两层无线传感网中节能的安全范围查询方法

刘怀进 陈永红 田 晖 王 田 蔡奕侨
(华侨大学计算机科学与技术学院 厦门 361021)

摘 要 在两层无线传感器网络中,存储节点作为一个中间节点介于传感器节点和 Sink 之间,既负责收集传感器节点的数据,又负责 Sink 的查询,因此更容易被攻击者攻击。一个被妥协的存储节点不仅可能泄漏传感器节点的数据,还有可能向 Sink 返回不完整的或虚假的查询结果。为了减少查询能耗开销并解决存储数据隐私保护问题,提出了一种节能的安全范围查询方法 PIRQ。该方法将数据查询和上传过程进行分离,并采用 R-D 判别方法将原来感知数据与查询范围区间上下界的大小比较过程转换成感知数据与查询范围中间值的距离和查询区间半径的大小比较过程,减少了能量开销。利用 0-1 编码和 Hash 消息认证机制对数据进行隐私保护,采用加密数据链技术对数据进行完整性检测。理论分析和实验表明,该方法在实现数据的隐私和完整性保护的同时具有很好的节能性。

关键词 两层传感器网络,范围查询,隐私保护,完整性检测,0-1 编码,加密数据链技术
中图法分类号 TP309 **文献标识码** A

Privacy and Integrity Protection Range Query Processing in Two-tiered Wireless Sensor Networks

LIU Huai-jin CHEN Yong-hong TIAN Hui WANG Tian CAI Yi-qiao
(Department of Computer Science and Technology, Huaqiao University, Xiamen 361021, China)

Abstract In two-tiered wireless sensor networks, storage node is an intermediate hode between sensor nodes and Sink nodes, which is responsible for collecting data of sensor nodes and the query of the Sink, so it is more easily attacked by the attacker. Storage nodes can not only reveal the compromise data of sensor nodes, but also is likely to return an incomplete or false results to Sink. To this end, this paper proposed a privacy and integrity protection range query method PIRQ. The PIRQ separates data query and upload process, and uses the R-D sensory data process to change the process of size comparison of the size of the lower and upper bounds on the range of the sensing data and the median into the distance between the perceptual data and the median of the query range and the size of the range of the query, which reduces the energy overhead. 0-1 coding and Hash message authentication mechanism are used for data privacy protection, and encrypted data link technology is used for data integrity verification. Theoretical analysis and experimental results show that the method can realize the privacy and integrality of the data, and have higher efficiency of energy consumption.

Keywords Two-tiered wireless sensor networks, Range query, Privacy protection, Integrity checking, 0-1 encoding, Encrypted data link technology

1 引言

两层无线传感器网络是一种拓扑结构简单、链路质量稳定、查询效率高和负载较为均衡的新型传感器网络[1]。该类型网络主要由少量资源丰富的存储节点和大量资源受限的感知节点组成[2]。存储节点处在中间层,其上层为 Sink,下层为传感器节点(见图 1)。在应用中,传感器节点与邻近的存储节点构成一个网络单元,传感器节点采集数据,并将数据发送给存储节点;存储节点接收并存储传感器节点数据,同时负责 Sink 的查询处理并将查询结果返回给 Sink。显然,在敌对环境中存储节点很容易遭受攻击,如果存储节点被妥协,将会对网络产生很大的威胁,如攻击者可能获取采集的数据,向 Sink 返回虚假的查询结果等。

范围查询作为无线传感器网络中的一种基本的数据查询方法,主要应用在数据管理和事件监测上。在当前两层无线传感器网络数据查询的研究工作中,安全和高效的范围查询受到了越来越多的关注。然而,在现有的研究工作中,关于传感器节点的能量消耗、数据的隐私和完整性保护方面依然存

