基于 Z-O 编码的两层 WSNs 隐私保护最值查询处理协议

戴 华*[①] 秦小麟[②] 刘 亮[②] 季一木[①] 付 雄[①] 孙 研[②]
[①](南京邮电大学计算机学院 南京 210003)
[②](南京航空航天大学计算机科学与技术学院 南京 210016)

摘 要：无线传感器网络中的隐私保护技术已经成为研究热点，其中具有隐私保护能力的最值查询处理技术已经成为富有挑战性的研究问题。该文提出一种基于 Zero-One(Z-O)编码的两层 WSNs 隐私保护最值查询处理(ZOPPM)协议。该协议通过引入 Z-O 编码技术，并结合 Hash 消息身份验证编码机制，对感知数据进行编码处理，然后由感知节点将编码数据发送至存储节点，与此同时，感知节点根据存储节点需求计算并传送加密数据；存储节点利用 Z-O 编码的数值比较特性，实现在无需感知数据明文参与下的数值线性关系比较，进而构造局部查询结果并发送给 Sink，由 Sink 完成最终的最值查询结果计算。理论分析和实验结果表明，ZOPPM 协议能够确保感知数据和最值查询结果的隐私安全性，并且其能耗优于现有的方法。

关键词：两层WSNs；隐私保护；最值查询；Zero-One编码
中图分类号：TP393 **文献标识码**： A **文章编号**：1009-5896(2013)04-0970-07
DOI: 10.3724/SP.J.1146.2012.00940

Z-O Encoding Based Privacy-preserving MAX/MIN Query Protocol in Two-tiered Wireless Sensor Networks

Dai Hua[①] Qin Xiao-lin[②] Liu Liang[②] Ji Yi-mu[①] Fu Xiong[①] Sun Yan[②]
[①](*College of Computer*, *Nanjing University of Posts and Telecommunications*, *Nanjing* 210003, *China*)
[②](*College of Computer Science & Technology*, *Nanjing University of Aeronautics and Astronautics*, *Nanjing* 210016, *China*)

Abstract: Privacy preservation in wireless sensor networks has attracted more and more attentions. Computing MAX/MIN query result in wireless sensor networks while preserving data privacy is a challenge. This paper proposes a Zero-One (Z-O) encoding based Privacy-Preserving MAX/MIN query protocol in two-tiered wireless sensor networks (ZOPPM). In ZOPPM, sensor nodes in the query range firstly convert their sensory data into encoded data, by using Z-O encoding and hashed message authentication code mechanism, and send the encoded data to the corresponding storage node, and encrypt sensory data and send the ciphertext to it in the demand. According to the numerical comparison theory of Z-O encoding method, every storage node generates a local MAX/MIN sensor node in its own query cell, without sensory data in plaintext. Then, the storage node constructs a local query result when receiving the encrypted data from a sensor node, and sends it to the sink node. Finally, the sink node calculates the MAX/MIN query result after receiving the local query result from all storage nodes. The theoretical analysis and experimental results show that the ZOPPM protocol can ensure the privacy of sensory data and the query result, and it costs less energy consumption than other similar method.

Key words: Two-tiered Wireless Sensor Networks (WSNs); Privacy preserving; MAX/MIN query; Zero-One (Z-O) encoding

1 引言

目前，无线传感器网络(Wireless Sensor Networks, WSNs)已被广泛用于诸如环境监测、医疗卫生、智能交通、国防军事等各种重要领域。而两层WSNs(Two-tiered Wireless Sensor Networks)[1]是一种以存储节点(storage nodes)为中间层的无线传感器网络，其中存储节点为计算、存储和能量资源充足的传感器节点，其上层为Sink节点，下层为资源受限的一般感知节点(sensor nodes)，存储节点与查询区域内其负责管理的所有感知节点构成查询单元(query cells)。由于两层WSNs的拓扑结构的简单性和中间层存储节点的资源充裕性，使得两层WSNs具有链路质量稳定、路由结构简单、查询高

2012-07-19 收到，2012-12-13 改回
国家 973 计划项目(2011CB302903)，国家自然科学基金(61272084, 61171053)，江苏省科技支撑计划(BE2011844, BE2011189)，江苏省自然科学基金(BK2011754)，江苏省高校自然科学研究重大项目(11KJA520002)和南京邮电大学引进人才科研启动基金(NY211043)资助课题
*通信作者：戴华 daihua@njupt.edu.cn

效和负载均衡等优点[1,2]。然而，由于存储节点所处位置的重要性，不仅存储着大量感知数据，同时还负责执行上层的查询请求，这就使得存储节点往往成为各种攻击的主要目标。研究和解决两层WSNs中的安全和隐私保护问题，对于促进无线传感器网络技术的大规模应用具有重要的现实意义。

