软件学报 ISSN 1000-9825, CODEN RUXUEW
*Journal of Software*,2014,25(Suppl.(1)):113−121

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

# 两层传感器网络隐私保护 Skyline 查询协议*

左开中[1,2], 胡 鹏[1,2], 王涛春[1,2], 罗永龙[1,2]

[1](安徽师范大学 数学计算机科学学院,安徽 芜湖 241003)

[2](安徽师范大学 网络与信息安全工程技术研究中心,安徽 芜湖 241003)

通讯作者: 左开中, E-mail: zuokz@mail.ahnu.edu.cn

**摘 要**: 无线传感器网络中隐私保护技术已经成为研究热点,其中隐私保护精确 Skyline 查询协议已成为富有挑战性的研究问题.提出一种两层传感器网络隐私保护 Skyline 查询协议(PPSQ).该协议通过采用 Z-O 编码技术并结合 HMAC 机制,使得存储节点可以在无需感知数据明文的情况下判断出元组的支配关系,从而得出密文查询结果,保护了数据的隐私安全性;并通过辅助计算节点计算的验证码来保证查询结果的完整性.理论分析和实验结果表明,PPSQ 协议能够保证感知数据、查询结果的隐私安全性和查询结果的完整性,且性能优于现有工作.

**关键词**: 物联网;无线传感器网络;隐私保护;Skyline 查询

中文引用格式: 左开中,胡鹏,王涛春,罗永龙.两层传感器网络隐私保护 Skyline 查询协议.软件学报,2014,25(Suppl.(1)):113−121. http://www.jos.org.cn/1000-9825/14013.htm

英文引用格式: Zuo KZ, Hu P, Wang TC, Luo YL. Privacy-Preserving Skyline query protocol in two-tiered sensor networks. Ruan Jian Xue Bao/Journal of Software, 2014,25(Suppl.(1)):113−121 (in Chinese). http://www.jos.org.cn/1000-9825/14013.htm

## Privacy-Preserving Skyline Query Protocol in Two-Tiered Sensor Networks

ZUO Kai-Zhong[1,2], HU Peng[1,2], WANG Tao-Chun[1,2], LUO Yong-Long[1,2]

[1](College of Mathematics and Computer Science, Anhui Normal University, Wuhu 241003, China)

[2](Engineering Technology Research Center of Network and Information Security, Anhui Normal University, Wuhu 241003, China)

Corresponding author: ZUO Kai-Zhong, E-mail: zuokz@mail.ahnu.edu.cn

**Abstract**: Privacy preservation has attracted more and more attentions in wireless sensor networks. It is a challenge to provide precise Skyline query result while preserving data privacy in wireless sensor networks. This paper proposes a privacy-preserving Skyline query protocol in two-tiered sensor networks (PPSQ). Using Z-O encoding and hash-based message authentication code mechanism, this protocol to allows storage node to attain tuple relations of domination judgment without the sensory data plaintext, and therefore protects privacy of sensory data. In addition, assisted computing node calculates the verification code to ensure the integrity of the query result. Theoretical analysis and experimental results show that the PPSQ can guarantee the privacy of sensory data and the integrity of query result, and it also has better performance than the previous work in skyline query processing.

**Key words**: Internet of things; wireless sensor network; privacy preserving; Skyline query

无线传感器网络作为物联网感知层的重要组成部分,已被大量部署和应用于医疗卫生、森林防火、国防军事等领域[1].本文主要讨论两层传感器网络[2],它由资源充足的存储节点作为中间层,下层是资源受限的感知节点,上层为 Sink 节点.感知节点收集数据并将其存储于存储节点,存储节点响应 Sink 节点的查询等任务.由于两层传感器网络的拓扑结构简单、稳定且存储节点资源丰富,从而有效减少了感知节点向 Sink 节点传输数据的能耗而延长了网络生命周期,能更高效地响应 Sink 节点的查询请求,因而获得了广泛关注与研究.

目前,针对两层传感器网络中隐私保护数据查询协议的研究,主要集中在范围查询[3−6]、最值查询[7,8]和

* 基金项目: 国家自然科学基金(61370050, 61402014)
收稿时间: 2014-05-10; 定稿时间: 2014-08-26

Top-$k$ 查询[9−11],而文献[12,13]对 Skyline 查询的研究旨在关注如何提高执行效率和减少通信开销,却很少涉及隐私保护问题的研究.文献[14]针对多维数据的安全查询提出了基于桶模式的安全 Skyline 查询协议(SSQ),但在该协议中,若一个感知节点被俘获,攻击者就可以获得所有感知节点的分桶方案及其标签与桶的对应关系,从而获取数据的大致分布,推证近似查询结果.因此,该方案对感知节点的隐私数据保护和查询结果的隐私保护程度有限.当然直观上,解决该问题还可用 End-to-End 的加密机制,即感知节点将隐私数据加密存储于存储节点,然后由存储节点将密文发送给 Sink,由 Sink 解密再计算出最后的查询结果,本文称此方案为 NAIVE 协议.但在 NAIVE 协议中,存储节点只拥有隐私数据密文,无法进行网内处理,致使大量的密文数据发送给 Sink,造成占用大量低速率、高成本的按需无线链接通信带宽,这不仅增加了网络的使用成本,也导致了计算查询结果的延迟.