本文受基于数字水印的网络入侵检测的研究(61370007),基于移动雾节点的传感云关键技术研究(61572206),福建省新世纪优秀人才计划项目(2014FJ-NCET-ZR06)资助。
刘怀进(1992-),男,硕士生,主要研究方向为网络信息安全,E-mail:2285316731@qq.com;陈永红(1974-),男,博士,教授,主要研究方向为物联网及安全、云计算与安全、入侵检测、数字水印、大数据安全等;田 晖(1982-),博士,副教授,主要研究方向为网络与信息安全、云计算安全、多媒体内容安全、数字取证、信息隐藏和隐藏通信等;王 田(1982-),男,博士,副教授,主要研究方向为移动计算、物联网及其安全问题、传感云、社交网络、大数据、安卓智能手机应用等;蔡奕侨(1983-),男,博士,讲师,主要研究方向为智能算法及其应用、数据挖掘等。

在不足之处。因此，研究和解决两层无线传感器网络具有节能的安全范围查询问题依然具有重大的现实意义。基于此，本文提出了一种能量高效的安全范围查询方法 PIRQ。PIRQ 通过对数据查询和上传过程进行分离，减少了传感器节点的通信能耗，采用 R-D 判别法减少存储节点的查询次数，提高了查询效率，利用 0-1 编码和加密数据链机制对数据进行了隐私和完整性保护。性能分析和实验对比表明，本方案具有很好的节能效果。

2 相关工作

近年来，两层无线传感器网络的安全范围查询受到研究者关注。在隐私保护方面，Sheng 等人[3]采用桶划分方法和 Encoding Number 机制来保护数据的隐私性和真实性，但在桶划分技术中，一个妥协的存储节点可能估算出数据与查询条件的实际值；为了提高隐私数据的安全性，Chen 等人[4]提出了一种称为 SafeQ 的安全查询协议，该协议提出前缀编码机制和加密数据链技术对范围查询的隐私性和完整性进行保护，但缺点是空间开销和通信开销很大。同时，在完整性保护方面，Chen 等人[5]引用哈希认证树技术来验证数据的完整性，但该技术更适合多维数据的查询；戴华等人[6]提出的 EPRQ 方法利用 0-1 编码和 Hash 消息身份认证机制相结合的方式对数据进行隐私保护，但缺点是无法验证查询结果的完整性；窦轶等人[7]提出了 ZOSR 协议，该协议利用 0-1 编码和 Encoding Number 机制实现数据的隐私和完整性保护，但缺点是只分析了每个时间周期内感知单个数据的情况，对多个感知数据的情况不太适用，且通信效率不高。

针对以上工作的不足，本文提出了一种节能的安全范围查询方法 PIRQ，其与 EPRQ 相比具有完整性保护，与 SafeQ 相比具有更高的能量效率。

3 模型

3.1 网络模型

本文采用与文献[7]类似的两层结构的传感器网络模型，如图 1 所示，整个网络被划分成多个单元，每个单元由一个资源丰富的存储节点和多个感知器节点组成。存储节点与存储节点之间能够进行远距离、高频率通信，形成多跳的上层网络关系；Sink 与临近的一些存储节点之间进行无线链接通信。

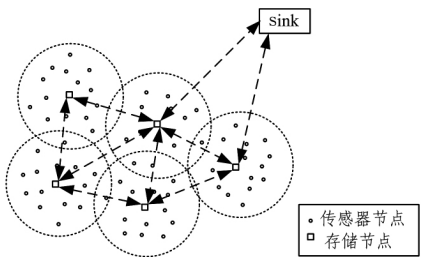

图 1 两层无线传感器网络的体系结构

3.2 范围查询模型

本文采用的传感器网络范围查询模型可表示为：

$$Q=(C,T,[a,b])$$

其中，C 为查询区域，T 为查询周期，$[a,b]$为查询范围。

范围查询$\{C,T,[a,b]\}$在指定的查询区域 C 和查询周期 T 内获取满足查询范围区间$[a,b]$的所有感知数据。

3.3 攻击模型

本研究重点关注存储节点被捕获后的攻击情况。攻击者的攻击方式包括 3 种：1)获取存储节点的存储数据；2)伪造查询结果返回给 Sink；3)篡改或返回部分查询结果给 Sink。