在面向两层 WSNs 的隐私保护查询处理技术中，现有研究重点关注范围(range)查询中的隐私保护技术[3−6]，对于最值(MAX/MIN)查询处理的研究相对较少，目前仅有文献[7]提出了初步的解决方法，该方法利用前缀编码验证(Prefix Membership Verification, PMV)机制[3]，给出了一种无需感知数据明文参与的数值线性关系比较方法，进而实现满足隐私保护要求的最值查询处理方法(记为 PMV-MQP)。然而，该方法采用的前缀编码机制产生的数据量较大，并且每一个感知节点都需要加密感知数据并传送密文数据，导致该查询处理过程需要较大的能耗开销。此外，文献[8]提出了工作于多跳 WSN 中基于 k-隐藏的最值聚集查询方法，但该方法只能查询最值数据，无法查询产生最值数据的传感器节点位置信息。

本文以两层WSNs为研究背景，重点讨论面向两层WSNs的隐私保护最值查询处理技术，即在实现最值查询处理的过程中，确保感知数据和最值查询结果不泄露，以保证感知数据和最值查询结果的隐私安全性。基于此，本文提出了基于Z-O编码的两层WSNs隐私保护最值查询处理协议。通过引入安全多方计算中的Z-O编码技术[9]，并结合Hash消息身份验证编码机制(Hashed Message Authentication Code, HMAC)[10]，对感知数据进行HMAC数值化Z-O编码处理，然后利用Z-O编码集合的数值比较特性，实现在无需感知数据明文参与下的数值线性关系比较，并利用加密技术确保感知数据传输过程中的隐私安全性。在上述隐私保护措施的基础上，给出基于Z-O编码的隐私保护最值查询处理协议(Z-O Encoding based Privacy Preserving Max/Min query process protocol, ZOPPM)，并对该协议进行能耗和隐私安全性分析。实验结果表明，ZOPPM协议的能耗优于现有的方法。

2　问题描述

在两层 WSNs 的查询处理过程中，如果不对感知数据进行处理，直接以明文形式参与查询，当存储节点被俘获，该节点将能够获取所有存储在该节点，以及利用该节点进行转发的感知数据，并且还能够获取由该节点计算出的部分查询结果。与此同时，由于传感器节点数据通信的广播特性，在感知节点发送数据的一跳(hop)范围内，其他任何节点(存储节点或感知节点)都可以收到数据。因此，需要在查询处理过程增加隐私保护措施，以确保感知数据和查询结果的隐私安全性。

最值查询即为获取查询区域内的感知节点采集到的数据最大值(MAX)或最小值(MIN)及其位置信息的计算过程。最值的计算必然需要比较数值的线性关系，所以解决最值查询问题，首先需要解决如何在不泄露隐私的情况下比较两个感知节点的数据大小问题，该问题类似于安全多方计算研究中一个经典问题 —— 百万富翁问题[11]。

与文献[3,7,8]类似，本文也假设查询发起节点 Sink 可信，并假设两层 WSNs 中的存储节点和感知节点都有试图窥探其他节点数据的企图，但仍然能够遵循查询处理协议进行最值计算，即符合 honest-but-curious 威胁模型[12]。此外，假设两层 WSNs 的拓扑结构稳定，感知节点采集感知数据，存储节点只负责计算和存储；存储节点拥有其负责的感知节点的位置和 ID 信息，而感知节点也拥有对应存储节点的位置和 ID 信息，Sink 则拥有所有感知节点和存储节点的位置和 ID 信息。

在上述假设条件下，实现具有隐私保护能力的最值查询，就必须确保查询处理过程满足：(1)对于网络中的任一感知节点的感知数据，只有该感知节点本身和 Sink 可以读取其明文数值；(2)对于最终的最值查询结果(包含数值和位置信息)，只有 Sink 拥有，而其他任何节点都无法获得。此外，存储节点的能量资源充足，而感知节点的能耗有限，因此，降低感知节点的能耗开销也是两层 WSNs 查询处理技术研究的一个重要目标。

3　基于 Z-O 编码的数值比较方法

本节我们将在文献[9]的基础上，给出基于 Z-O 编码数值比较方法。

定义 1　Z-O 编码(Zero-One encoding)：设包含 w 个二进制位的数值 $x = b_1 b_2 \cdots b_{w-1} b_w$ ($b_i \in \{0,1\}$ 且 $1 \le i \le w$)，对 x 进行 Z-O 编码，得到的 Z 编码集合 $Z(x)$和 O 编码集合 $O(x)$为

$$Z(x) = \{b_1 b_2 \cdots b_{i-1} 1 \mid b_i = 0 \wedge 1 \le i \le w\} \quad (1)$$

$$O(x) = \{b_1 b_2 \cdots b_i \mid b_i = 1 \wedge 1 \le i \le w\} \quad (2)$$

其中 $b_1 b_2 \cdots b_{w-1} b_w$ 是数值 x 的二进制编码表示，b_1 为最高位，b_w 为最低位。

性质 1　设数值 x 为包含 w 个二进制位，则 $Z(x)$ 和 $O(x)$满足如下性质：

(1) $b_1 b_2 \cdots b_i \in Z(x) \bigcup O(x) \Rightarrow b_i = 1$；

(2) $Z(x) \bigcap O(x) = \varnothing$；

(3) $|Z(x)|+|O(x)|=w$ 。

由定义 1 容易得到性质 1 成立(证略)。

性质 2 若已知数值 x 的 Z 编码集合或 O 编码集合，不难反向逆推出数值 x。

由定义 1 中的 Z-O 编码方法及性质 1 的内容，易得性质 2 成立。例如，若已知包含 4 个二进制位的数值 x 的 Z 编码集合 $Z(x)=\{1\}$，则 x 必定为 0111。