为了保护数据的隐私安全性和降低存储节点与 Sink 间的通信开销,本文设计了一个两层传感器网络隐私保护 Skyline 查询协议.该协议中存储节点在无需获知明文的情形下能够对感知数据的密文进行支配关系的判断,得到的密文 Skyline 查询结果,并最终由 Sink 解密得到隐私数据的查询结果和完整性验证.所以,即使存储节点被捕获,攻击者也无法获知感知节点的隐私数据.最后,理论分析和实验验证了 PPSQ 协议的正确性和有效性.

## 1 相关知识

传感器网络中具有多目标优化的 Skyline 查询算子在多个领域具有重大的应用价值,如:在森林防火中,感知节点监测周围环境的温度和风速[15].那些具有高温度、高风速或二者兼有的地区会成为潜在的火灾发生区域,森林工作人员应给予更多的关注.针对温度和风速,应用 Skyline 查询就可以很好地识别灾情易发区域.因此两维数据空间上的隐私保护 Skyline 查询是本文的研究重点.下面给出关于 Skyline 查询以及基于 Z-O 编码的元组支配关系判断的相关知识.文中用二元组 $(x,y)$ 表示感知节点采集的一组数据,而元组的属性可以是温度、湿度、风速等.记 $p=(x,y)$,则用 $p.x$ 表示元组 $p$ 在第 $x$ 维的属性值.

### 1.1 Skyline查询

Skyline 查询涉及元组支配关系的比较,不失一般性,本文中对于元组 $p,q$ 属性值优劣的判断用属性“越小”表示“越优”.用符号“$\succ$”和“$\prec$”表示支配与被支配关系.

**定义 1**. 对于元组 $p,q$,若 $p$ 至少在某个属性上比 $q$ 优,其他属性上都不比 $q$ 劣,则称元组 $p$ 支配元组 $q$,记为 $p\succ q$ 或 $q\prec p$.

**定义 2**. 针对给定元组集合 $D$ 的查询 $Q$,如果该查询发现了 $D$ 的一个最大子集 $SP$,并且 $SP$ 中的任意一个元组 $p$ 都不受 $D$ 中任意一个元组的支配,则称该查询为 Skyline 查询,$SP$ 称为 Skyline 查询的结果集.

### 1.2 支配关系的判断

根据文献[8,16],数值的 Z 编码集合和 O 编码集合分别记为 $Z(x)$,$O(x)$,数值化方法记为 $N(x)$,哈希消息认证机制为 $HMAC(x)$.下面给出两元组支配关系的判定定理及其证明.

**定理 1**. 对于任意元组 $p,q$,其 $x,y$ 属性值都经过 Z-O 编码、数值化和 HMAC 处理,则有下面关系成立:

$$\begin{aligned}p\succ q\Leftrightarrow{}&(HMAC(N(Z(p.x)))\cap HMAC(N(O(q.x)))\neq\varnothing\wedge HMAC(N(O(p.y)))\cap HMAC(N(Z(q.y)))=\varnothing)\\&\vee(HMAC(N(O(p.x)))\cap HMAC(N(Z(q.x)))=\varnothing\wedge HMAC(N(Z(p.y)))\cap HMAC(N(O(q.y)))\neq\varnothing)\end{aligned}\tag{1}$$

$$\begin{aligned}p\prec q\Leftrightarrow{}&(HMAC(N(O(p.x)))\cap HMAC(N(Z(q.x)))\neq\varnothing\wedge HMAC(N(Z(p.y)))\cap HMAC(N(O(q.y)))=\varnothing)\\&\vee(HMAC(N(Z(p.x)))\cap HMAC(N(O(q.x)))=\varnothing\wedge HMAC(N(O(p.y)))\cap HMAC(N(Z(q.y)))\neq\varnothing)\end{aligned}\tag{2}$$

证明:由文献[16]可知,数值 $u,v$ 的大小比较可转化为 Z 编码集合与 O 编码集合是否存在交集的问题,并有:

$$u>v\Leftrightarrow O(u)\cap Z(v)\neq\varnothing\tag{3}$$

$$u\leqslant v\Leftrightarrow O(u)\cap Z(v)=\varnothing\tag{4}$$

为简化集合相交的判定,用文献[8]的数值化方法,将 $u,v$ 的 Z 编码与 O 编码数值化得到集合 $N(O(u))$ 与 $N(Z(u))$.同时为消除 Z-O 编码的逆推性,用具有单向性和抗冲突性的 HMAC 对数值化后数据进行处理.因此有:

$$u>v\Leftrightarrow HMAC(N(O(u)))\cap HMAC(N(Z(v)))\neq\varnothing\tag{5}$$

$$u \leqslant v \Leftrightarrow HMAC(N(O(u))) \cap HMAC(N(Z(v))) = \varnothing \quad (6)$$

那么对于元组 $p,q$ 可知:若 $p \succ q \Leftrightarrow ((p.x < q.x) \wedge (p.y \leqslant q.y)) \vee ((p.x \leqslant q.x) \wedge (p.y < q.y))$, 根据以上分析可知,定理 1 的式(1)是正确的;同理可知定理 1 的式(2)也正确.综上定理 1 成立. □

## 2 模 型

### 2.1 网络模型

两层传感器网络拓扑图与文献[9]相同,如图 1 所示.它由 3 类节点构成:底层的感知节点、中间层的高资源节点和上层的 Sink 节点.中间层的高资源节点分为存储节点和辅助计算节点,存储节点在能量、存储、计算方面都很充裕,它响应 Sink 查询指令;辅助计算节点用于辅助存储节点进行网内数据计算处理.一个存储节点、一个辅助计算节点和多个感知节点构成查询单元.为方便说明,假定一个感知节点最多在一个查询单元内.感知节点是资源受限的廉价设备,负责收集感知区域内的数据并按一定的周期将数据存储于存储节点.Sink 作为网络对用户的接口,它解释用户的各种查询指令并将查询指令发送给指定查询单元的存储节点.