4 PIRQ 算法

本节先介绍 PIRQ 的 3 个主要技术，然后再具体描述 PIRQ 的基本流程。

4.1 主要技术

PIRQ 主要涉及的技术有 R-D 判别法、0-1 编码认证技术和加密数据链技术，下面将详细介绍这些技术。

4.1.1 R-D 判别法

在 PIRQ 的查询方法中，为了减少查询次数，提高查询效率，采用 R-D 判别法。R-D 判别法是在查询过程中将查询范围区间的中间值与查询数值之间的距离和查询范围区间的半径进行比较。假设查询区间范围为$[a,b]$，查询数值为 d_i，需要查询数值是否在查询范围中。首先根据式(1)和式(2)分别求出查询范围中间值 m 和半径值 r。

$$m=(a+b)/2 \tag{1}$$

$$r=(b-a)/2 \tag{2}$$

然后通过查询数值 d_i 使用式(3)求出 I_i，最后将 I_i 与半径 r 进行比较。如果 $I_i>r$，则表示查询值不在查询范围内；反之，如果 $I_i\leqslant r$，则表示查询值在查询范围内。

$$I_i=|d_i-m| \tag{3}$$

4.1.2 0-1 编码认证技术

为了使存储节点在不知道真实数据的情况下仍能高效地完成查询过程，应用了 0-1 编码认证技术。0-1 编码认证技术是将数值的大小比较问题转换成两个数据之间是否存在交集的问题，主要经过 0-1 编码、0-1 编码数值化和 Hash 数值化 0-1 编码 3 个阶段。0-1 编码的定义如下。

定义 1 设数值 x 表示为 n 位二进制数 $x=x_1x_2\cdots x_n$，其中 x_i 的取值为 1 或 0。对 x 进行 0 编码的公式如下：

$$E^0(x)=\{x_1x_2\cdots x_{i-1}1\,|\,x_i=0\wedge 1\leqslant i\leqslant n\} \tag{4}$$

对 x 进行 1 编码的公式如下：

$$E^1(x)=\{x_1x_2\cdots x_n\,|\,x_i=1\wedge 1\leqslant i\leqslant n\} \tag{5}$$

0-1 编码具有如下性质。

性质 1 设数值 x 由 n 位的二进制数表示，则 x 的 0 编码集合 $E^0(x)$和 1 编码集合 $E^1(x)$的元素总和为 n。

性质 2 设数值 x 的 0 编码集合为 $E^0(x)$，数值 y 的 1 编码集合为 $E^1(x)$，当 $E^0(x)\cap E^1(y)\neq\varnothing$ 时，$x<y$，反之亦然。

在判断 $E^0(x)$和 $E^1(x)$是否存在交集的过程中，为了降低计算的复杂度，对 0-1 编码进行数值化处理，利用数值化函数将 0-1 编码的集合元素转换成具体的数值。由于数值化方法不唯一，采用在编码最高位之前加“1”实现其数值化。例如：$x=5=0101_2$，$y=3=0011_2$，首先对 x 进行 0 编码得到编码集合$\{011,1\}$，对 y 进行 1 编码得到编码集合$\{0011,001\}$，根据性质 2 可知，$x>y$。但在实际比较过程中，考虑到对编码比较计算的复杂度，在编码元素最高位之前加“1”，实现数值化得到 x 的 0 编码数值集合$\{11,3\}$和 y 的 1 编码数值集合$\{19,1\}$，从而简化寻找集合是否存在交集的过程。注意，如果不在编码最高位之前加“1”而直接进行数值化转换，就会错误判断为 $x=y$。

在 0-1 编码数值化后，攻击者可能逆推出原始数据。为了保证数据的安全性，采用文献[10]中 Hash 消息身份认证编码机制对数据进行保护。根据 Hash 函数的单向性和抗冲突性，经过 Hash 数值化后的数据依然能够进行大小比较，即当 $H_K(N(E^0(x)) \cap H_K(N(E^1(x)) \neq \emptyset$ 时，$x < y$；当 $H_K(N(E^0(x)) \cap H_K(N(E^1(x)) = \emptyset$ 时，$x \geqslant y$。

4.1.3 加密数据链技术

PIRQ 采用加密数据链技术来实现查询结果的完整性验证，其基本思想是普通传感器节点对采集的所有数据进行排序，分段加密形成加密数据链，然后发送满足查询结果的加密数据链给存储节点。Sink 接收存储节点发来的加密数据链后，根据数据项之间的连续性进行查询结果的完整性验证。