定理 1 对于都包含 w 个二进制位的数值 x 和 y，当且仅当 $O(x)$与 $Z(y)$不相交时，$x>y$ 成立；当且仅当 $O(x)$与 $Z(y)$存在非空交集时，$x\le y$ 成立，即有式(3)和式(4)成立。

$$x>y \Leftrightarrow O(x)\bigcap Z(y)\neq\varnothing \tag{3}$$

$$x\le y \Leftrightarrow O(x)\bigcap Z(y)=\varnothing \tag{4}$$

定理 1 的证明详见文献[9]。由定理 1 可知，数值 x 和 y 的大小比较问题，可以转化为判断 Z 编码集合与 O 编码集合是否存在交集的问题。显然，如果将 Z 编码集合和 O 编码集合中的元素都转换为具体数值，则可以简化集合相交的计算过程。为了保持 Z-O 编码的数值比较特性，对于 Z-O 编码的数值化方法必须满足定义 2 要求。

定义 2 若将任意 Z-O 编码二进制序列 p 的数值化方法记为 N，得到的数值化 Z-O 编码记为 $N(p)$，则对于任意两个 Z-O 编码二进制序列 p_1 和 p_2，该数值化方法应满足：

(1) $p_1=p_2 \Leftrightarrow N(p_1)=N(p_2)$；

(2) $p_1\neq p_2 \Leftrightarrow N(p_1)\neq N(p_2)$。

显然，针对 Z-O 编码的数值化方法并不唯一。本文给出一种简单的数值化方法 N_s：对于数值 x 的任一 Z-O 编码序列 $p=b_1b_2\cdots b_i$，则 p 数值化后得到 $N_s(p)=1b_1b_2\cdots b_i$，即在二进制序列 $b_1b_2\cdots b_i$ 的最高位之前增加“1”。容易证明，该数值化方法 N_s 符合定义 2 要求。

4 基于 Z-O 编码的隐私保护最值查询处理方法

4.1 基本思想

在介绍本文研究工作的基本思想之前，我们首先给出查询单元的形式化定义。

定义 3 查询单元(query cell)：存储节点 S 与其在查询区域内的负责的所有感知节点 $\mathbb{N}=\{s_1,s_2,\cdots,s_n\}$($\mathbb{N}\neq\varnothing$)构成一个查询单元，记为 $\mathrm{qc}_S=(S,\mathbb{N})$。

根据定义 3 的要求，任一查询单元只包含一个存储节点，且至少包含一个感知节点。此外，由于存储节点拥有其负责的感知节点的位置信息，因此，该存储节点能够计算出其所在的查询单元或者不构成查询单元。为了方便讨论，我们假设任一感知节点最多只存在于一个查询单元中。

本文的面向隐私保护的最值查询处理方法的基本思想主要包含如下两个阶段：

(1)**查询指令广播阶段** 首先 Sink 将查询指令 $M_Q=\{t,qa,\mathrm{MAX/MIN}\}$(表示查询满足时刻 t 和区域 qa 要求的最大/最小的感知数据)广播到所有存储节点；存储节点 S 收到 M_Q 后，判断是否构成查询单元 qc_S，若构成，则 S 再将 M_Q 转发至 qc_S 内的所有感知节点，否则不参与查询处理。

(2)**最值查询处理阶段** 在每一个查询单元 $\mathrm{qc}_S=(S,\{s_1,s_2,\cdots,s_n\})$中，$s_i$ 发送其感知数据的 HMAC 数值化 Z-O 编码数据给 S；根据收到的 qc_S 内所有感知节点发来的编码数据，S 计算出 qc_S 内产生最值的节点 s_j，并通知 s_j 发送感知数据；当 s_j 收到 S 的数据请求，s_j 立即加密其感知数据，并将密文发回给 S；而 S 收到密文数据后，构造 qc_S 的局部查询结果 lqr (local query result)并发送给 Sink；最后，Sink 根据各个查询单元发送的 lqr，计算出最终的全局查询结果 gqr(global query result)，并返回给用户。

在查询处理阶段，为了确保感知数据和查询结果的隐私安全性，我们采取如下隐私保护措施：

(1)当 s_i 需要发送其感知数据 d_i 给 S 时，首先利用对称加密方法(如 RC4, RC5, IDEA 等)对 d_i 进行加密处理，生成密钥为 k_i 的加密数据 $(d_i)_{ki}$，s_i 仅与 Sink 共享 k_i，然后将 $(d_i)_{ki}$ 发送给 S；

