doi:10.11959/j.issn.1000-436x.2015034

# 两层传感器网络中安全分类协议研究

李睿[1]，李晋国[2]，陈浩[1]
（1. 湖南大学 信息科学与工程学院，湖南 长沙 410082；2. 上海电力学院 计算机科学与技术学院，上海 200090）

**摘 要**：提出了一种安全分类协议 SSC，该协议在保护待分类数据和分类规则隐私的情况下使存储节点进行正确分类，并且 sink 节点可以对分类结果进行抽样认证，防止妥协存储节点伪造分类结果。提出了一种不经意比较（oblivious comparison）技术 MHash, 该技术首先将分类需要的大小比较转换成等值比较，并进一步采用模运算和散列技术实现隐私保护下的数据分类。提出了一种“十”字邻居技术, 分别将传感器以及传感器采集的数据组织成链，并采用倒置布鲁姆过滤器技术同步传感器节点之间的数据，sink 利用该技术可以抽样检查存储节点分类统计结果的正确性，分析和实验结果验证了所提方案的有效性。
**关键词**：两层传感器网络；安全分类；隐私保护；完整性认证
**中图分类号**：TP393.08 **文献标识码**：A

# Safe and secure classification protocol in two-tiered sensor networks

LI Rui[1], LI Jin-guo[2], CHEN Hao[1]
(1. College of Information Science and Engineering, Hunan University, Changsha 410082, China;
2. College of Computer Science and Technology, Shanghai University of Electric Power, Shanghai 200090, China)

**Abstract:** A safe and security classification protocol named SSC was proposed for two-tiered sensor networks, which enable storage nodes to process classification correctly without knowing both the value of classifying rules and the data which will be classified. To protect privacy, an oblivious comparison technique was presented. MHash, which enable storage nodes to compare data items from sink and sensors without knowing their values. Based on MHash and prefix membership verification technique, classification target was achieved in protecting the privacy of both sensor collected data and sink issued classification rules. To verify the correctness of classification results, a crossed neighborhood technique was proposed which organize sensors and data items in one sensor in sequences, to allow the sink checking the correctness of sampling classification results. Analysis and experimental results validate the efficacy and efficiency of SSC protocol.
**Key words:** two-tiered sensor networks; secure classification; privacy preserving; integrity verification

## 1 引言

无线传感器网络[1~3]一个重要的用途是对特定环境和目标进行有效识别和跟踪，例如在军事领域利用无线传感器网络监控战场状况；在生物领域对特定物种的活动进行监测[4]。在实现目标识别和跟踪时，传感器网络需要分类和统计相关环境数据，克服监控区域内运动物体的不可预测性以及监测环境中物种的多样性带来的影响，达到最终识别和跟踪特定目标的目的。在监测区域内，众多的传感器节点通常会收集很多监测数据，如果将传感器节点收集到的所有监测数据都传输到sink节点进行处理后再分类和统计，则传感器网络内产生的巨大网内数据流不但会过多消耗传感器节点能量，缩短了

**收稿日期**：2013-08-10；**修回日期**：2013-11-20
**基金项目**：国家自然科学基金资助项目（61370226, 61472132）；中国博士后科学基金资助项目；湖南大学青年教师成长计划基金资助项目；上海电力学院引进人才启动基金资助项目(K2015-008)
**Foundation Items:** The National Natural Science Foundation of China (61370226, 61472132); China Postdoctoral Science Foundation; Young Teacher Growth Plan of Hunan University; Startup Fund for Talent Introduction of Shanghai Universiry of Electri (K2015-008)

传感器网络的生命周期，更重要的是这些数据流会消耗过多的网络带宽造成传输时延，无法达到对特定目标的实时监测。

两层传感器网络从单层无结构传感器网络进化而来。由于其简单、易扩展、节能等特点[5,6]，两层传感器网络已广泛使用在各个领域，其典型结构如图 1 所示。在两层无线传感器网络中包含 3 类节点。1) 普通传感器节点。该类节点与单层传感器网络中的传感器节点一致，数目众多，分散在整个监测区域的各个角落，能量和计算资源都非常有限。2) sink 节点。该节点与传统单层传感器网络中的 sink 节点也一致，是一个终端节点，负责对网络内发送查询请求，并获得相应的查询结果。3) 存储节点。该类节点数目相对于传感器节点较少，但配备了相对丰富的存储和计算资源，负责收集临近传感器节点采集的监测数据并处理 sink 节点发送的处理请求。

如果利用两层传感器网络中存储节点的计算和存储能力，各个存储节点首先对其收集到的数据进行分类和统计，再将分类和统计的结果传给 sink 节点无疑会极大地减小网内数据流，达到对特定目标快速跟踪和识别的目的。

然而，在两层传感器网络中存储节点处在传感器节点和 sink 节点的中间，扮演了至关重要的角色，因此在敌对环境中更容易遭受攻击者的攻击。被攻击者妥协的存储节点将对整个网络产生较大的破坏性。其破坏性体现在如下几个方面：1) 妥协的存储节点自身存储的大量传感器节点，采集的敏感数据会被泄漏；2) 存储在妥协存储节点上的 sink 分类统计规则会被泄漏；3) 攻击者可操纵妥协的存储节点伪造虚假的分类统计结果。因此，在两层结构的传感器网络下亟需设计安全的分类协议，避免以上 3 个破坏性方面问题的出现。但设计这样一个安全分类协议具有很大的困难性，需要解决以下 2 个关键问题：1) 需要存储节点在不知道分类和统计规则以及传感器节点采集的数据真实值情况下进行正确地分类和统计，该条件是为了避免妥协的存储节点泄露存储在其上的敏感信息；2) 需要对分类结果进行相应的抽样认证，该条件是为了避免攻击者恶意伪造虚假结果。

本文研究两层传感器网络中的安全分类问题，并提出了一种安全分类(SSC, safe and secure classification)协议。SSC 协议能实现在保护分类数据和分类规则隐私的情况下，存储节点进行正确分类；sink 节点可以采用抽样检查的方法对分类结果进行认证，检测出妥协存储节点伪造的分类统计结果。在 SSC 协议中，首先需要解决的一个问题是实现在隐私保护的情况下实现数据的分类，为了解决这个问题，本文采用前缀技术将判断一个数据隶属于某一个区间变成判断一个数据是否隶属于某一个集合。该变换消除了分类过程中的大小比较，在只有等值比较的情况下实现了判断数据与范围的隶属关系。在此基础上提出了一种不经意比较技术 MHash。MHash 采用模运算和单向散列技术, 在保护传感器采集数据和分类规则安全性的基础上实现了正确的分类。针对查询结果正确性认证问题，本文的思路是将传感器节点采集的数据组织成 2 条链：单个传感器节点采集的数据形成一条链；相邻传感器节点采集的数据形成另外一条链，本文称这种技术为“十”字邻居技术。利用该技术，sink 可以对分类统计的最终结果进行抽样检查来验证分类结果的正确性。本文算法最终在 Intel Lab[7]提供的数据集上进行验证，实验结果证实了所提算法的有效性。

本文主要贡献有：1) 提出了两层传感器网络中的安全分类问题；2) 提出了 MHash，一种不经意比较方案，并结合前缀编码和 MHash 提出安全分类技术；3) 提出了用于抽样认证分类结果的“十”字邻居技术。

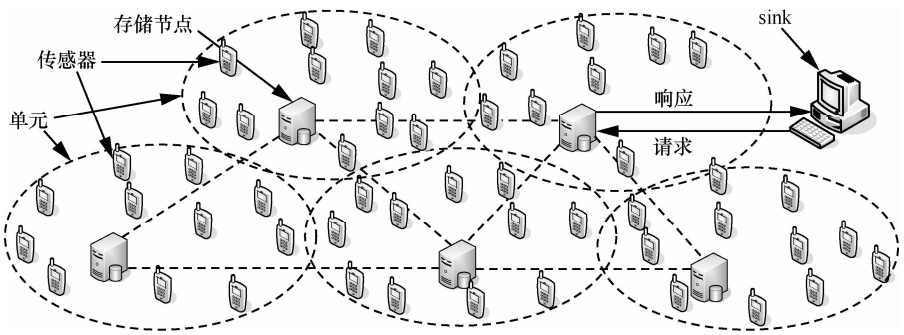



图 1　两层结构的传感器网络

## 2 相关工作

就目前所知，有关两层传感器网络安全数据分类方面的研究还没有，和本文研究最为相关的是：针对普通传感器网络的数据分类算法和针对两层传感器网络的相关安全协议。下面将从这些方面分析现有工作。