假设传感器节点 S_i 采集了 N 个感知数据，它们排序后分别是 $d_1, \cdots, d_N$，对它们进行分段加密后得 $\{(d_0 \mid d_1)_{k_i}, \cdots, (d_{N-1} \mid d_N)k_i, (d_N \mid d_\infty)_{k_i}\}$，这里“|”代表连接，$d_0$ 和 d_∞ 代表所有感知数据的最下界和最上界。对于任何数据项 $(d_j \mid d_{j+1})_{k_i}$，称 $(d_{j+1} \mid d_{j+2})_{k_i}$ 为数据 d_{j+1} 的右邻接项。在发送满足查询范围的查询结果时，还需发送满足查询结果的最大值的右邻接项给存储节点，这样 Sink 才能验证 S_i 是否发送完了所有查询结果。

4.2 低能耗的安全范围查询算法

本节给出了实现安全范围查询协议 PIRQ 的具体过程，主要分为以下 4 个阶段。

4.2.1 前期准备阶段

1)在网络开始进行前，先对每个感知节点 S_i 进行必要的信息存储，包括 Hash 函数、认证密钥 K 和 k_i。其中 K 为 Sink 和所有传感器节点共享的密钥，用于计算 Hash 值；k_i 为 Sink 和 S_i 共享的私密密钥，用于加密数据。

2)在每次范围查询开始前，通过 R-D 判别式(1)和式(2)分别求出参数 m 和 r，并将 m 通过密钥 K 加密后广播给各个传感器节点。

4.2.2 数据存储阶段

1)在时间周期 t 内，假设每个传感器节点 S_i 感知了 N 个数据，采集完数据后通过加密数据链技术对所有感知数据进行排序、分段并通过对称加密方法进行加密，生成具有连续性的数据项集合，例如 $\{(d_1 \mid d_2)_{k_i}, \cdots, (d_N \mid d_{N+1})_{k_i}\}$。

2)采用 R-D 判别式(3)对每个数据 d_j 求出 I_j，然后对 I_j 进行 0-1 编码并数值化处理，得到编码集合 $N(E^0(I_j))$ 和 $N(E^1(I_j))$。最后通过 Hash 消息身份认证机制(如 HMAC-MD5)进行 HMAC 处理得到最小化比较因子 $H_{K_i}(\min\{N(E^0(I_j), N(E^1(I_j))\})$，其中 $\min\{N(E^0(I_j), N(E^1(I_j))\}$ 表示从 0 编码集合和 1 编码集合中选出包含元素最少的集合。在接下来的描述中，为了方便，用 $H_{K_i}(X_j)$ 表示 I_j 的最小化比较因子。

3)传感器节点 S_i 将最小化比较因子、传感器节点 ID 和时间周期 t 发送给单元内的存储节点 M：

$$S_i \rightarrow M: \langle ID_{(S_I)}, t, H_{K_i}(X_{i,1}), \cdots, H_{K_i}(X_{i,N}) \rangle$$

4.2.3 查询处理阶段

1)Sink 对范围区间半径 r 进行 0-1 编码和 Hash 编码处理，得到 0 编码集合 $H_{K_i}(N(E^0(r)))$ 和 1 编码集合 $H_{K_i}(N(E^1(r)))$，然后发送给存储节点 M：

$$\text{Sink} \rightarrow M: \{H_{K_i}(N(E^0(r))), H_{K_i}(N(E^1(r)))\}$$

2)存储节点 M 收到半径 r 的 0-1 编码的比较因子后，与 I_j 的最小化比较因子进行比较，根据性质 2，若存在交集，则说明感知数据 d_j 在查询范围内，否则不在查询范围。

3)存储节点 M 将符合查询范围的 I_j 的最小化比较因子 $H_{K_i}(X_{i,j})$ 中的所有 Hash 数值进行相加得到数值 $\xi_{i,j}$，然后返回给传感器节点 S_i。