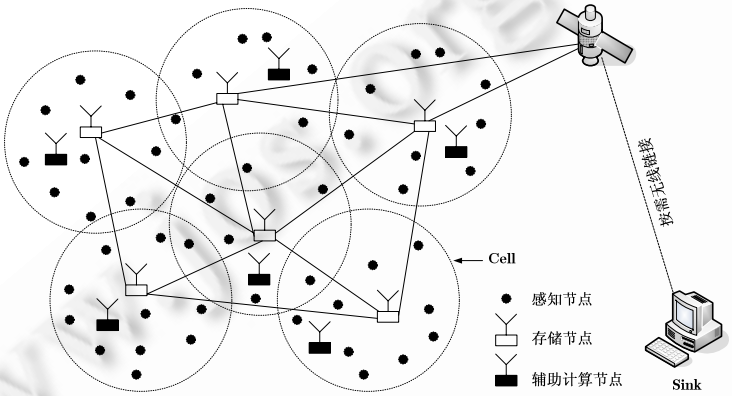


Fig.1 Two-Tiered sensor networks architecture
图1 两层传感器网络示意图

### 2.2 查询模型

文中查询指令中的参数分别是查询单元 cell、查询周期 epoch、查询类型 demo,查询指令 $Q$ 形式化表示为

$$Q = (cell = C) \wedge (epoch = t) \wedge (demo = Skyline) \quad (7)$$

该指令表示对查询单元 $C$ 中所有的感知节点在查询周期 $t$ 内所感知的数据进行 Skyline 查询.

### 2.3 攻击模型和安全目标

相对于感知节点上的少量感知数据,攻击者对存储大量感知数据的存储节点更感兴趣,一旦存储节点被攻击者捕获就能获得大量隐私数据,并能得到部分查询结果.所以,本文假定攻击者想获知感知节点收集的敏感数据来破坏数据的隐私.与文献[11]类似,假定 Sink 和感知节点可信,同时辅助计算节点也可信,不会被攻击.

在上述假设情况下,隐私保护 Skyline 查询协议的安全目标是:

(1) 感知数据的明文只有相应的感知节点和 Sink 可知,其他感知节点、辅助计算节点和存储节点都无法获知;

(2) 最终的 Skyline 查询结果只有 Sink 拥有,其他节点都无法获得;

(3) Sink 有能力鉴别出查询结果是否被篡改和伪造,即能够保证查询结果的完整性和真实性.

## 3 PPSQ 协议

文中只针对一个查询单元 $C$ 进行 Skyline 查询,$C$ 中的存储节点为 $CH$,辅助计算节点为 $CA$.查询单元 $C$ 中

有 $n$ 个感知节点,每个感知节点 $S_i$ 都与 Sink 共享密钥 $k_i$.此外,还存在辅助计算节点 $CA$ 与 Sink 的共享密钥 $k_{ca}$,一个所有节点共享的 HMAC 密钥 $g$.同时,设感知节点 $S_i$ 的标识符就是 $S_i$, $d_{it}$ 为 $S_i$ 在查询周期 $t$ 内采集的隐私数据,$CSP$ 为查询单元 $C$ 中密文数据的 Skyline 查询结果集.

整个隐私保护 Skyline 查询过程由感知节点、存储节点、辅助计算节点和 Sink 共同协作完成.首先 Sink 发送查询命令给存储节点,存储节点收到后广播该查询命令给本查询单元内的所有感知节点,感知节点收到查询命令后即对隐私数据处理并上传到存储节点和辅助计算节点,之后存储节点根据定理 1 计算密文数据的 Skyline 查询结果集,并将查询结果和辅助计算节点计算的验证码发送给 Sink,最后由 Sink 解密得到隐私数据的 Skyline 查询结果并验证查询结果的完整性.具体的协议执行过程见表 1.