### 2.1 传感器网络中的数据分类研究

无线传感器网络的重要任务之一是有效识别和跟踪特定目标。Wang 等人使用 Mica 声音传感器跟踪目标，采用分类器将特征信号从白噪声数据中提取[8]。Simon 等人研究了狙击手定位系统，根据声音信号处理特征进行了应用[9]，通过 DSP 芯片对狙击步枪和普通手枪进行分类识别。文献[10]和文献[11]以大鸭岛为研究环境，设置大量传感器研究野生动物，使用多种传感器分类识别各种野生动物，sink 节点主要负责分类部分的工作。

识别和跟踪特定目标也是智能交通的重要研究方向。文献[12]分类识别了行人、车辆等运动目标，通过结合较为先进的硬件设施实现高识别率。主要结合 Mica2 节点和磁力及声音感应器，同时安装了少量 MIR 传感器，可处理雷达信号。然而该方案采用的传感器节点较为昂贵，因此限制了其实际的应用价值。

此外，通过设计可实现分类器进一步提高针对各种特征的分类精确度[13~17]。但这些分类工作通常是使用 sink 节点对采集的信号集中进行分类和识别，需要传感器节点上传所有数据，因此，对网络造成了较大的负担。Zhao 等设计了协作式的分类算法，节点在传数据前完成分类，并将最终结果反馈至 sink。Pattem 等提出了一种针对能量有限环境的跟踪识别算法评价体系[16]。然而文献[15,16]需要限制网内节点全部同构，且存储和运算能力较强，增加了实际部署的成本。

两层结构的传感器网络也有相关分类工作，Wang 等人提出针对该结构的基于协作和任务分解的分类识别算法[17]，但未考虑存储节点受到威胁的情形。

### 2.2 两层传感器网络中的数据安全查议

两层传感器网络近年来在隐私与数据完整性方面有着较为丰富的研究工作。以下从这 2 个方面对国内外研究工作进行分析。

1) 隐私保护

范围查询的隐私保护问题在两层传感器网络中最先受到关注，文献[18~20]采用应用在数据库领域的桶划分方法[21]实现了在两层传感器网络下对范围查询数据的隐私性和完整性保护。然而桶方案易被估算实际数据值，且多维情形下能耗随维度指数增长[22]。Chen&Liu 提出 SafeQ 安全查询协议[23]避免桶方案的缺陷。但是 SafeQ 的能耗仍然过高，因此本文作者提出 QuerySec[24]，一种利用多项式技术进行隐私保护的安全协议。

Top-$k$ 查询在两层传感器网络中也较为重要。Zhang 等人[25]最先提出针对两层传感器网络的 top-$k$ 协议，但是该协议只考虑了查询结果的可校验，并未考虑数据隐私。陈红等人提出了基于辅助计算节点的安全 top-$k$ 查询协议[26]，该协议需要额外的硬件支持。本文作者进一步提出 SecTQ 协议[27]，通过采用估算相关技术转换 top-$k$ 查询。李建中等随后提出安全 top-$k$ 隐私保护数据传输协议[28]。本文作者进一步考虑了网络中上层安全传输问题，提出了一种针对两层传感器网络的安全数据聚合协议[29]，通过布鲁姆过滤器结合前缀保护数据隐私。

2) 完整性保护

Sheng 和 Li[18]提出以桶为基础设计的编码技术，使各个传感器的空桶具有唯一编码数，编码数可以用于认证查询结果的完整性。Shi 等[19,20]提出时空交错校验(spatiotemporal crosscheck)方案降低了通信开销。其核心算法是以比特图(bit map)作为传感器描述桶数据的技术手段，传感器之间相互广播比特图。但是妥协的传感器伪造位图会对其他节点造成破坏。Chen 和 Liu[21]提出邻居链表(neighborhood chain)避免此类问题，但是邻居链表需要存储两次数据，通信能量和存储空间开销由此增大。假如存在数据(6,5,8)和(4,3,5)，最高界与最低界分别为(10,10,10)和(0,0,0)，SafeQ 协议中，二者的邻居链为{(0,0,0)|(4,3,5), (4,3,5)|(6,5,8), (6,5,8)|(10,10,10), (10,10,10)}，数据量增加了 2 倍以上。

## 3 模型与问题陈述

### 3.1 系统模型

图 1 是典型的两层传感器网络，节点分为 3 种类型：存储节点、传感器节点和 sink 节点。多个传感器部署在单个存储节点旁边，构成单元(cell)。采集温度、湿度等环境数据是传感器节点的主要任务，然而传感器节点易失效，计算与存储能力有限。存储节点计算能力较强、存储容量较大、节点不易

失效又能移动。传感器节点将采集数据后周期性地反馈至存储节点。根据用户需要 sink 制定分类标准，存储节点收到 sink 的分类标准后执行分类统计，反馈分类结果至 sink，sink 根据用户要求整理计算返回的结果。

### 3.2　基本假设

两层传感器网络基本假设。

1) 传感区域有多个单元，每个单元含一个存储节点和多个传感器节点，节点本身的位置已知，节点所在的单元已知，每个传感器具有唯一的 ID。

2) 存储节点和传感器松散同步，收集时间由多个互不重叠的周期组成，节点在一个周期内采样 $n$ 次，$(\eta,t,\{d_1,d_2,\cdots,d_n\})$ 表示传感器 $s_\eta$ 采集的数据，其中周期序号由 $t$ 表示，传感器节点采集的数据由 $d_1,d_2,\cdots,d_n$ 表示；每个周期末传感器会向存储节点传输数据。

3) sink 和传感器共享密钥 $k_p$，同时各个传感器节点单独和 sink 共享一个惟一的各不相同的密钥。例如，sink 和传感器 $s_\eta$ 共享的密钥用 $k_\eta$ 表示；同时各个存储节点和 sink 各自共享一个唯一的各不相同的密钥，例如，负责第 $i$ 个单元数据收集的存储节点和 sink 共享的密钥表示为 $k_i$。

### 3.3　威胁模型

本文的威胁模型中，可信的是 sink，个别或少量的存储节点和传感器节点可能被攻击者妥协。存储节点被妥协后，会对数据隐私造成破坏，泄露 sink 的分类规则和传感器的数据；传感器被妥协后，会修改分类结果，也会泄露 sink 的分类规则，需要抽样认证分类结果的正确性。

本模型中假设传感器节点被妥协后不会伪造自身数据。这是由于：1) 这一类的传感器数据伪造很难被阻止；2) 单个周期单个传感器传输的数据极为有限，被妥协的少量传感器伪造自身数据不会对最终的结果造成太大影响[30,31]。本文的威胁模型是半可信模型[32]，即存储节点和传感器节点均试图找到 sink 节点的分类规则实际值，此外存储节点也试图找到传感器节点的数据，但二者之间不会存在合作。

## 4　不经意比较

本文系统模型中考虑的不经意比较问题是：假定 $d_i$ 是 sink 节点的数据，$d_j$ 是传感器 $S_\eta$ 的数据，存储节点负责比较二者数据是否相等。然而在这个过程中，存储节点不能知道二者数据真实值，sink 节点和传感器也不能相互知道彼此数据的真实值。该问题的困难之处在于，由于节点是无线通信，信号具有广播性，传感器节点 $S_\eta$ 和 sink 无法约定同一密钥，同时存储节点在比较数据过程中不能泄露相应的隐私信息。这是接下来的不经意比较协议考虑的问题，首先介绍不经意比较函数。