4.2.4 验证阶段

1)传感器节点 S_i 收到 $\xi_{i,j}$ 后，将 I_j 对应的最小化比较因子 $H_{K_i}(X_{i,j})$ 采用同样的 Hash 数值求和并与 $\xi_{i,j}$ 进行比较。

2)验证完所有 $\xi_{i,j}$ 值后，传感器节点 S_i 发送所有的与 $\xi_{i,j}$ 相等的加密数据项给 Sink：

$$S_i \rightarrow M \rightarrow \text{Sink}: \{(d_{i,j} \mid d_{i,j+1})_{k_i}, \cdots, (d_{i,N} \mid d_{i,N+1})_{k_i}\}$$

其中，$\{(d_{i,j} \mid d_{i,j+1})_{k_i}, \cdots, (d_{i,N} \mid d_{i,N+1})_{k_i}\}$ 为查询结果，$(d_{i,N} \mid d_{i,N+1})_{k_i}$ 为验证对象。

3)Sink 收到加密数据链后，通过与传感器节点 S_i 共享的私密密钥 k_i 解密数据项，然后通过数据项之间的连续性判断数据是否被篡改，通过验证对象验证查询结果是否完整。

5 安全与能耗分析

综上所述，PIRQ 方案在实行查询过程中很好地保护了感知数据和查询范围的隐私，降低了传感器节点的能量消耗，同时验证了查询结果的完整性。下面分析该方法的安全性。

5.1 隐私性分析

在数据的隐私保护方面，主要分析两方面数据的隐私安全性。1)Hash 编码数据的隐私安全性，传感器节点和 Sink 通过 0-1 编码和 Hash 编码机制对感知数据或查询范围区间值进行编码处理，根据 Hash 函数的单向性，攻击者或妥协的存储节点无法逆推出明文数据，从而很好地保护了查询数据的隐私安全性。2)查询结果的隐私安全性，传感器节点在发送查询结果给 Sink 的过程中，攻击者或被妥协的存储节点在不知道加密密钥 k_i 的条件下将无法对密文进行解码，而加密密钥 k_i 为 Sink 和 S_i 共享的私密密钥，因此很好地保护了查询结果的隐私安全性。

5.2 完整性分析

针对数据可能被攻击者或妥协的存储节点进行篡改或伪造的问题，采用加密数据项链技术对数据进行完整性保护。传感器节点在发送满足查询范围的加密数据链给 Sink 的过程中，根据数据项之间的连续性，如果攻击者删除或篡改了链中的某个数据项，最后在 Sink 中很容易被检测出来。

接下来分析满足查询范围的所有感知数据是否都在查询结果内。如果存储节点只上传了部分查询结果给 Sink，Sink 将根据数据项的连续性和验证对象，很容易验证出查询结果是否完整。假设 Sink 接收了数据链 $\{(d_i \mid d_{i+1})_{k_i}, \cdots, d_{N-1} \mid d_N)_{k_i}\}$，解密后与查询范围区间进行比较发现数据其实也属于查询范围内，这与验证对象的特性不符合，则可判断查询结果不完整。

5.3 能耗分析

在两层无线传感器网络中，存储节点具有充足的能量储备。因此，主要详细分析感知节点的能量消耗问题。

在 PIRQ 协议中，任意传感器节点 S_i 主要包含两个方面的能耗：1)计算能耗 E_c，由加密和 Hash 函数计算产生；2)传感器节点的通信能耗 E_{RS}，由发送和接收消息产生。因此，传

感器节点的总能耗 E_{ALL} 如式(6)所示：

$$E_{ALL}=E_{RS}+E_C \tag{6}$$

假设 S_i 在单位时间周期内产生了 N 个感知数据，每个感知数据的长度为 ω，单位密文的数据长度为 α，Hash 编码的数据长度为 λ，传感器节点 ID 的数据长度为 l_{id}，单位时间周期 t 的数据长度为 l_t，加密的单位能耗为 e_c，Hash 编码计算的单位能耗为 e_h，接收和发送单位数据的能耗为 e_r 和 e_s。