(2)为了消除 Z-O 编码的可逆推性，在编码过程中增加 HMAC 处理。HMAC 机制的单向性和抗冲突性，将使得感知数据 d_i 经过 HMAC 数值化处理后，即可得到不可逆的 HMAC 数据集合 $\mathrm{HMAC}_g(N_s(Z(d_i)))$和 $\mathrm{HMAC}_g(N_s(O(d_i)))$，其中 g 为所有感知节点共享的 HMAC 密钥。

4.2 具有隐私保护能力的最值查询处理协议 ZOPPM

下面，我们以最大值查询处理为例，给出两层 WSN 中基于 Z-O 编码的隐私保护最值查询处理协议。我们分别从查询单元和 Sink 节点这两个方面，讨论 ZOPPM 协议的工作过程。

设 $\mathrm{lqr}_{\mathrm{HMAC}}$ 为存放 HMAC 数值化 Z-O 编码数据的变量，$\mathrm{lqr}_{\mathrm{node}}$ 为存储感知节点 ID 的变量，$\mathrm{lqr}(S)=\{\mathrm{id},\mathrm{cv}\}$为存储节点 S 所在查询单元的局部查询结果变量，$\mathrm{gqr}=\{\mathrm{id},\mathrm{pv}\}$为存储全局查询结果的变量，其中 id 为感知节点 ID, cv 为密文数据，pv 为明文数据，M_D 为密文传送指令。则具体协议内容如表 1 所示。

由 ZOPPM 协议内容可知，两层 WSN 中的最

表 1 基于 Z-O 编码的隐私保护最值查询处理协议

基于 Z-O 编码的隐私保护最值查询处理协议(ZOPPM)

查询单元：

对于网络中的任一查询单元 $qc_S=(S,\{s_1,s_2,\cdots,s_n\})$，设 s_i 在 t 时间内的本地感知数据的最大值为 d_i，则 qc_S 内的查询处理过程如下：

(1)对于 qc_S 中的任一 $s_i(1\le i\le n)$，s_i 根据 S 消息指令的不同，进行如下处理：

(a)若 s_i 收到 M_Q，则 s_i 首先计算 d_i 的 HMAC 数值化 Z-O 编码集合 $\mathrm{HMAC}_g(N_s(Z(d_i)))$和 $\mathrm{HMAC}_g(N_s(O(d_i)))$，然后将该集合发送给 S。

(b)若 s_i 收到 M_D，则 s_i 利用密钥 k_i，加密 d_i 生成密文$(d_i)_{ki}$，然后再将$(d_i)_{ki}$发送给 S。

(2)对于 qc_S 中的 S, S 根据 Sink 和 $s_i(1\le i\le n)$ 发送的消息类型的不同，进行如下处理：

(a)若 S 收到 Sink 发送的 M_Q，则首先初始化 $\mathrm{lqr}_{\mathrm{HMAC}}=\varnothing$，$\mathrm{lqr}_{\mathrm{node}}=\varnothing$，$\mathrm{lqr}(S)=\varnothing$，并设置$\{s_1,s_2,\cdots,s_n\}$为未处理节点，然后再将 M_Q 广播至 qc_S 内的所有感知节点。

(b) 若 S 收到 s_i 发送的$\{\mathrm{HMAC}_g(N_s(Z(d_i))),\ \mathrm{HMAC}_g(N_s(O(d_i)))\}$，则

(i)判断 $\mathrm{lqr}_{\mathrm{HMAC}}$ 是否为空：若为空，则设置 $\mathrm{lqr}_{\mathrm{HMAC}}=\{\mathrm{HMAC}_g(N_s(Z(d_i))),\mathrm{HMAC}_g(N_s(O(d_i)))\}$, $\mathrm{lqr}_{\mathrm{node}}=s_i$；若不为空，不妨设当前 $\mathrm{lqr}_{\mathrm{HMAC}}=\{\mathrm{HMAC}_g(N_s(Z(d_j))),\mathrm{HMAC}_g(N_s(O(d_j)))\}$，通过判断 $\mathrm{HMAC}_g(N_s(O(d_i)))\cap\mathrm{HMAC}_g(N_s(Z(d_j)))$是否为空，比较 d_i和 d_j大小，如果 $d_i>d_j$，则设置 $\mathrm{lqr}_{\mathrm{HMAC}}=\{\mathrm{HMAC}_g(N_s(Z(d_i))),\mathrm{HMAC}_g(N_s(O(d_i)))\}$, $\mathrm{lqr}_{\mathrm{node}}=s_i$.id。然后，设置 s_i 为已处理节点。

(ii)判断 qc_S 中所有感知节点是否都已处理：若是，则发送 M_D 给感知节点 $\mathrm{lqr}_{\mathrm{node}}$，并等待 $\mathrm{lqr}_{\mathrm{node}}$ 发回密文数据；若否，则继续等待其他感知节点发送数据，并按照步骤(2)中的(b)进行处理。