### 4.1　不经意比较函数

加密函数在满足以下条件后，称为不经意比较函数，假定有函数 $f_1$、$f_2$，$f_1$ 又叫内层函数，$f_2$ 又叫外层函数。

数据用 $x$ 来表示，密钥为 $k$、$k_1$、$k_2$。

1) 可区分：任意 $k$ 、$x_1$ 和 $x_2$，若 $x_1\neq x_2$，则 $f_2(x_1, k)\neq f_2(x_2, k)$ 且 $f_1(x_1, k)\neq f_1(x_2, k)$。

2) 安全性：通过 $f_1$ 的加密结果 $f_1(x, k)$，不能计算 $x$ 和 $k$；同样，通过 $f_2$ 的加密结果 $f_2(x, k)$ 和 $x$ 不能计算 $k$。

3) 可交换：任意 $k_1$、$k_2$ 和 $x$，$f_2(f_1(x, k_2), k_1) = f_2(f_1(x, k_1), k_2)$。

### 4.2　不经意比较协议

假设有 $f_1$ 和 $f_2$ 这 2 个不经意比较函数，存储节点负责比较传感器 $S_\eta$ 的数据 $d_j$ 和 sink 数据 $d_i$ 是否相等，步骤如下。

1) sink 用共享密钥 $k_p$ 加密数据 $d_i$，加密结果为 $(d_i)_{kp}$，用函数 $f_1$ 和共享密钥 $k_s$ 对加密数据再次进行加密，加密结果为 $f_1((d_i)_{kp}, k_s)$，随后把加密结果 $f_1((d_i)_{kp}, k_s)$ 传输到存储节点。

2) sink 节点向存储节点传输加密结果 $f_1((d_i)_{kp}, k_s)$，再由 sink 转发到传感器 $S_\eta$。

3) 传感器接收加密结果 $f_1((d_i)_{kp}, k_s)$，随后采用加密函数 $f_2$ 和共享密钥 $k_\eta$ 将加密结果加密，得到 $f_2(f_1((d_i)_{kp}, k_s), k_\eta)$，该结果最终传输到存储节点。

4) 传感器 $S_\eta$ 用共享密钥 $k_p$ 对数据 $d_j$ 进行加密，得到 $(d_j)_{kp}$，随后应用加密函数 $f_1$ 和共享密钥 $k_\eta$ 对数据进一步加密，得到 $f_1((d_j)_{kp}, k_\eta)$，最后传输至存储节点。

5) 存储节点接收来自传感器的加密数据 $f_1((d_j)_{kp}, k_\eta)$ 后，使用函数 $f_2$ 和共享密钥 $k_s$ 进行加密，得到 $f_2(f_1((d_j)_{kp}, k_\eta), k_s)$。

6) 存储节点最终对比结果 $f_2(f_1((d_i)_{kp}, k_s), k_\eta)$ 和 $f_2(f_1((d_j)_{kp}, k_\eta), k_s)$，若二者相等，则有 $d_i$ 和 $d_j$ 相等；反之则 $d_i$ 不等于 $d_j$。

上述过程的加密中，内层加密可以采用 $f_1$ 和 $f_2$

以外的加密方法。sink 在第一步中用密钥 $k_s$ 和 $k_p$ 对数据进行加密，保护数据的隐秘性，此外，传感器传输的数据也是通过 2 次加密保证了数据的安全。图 2 所示是不经意比较协议基本过程。

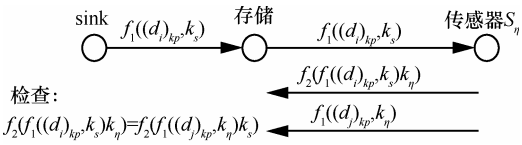



图 2 不经意比较协议

### 4.3 MHash 协议

不经意比较函数可以通过交换加密技术（commutative cipher）[33~36]来实现，然而交换加密大部分是以 Pohling-Hellman 函数为基础(例如，$CE(x, k)=x^k \bmod M$，$M$ 表示大素数，$k$ 表示密钥，$x$ 表示明文)，该类指数级的运算很难被传感器网络支持，计算代价过高。本文以轻量级计算为设计目标提出 MHash 协议。MHash 是以模运算和散列函数为基础进行设计的，结合考虑二者的单向性和可交换性。存储节点仍然负责比较传感器 $S_\eta$ 的节点数据 $d_i$ 和 sink 节点数据 $d_j$ 是否大小相等，本文以此为例解释 MHash 协议的基本工作原理，内层加密利用模运算减少其计算量，即$(x+k) \bmod M$表达的是函数 $E(x, k)$。

1) sink 加密数据 $d_i$ 得到结果 $E(d_i, k_p+ k_s)$, 随后将结果传输至存储节点；

2) 一旦接收 $E(d_i, k_p+ k_s)$，存储节点会将加密结果后传输至传感器 $S_\eta$；

3) 收到结果 $E(d_i, k_p+ k_s)$，$S_\eta$ 随后计算其散列值 $H(E(E(d_i, k_p+ k_s), k_\eta))$, 将结果传输至存储节点；

4) 传感器 $S_\eta$ 加密数据 $d_j$ 得到结果 $E(d_j, k_p+k_\eta)$, 将结果传输至存储节点；

5) 接收 $E(d_j, k_p+k_\eta)$后，存储节点 $S_\eta$ 计算其散列值 $H(E(E(d_j, k_p+k_\eta), k_s))$；

6) 最终，存储节点对比 $H(E(E(d_j, k_p+k_\eta), k_s))$ 和 $H(E(E(d_i, k_p+ k_s), k_\eta))$是否大小相等，若二者相等，则 $d_i$ 等于 $d_j$，反之 $d_i$ 不等于 $d_j$。

图 3 给出了 MHash 的基本工作过程。MHash 协议中，$M$ 为大素数，被加密数据均小于 $M$。$H$ 表示散列函数，例如具有单向性的 SHA1 或 MD5。散列函数具有单向性的特性，通过 $H(x)$ 无法获取 $x$ 的实际值。尽管散列函数有可能存在冲突，但实际应用中很难存在不同数值被散列到同一位置的情况。

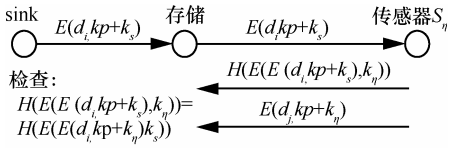



图 3 MHash 协议

MHash 协议下，$f_1$ 函数设计为：$f_1(x, k)=(x+k) \bmod M$；$f_2$ 函数设计为；$f_2(x, k)=H((x+k) \bmod M)$；不经意函数的设计要求均被这 2 个函数满足。

可区分：散列函数较低的冲突几率集合模运算的特性保证了函数 $f_1$ 和 $f_2$ 的可区分性。

安全性：通过 $f_1(x, k)= (x+k) \bmod M$ 无法获取 $x$ 和 $k$ 的实际值，通过 $f_2(x, k)=H((x+k) \bmod M)$和 $x$ 无法获取密钥 $k$。这些特性是由密钥的隐秘性和散列函数单向性保证的。

可交换：由于协议是基于模运算，而模运算具有可交换性，因此协议具有可交换性，即任意 $k_1$、$k_2$ 和 $x$，满足$((x+ k_2) \bmod M + k_1) \bmod M=((x+ k_1) \bmod M + k_2) \bmod M$。

