是，本文提出 ERM-MQP 协议，在存储节点不知道随机参数的情况下，无法通过隐私数据找出原始数据相等的情况，进而无法找出所有取得最值的点。因此，协议局限于无需查找所有最值点具体信息的应用。下一步工作将针对这一局限进行深入研究。

参 考 文 献

[1] Gnawali O, Jang K Y, Paek J, et al. The tenet architecture for tiered sensor networks[C]// Proceedings of the 4th ACM Conference on Embedded Networked Sensor Systems. Boulder, Colorado, USA, 2006: 153-166

[2] Desnoyers P, Ganesan D, Shenoy P. TSAR: a two tier sensor storage architecture using inteval skip graphs[C]// Proceedings of the 3rd ACM Conference on Embedded Networked Sensor Systems. San Diego, Calif, USA, 2005: 39-50

[3] 许建，杨庚，陈正宇，等. WSN 数据融合中的隐私保护技术研究[J]. 计算机工程，2012，38(15)：134-138

[4] Sheng Bo, Li Qun. Verifiable privacy-preserving range query in two-tiered sensor networks[C]// 27th IEEE International Conference on Computer Communications. Phoenix, AZ, USA, 2008: 46-50

[5] Chen Fei, Liu Alex X. SafeQ: secure and efficient query processing in sensor networks[C]// 29th IEEE International Conference on Computer Communications. San Diego, CA, USA, 2010: 1-9

[6] 窦轶，黄海平，王汝传，等. 两层无线传感器网络安全范围查询协议[J]. 计算机研究与发展，2013，50(6)：1253-1266

[7] Shi Jing, Zhang Rui, Zhang Yan-chao. A spatiotemporal approach for secure range queries in tiered sensor networks[J]. IEEE Transactions on Wireless Communications, 2011, 10(1): 264-273

[8] Yao Yong-lei, Xiong Nai-xue, Park J H, et al. Privacy-preserving max/ min query in two-tiered wireless sensor networks[J]. Computers & Mathematics with Applications, 2013, 65: 1318-1325

[9] 戴华，秦小麟，刘亮，等. 基于 Z-O 编码的两层 WSNs 隐私保护最值查询处理协议[J]. 电子与信息学报，2013，35(4)：970-976

[10] Dai Hua, Yang Geng, Qin Xiao-lin. EMQP: An Energy-Efficient Privacy-Preserving MAX/MIN Query Processing in Tiered Wireless Sensor Networks[J]. International Journal of Distributed Sensor Networks, 2013(2013)

[11] Lin Hsiao-ying, Tzeng Wen-guey. An efficient solution to the millionaires' problem based on homomorphic encryption[C]// Proceedings of the 3rd International Conference on Applied Cryptography and Network Security. New York, NY, USA, 2005: 97-134

[12] 查俊，苏锦海，闫少阁，等. 姚氏百万富翁问题的高效解决方案[J]. 计算机工程，2010，36(14)：124-126

[13] Zhang Lan, Li Xiang-yang, Liu Yun-hao, et al. Verifiable Private Multi-party Computation: Ranging and Ranking[C]// IEEE INFOCOM 2013. Turin Italy, 2013: 605-609

[14] 李顺东，王道顺. 基于同态加密的高效多方保密计算[J]. 电子学报，2013，41(4)：798-803

[15] 肖倩，罗守山，陈萍，等. 半诚实模型下安全多方排序问题的研究[J]. 电子学报，2008，36(4)：709-714

[16] 邱梅，罗守山，刘文，等. 利用 RSA 密码体制解决安全多方多数据排序问题[J]. 电子学报，2009，37(5)：1119-1123

[17] 刘文，王永滨. 安全多方信息比较相等协议及其应用[J]. 电子学报，2012，40(5)：871-876

(下转第 128 页)

第 2 轮通信：阅读器与标签正常通信，此时两端的 IDS 数据情况为：

Reader：$(IDS_{new+2}, s_{i+2}, t_{i+2})$，$(IDS, s_i, t_i)$

Tag：$(IDS_{new+2}, t_{i+2}, N_{x+2})$

第 3 轮通信：攻击者发送 request 请求，收到标签返回的 $(IDS_{new+2} \| M_{i+2})$ 消息之后，重放第一轮窃听到的消息 $(N_{i+2} \| P_{i+2})$，由于此时标签中的 N_x 数据已经更新，标签验证消息 $P^*_{i+2} \neq P_{i+2}$，协议终止，攻击失败。

攻击者使用重放攻击的方式来攻击文献[6]协议，可能造成协议失效，将其用来攻击本文协议则是无效的，最终协议能正常执行。主要原因是文献[6]协议中，阅读器单向认证标签，而在改进的协议中，通过增加通信过程，实现了阅读器和标签的双向认证；而且标签用动态数据 N_x 来加密消息，N_x 在收到标签消息后就会刷新数据，这样协议中的消息具有了时效性，协议就可以防重放攻击，同时拒绝服务攻击也失效了。

6.2 性能比较

本文从通信量、计算量、标签上的存储量 3 方面对文献[6]协议、文献[7]协议、文献[8]方案中的两种协议（closed loop 协议和 open loop 协议）与本文协议进行比较。5 种协议标签上的存储量不同：文献[6]协议中标签端保存数据 t_i；文献[7]协议标签端保存数据 ik、uk、id；文献[8]方案中的两种协议标签端保存的数据是一样的，都是 $h(\mathrm{TID})$、K_{TID}、r、n；本文协议中标签端保存数据 IDS、t_i、N_x。假设 3 种协议的单位消息长度相同都为 L，文献[6]协议的通信量为 $3L$；文献[7]协议的通信量为 $5L$；文献[8]方案中的两种方案的通信量都是 $7L$；本文协议的通信量为 $5L$。当协议执行完毕时，5 种协议标签计算量比较结果如表 1 所列。设每次计算操作消耗的时间单位为 $T(s)$，协议中的密钥长度是 l；两种协议的计算量比较如表 1 所列。