**Table 1** Privacy-Preserving Skyline query protocol (PPSQ)

**表 1** 隐私保护 Skyline 查询协议(PPSQ)

| |
|---|
| **Step1**: Sink 将查询命令 $Q$ 发给查询单元 $C$ 的存储节点 $CH$. |
| **Step2**: 存储节点 $CH$ 收到查询命令 $Q$ 后,向 $C$ 中所有感知节点广播查询命令 $Q$. |
| **Step3**: $C$ 中的感知节点 $S_i(1\leqslant i\leqslant n)$ 收到查询命令 $Q$ 后,则进行如下处理:<br>(1) 感知节点 $S_i$ 对查询周期 $t$ 内的隐私数据 $d_{it}$ 的每个 $\alpha(\alpha\in\{x,y\})$ 属性值进行 Z-O 编码、数值化和 HMAC 处理,得到集合 $HMAC_g(N(Z(d_{it}.\alpha)))$ 和 $HMAC_g(N(O(d_{it}.\alpha)))$;<br>(2) 感知节点 $S_i$ 用密钥 $k_i$ 加密 $d_{it}$ 得到密文 $(d_{it})_{k_i}$;<br>(3) 感知节点 $S_i$ 发送消息给 $CH$,$CA$,消息形式如下:<br>$$S_i\rightarrow CH,CA:\left\langle S_i,(d_{it})_{k_i},\{HMAC_g(N(O(d_{it}.\alpha))),HMAC_g(N(Z(d_{it}.\alpha)))\},\alpha\in\{x,y\}\right\rangle.$$ |
| **Step4**: 辅助计算节点 $CA$ 收到 $C$ 中全部感知节点的消息后,进行如下处理:<br>(1) $CA$ 根据感知节点 $S_i(1\leqslant i\leqslant n)$ 的数据 $d_{it}$ 经 HMAC 数值化处理的 Z-O 编码 $HMAC_g(N(Z(d_{it}.\alpha)))$ 和 $HMAC_g(N(O(d_{it}.\alpha)))$, 再结合定理 1 和定义 2,在不需要隐私数据 $d_{it}$ 明文的情况下判定出 $d_{it}$ 是否属于 Skyline 查询结果集 $SP$,若式子 $d_{ij}\in SP$ 成立,则将 $HMAC_g(N(Z(d_{it}.\alpha)))$ 放入集合Δ;<br>(2) $CA$ 重复进行步骤(2),直到每个感知节点 $S_i$ 的 $HMAC_g(N(Z(d_{it}.\alpha)))$ 被处理为止;<br>(3) $CA$ 用密钥 $k_{ca}$ 对Δ中的 HMAC 数据进行级联求哈希,得到验证码 $\delta=HMAC_{k_{ca}}(\|HMAC_g(N(Z(d_{it}.\alpha)))$, 并将其发送给 $CH$. |
| **Step5**: 存储节点 $CH$ 收到 $C$ 中全部感知节点和辅助计算机节点 $CA$ 的消息后,进行如下处理:<br>(1) $CH$ 根据感知节点 $S_i(1\leqslant i\leqslant n)$ 的数据 $d_{it}$ 经 HMAC 数值化处理的 Z-O 编码 $HMAC_g(N(Z(d_{it}.\alpha)))$ 和 $HMAC_g(N(O(d_{it}.\alpha)))$, 再结合定理 1 和定义 2,在不需要隐私数据 $d_{it}$ 明文的情况下判定 $d_{it}$ 是否属于 Skyline 查询结果集 $SP$,若 $d_{ij}\in SP$, 则将 $(d_{it})_{k_i}$ 和感知节点的标识符 $S_i$ 作为一个元组存入 $CSP$;<br>(2) $CH$ 重复进行步骤(2),直到每个感知节点 $S_i$ 的密文 $(d_{it})_{k_i}$ 被处理为止;<br>(3) $CH$ 将密文数据的 Skyline 查询结果集 $CSP$ 和验证码$\delta$发送给 Sink. |
| **Step6**: Sink 收到 $CH$ 的响应后,获得查询结果并验证查询结果的完整性,具体如下:.<br>(1) Sink 用与感知节点 $S_i$ 的共享密钥 $k_i$ 解密密文 $(d_{it})_{k_i}$ (其中 $(d_{it})_{k_i}\in CSP$), 得到 Skyline 查询结果集 $SP$,并通过密钥 $k_i$ 和 $g$ 构造 HMAC 数值化 Z 编码,进而用 $k_{ca}$ 构造验证码$\delta'$;<br>(2) 若$\delta$与$\delta'$相等,则查询结果是完整的,接受查询结果;否则丢弃查询结果. |

## 4 协议分析

### 4.1 协议正确性分析

**定理 2**. Sink 针对查询单元 $C$ 运用 PPSQ 协议得到的输出集是精确 Skyline 查询结果集 $SP$.

证明:对 $\forall S\in C$, 感知节点 $S_i$ 将隐私数据 $d_{it}$ 用 $k_i$ 加密得到密文 $(d_{it})_{k_i}$. 而且 $S_i$ 将隐私数据 $d_{it}$ 的集合 $HMAC_g(N(Z(d_{it}.\alpha)))$ 和 $HMAC_g(N(O(d_{it}.\alpha)))$ 都发送给存储节点 $CH$.存储节点 $CH$ 得到查询单元中所有感知节点上传的数据后,运用定理 1 对所有 $S_i(S_i\in C)$ 的隐私数据 $d_{it}$ 的密文 $(d_{it})_{k_i}$ 进行支配关系的判断,进而计算出查

询单元 $C$ 中密文数据的 Skyline 查询结果集 $CSP$.由定理 1 的正确性可知,存储节点 $CH$ 在执行协议过程中能得到精确 $CSP$.最后 Sink 用共享密钥解密 $CSP$,得到精确的 Skyline 查询结果集 $SP$. □