(c)若 S 收到 s_i 发送的$(d_i)_{ki}$，则设置 $\mathrm{lqr}(S)=\{s_i.\mathrm{id},(d_i)_{ki}\}$，并将 $\mathrm{lqr}(S)$发送给 Sink。

Sink 节点：

假设网络中共有 m 个存储节点$\{S_1,S_2,\cdots,S_m\}$构成查询单元，Sink 按照如下过程执行处理：

(1)将查询指令 M_Q 发送给所有存储节点，初始化 $\mathrm{gqr}=\varnothing$，并设置$\{S_1,S_2,\cdots,S_m\}$为未处理节点。

(2)等待 $S_p(1\le p\le m)$ 发送 $\mathrm{lqr}(S_p)$，并按照如下步骤计算 gqr：

(a)若收到 S_p 发来的 $\mathrm{lqr}(S_p)=\{s_i.\mathrm{id},(d_i)_{ki}\}$，则利用与 s_i 共享的密钥 k_i 解密$(d_i)_{ki}$，得到 d_i。

(b)判断 gqr 是否为空：若为空，则设置 $\mathrm{gqr}=\{s_i.\mathrm{id},d_i\}$；若不为空，则比较 d_i 和 gqr.pv 的大小，如果 $d_i>\mathrm{gqr.pv}$，则设置 $\mathrm{gqr}=\{s_i.\mathrm{id},d_i\}$。然后，设置 S_p 为已处理节点。

(c)判断所有存储节点$\{S_1,S_2,\cdots,S_m\}$是否都已处理：若否，则转步骤(2)，继续等待局部查询结果；若是，则当前 gqr 即为全局查询结果，整个查询处理过程结束。

值查询处理由 Sink，存储节点和感知节点共同协作完成。在查询处理过程中，加密机制确保了感知数据在传输过程中的安全性，而 HMAC 机制的应用，使得恶意节点无法利用 Z-O 编码反向逆推原始感知数据，进而保证了两层 WSN 中感知节点的隐私安全性。

4.3 协议分析

4.3.1 隐私安全性分析　我们主要从感知数据和查询结果角度，分析 ZOPPM 协议的隐私安全性。

(1)感知数据的隐私安全性　在本文基于可信 Sink 节点的前提下，对于任意感知节点 s_i 及其本地感知数据 d_i 而言，仅当查询处理方法能够确保其它感知节点和存储节点都无法获取 d_i 时，d_i 才是隐私安全的。而我们提出的 ZOPPM 协议能够保证感知数据的隐私安全性：

首先，在最值查询处理过程中，s_i 在传输 d_i 时，需首先利用对称加密方法对 d_i 进行加密处理(密钥仅与 Sink 共享)。因此，在无密钥的情况下获取 d_i 的复杂度与破解加密算法相同，从而确保任意传输路径中的其它感知节点或存储节点都无法获取其明文数据。

其次，我们利用 HMAC 机制，对感知节点发送给存储节点的数值化 Z-O 编码集合进行 HMAC 处理，使得存储节点在无需感知数据明文参与的情况下，即可实现各感知数据的大小比较；同时也使得其它能够获得 HMAC 数据的节点，都无法反向逆推其对应的感知数据。

(2)最值查询结果的隐私安全性　最值查询结果由最值数据和最值位置这两方面组成。其中，最值数据同样也是由某个感知节点产生的感知数据，由本节(1)中的讨论可知，最值数据的隐私安全性同样能够保证。这里，我们重点分析 ZOPPM 协议对于最值位置的隐私保护能力。

对于最值查询处理而言，产生最值的感知节点的位置信息同样也需要保护。假设网络中共有 k 个构成查询单元的存储节点，则这些存储节点将产生 k 个局部查询结果(包含局部最值的位置信息)，而最终的全局查询结果在其中产生，并由 Sink 负责计算。可见，全局查询结果的位置信息，隐藏在 k 个局部查询结果中，任一存储节点获得全局查询结果位置的概率仅为 $1/k$。因此，ZOPPM 协议对最值位置的隐私保护满足 k-隐藏(k-indistinguishable)特性，其中 k 为网络中构成查询单元的存储节点的数量。

由上述隐私安全性分析可知，ZOPPM 协议具有较好的隐私安全保护能力，不仅能够确保感知数据的隐私安全，同样能够保护最值查询结果的隐私安全性。

4.3.2 能耗分析　在两层 WSN 中，由于存储节点具有充足的存储空间和能量储备，因此，整个网络的生命周期主要受感知节点的能耗影响。为了尽可能

提高网络的生命周期，我们以降低感知节点的能耗为主要目标。

在本文的最值查询处理方法中，感知节点的总能耗 E_{total} 的计算公式如式(5)所示，

$$E_{\text{total}} = E_{\text{comm}} + E_{\text{comp}} \tag{5}$$

其中 E_{comm} 表示感知节点接收和发送数据所带来的通信能耗，E_{comp} 表示感知节点进行加密和 HMAC 计算所带来的计算能耗。

我们假设两层 WSN 中共有 m 个存储节点，查询区域中感知节点的总数量为 n。假设感知数据的二进制编码长度都为 w，加密数据和 HMAC 数据的长度分别为 l_D 和 l_H；查询指令 M_Q 和密文传送指令 M_D 的长度分别为 l_{M_Q} 和 l_{M_D}；加密和 HMAC 计算的单位能耗分别为 e_d 和 e_h，接收和发送 1 个字节的平均能耗分别为 e_r 和 e_s；感知节点到存储节点的平均路径长度(跳数)为 L，而存储节点由于其较强的通信能力，不妨设其到感知节点仅需 1 跳。