由协议 1 可知，传感器节点不需要上传所有的感知数据给存储节点，只上传满足查询范围的感知数据给存储节点，这里用变量 κ 表示。同时上传的数据还有 N 个最小化比较因子，由性质 1 可知，最小化比较因子平均包含了 $\frac{\omega}{4}$ 个哈希值。因此 E_{RS} 可近似为：

$$E_{RS}\approx(l_{id}+l_t+N\times\frac{\omega}{4}\times\lambda+\kappa\times\alpha)\times e_s+(\kappa\times\lambda)\times e_r \tag{7}$$

计算能耗 E_C 为 S_i 进行对称加密计算和 Hash 编码计算的能耗总和，即：

$$E_C\approx N\times e_c+N\times\frac{\omega}{4}\times e_h \tag{8}$$

由式(9)和式(10)可知，S_i 的总能耗 E_{ALL} 为：

$$E_{ALL}\approx(l_{id}+l_t+N\times\frac{\omega}{4}\times\lambda+\kappa\times\alpha)\times e_s+(\kappa\times\lambda)\times e_r+N\times e_c+N\times\frac{\omega}{4}\times e_h \tag{9}$$

公式中加密的单位能耗 e_c 采用文献[9]给出的 TelosB 中 RC4 对数据进行加密的能耗数据，Hash 函数编码计算的单位能耗 e_h 采用文献[10]给出的 HMAC-MD5 进行 Hash 编码运算，并假设 e_h 和 e_c 的计算能耗相同。接收和发送单位数据的能耗 e_r 和 e_s 采用文献[12]中的单位数据能耗计算公式，即：

$$e_s=\begin{cases}Eel+Efs\times d^2, & d\leqslant 75\\ Eel+Emp\times d^4, & d>75\end{cases} \tag{10}$$

$$e_r=Eel+Eda \tag{11}$$

6 实验分析

本文在 Matlab 实验平台上对 PIRQ 进行模拟仿真，并与文献[4]的 SafeQ 和文献[6]的 EPRQ 方案进行比较。

假设网络覆盖区域为 100m×100m，传感器节点个数为 20，通信半径为 20m，单位时间周期内感知数据为 20，通过 128b 的 HMAC-MD5 实现 Hash 编码计算，采用 RC4 进行数据的加解密；通信能耗方面采用文献[11]中的单位能耗计算公式，其中平均跳数 d 为 10，其他具体参数设置与文献[12]相同。由于存储节点和 Sink 能量资源丰富，因此主要基于在查询过程中传感器节点和存储节点的平均能耗开销和几个主要的因素对传感器节点的能量消耗的影响进行分析和比较。

实验 1　查询时间间隔 t 为自变量，其他参数保持初始化状态，在每个时间间隔内执行 30 次随机范围查询，计算 30 次传感器节点在查询范围过程中的平均能耗。如图 2 所示，随着时间间隔的增加，提交的感知数据量也在增加，导致 3 种方案的能耗均在增加，其中 SafeQ 的增幅比 PIRQ 的大，这是因为随着感知数据的增加，使用前缀编码机制的普通传感器节点提交的 Hash 数据要比 0-1 编码机制传输的 Hash 数据量大。而 PIRQ 由于增加了数据完整性验证，传输的数据会比 EPRQ 多一点，因此在能耗方面会比 EPRQ 稍微大一点。