## 5 安全数据分类协议

本节将结合不经意比较协议 MHash 和前缀成员确认算法设计安全分类协议。

### 5.1 前缀成员确认

为了保护数据隐私不被妥协的存储节点以及少量传感器泄露，本文采用前缀成员技术[37,38]将隶属范围计算变换为成员判断。前缀成员确认技术可以将判断数据是否属于指定范围的问题变换成判断 2 个集合是否存在交集的问题。将数据用二进制表示。$\{0,1\}^k\{*\}^{w-k}$表示 $k$ 长前缀，即首先是 $k$ 个“0”或“1”字符，随后跟着 $w$-$k$ 个“*”字符的前缀。如 2 长度前缀“11***”。$x$ 和 $k$ 长度前缀匹配是指该前缀表达的范围包含了数据 $x$，当该前缀和数据 $x$ 前 $k$ 位是完全一样时，$x$ 一定与该 $k$ 前缀匹配。如 11**和 $x$ 匹配，$x$ 的前 2 位一定是 11。若前缀 $P$ 的范围在前缀 $Q$ 之内，则前缀 $Q$ 称为 $P$ 的祖先前缀。例如，前缀 11**是 110*的祖先前缀。若前缀 $Q$ 为 $P$ 祖先前缀中的最小前缀，则前缀 $Q$ 称为 $P$ 的父前缀。前面 11**即是 110*的父前缀。若一个集合包含了某数据的所有前缀，则该集合在本文称为前缀科(即 Prefix Family)。例如，用二进制 $b_1b_2\cdots b_w$ 表示数据 $N$，则其前缀科为：$\{b_1b_2\cdots b_w, b_1b_2\cdots b_{w-1}*, \cdots, b_1*\cdots*, **\cdots*\}$，用 $F(x)$ 表示，共含 $w$+1 个元素。

对于任意前缀 $P$ 和数据 $x$，$x$ 匹配 $P$ 当且仅当 $P$

属于 $F(x)$。因此，要确认数据 $x$ 和范围$[a, b]$的关系，必须首先转换$[a, b]$为最小前缀集合，表示为 $S([a, b])$，集合中所有前缀代表的范围合并后刚好为$[a, b]$。例如，$S([6, 11])=\{011^*, 10^{**}\}$，随后转换 $x$ 为前缀科 $F(x)$，只有在 $F(x)\cap S([a, b])\neq\Phi$ 时，$x$ 属于范围$[a, b]$。

为了便于集合运算，文献[39]提出一种前缀转换成唯一数字的方法，也是本文采用的方案：通过“1”字符作为分界符，分离“0”或“1”字符和后面的“*”字符，随后用“0”字符表示“*”。例如前缀 101**，先加入分界符得到 1011***，之后替换“*”字符为“0”字符得到 1011000。图 4 是判别数据 2 和范围[0, 4]相互关系的过程。

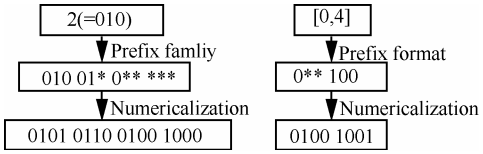



图 4　前缀成员确认

## 5.2　安全分类协议的建立

sink 以设计好的分类规则为基础，建立分类协议，建立步骤如下：1) 变换分类规则的各个区间为前缀；2) 变换前缀为对应的数，模糊化分类结果；3) 用共享密钥 $k_p$ 和 $k_s$ 加密各个数；4) 将最终结果传输至存储节点。

收到加密的结果后，存储节点将其转发至单元内各个传感器。传感器对收到的加密分类规则做如下处理：1) 采用单独和 sink 共享的密钥再次加密分类标准；2）使用散列函数散列加密结果；3) 扰乱分类结果，构建扰乱表后再用单独和 sink 共享的密钥加密；4) 使用随机算法扰乱分类规则；5) 传输处理好的分类规则和扰乱表至存储节点。收到分类规则后，存储节点保存分类规则作为分类标准，并将扰乱表传输至 sink。

图 5 中(1)给出了简单分类规则的一个示例，将属于不同区间的各个数据分到不同的类当中，本示例将用这个简单的分类规则为基础，描述建立分类规则协议的整个过程。从图 5 中(2)开始，sink 首先将所有的区间变换成前缀；随后将前缀全部数值化；由于单个区间总有多个前缀，因此可以用来对分类规则进一步模糊化，即使各个分类结果和各个集合对应，随后随机从集合中抽取一个数来表示分类结果。如图 5 所示，“a”可以对应“Ⅱ、Ⅳ、Ⅸ”，因此，规则[0，11]→a 可变为规则“10100→Ⅸ”和“01000→Ⅳ”，最终实现模糊化。

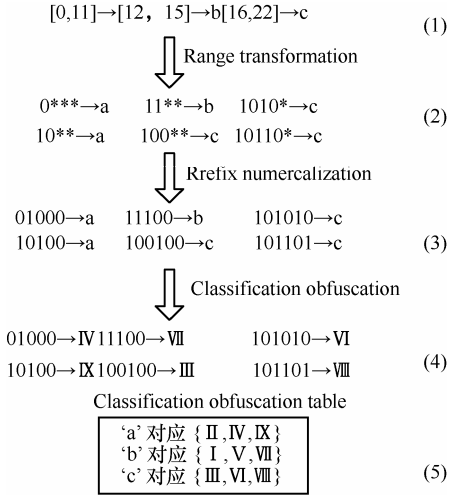



图 5　分类规则预计算示例

上述处理过程完成后，sink 以及各个传感器节点分别加密分类规则，步骤如下：1) sink 使用共享密钥 $k_p$ 和 $k_s$ 加密结果，图 6 中(2)给出了这个过程；2) sink 传输加密结果至存储节点；3) 存储节点将加密结果进一步传输至单元内的所有传感器；4) 传感器节点加密分类规则，并对其进行散列，图 6 中(3)给出了这个过程；5)传感器节点随机扰乱分类结果和规则顺序，图 6 中(4)给出了这个过程；6)传感器节点加密扰乱表，将扰乱表和加密乱后的分类规则全部传输至存储节点；7)存储节点保存分类规则作为对传感器数据的分类标准，并将加密扰乱表传输至 sink。

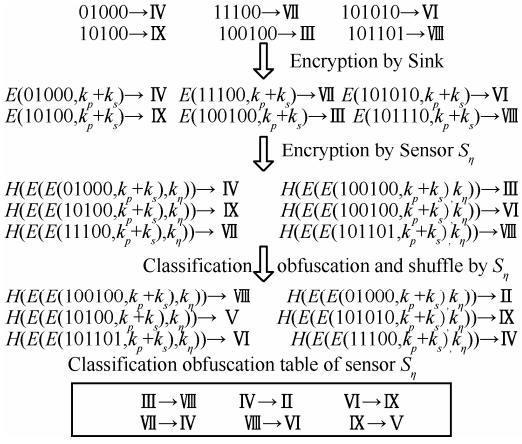



图 6　分类规则加密和扰乱示例

## 5.3　安全分类协议执行

以上是建立分类协议的过程，本节描述如何执

行分类协议。

假定传感器 $S_\eta$ 采集了数据“6”。$S_\eta$ 在周期末对收集的数据处理步骤如下：1) 如图 7 中(2)，转换各个数据为前缀科；2) 如图 7 中(3)，数字化所有前缀；3) 如图 7 中(4)，采用 2 个共享的密钥加密所有数字；4)将加密结果传输至存储节点。收到传感器传输的数据后，存储节点处理步骤如下：1) 如图 7 中(5)，用和 sink 共享的密钥再次加密数据，散列加密结果；2) 利用传感器的分类规来分类。比如，$H(\mathrm{E}(\mathrm{E}(01000, k_p+k_\eta), k_s))=H(\mathrm{E}(\mathrm{E}(01000, k_p+k_s), k_\eta))$，根据规则 $H(\mathrm{E}(\mathrm{E}(01000, k_p+ k_s), k_\eta))\rightarrow$ Ⅱ，分类该数据到第Ⅱ类。存储节点用共享密钥 $k_s$ 加密分类结果后传输至 sink 节点，本示例中存储节点使 sink 知道，传感器节点 $S_\eta$ 在类别Ⅱ中存在数据。sink 进一步对分类结果转换，得到正确的数据和类的映射：1) sink 根据扰乱表获取正确的分类结果，例如 sink 在分类表中得到Ⅳ→Ⅱ，由此知道数据实际要分到类Ⅳ；2)随后以自身的扰乱表为基础得到其所属的真实类，例如本示例中，若存在“a”对应{Ⅱ，Ⅳ，Ⅸ}，则数据最终是类“a”的成员。