由 ZOPPM 协议可知：每个感知节点收到存储节点发送的 M_Q 和 M_D 各一次；并且，每个包含 w 位的感知数据对应的 Z-O 编码集合将包含 w 个 HMAC 数据；此外，每个查询单元中将有一个感知节点对本地感知数据进行加密，并发送密文数据给存储节点。因此，通信能耗 E_{comm} 为

$$E_{\text{comm}} = n\cdot(l_{M_Q} + l_{M_D})\cdot e_r + (n\cdot w\cdot l_H + m\cdot l_D) \cdot(L\cdot e_s + (L-1)\cdot e_r) \tag{6}$$

此外，计算能耗 E_{comp} 为感知节点进行加密和 HMAC 计算的能耗之和，则有

$$E_{\text{comp}} = m\cdot e_d + n\cdot w\cdot e_h \tag{7}$$

由式(6)，式(7)进而可以得到感知节点的总能耗 E_{total} 的最终计算公式为

$$E_{\text{total}} = n\cdot(l_{M_Q} + l_{M_D})\cdot e_r + (n\cdot w\cdot l_H + m\cdot l_D) \cdot(L\cdot e_s + (L-1)\cdot e_r) + m\cdot e_d + n\cdot w\cdot e_h \tag{8}$$

而文献[7]提出的基于前缀成员验证的两层 WSN 最值查询处理方法(PMV-MQP)，其基本思想为：对于任一感知节点 s_i 的感知数据 $d_i\in[d_{\text{bot}},d_{\text{top}}]$ (d_{bot} 和 d_{top} 分别为感知数据的已知下界和上界)，s_i 针对 d_i 和 $[d_i,d_{\text{top}}]$ 分别计算相应的 HMAC 数值化前缀编码集合 F 和 S，若 d_i 包含 w 个二进制位，则 F 和 S 满足 $|F|=w+1$ 和 $1\le|S|\le 2w-2$，s_i 需要计算的 HMAC 数据总量为 $|F|+|S|\in[w+2, 3w-1]$；同时，s_i 还对 d_i 进行加密处理，然后将 HMAC 数据和加密数据都发送给存储节点，以进行后续的最值查询处理。可见，PMV-MQP 总能耗在理论上存在上限和下限；并且，与本文提出的 ZOPPM 相比，在同等情况下 PMV-MQP 将消耗更多的通信和计算能耗。我们将在第 5 节对 ZOPPM 和 PMV-MQP 的能耗问题作进一步的实验对比分析。

5 实验分析

为了对协议的性能进行比较和分析，本文在文献[13]的仿真器上实现了 ZOPPM 与 PMV-MQP。通过模拟仿真，我们对这两种方法的能耗进行对比试验，其中，PMV-MQP(top)和 PMV-MQP(bot)分别表示 PMV-MQP 的能耗上限和下限；同时，我们还对 ZOPPM 的通信和计算能耗进行对比实验，以评测通信和计算能耗对总能耗的影响情况。本文的实验环境为 Pentium E5700(双核 3.0 GHz)CPU, 3 G 内存；软件环境为 Windows XP 操作系统，Eclipse 和 Matlab；实验数据集为 Intel Lab Data[14]。

本文采用与文献[15]相同的能耗计算方法：无线通信电路发送和接收1 byte的能量消耗公式为 $e_s=\alpha+\gamma\times d^k$ 和 $e_r=\beta$，其中，α 为通信发送电路消耗的能量，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，β 为通信接收电路消耗的能量。我们采用文献[13]的参数：γ =10 pJ/bit/m^2, α = 45 nJ/bit, β =135 nJ/bit, k=2。此外，感知数据长度初始设置为10 bit，加密计算的初始能耗采用文献[8]给出的TelosB中利用RC4对10 bit数据进行加密的能耗数据8.92 μJ，并假设HMAC计算的能耗与加密计算相同。其它参数设置如表2所示。

表2 实验参数

网络覆盖区域	100×100 m^2	实验次数(网络ID)	20
节点通信半径	10 m	密文数据消息	20 byte
感知节点分布	随机分布	HMAC数据消息	20 byte
查询单元	1	查询指令消息长度	24 byte
感知节点数量	480	密文传送指令消息长度	4 byte