### 4.2 隐私安全性分析

**定理 3**. PPSQ 协议正确完成 Skyline 查询过程中,感知节点发送的隐私数据是安全的.

证明:由于 Sink 可信,对任意感知节点 $S_i$ 的隐私数据 $d_{it}$ 被上传至存储节点之前,先用与 Sink 共享的密钥 $k_i$ 加密 $d_{it}$ 得到 $(d_{it})_{k_i}$.在无密钥 $k_i$ 的前提下,存储节点和其他感知节点即便获取了 $(d_{it})_{k_i}$ 也无法获得数据明文 $d_{it}$.感知节点 $S_i$ 对 $d_{it}$ 的 $x$,$y$ 属性值进行了 Z-O 编码、数值化和 HMAC 处理,而且 HMAC 具有单向性,使得存储节点和其他感知节点无法反推 $S_i$ 的隐私数据.综上,在 PPSQ 协议执行的过程中,感知节点发送的隐私数据是安全的. □

**定理 4**. PPSQ 协议正确完成 Skyline 查询过程中,存储节点对感知节点的隐私数据处理是安全的.

证明:存储节点获得所有感知节点隐私数据的密文后,需要对密文进行 Skyline 查询处理.然而在密文数据支配关系的判断过程中,存储节点不需要明文数据,而是根据数据 Z-O 编码的比较特性,使用定理 1 就能判断密文的支配关系.再由定理 2 可知,在 PPSQ 协议正确执行的过程中,存储节点对感知节点的隐私数据处理是安全的.证毕. □

### 4.3 查询完整性分析

**定理 5**. PPSQ 协议正确完成 Skyline 查询过程中,Sink 能够验证查询结果的完整性.

证明:Sink 收到存储节点返回的数据后,需要解密 $CSP$ 中的数据,并通过密钥 $k_i$,$g$ 和 $k_{ca}$ 构造验证码 $\delta'$,通过判断等式 $\delta'=\delta$ 是否成立来验证查询结果的完整性.由于辅助计算节点 $CA$ 可信,而且从表 1 可知 $\delta = HMAC_{k_{ca}}(\| HMAC_g(N(Z(d_{it}.\alpha))$,在无密钥 $k_{ca}$ 的前提下,存储节点无法构造出合法的验证码 $\delta$.综上,在 PPSQ 协议执行的过程中,Sink 能够验证查询结果的完整性. □

### 4.4 能耗与通信开销分析

本节主要讨论感知节点的能耗以及存储节点与 Sink 间的通信开销.为方便说明,假设查询指令长度为 $l_Q$ bits,感知节点的身份标识与采集的环境属性数据的二进制编码长度都为 $w$bits,加密元组的能耗和加密后的长度为 $E_d$,$l_D$ bits,HMAC 处理元组属性值的能耗和处理后长度为 $E_h$,$l_H$ bits,发送和接收 1bit 的能耗为 $E_s$ 和 $E_r$.查询单元内感知节点到存储节点的平均跳数为 $L$,而存储节点通信能力强,不妨设其到感知节点为 1 跳.令感知节点的能耗为 $E$,存储节点与 Sink 间的通信开销为 $C_{storage}$.因此有:

$$E=(w+l_D+2\cdot w\cdot l_H)\cdot L\cdot E_s+l_Q\cdot E_r+E_d+2\cdot w\cdot E_h \tag{8}$$

$$C_{storage}=(l_D+w)\cdot|CSP|+l_H \tag{9}$$

从式(8)、式(9)可知,在 PPSQ 中,感知节点的能耗主要用于加密、HMAC、发送和接收消息.感知节点向存储节点发送密文的同时,需发送 HMAC 数据.但相比于广播机制的 SSQ 协议,在大量感知节点的环境中,PPSQ 中感知节点的能耗较低.在存储节点与 Sink 间的通信开销上,由于 PPSQ 中存储节点对所有感知数据进行了网内处理,大量减少了上传给 Sink 的数据、降低了带宽占用率和网络使用成本,因此 PPSQ 优于 NAIVE 和 SSQ 协议.

## 5 实验分析

本节主要从感知节点能耗和存储节点与 Sink 间的平均通信开销方面来评估 PPSQ,SSQ 和 NAIVE 协议.实验环境为 Intel Core(TM)(双核 2.83GHz)CPU,2G 内存;软件为 Windows XP 操作系统,并在 Matlab 软件实现 PPSQ,SSQ 和 NAIVE 协议,SSQ 中每个属性的桶划分使用文献[17]的方案.实验中测试数据选自 Intel Lab[18].

实验中感知节点对数据的加密算法用 DES,HMAC 处理使用 MD5 算法和 128 位的共享密钥.根据文献[19]能耗计算的方法: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,$\alpha$为通信发送

电路消耗的能量,$\gamma$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,$\beta$为通信接收电路消耗的能量.并采用文献[20]的参数: $\alpha$=45nJ/bit,$\gamma$=10pJ/bit/m$^2$,$\beta$=135nJ/bit,$k$=2.此外,假设感知节点通信半径为 10m,而且能够在通信半径内到达存储节点,DES 对元组加密能耗和 HMAC 计算能耗都为文献[21]中给出的 8.92μJ,查询命令的长度为 24bit.

### 5.1 感知节点能耗对比实验

本组实验用于比较 PPSQ、SSQ 和 NAIVE 协议中感知节点的能耗.具体实验结果分析如下.