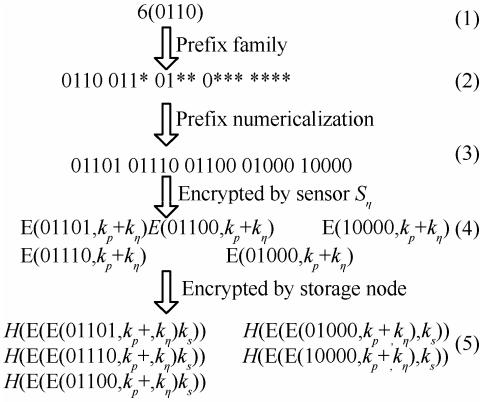



图 7 分类示例

## 6 抽样结果的正确性认证

以上分类协议的建立可以确保存储节点执行正确分类的同时不获取传感器采集数据和分类规则的实际值，随后将分类结果传输至 sink。然而妥协的存储节点可能会修改分类结果，因此本文通过抽样认证实现对分类结果的认证，检测存储节点的恶意行为，即由 sink 集中指定特定存储节点反馈特定传感器特定区间中的数据抽样认证分类结果。和范围查询协议的完整性认证方案不同在于，已有方法是以有序数据为基础的，数据通常事先排好序或者根据编码排序，本文算法则通过加密和散列使数据的大小信息无法分辨，且数据完全保持无序状态，然而在存储节点返回空数据结果时，算法无法区分是否确实无数据还是因为存储节点恶意删除了数据。

本文设计了“十”字邻居技术认证抽样结果完整性。“十”字邻居技术从 2 个角度使传感器节点采集的数据具备相关性：相关同节点的数据和相关相邻传感器节点的数据。首先连接传感器节点形成链。即在周期末将各个传感器的数据传输至其前驱节点，如图 8 所示。传感器的前驱是指这个传感器可以通过一跳通信到达的节点，而 sink 知道该链信息。执行了上面的步骤后，本文排序各个传感器节点的数据(包含各个后继的数据)，在数据间形成邻居关系。假定传感器 $S_1$ 是 $S_2$ 的前驱，$S_1$ 在某周期内获取数据{3，5，6，8}，$S_2$ 获取数据{5，8，9}，$S_2$ 同步数据到 $S_1$，则数据邻居链如图 9 所示，其中的二进制符号“01”、“10”、“11”用来区分该数据属于本地节点还是后继节点，“01”表示数据属于后继节点，“10”表示数据属于本身节点，“11”表示数据同时属于后继节点和本身节点。

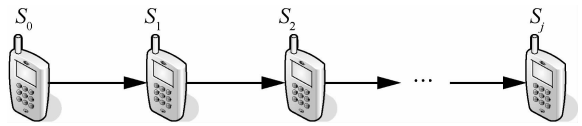



图 8 传感器节点链

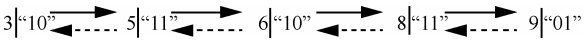



图 9 数据链

本文只计算和加密传感器自身采集数据的前缀科，直接嵌入后继节点数据，这样才能确保分类结果的正确性。数据链则基于 SafeQ 中提出的邻居链技术实现，如图 10 所示，加密图 9 的 3 个数据“5”，“6”，“8”得到数据链。

$$(3|\text{“10”}|5|\text{“11”}|6|\text{“10”})_{kl}(5|\text{“11”}|6|\text{“10”}|8|\text{“11”})_{kl}(6|\text{“10”}|8|\text{“11”}|9|\text{“01”})_{kl}$$

图 10 加密数据链

### 6.1 数据同步

相邻传感器之间如何实现数据同步建立联系是本节主要讨论的问题。若直接传输传感器的数据至它的前驱节点，会造成较大通信开销，经过详细分析 Intel Lab 的实际采集数据，发现被采集的数据重复率在同一个周期的相邻节点间很高，统计一维

数据的情形发现，数据平均重复率在同周期相邻节点之间高达 91.3%。文献[40]利用普通传感器网络相邻节点间的采集数据重复较大的特点研究了数据压缩算法。本文结合倒置布鲁姆过滤器[41]技术实现数据传输，减少节点间的通信开销。

若 2 个数据集的不同数据共有 $d$ 个，倒置布鲁姆过滤器消耗 $O(d)$空间就足够以较大的概率同步这 2 个数据集，同时不需要考虑数据集的元素个数。倒置布鲁姆过滤器的基础是布鲁姆过滤器的和异或运算的特殊性。异或具有如下特性：$x \oplus y=y \oplus x$；$x \oplus x=0$；$x \oplus 0=x$。倒置布鲁姆过滤器的各个单元包含 3 个元素，即数据异或值 DataSum，数据散列结果异或值 HashSum 和计数器 count。数据散列结果异或可以用于指定单元具有单个还是多个异或结果，此时计数器值是 1 或−1。倒置布鲁姆过滤器的基础构成是同构的布鲁姆过滤器结构，对倒置布鲁姆过滤器执行减法运算是指二者各个对应单元的计数器执行减法运算，数据散列异或值和数据异或值随后相应异或。该运算可以表达为 IBF($C$)-IBF($D$)=IBF($C$-$D$)，其中 $C$ 和 $D$ 是集合，$C$-$D$ 是 2 个集合中的不重复数据；如 $C$={$a$，$b$，$c$，$d$}，$D$={$b$，$d$，$e$，$f$}，那么 $C$-$D$={$a$，$c$，$e$，$f$}。

以下描述本文方案中倒置布鲁姆过滤器的整体工作流程，仍然采用以上的例子来说明。假定传感器节点 $S_1$ 是 $S_2$ 的前驱，同一周期内，$S_1$ 获得数据{3，5，6，8}，$S_2$ 获得数据{5，8，9}。二者分别建立图 11(a)以及图 11(b)所示的倒置布鲁姆过滤器。$S_2$ 将建立的倒置布鲁姆过滤器传输至 $S_1$，$S_1$ 计算如图 11(c)的结果 $IBF_3$=$IBF_1$−$IBF_2$。

根据 $IBF_3$ 传感器节点 $S_1$ 能够恢复节点间的不同数据。首先扫描布鲁姆过滤器计数器值等于 1 或者−1 的部分，对比 HashSum 和 DataSum 散列值。若存在 HashSum 和 $H$(DataSum)相等，则取出相应部分的数据，删除布鲁姆过滤器中对应这些数据的信息，反复操作。图 12 给出了利用 $IBF_3$ 恢复了数据 3 的整个过程。若计数器值等于“1”，恢复的数据属于 $IBF_2$，不属于 $IBF_1$；反之，若计数器值等于“−1”，恢复的数据属于 $IBF_1$，不属于 $IBF_2$。