在每一组实验中，我们通过在网络覆盖区域中随机分布感知节点，生成20组不同拓扑结构的网络(用不同的网络ID标识)，进而通过计算20组网络的平均能耗值确定最值查询的总能耗。具体实验结果及分析如下：

(1)在实验设置的初始参数条件下，随机生成的20组网络的能耗实验结果如图1所示。

由图1(a)可知，在不同拓扑的网络中，ZOPPM和PMV-MQP的能耗均变化不大，且分布都较为均匀，但ZOPPM的能耗始终低于PMV-MQP。并且，与其能耗下限相比，ZOPPM平均节省约23.03%的

能耗开销。由图1(b)可知，在ZOPPM的总能耗中，计算能耗E_{comp}和通信能耗E_{comm}的变化都不大，但通信能耗占总能耗的绝大部分(约99.96%)。可见，在随机生成的不同拓扑结构的网络中，ZOPPM和PMV-MQP的能耗均变化不大，但ZOPPM的能耗表现明显较优，其能量消耗绝大部分由数据通信产生。

(2)以感知节点数量n为自变量，其它参数保持初始设置不变，得到如图2所示的实验结果。

由图2(a)可知，随着感知节点数量n的增长，感知节点发送的数据消息也增多，导致ZOPPM和PMV-MQP的总能耗都显著增长，其中PMV-MQP的增长幅度较大，这是由于前者的任一查询单元中，仅有一个感知节点需要发送密文数据，而后者所有的感知节点却都需要发送。在本组实验设置下，ZOPPM的总能耗始终少于PMV-MQP，与后者的能耗下限相比，ZOPPM平均节省约23.05%的能耗开销。由图2(b)可知，在ZOPPM的能量消耗中，随着n的增长，E_{comm}有显著增长，虽然E_{comp}也同步增长，但由于其占总能耗的比重非常小(平均约占0.02%)，其增长趋势不明显。

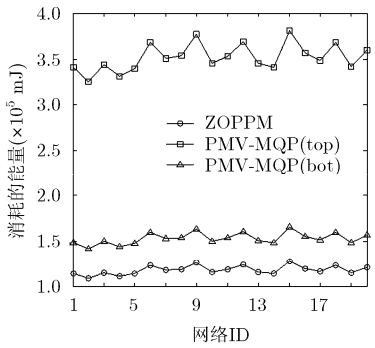
(3)以w为自变量，其它参数保持初始设置不变，得到如图3所示的实验结果。

由图3(a)可知，随着感知数据长度w的增大，ZOPPM和PMV-MQP的总能耗也随之增大，这是由于查询单元中的所有感知节点都需要传送HMAC数据，而w的长度与感知节点传送HMAC数据的数量成正比，因此，两者的总能耗都同步增长，但ZOPPM的总能耗始终少于PMV-MQP，与后者的能耗下限相比，ZOPPM平均节省约17.1%的能耗开销。由图3(b)可知，在ZOPPM消耗的总能量中，通信能耗占总能耗的绝大部分(平均约99.96%)，计算能耗所占比重则非常小。

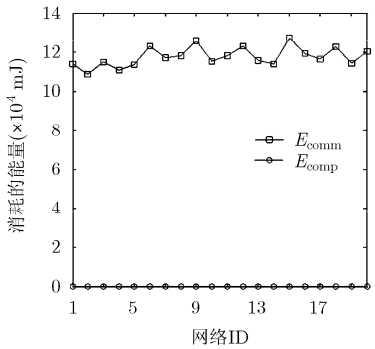
综合上述实验结果及分析可知：本文的ZOPPM的能耗优于文献[7]提出的PMV-MQP，在本文的实验设置条件下，ZOPPM比PMV-MQP的能耗下限平均节省近 20%的能量消耗；并且，在ZOPPM 协议中，收发数据的通信能耗占总能耗的绝大部分，而计算能耗所占的比重较小。

6　总结

数据隐私保护问题是无线传感器网络中具有共性要求的问题，在诸如环境监测、医疗卫生、智能交通、国防军事等各种重要领域都有着迫切的需求，是无线传感器网络研究中的一个热点问题。然而，现有的两层 WSNs 重点关注范围等查询处理方法，对最值查询处理方法的研究相对较少。本文提出了一种基于 Z-O 编码的两层 WSNs 隐私保护最值查询处理协议。在该协议中，感知节点利用 Z-O 编码机制，并结合 Hash 消息身份验证编码方法，对本地感