(1) 当 $n$ 为定值时,感知节点在执行 3 个协议时的能耗如图 2 所示.从图 2 可知,PPSQ 中感知节点能耗略高于 NAIVE,而明显低于 SSQ.这是由于 PPSQ 中,感知节点要进行加密和 HMAC 处理,增加了计算能耗;感知节点发送额外的 HMAC 数据,而且 HMAC 数据随着 $w$ 的增大而增加,所以增加了发送数据的能耗.因此 PPSQ 中感知节点的能耗高于 NAIVE,平均高 20.82%的能耗.而在 SSQ 中感知节点增加了广播机制来保证结果的完整性,致使感知节点接收数据的能耗增加,造成感知节点的能耗高于 PPSQ.所以在保证查询结果正确性、感知节点数据隐私性和查询完整性的前提下,PPSQ 相比于 SSQ 具有更低的通信能耗,而且平均降低约 94.08%.

(2) 当 $w$ 为定值时,感知节点在执行 3 个协议时的能耗如图 3 所示.由图 3 可知,随着 $n$ 的增加,PPSQ 和 NAIVE 中感知节点能耗基本不变,但 PPSQ 中感知节点需发送额外的 HMAC 数据使其能耗高于 NAIVE 协议 16.51%.而广播机制使得 SSQ 中感知节点能耗随着 $n$ 的增加而增大,故 PPSQ 中感知节点能耗少于 SSQ,并且平均降低约 95.89%.

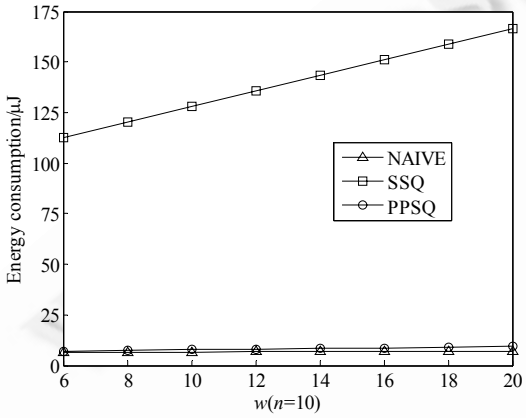


Fig.2 $w$ effect on energy consumption of sensor nodes

图2 $w$对感知节点能耗的影响

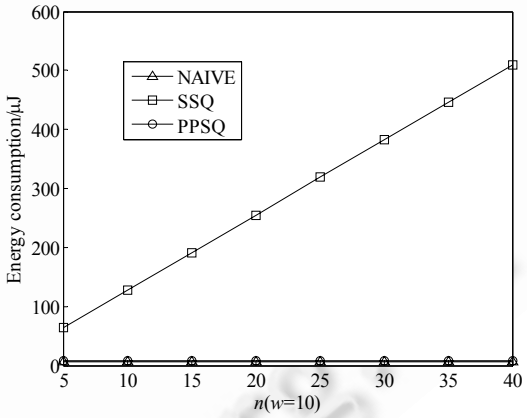


Fig.3 $n$ effect on energy consumption of sensor nodes

图3 $n$对感知节点能耗的影响

### 5.2 存储节点与Sink间通信开销对比实验

在本组实验中,各感知节点的数据随机地选自测试数据集,每组实验进行 50 次,根据 50 次实验的平均通信开销来评估 PPSQ,SSQ 和 NAIVE 协议在存储节点与 Sink 节点间通信开销方面的性能.

(1) 当 $w$ 为定值时,存储节点在执行 3 种不同协议时与 Sink 节点间的通信开销如图 4 所示.随着感知节点数目的增加,存储节点接收的密文也增多,存储节点与 Sink 间的通信开销逐渐增大.但在 PPSQ 协议中,存储节点的通信开销上升趋势明显比 SSQ 和 NAIVE 协议缓慢,这是因为存储节点在密文上执行了 Skyline 查询处理,可过滤不属于 Skyline 查询结果的密文数据,从而减少了存储节点的通信开销;NAIVE 协议中存储节点并没有过滤密文数据,存储节点发送所有感知节点的密文给 Sink,故通信开销较大;虽然在 SSQ 协议中,存储节点也能过滤不属于 Skyline 查询结果的密文数据,但是基于桶模式只能过滤部分不属于 Skyline 查询结果的密文数据,存储节点的通信开销高于 PPSQ 协议.从图 4 可知,在保证查询结果正确性、感知节点数据隐私性和查询完整性的

前提下,PPSQ 相比于 NAIVE 和 SSQ 协议分别平均降低约 67.04%和 69.23%的通信开销.

(2) 当 $n$ 为定值时,存储节点在执行 3 种不同协议时与 Sink 节点间的通信开销如图 5 所示.PPSQ 协议中存储节点与 Sink 间的通信开销明显低于 SSQ 和 NAIVE 协议.在 PPSQ 协议中,虽然 $w$ 与 HMAC 数据量成正比,但存储节点并不发送 HMAC 数据,所以对存储节点与 Sink 间的通信开销影响不大.与其他两个协议相比,PPSQ 之所以有较低的通信开销,主要是因为存储节点执行了查询处理而过滤了全部非 Skyline 查询结果的密文数据而减少了通信开销.从图 5 可知,在保证查询结果正确性、感知节点数据隐私性和查询完整性的前提下,PPSQ 相比于 NAIVE 和 SSQ 协议分别平均降低约 58.80%和 63.95%的通信开销.