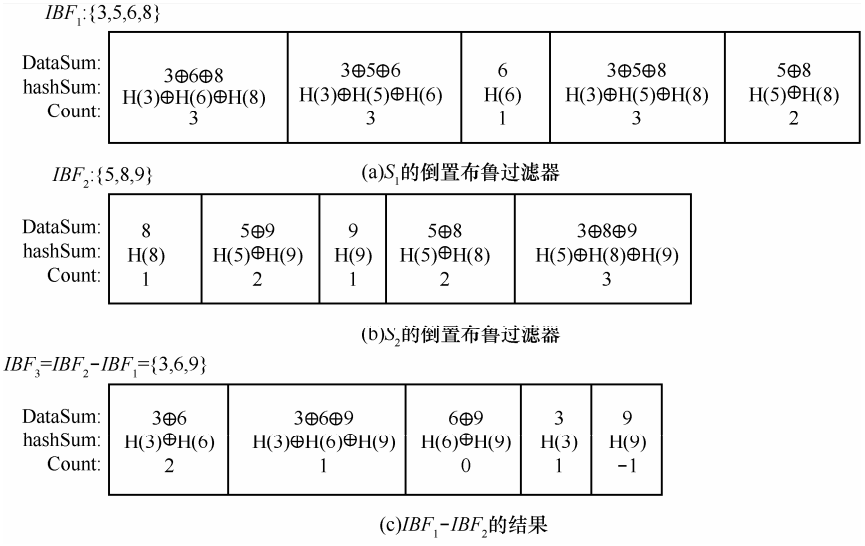



图 11　IBF 示例

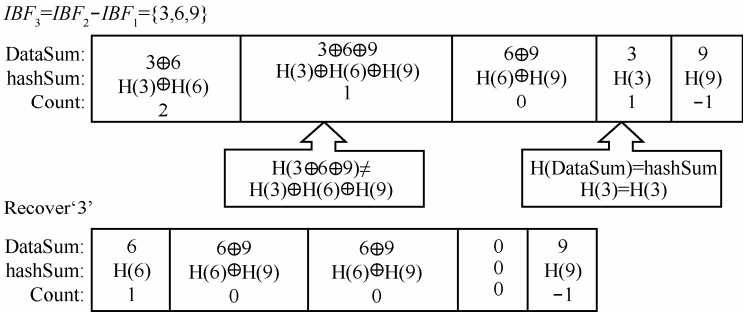



图 12　数据恢复示例

倒置布鲁姆过滤器只有在散列表中存在至少一个 count 等于 1 或−1，同时 hashSum 和 DataSum 散列值相等才能恢复数据，这种情形的出现概率很高[41]。数据集间有 $d$ 个不同数据且散列函数有 $k$ 个时，恢复数据失败的概率是 $O(d^{-k})$。本文的方案中，只需在抽样反馈结果为空时，恢复抽样节点的数据已确认结果。传感器节点在传输倒置布鲁姆过滤器时，采用前驱和后继节点间的共享密钥事先加密以保护数据隐私[42]。

### 6.2 抽样结果正确性的认证

分类结果的正确性认证有 2 种情况。

1) 抽样区间的分类结果有数据

当抽样区间存在数据即不为空时，存储节点反馈数据后，sink 节点解密这些数据得到原始数据，随后进行判断：① 数据链必须连续；② 抽样区间内，最大数据的后继和最小数据的前驱形成的区间必须覆盖整个抽样区间。只有同时满足这 2 个条件，且区间内传感器获得的数据和分类结果个数吻合，则分类结果正确，反之错误。

2) 反馈的抽样区间没有数据

当抽样区间不存在数据即为空时，则需分 2 种情况来确认结果的正确性。第一，节点的各个区间统计值不是全部为零，则解密抽样区间最接近的区间内的数据来计算相关数据；假定抽样区间边界比最近区间边界要大，那么可以通过判断抽样区间是否包含于最近区间内的最大数据和其后继形成的区间，若包含，则分类结果正确，反之错误。第二，节点的各个区间统计值全部等于零，则 sink 对节点前驱统计值进行查找，若前驱各个区间统计值不是全不等于零，则通过解密这些不等于零的区间内数据来判别前驱是否存在节点的数据，若存在，则分类结果错误，反之能以很高概率判断分类的正确性。

## 7 分析

本节主要分析 SSC 协议的算法复杂度和安全性。算法复杂度有空间和时间复杂度，安全性则包含隐私性和正确性。

### 7.1 复杂度分析

假设 sink 分类规则含类 $m$ 个，传感器节点单个周期采集数据 $n$ 个，相邻传感器有不同数据 $d$ 个。表 1 给出了本文方案的最坏情况下计算复杂度以及通信开销、空间复杂度。

**表 1 SSC 协议中的算法复杂度分析**

| 节点名 | 计算复杂度 | 通信开销 | 空间复杂度 |
|---|---|---|---|
| 传感器 | $O(m)$ Rule Processing<br>$O(n)$ Data Encryption<br>$O(n)$ IBF Construction<br>$O$(d) IBF Data recovery | $O(m)$ Rule<br>$O(n)$ Encrypted Data<br>$O(d)$Data Synchro-niz –ation | $O(n)$<br>$O(d)$ |
| 存储节点 | $O$(1) Rule Processing<br>$O(n)$ Data encryption and Classification | $O(m)$ Classification Results | $O(m)$ |
| sink | $O(m)$ Rule Processing | $O$(m) Rules | $O(m)$ |

### 7.2 安全性分析

1) 分类协议隐私性

SSC 协议能在有妥协存储节点的情形下确保 sink 分类规则的隐私。这是由于 sink 对分类规则做了如下处理：1) 转换范围为前缀，单个范围可以对应多个前缀，同时扰乱分类结果，因此存储节点很难通过数据值本身分析出分类规则的真实值；2) 用 2 种共享密钥对数据进行加密，存储节点很难在不知道密钥时解密结果；3) 用共享密钥加密和散列分类规则，同时通过各个传感器节点单独扰乱，存储节点几乎无法通过处理后结果分析分类规则。部分传感器被妥协时，存储节点和 sink 共享的密钥不被知道的情形下，分类规则也很难破解。

接下来进一步分析分类规则，若存储节点和其同单元的某个传感器节点同时被妥协，且相应密钥也被知道，那么 sink 的分类规则将被解密，然而由于规则被重新扰乱，因此分类规则的确切值仍然很难知道；此外，剩下的传感器上的规则也不会被知道，这是由于这些规则是用 sink 和传感器单独共享密钥进行了加密和散列处理，各个分类规则也再次执行了扰乱，所以剩下节点上的规则确切值也不会被知道。

2) 传感器数据和分类结果的隐私性

SSC 协议采用 2 种密钥对对传感器数据进行加密，即单元内的共享密钥和节点的独立共享密钥，妥协的存储节点在不知道密钥实际值的情况下，较难破解数据的实际值；此外，各个传感器的分类规则都具备了本身的特征，因此数据的分类结果真实值很难被攻击者获取。

3) 抽样结果正确性

指定抽样节点的区间统计值不等于零，就可以完全认证分类结果的正确性。而该区间统计值等于零时，需要看该节点的前驱节点提供的数据是否包含该节点数据，含有此类数据，但无法通过倒置布鲁姆过滤器对数据进行恢复，则恶意行为无法判断，数据正确性也认证不了。这种情况发生的概率

为 $O(d^{-k})$[41]，而 $k$=3，$d$>5 时这种情形出现的概率极小，因此本文算法不能认证数据正确性，检测恶意行为的概率非常小。

## 8　实验

本文以网内传输的数据量和分类结果数据量大小来评估算法性能，最终验证所提协议(SSC)的有效性。算法在 OMnet++上仿真，实验数据集是 Intel Lab[7]部署的 44 个传感器节点在 2004 年 1 月 3 日到 2004 年 3 月 10 日之间采集的数据。实验将 44 个节点分成 4 组，每组含 11 个传感节点，并带有存储节点。sink 通过将分类规则分发到传感器节点和存储节点以建立分类协议，因此首要分析的是分类规则带来的传输功耗。如图 13 所示，在不同的分类粒度大小下，非加密和加密分类规则传输功耗不断变少，分类数目也随着分类粒度增大而减少。加密规则是非加密规则的 8 倍，但占用空间有限的分类规则产生的传输功耗并不大，传感网络还是可以承受。

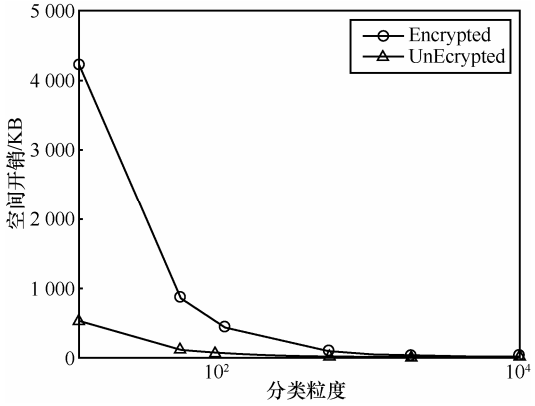



图 13　分类规则的传输功耗

传感器节点将采集的数据加密并计算其前缀编码。接下来需要分析的是前缀编码所消耗的传输功耗。不采用前缀编码和采用前缀编码时，网内数据传输量如图 14 所示，前者功耗不会随分类粒度大小发生变化，传输量一直是 $2.23\times10^5$ KB，后者功耗随着分类粒度的变大而增大，在粒度为 100 和 10 000 时，功耗相对前者分别增加 24.7%和 53.6%。在此期间前缀编码是不断增长的。前缀编码引入了额外的传输功耗，但这部分功耗很小，随后的分类机制大大减少了网内数据的传输量。