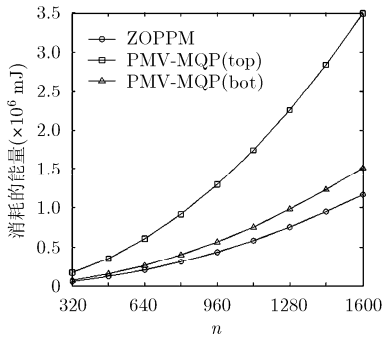


(a) ZOPPM与PMV-MQP的总能耗

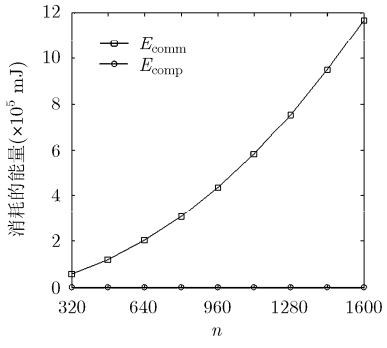


(b) ZOPPM的通信能耗和计算能耗

图1 不同网络拓扑下的能耗实验结果

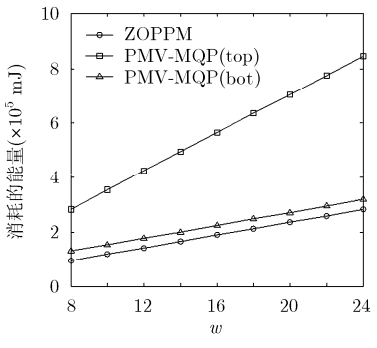


(a) ZOPPM与PMV-MQP的总能耗

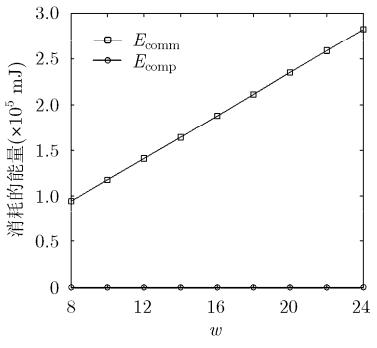


(b) ZOPPM的通信能耗和计算能耗

图2 以n为自变量时的能耗实验结果



(a) ZOPPM与PMV-MQP的总能耗



(b) ZOPPM的通信能耗和计算能耗

图3 以w为自变量时的能耗实验结果

知数据进行 HMAC 数值化 Z-O 编码处理，并发送至存储节点；而存储节点则利用 Z-O 编码的数值比较特性，实现在无需感知数据明文参与下的数值线性关系比较，进而获得所在查询单元中产生局部最值的感知节点，并通知该感知节点计算并传送加密数据，然后构造局部查询结果并发送给 Sink；最终由 Sink 完成最值查询结果的计算，并返回给用户。理论分析和实验结果表明，ZOPPM 协议能够确保感知数据和最值查询结果的隐私安全性，并且其能耗优于现有的方法。

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] Yang D, Misra S, Fang X, *et al*.. Two-tiered constrained relay node placement in wireless sensor networks: computational complexity and efficient approximations[J]. *IEEE Transactions on Mobile Computing*, 2012, 11(8): 1399–1411.

[3] Chen F and Liu A 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.

[4] Sheng B and Li Q. 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] Shi J, Zhang R, and Zhang Y. Secure range queries in tiered sensor networks[C]. 28th IEEE International Conference on Computer Communications, Rio de Janeiro, Brazil, 2009: 945–953.

[6] Shi J, Zhang R, and Zhang Y. A spatiotemporal approach for secure range queries in tiered sensor networks[J]. *IEEE Transactions on Wireless Communications*, 2011, 10(1): 264–273.

[7] Yao Y, Xiong N, Park J H, *et al*.. Privacy-preserving max/min query in two-tiered wireless sensor networks[OL]. Computers & Mathematics with Applications. http://www.sciencedirect.com/science/article/pii/S0898122112001174. 2012, 2.

[8] Groat M M, Hey W, and 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.

[9] Lin H Y and Tzeng W G. 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.

[10] Krawczyk H, Canetti R, and Bellare M. HMAC: keyed-hashing for message authentication[R]. RFC 2104, 1997.

[11] Yao A C. Protocols for secure computations[C]. 23rd Annual Symposium on Foundations of Computer Science, Chicago, Illinois, USA, 1982: 160–164.

[12] Bozovic V, Socek D, Steinwandt R, *et al*.. Multi-authority attribute-based encryption with honest-but-curious central authority[J]. *International Journal of Computer Mathematics*, 2012, 89(3): 268–283.

[13] Coman A, Sander J, and Nascimento M A. Adaptive processing of historical spatial range queries in peer-to-peer sensor networks[J]. *Distributed and Parallel Databases*, 2007, 22(2): 133–163.

[14] Samuel M. Intel lab data[OL]. http://db.csail.mit.edu/labdata/labdata.html. 2004.6.

[15] Coman A, Nascimento A M, and Sander J. A framework for spatio-temporal query processing over wireless sensor networks[C]. Proceeedings of the 1st International Workshop on Data Management for Sensor Networks, Toronto, Canada, 2004: 104–110.

戴 华： 男，1982 年生，博士，讲师，研究方向为传感器网络数据管理与安全、数据库安全.

秦小麟： 男，1953 年生，教授，博士生导师，研究方向为分布式数据管理与安全、空间/时空数据管理.

刘 亮： 男，1985 年生，博士生，研究方向为传感器网络数据管理、大规模数据处理.