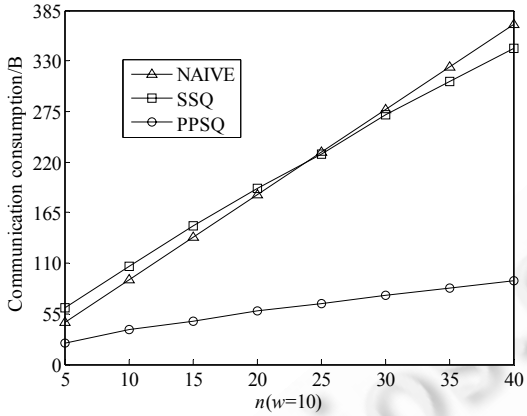


Fig.4 $n$ effect on average communication overhead of storage node

图4 $n$对存储节点平均通信开销的影响

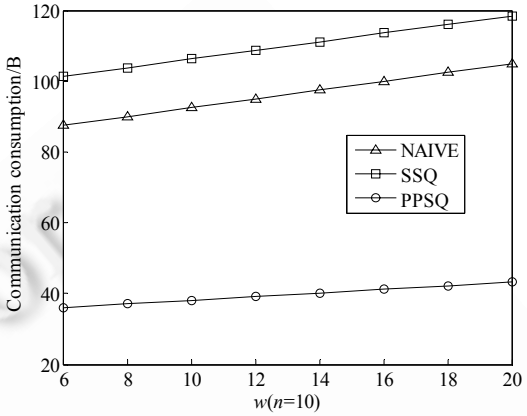


Fig.5 $w$ effect on average communication overhead of storage node

图5 $w$对存储节点平均通信开销的影响

综合上述实验结果及分析可知:在保证查询结果正确性、感知节点数据隐私性和查询完整性的前提下,本文针对两层传感器网络所设计的隐私保护 Skyline 查询协议中感知节点能耗略高与 NAIVE 协议,但低于 SSQ 协议;而且与 NAIVE 协议和 SSQ 协议相比,PPSQ 协议中存储节点与 Sink 节点间具有较低的通信开销.因此与现有的研究工作 SSQ 协议相比,本文的 PPSQ 协议具有更优的性能.

## 6 结 语

本文针对两层传感器网络中 Skyline 查询的隐私保护问题,在综合分析现有方案的基础上,设计了一种隐私保护 Skyline 查询协议:PPSQ,该协议能够在获得正确查询的同时有效地保护数据的隐私和查询结果的完整性.为了保护数据隐私以及能够使得存储节点获得密文 Skyline 查询结果集,感知节点在发送数据密文给存储节点的同时,也要发送该数据的 HMAC 数值化 Z-O 编码数据.存储节点能够根据 Z-O 编码数值比较特性获得 Skyline 查询结果的密文,从而保证了数据的隐私安全,也减少了存储节点与 Sink 间的通信开销.在完整性方面,通过辅助节点计算验证码使得 Sink 能够验证查询结果的完整性.最后协议分析和真实数据集的实验结果表明,与同类协议相比,PPSQ 具有更好的隐私保护性和较低的通信开销.

**致谢** 在此,特别感谢安徽师范大学网络与信息安全工程技术研究中心的老师和同学们对本文工作的帮助和支持.

**References**:

[1] Akyildiz I, Su W, Sankarasubramaniam Y, Cayirci E. A survey on sensor networks. IEEE Communications Magazine, 2002,40(8): 102−114. [doi: 10.1109/MCOM.2002.1024422]

[2] Gnawali O, Jang KY, Paek J, Vaeira M, Govindan R, Greenstein B, Joki A, Estrin D, Kohler E. The tenet architecture for tiered sensor networks. In: Proc. of the 4th ACM Conf. on Embedded Networked Sensor Systems. Boulder: ACM Press, 2006. 153−166. [doi: 10.1145/1182807.1182823]

[3] Chen F, Liu A X. SafeQ: Secure and efficient query processing in sensor networks. In: Proc. of the 29th IEEE Int'l Conf. on Computer Communications. San Diego: IEEE Press, 2010. 1−9. [doi: 10.1109/INFCOM.2010.5462094]

[4] Sheng B, Li Q. Verifiable privacy-preserving range query in two-tiered sensor networks. In: Proc. of the 27th IEEE Int'l Conf. on Computer Communications. Phoenix: IEEE Press, 2008. 46−50. [doi: 10.1109/INFOCOM.2008.18]

[5] Shi J, Zhang R, Zhang Y. Secure range queries in tiered sensor networks. In: Proc. of the 28th IEEE Int'l Conf. on Computer Communications. Rio de Janeiro: IEEE Press, 2009. 945−953. [doi: 10.1109/INFCOM.2009.5062005]

[6] Shi J, Zhang R, Zhang Y. A spatiotemporal approach for secure range queries in tiered sensor networks. IEEE Trans. on Wireless Communications, 2011,10(1):264−273. [doi: 10.1109/TWC.2010.102210.100548]

[7] Yao Y, Xiong N, Park JH, Ma L, Liu J. Privacy-Preserving max/min query in two-tiered wireless sensor networks. Computers & Mathematics with Applications, 2013,65(9):1318−1325. [doi: 10.1016/j.camwa.2012.02.003]