存储节点在分类结束后会向 sink 反馈最终的分类统计的结果，因此，需要对其传输功耗和延迟进一步进行分析。如图 15 所示，非加密和加密的分类结果在分类粒度不断变大时，功耗会逐渐减少，加密结果的功耗在同等条件下是非加密结果的 7 倍。如图 16 所示，固定分类粒度大小为 100，采用不分类和本文的分类协议时，分类情形下的传输功耗一直是 $0.13\times10^5$KB，而不分类情形下传输功耗随着数据量增大而迅速增长，该功耗是分类情形下的数十倍甚至上百倍。例如数据量分别为 1 338、5 741、11 677，16 854 时，非分类的传输功耗分别为 $0.17\times10^6$ KB、$0.74\times10^6$ KB，$1.49\times10^6$ KB，$2.16\times10^6$ KB，分别是分类传输功耗的 12.38、56.41、115.77、167.54 倍。

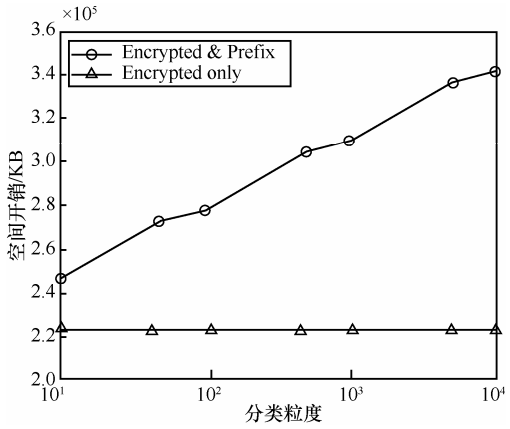



图 14　数据传输功耗

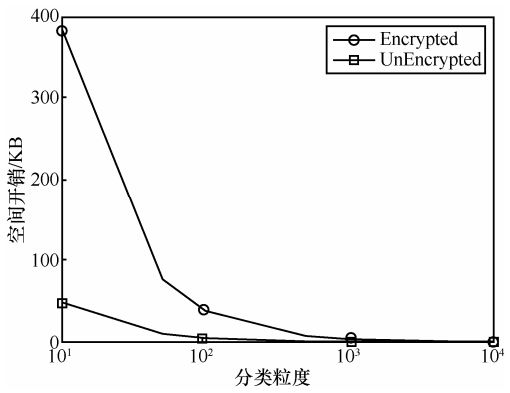



图 15　分类结果的空间开销

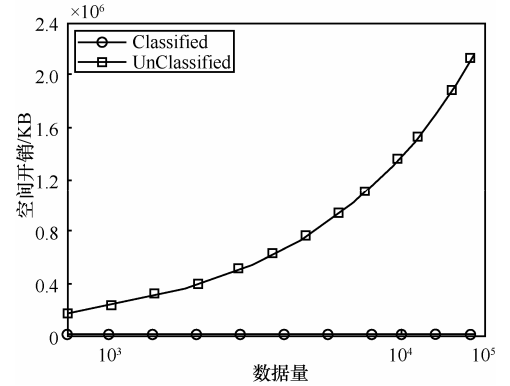



图 16　分类和不分类空间开销比较

如图 17 所示，存储节点的传输延迟在同样数据量的情形下，若经 1-2 跳传输至 sink，分类方案比非分类方案高出 9 到 1.5 倍，3 跳以上时，分类方案的传输延迟开始具有优势，低于非分类方案 37.5%以上。

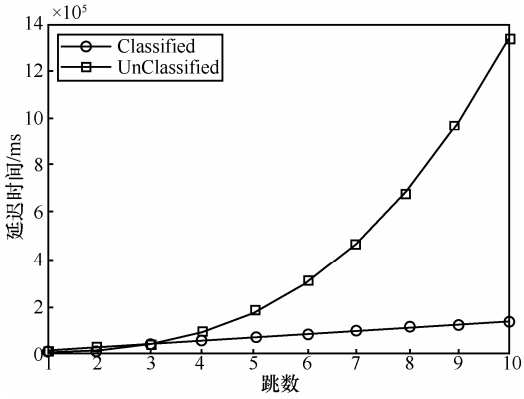



图 17 传输延迟

## 9 结束语

无线传感器网络中进行特定目标的识别和跟踪的基础技术是分类统计，本文以两层传感器网络自身的特点设计了一套安全的分类协议 SSC。该协议中，待分类敏感数据和分类规则的真实值不被存储节点所知，但仍能进行正确的分类。本文通过提出不经意比较技术 MHash 保护了传感器采集数据和分类规则的隐私性。利用该技术，存储节点能够在不知道任何数据真实值的情况下判断数据实际值是否相等；本文进一步通过结合前缀成员确认算法和 MHash 协议实现对未知数据的最终正确分类。此外，本文通过”十”字邻居技术认证了分类统计最终结果的正确性。该技术首先组织传感器节点形成链，使用倒置布鲁姆过滤器同步各个传感器节点和其相应前驱节点的数据，随后以排序方法组织各个节点的数据形成链。利用该技术，sink 可以对分类统计的最终结果进行抽样检查。本文算法最终在 Intel Lab[7]提供的数据集上进行了验证，证实算法的有效性。

## 参考文献：


[1] 李建中, 李金宝, 石胜飞. 传感器网络及其数据管理的概念、问题与进展[J]. 软件学报, 2003,14(10):1717-1727.
LI J Z, LI J B, SHI S F. Concepts, issues and advance of sensor networks and data management of sensor networks[J]. Journal of Software, 2003, 14(10):1717-1727.

[2] 崔莉, 鞠海玲, 苗勇等. 无线传感器网络研究进展[J]. 计算机研究与发展, 2005,42(1):163-174.
CUI L, JU HL, MIAO Y, *et al*. Overview of wireless sensor network[J]. Computer Research and Development, 2005, 42(1): 163-174.

[3] 唐勇, 周明天, 张欣. 无线传感器网络路由协议研究进展[J]. 软件学报, 2006,17(3):422-433.
TANG Y, ZHOU M T, ZHANG X. Overview of routing protocols in wireless sensor networks[J]. Journal of Software, 2006, 17(3): 410-421

[4] HU W, TRAN V N, BULUSU N, *et al*. Design and evaluation of a hybrid sensor network for cane-toad monitoring[J]. ACM Transactions on Sensor Networks, 2009, 5(1): 1-28.

[5] DESNOYERS P, GANESAN D, LI H, *et al*. PRESTO: a predictive storage architecture for sensor networks[A]. Proceeding of Workshop on Hot Topics in Operating Systems (HotOS’05)[C]. Berkeley, CA: USENIX Association, 2005.

[6] RATNASAMY S, KARP B. SHENKER S, *et al*. Data-centric storage in sensor nets with ght, a geographic hash table[J]. Mobile Networks and Applications, 2003,4(8):427-442.

[7] Intel lab data[EB/OL]. http://berkeley.intel-research.net/ labdata.

[8] WANG Q, CHEN W, ZHENG R, *et al*. Acoustic target tracking using tiny wireless sensor devices[A]. Proc of 2nd Intl Conf on Information Processing in Sensor Networks[C]. Palo Alto, CA, 2003.642-657.

[9] HE T, KRISHNAMURTHY S, STANKOVIC J A, *et al*. An energy-efficient surveillance system using wireless sensor networks[A]. Proc of Intl Conf on Mobile Systems, Applications, and Services[C]. Boston, MA, 2004.270-283.

[10] BROOKS R R, SAYEED A M. Distributed target classification and tracking in sensor networks[J]. Proceedings of the IEEE, 2003, 91(8): 1163-1171.

[11] GU L, JIA D, VICAIRE P, *et al*. Lightweight detection and classification for wireless sensor networks in realistic environments[A].Third ACM Conference on Embedded Networked Sensor Systems[C]. New York: ACM Press, 2005.205-217.