表 1 两种协议的计算量比较结果表

协议	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
A	0T	2T	1T	0T	0T	0T	0T	0T	2T
B	1T	1T	0T	0T	4T	0T	0T	3T	1T
C	0T	19T	0T	0T	5T	3T	1T	5T	2T
D	0T	20T	0T	0T	6T	3T	0T	5T	2T
E	1T	2T	1T	1T	0T	0T	0T	0T	2T

注：(1)表示"+"操作；(2)表示"⊕"操作；(3)表示 SQUASH 方案操作；(4)表示 MIXBITS(x,y)函数操作；(5)表示 Hash(哈希)操作；(6)表示 mod(求余)操作；(7)表示 CRC(循环校验)操作；(8)表示 PRNG(伪随机数发生器)操作；(9)表示比较操作。A 表示文献[6]协议方案；B 表示文献[7]协议方案；C 表示文献[8]中的 closed loop 协议方案；D 表示文献[8]中的 open loop 协议方案；E 表示表示本文协议方案。

结束语 本文通过分析现有的 RFID 所有权转移协议，针对文献[6]协议的缺陷，提出了一种改进的超轻量级 RFID 所有权转移协议，该协议实现了阅读器和标签的双向认证功能，并基于 GNY 逻辑给出了协议的形式化证明。对协议的安全性分析和性能比较表明，本文协议可以抵抗拒绝服务攻击、重放攻击等常见攻击方式；协议中标签端没有使用伪随机数发生器，实现了超轻量的特性。与现有一些方案比较表明，本文协议具有更高的安全性、更少的硬件成本，可以满足低成本 RFID 系统的应用需求。

参 考 文 献

[1] 邵婧，陈越，常振华. RFID 标签所有权转换模式及协议设计[J]. 计算机工程，2009，35(15)：143-145

[2] Molnar D，Soppera A，Wagner D. A Scalable，Delegatable Pseudonym Protocol Enabling Ownership Transfer of RFID Tags[C]// Proc. of SAC'05. Kingston，Jamaica：Springer-Verlag，2005：276-290

[3] Osaka K，Takagi T，Yamazaki K，et al. An Efficient and Secure RFID Security Method with Ownership Transfer[C]// Proc. of CIS'06. Springer-Verlag，2006：778-787

[4] Fouladgar S，Afifi H. An Efficient Delegation and Transfer of Ownership Protocol for RFID Tags[C]// Proc. of the 1st International Workshop on RFID Technology. Vienna，Austria，2007

[5] Kulseng L，Yu Zhen，Wei Ya-wen，et al. Lightweight mutual authentication and ownership transfer for RFID systems [C]// Proc of the 29th Conf on Computer Communications IEEE INFOCOM 2010. Piscataway，NJ：IEEE，2010：1-5

[6] 金永明，孙惠平，关志，等. RFID 标签所有权转移协议研究[J]. 计算机研究与发展，2011，48(8)：1400-1405

[7] Fernandez-Mir A，Trujillo-Rasua R，Castella-Roca J，et al. A Scalable RFID Authentication Protocol Supporting Ownership Transfer and Controlled Delegation. RFID，Security and Privacy，LNCS，2012，7055：147-162

[8] Doss R，Zhou Wan-lei，Yu Shui. Secure RFID Tag Ownership Transfer Based on Quadratic Residues[J]. IEEE Transcations on information forensics and security，2013，8(2)：390-401

[9] 彭朋，赵一鸣，韩伟力，等. 一种超轻量级的 RFID 双向认证协议[J]. 计算机工程，2011，37(16)：140-142

[10] Shamir A. SQUASH-A new MAC with provable security properties for constrained devices such as RFID tags [C]// LNCS 5086：Proc of 15th Annual Fast Software Encryption Workshop. Springer，2008：144-157

[11] 李杰. RFID 安全认证协议研究与设计[D]. 西安：西安电子科技大学，2012：40-46

(上接第 100 页)

[18] Yao A. Protocols for secure computation [C]// Proceeding of the 23th IEEE Symposium on Foundations of Computer Science. IEEE Computer Society Press，Los Alamitos，USA，1982：160-164

[19] 杨庚，王江涛，程宏兵，等. 基于身份加密的无线传感器网络密钥分配方法[J]. 电子学报，2007，35(1)：180-184

[20] 刘梦君，刘树波，刘泓晖，等. 异构无线传感器网络动态混合密钥管理方案研究[J]. 山东大学学报：理学版，2012，47(11)：67-73

[21] 郭萍，张宏，傅德胜，等. 一种混合轻量型无线传感器网络公钥密码方案[J]. 计算机科学，2012，39(1)：69-81

[22] Boneh D，Franklin M. Identity-based encryption from the Weil pairing [C]// Advances in Cryptology，CRYPTO 2001，Lecture Notes in Computer Science. Berlin：Springer-Verlag，2001，2139：213-229

[23] Groat M M，Hey W，Forrest S. KIPDA：k-indistinguishable privacy-preserving data aggregation in wireless sensor networks [C]// 30th IEEE International Conference on Computer Communications. Shanghai，China，2011：2024-2032