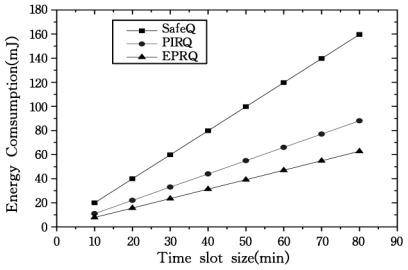

图 2　感知节点的平均能量开销

实验 2　查询时间间隔 t 为自变量，其他参数设置为初始化状态，在单元网络内对 20 个传感器节点进行 30 次固定的范围查询，计算 30 次存储节点在查询过程中的平均能量开销。如图 3 所示，随着 t 的增加，存储节点接收的数据量也在逐渐增加，导致 3 种方案的能量消耗均在增加。在 SafeQ 中，存储节点的能量消耗较大，因为存储节点需要对每个数据区间的前缀编码进行两次查询才能够判断出查询范围区间的下界和上界的最大和最小数据区间。在 EPRQ 方案中，存储节点除了需要对每个感知数据所对应的最小化比较因子与查询范围区间下界值的比较因子进行比较外，还需要对区间上界值的比较因子进行比较，但由于不需要对数据进行完整性验证，因此在能量消耗方面较小。在 PIRQ 方案中，存储节点只需要对每个感知数据所对应的最小化比较因子与范围查询区间半径的比较因子进行比较即可，但因加入了完整性验证机制，所以在能量消耗方面会比 EPRQ 大一点。

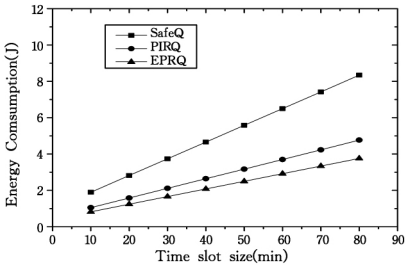

图 3　存储节点的平均能量开销

实验 3　平均跳数 d 为自变量，时间间隔设置为 10min，其他参数设置为初始化状态，在每个平均跳数条件下，执行 30 次随机范围查询，计算 30 次感知节点在查询范围过程中的平均能耗。如图 4 所示，随着跳数的增加，3 种方案的能量消耗均有所增加，但增幅不是很大。其中，在 PIRQ 方案中，传感器节点的平均能耗消耗是 SafeQ 的 48.6%，与 EPRQ 相比，只多了 16.6%的能量开销。

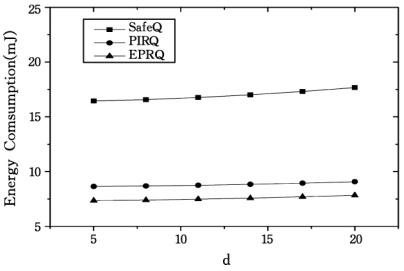

图 4　平均跳数对感知节点的能耗影响

实验 4　传感器节点感知的数据量 N 为自变量，时间间隔设置为 10min，其他参数设置为初始化状态，在每个感知的数据量 N 条件下，执行 30 次随机范围查询，计算 30 次传感器节点的平均能量开销。如图 5 所示，随着 N 的逐渐增大，

传感器节点发送的感知数据也逐渐增多，导致3种方案中的传感器节点能耗也随之增多。其中SafeQ的能量消耗最大，EPRQ的能量消耗最小，这是因为传感器节点发送的前缀编码数据量要比0-1编码机制产生的数据量更大。然而，在PIRQ方案中，传感器节点不需要发送所有的感知数据给存储节点，降低了能耗开销，但由于加入了完整性保护机制，因此在能耗方面会比EPRQ大一点。

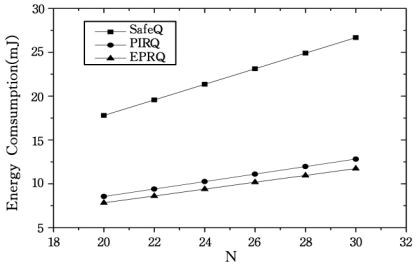

图5　N对感知节点的能量消耗影响

结束语　本文提出了一种能量高效的安全范围查询方法PIRQ。与SafeQ和EPRQ方案相比，PIRQ具有更好的安全性和节能性，但由于引入了完整性保护机制，在能量消耗方面仍然相对较高，在未来仍有不小的改进空间。

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 International Conference on Embedded Networked Sensor Systems. ACM, 2006:153-166

[2] Ratnasamy S, Karp B, Shenker S, et al. Data-centric storage in sensornets with GHT, a geographic hash table[J]. Mobile Networks and Applications, 2003, 8(4):427-442

[3] Sheng B, Li Q. Verifiable privacy-preserving range query in two-tiered sensor networks[C]// The 27th Conference on Computer Communications(INFOCOM 2008). IEEE, 2008

[4] Chen F, Liu A X. SafeQ: Secure and efficient query processing in sensor networks[C]//2010 Proceedings IEEE INFOCOM. IEEE, 2010:1-9