[12] HUANG Q, XING T, LIU H. Vehicle classification in wireless sensor networks based on rough neural networks[A]. Proceedings of the 2nd IASTED International Conference on Advances in Computer Science and Technology[C]. Anaheim: ACTA Press, 2006.141-144.

[13] PAI H, HAN Y, SUNG J. Two-dimensional coded classification schemes in wireless sensor networks[J]. IEEE Transactions on Wireless Communications, 2008, 7(5): 1450-1455.

[14] KULAKOV A, DAVCEV D, TRAJKOVSKI G. Implementing artificial neural-networks in wireless sensor networks[A]. Proceedings of IEEE Sarnoff Symposium on Advances in Wired and Wireless Communications[C]. Piscataway: IEEE, 2005.94-97.

[15] ZHAO F, LIU J, GUIBAS L, *et al*. Collaborative signal and information processing: an information directed approach[A]. Proceedings of the IEEE, Piscataway[C]. 2003, 91(8): 1199-1209.

[16] PATTEM S, PODURI S, KRISHNAMACHARI B. Energy-quality tradeoffs for target tracking in wireless sensor networks[A]. Proc of 2nd Intl Conf on Information Processing in Sensor Networks[C]. Berlin: Springer-Verlag, 2003.32-46.

[17] WANG H, ESTRIN D, GIROD L. Preprocessing in a tiered sensor network for habitat monitoring[J]. EURASIP Journal on Applied Signal Processing, 2003(4): 392-401.

[18] SHENG B, LI Q. Verifiable privacy-preserving sensor network storage for range query[J]. IEEE Transaction on Mobile Computing, 2011, 10(9): 1312-1326.

[19] SHI J, ZHANG R, ZHANG Y. A spatiotemporal approach to secure range queries in tiered sensor networks[J]. IEEE Transactions on Wireless Communications. 2011,10(1): 264-273.

[20] ZHANG R, SHI J, ZHANG Y, *et al*. Secure cooperative data storage and query processing in unattended tiered sensor networks[J]. IEEE

Journal on Selected Areas in Communications, Special Issue on Co-operative Networking Challenges and Applications, 2012, 30(2): 433-441.

[21] HACIGUMUS H, IYER B, LI C, *et al*. Executing sql over encrypted data in the database-service-provider model[A]. Proc ACM Inte Conf on Management of Data (SIGMOD2002)[C]. 2002. 216-227.

[22] HORE B, MEHROTRA S, TSUDIK G. A privacy-preserving index for range queries[A]. Proc 30th Inte Conf on Very Large Data (VLDB2004)[C]. 2004.720-731.

[23] 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.

[24] YI Y Q, LI R, CHEN F, *et al*. A digital watermarking approach to secure and precise range query processing in sensor networks[A]. Proceedings of the IEEE Conference on Computer Communications 2013 (INFOCOM2013)[C]. Turin, Italy, 2013.

[25] ZHANG R, SHI J, LIU Y Z, *et al*. Verifiable fine-grained top-*k* queries in tiered sensor networks[A]. Proceeding of IEEE International Conference on Computer Communications (INFOCOM 2010)[C]. Piscataway, NJ: IEEE, 2010. 1199-1207.

[26] 范永健, 陈红. 两层传感器网络中可验证隐私保护的 top-*k* 查询协议[J]. 计算机学报. 2012, 35(3): 423-433.
FAN Y J, CHEN H. Verifiable privacy-preserving top-*k* query protocol in two-tiered sensor networks[J]. Chinese Journal of Computers, 2012,35(3):423-433.

[27] 李睿, 林亚平, 易叶青等. 两层传感器网络中安全 top-*k* 查询协议[J]. 计算机研究与发展, 2012, 49(9):1947-1958.
LI R, LIN YP, YI Y Q, *et al*. A secure top-*k* query protocol in two-tiered sensor networks[J]. Computer Research and Development, 2012,49(9):1947-1958.

[28] 廖小静, 李建中, 余磊. 一种能量有效的双层传感器网络安全 top-*k* 查询机制[J]. 计算机研究与发展, 2013, 50(3): 490-497.
LIAO X J, LI J Z, YU L. Secure and efficient top-*k* query processing in two-tier sensor network[J]. Computer Research and Development, 2013, 50(3): 490-497.

[29] 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, 33(12):58-68.
LI R, LIN Y P, LI J G. Efficient conditional aggregation of encrypted data in tiered sensor networks[J]. Journal on Communications, 2012,33(12):58-68.

[30] CHAN H, PERRIG A, SONG D. Secure hierarchical in-network aggregation in sensor networks[A]. Proceedings of the 13th ACM Conference on Computer and Communications Security[C]. New York: ACM Press, 2006.278-287.

[31] YANG Y, WANG X. ZHU S, *et al*. Sdap: a secure hop-by-hop data aggregation protocol for sensor networks[J]. ACM Transactions on Information and System Security, 2008, 11(4):1-43.

[32] YAO Y Y, XIONG N, PARK J, *et al*. Privacy-preserving max/min query in two-tiered wireless sensor networks[J]. Computer and Mathematics with Application, 2012, 2: 1-8.

[33] AGRAWAL R, EVFIMIEVSKI A, SRIKANT R. Information sharing across private databases[A]. Proceedings of the 2003 ACM SIGMOD International Conference on Management of data[C]. New York: ACM Press, 2003. 86-97.

[34] BAWA M, BAYARDO R R. Privacy-preserving indexing of documents on the network[A]. Proceedings of the 29th International Conference on Very Large Data Bases[C]. Berlin: VLDB Endowment, 2003.922-933.

[35] HORE B, MEHROTRA S, TSUDIK G. A privacy-preserving index for range queries[A]. Proceedings of the 30th International Conference on Very Large Data Bases[C]. Toronto: VLDB Endowment, 2004. 720-731.

[36] CHENG J, YANG H, WONG S, *et al*. Design and implementation of cross-domain cooperative firewall[A]. IEEE International Conference of Network Protocol Piscataway IEEE[C]. 2007.284-293.

[37] CHENG J, YANG H, WONG S H, *et al*. Design and implementation of cross-domain cooperative firewall[A]. Proc International Conference on Network Protocols[C]. Piscataway: IEEE, 2007. 284-293.

[38] LIU A X, CHEN F. Collaborative enforcement of firewall policies in virtual private networks[A]. Proceedings of the Twenty-Seventh ACM Symposium on Principles of Distributed Computing[C]. New York: ACM Press, 2008: 95-104.

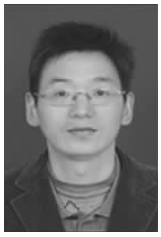
[39] CHANG Y K. Fast binary and multiway prefix searches for packet forwarding[J]. Computer Networks, 2007, 51(3): 588-605.

[40] HU Y P, LI R, ZHOU S W, *et al*. CCS-MAC: Exploiting the overheard data for compression in wireless sensor networks[J]. Computer Communication, 2011,34: 1696-1707.

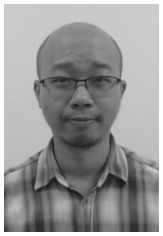
[41] EPPSTEIN D, GOODRICH M T, UYEDA F, *et al*. What's the difference? efficient set reconciliation without prior context[A]. ACM SIGCOMM Computer Communication Review[C]. New York: ACM Press, 2011: 218-229.

[42] XIAO S, GONG W, TOWSLEY D. Secure wireless communication with dynamic secrets[A]. Proc IEEE Inte Conf on Computer Communications, Piscataway: IEEE[C]. 2010.1-9.

## 作者简介：



**李睿**（1975-），男，湖南汨罗人，博士，湖南大学副教授，主要研究方向为无线传感器网络、网络安全、云计算安全。



**李晋国**（1985-），男，湖南衡阳人，博士，上海电力学院讲师，主要研究方向为信息安全。

**陈浩**（1975-），男，湖南邵阳人，博士，湖南大学副教授，主要研究方向为移动推荐、网络安全。