[8] Dai H, Qin X, Liu L, Ji Y, Fu X, Sun Y. Z-O encoding based privacy-preserving max/min query protocol in two-tiered wireless sensor networks. Journal of Electronics & Information Technology (in Chinese with English abstract), 2013,35(4):970−976. [doi: 10.3724/SP.J.1146.2012.00940]

[9] Fan Y, Chen H. Verifiable privacy-preserving top-*k* query protocol in two-tiered sensor networks. Chinese Journal of Computers, 2012,35(3):423−433 (in Chinese with English abstract). [doi: 10.3724/SP.J.1016.2012.00423]

[10] Li R, Lin Y, Yi Y, Xiong S, Ye S. A secure top-*k* query protocol in two-tiered sensor networks. Journal of Computer Research and Development, 2012,49(9):1947−1958 (in Chinese with English abstract).

[11] Yao Y, Ma L, Liu J. Privacy-Preserving top-*k* query in two-tiered wireless sensor networks. Int'l Journal of Advancements in Computing Technology, 2012,4(6):226−235. [doi: 10.4156/ijact.vol4.issue6.27]

[12] Chen B, Liang W, Yu JX. Energy-Efficient Skyline query optimization in wireless sensor networks. Wireless Networks, 2012, 18(8):985−1004. [doi: 10.1007/s11276-012-0446-z]

[13] Roh YJ, Song I, Jeon JH, Woo KG, Kim MH. Energy-Efficient two-dimensional Skyline query processing in wireless sensor networks. In: Proc. of the 10th Annual IEEE-CCNC Smart Spaces and Sensor Networks. Las Vegas: IEEE Press, 2013. 294−301. [doi: 10.1109/CCNC.2013.6488461]

[14] Yu CM, Tson YT, Lu CS, Kuo SY. Practical and secure multidimensional queries in tiered sensor networks. IEEE Trans. on Information Forensics and Security, 2011,6(2):241−255.

[15] Pripuzic K, Belani H, Vukovic M. Early forest fire detection with sensor networks: Sliding window Skylines approach. In: Proc. of the 12th Int'l Conf. on Knowledge-Based Intelligent Information and Engineering Systems. Zagreb: Springer-Verlag, 2008. 725−732. [doi: 10.1007/978-3-540-85563-7_91]

[16] Lin HY, Tzeng WG. An efficient solution to the millionaires' problem based on homomorphic encryption. In: Proc. of the 3rd Int'l Conf. on Applied Cryptography and Networks Security. New York: Springer-Verlag, 2005. 97−134. [doi: 10.1007/11496137_31]

[17] Dou Y, Huang H, Wang R, Qin X. Secure range query in two-tiered wireless sensor networks. Journal of Computer Research and Development, 2013,50(6):1253−1266 (in Chinese with English abstract).

[18] Bodik P, Hong W, Guestrin C, Madden S, Paskin M, Thibaux R. Intel Lab Data. 2004. http://db.csail.mit.edu/labdata/labdata.html

[19] Coman A, Nascimento MA, Sander J. A framework for spatio-temporal query processing over wireless sensor networks. In: Proc. of the 1st Int'l Workshop on Data Management for Sensor Networks. Toronto: ACM Press, 2004. 104−110. [doi: 10.1145/1052199.1052217]

[20] Coman A, Sander J, Nascimento MA. Adaptive processing of historical spatial range queries in peer-to-peer sensor networks. Distributed and Parallel Databases, 2007,22(2/3):133−163. [doi: 10.1007/s10619-007-7018-8]

[21] Groat MM, He W, Forrest S. KIPDA: *k*-Indistinguishable privacy-preserving data aggregation in wireless sensor networks. In: Proc. of the 30th IEEE Int'l Conf. on Computer Communications. Shanghai: IEEE Press, 2011. 2024−2032. [doi: 10.1109/INFCOM.2011.5935010]

**附中文参考文献**:

[8] 戴华,秦小麟,刘亮,季一木,付雄,孙研.基于 Z-O 编码的两层 WSNs 隐私保护最值查询处理协议.电子与信息学报,2013,35(4):970−976. [doi: 10.3724/SP.J.1146.2012.00940]

[9] 范永健,陈红.两层传感器网络中可验证隐私保护 Top-$k$ 查询协议.计算机学报,2012,35(3):423−433. [doi: 10.3724/SP.J.1016.2012.00423]

[10] 李睿,林亚平,易叶青,雄帅,叶松涛.两层传感器网络中安全 Top-$k$ 查询协议.计算机研究与发展,2012,49(9):1947−1958.

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

**左开中**(1974－),男,安徽宿州人,博士,教授,CCF 会员,主要研究领域为网络与信息安全,隐私保护.
E-mail: zuokz@mail.ahnu.edu.cn

**胡鹏**(1988－),男,硕士,主要研究领域为无线传感器网络,隐私保护.
E-mail: dearhu111@sina.com

**王涛春**(1979－),男,副教授,主要研究领域为无线传感器网络,隐私保护.
E-mail: wangtc@nuaa.edu.cn

**罗永龙**(1972－),男,博士,教授,博士生导师,主要研究领域为可信计算,安全计算,空间数据处理.
E-mail: ylluo@ustc.edu.cn