[5] Chen F, Liu A X. Privacy-and integrity-preserving range queries in sensor networks[J]. IEEE/ACM Transactions on Networking, 2012, 20(6):1774-1787

[6] 戴华，杨庚，肖甫，等. 两层传感网中能量高效的隐私保护范围查询方法[J]. 计算机研究与发展，2015，52(4)：983-993

[7] 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

[8] 周强，杨庚，李森，等. 一种可检测数据完整性的隐私数据融合算法[J]. 电子与信息学报，2013，35(6)：1277-1283

[9] Groat M M, He W, Forrest S. KIPDA: k-indistinguishable privacy-preserving data aggregation in wireless sensor networks[C]// 2011 Proceedings IEEE INFOCOM. IEEE, 2011:2024-2032

[10] Rivest R. RFC1321, The MD5 message-digest algorithm request for comments[S]. Cambridge: MIT and RSA Data Security, 1992

[11] Rappaport T S. Wireless communications: principles and practice [M]. New Jersey: Prentice Hall PTR, 1996

[12] 武佩宁. 两层无线传感器网络中安全数据查询协议的研究[D]. 南宁：广西大学，2014

[13] Coman A, Nascimento M A, 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: in Conjunction with VLDB 2004. ACM, 2004:104-110

(上接第357页)

了运算效率，又避免了单个KGC被摧毁的风险性，符合联合作战的、以网络为中心的、分布力量结构柔性重组的作战思想，进一步增强了信息装备网络的抗毁性，为后续保密装备网络体系构建奠定了基础。

参 考 文 献

[1] Shamir A. Identity-Based cryptosystems and signature schemes [C]// Advances in Cryptology-CRYPTO'84. Berlin, Heidelberg: Springer-Verlag, 1984:47-53

[2] Boneh D, Franklin M K. Identity-based encryption from the Weilpairing[C]// Proceedings of the 21st Annual International Cryptology Conference onAdvances in Cryptology. LNCS 2139. Berlin, Heidelberg: Springer-Verlag, 2001:213-229

[3] Chen L, Harison K, Soldera D, et al. Applications of multiple trust authorities in pairing based cryptosystems[C]// Proc of the International Conference on Infrastructure Security 2002. Berlin Springer, 2002:260-275

[4] Goldberg K I. A distributed private-key generator for identity-based cryptography[R]. University of Waterloo, 2007

[5] Al-Riyami S S, Paterson K G. Certificateless public key cryptography[C]// Proc of the 9th International Conference on the Theory and Application of Cryptography and Information Security. Berlin: Springer 2003:452-473

[6] Lee B, Boyd C, Dawson E, et al. Secure key issuing in id-based cryptography[C]// Proc of the 2nd Australasian Information Security Workshop. Austrlia: CRPIT, 2004:251-230

[7] Gangishetti R, Gorantla M C, Das M, et al. Threshold key issuing in identity-based cryptosystems[J]. Computer Standards & Interfaces, 2007, 29(2):260-264

[8] X Chun-xiang, Z Jun-hui, Q Zhi-guang. A Note on Secure Key Issuing in ID-based Cryprography[EB/OL]. http://eprint.iacr.org/2005/180

[9] Kate A, Goldberg I. Asynchronous Distributed Private-Key Generators for Identity-Based Cryptography [EB/OL]. http://eprint.iacr.org/2009/355

[10] 郝云芳，吴静，王立炜. Boneh-Boyen1基于身份加密体制的安全密钥分发[J]. 计算机科学，2012，39(6A)：35-37

[11] 任艳丽，蔡建兴，黄春水，等. 基于身份加密中可验证的私钥生成外包算法[J]. 通信学报，2015，36(11)：1-6

[12] Lewko A, Waters B. New techniques for dual system encryption and fully secure HIBE with short ciphertext[C]// Micciancio D. ed., Theory of Cryptography, Theory of Cryptography(TCC). LNCS 5978. Zurich, Switzerland: Springer, 2010:455-475

[13] 潘清. 网络中心战装备体系[M]. 北京：国防工业出版社，2010：5-10