# TMWSNs中一种确保数据完整性的高能效时空Top-$k$查询协议

马行坡[1],危 锋[2],梁俊斌[3],李 然[1],马文鹏[1],祁传达[1]
(1.信阳师范学院计算机与信息技术学院,河南信阳 464000;2.河南经贸职业学院计算机工程学院,河南郑州 450046;
3.广西大学计算机与电子信息学院,广西南宁 530004)

**摘 要:** 时空Top-$k$查询是TMWSNs(双层移动无线传感网)中的一类重要查询.在敌对环境中,攻击者易通过捕获TMWSNs中的关键节点来破坏时空Top-$k$查询的数据完整性.提出一种确保数据完整性的时空Top-$k$查询处理协议VIP-TQ.该协议利用虚拟化节点技术与绑定加密技术通过构建传感器节点的数据预处理方法、数据存储节点的时空Top-$k$查询处理方法以及Sink端的数据完整性验证方法来实现TMWSNs中时空Top-$k$查询的数据完整性保护.理论分析和实验结果显示,VIP-TQ能够以100%的概率侦测出不完整的时空Top-$k$查询结果,并具有相对已有方案更高的能效性.

**关键词:** 双层可移动传感器网络;时空Top-$k$查询;完整性保护;位置关联;多层协作
**中图分类号:** TP393 **文献标识码:** A **文章编号:** 0372-2112 (2018)05-1274-07
**电子学报URL:** http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2018.05.039

# An Integrity-Verifiable Protocol for Spatio-Temporal Top-$k$ Queries in Two-Tiered Mobile Wireless Sensor Networks

MA Xing-po[1],WEI Feng[2],LIANG Jun-bin[3],LI Ran[1],MA Wen-peng[1],QI Chuan-da[1]
(1. *School of Computer and Information Technology,Xinyang Normal University,Xinyang,Henan* 464000,*China*;
2. *School of Computer Engineering,Henan Institute of Economics and Trade,Zhengzhou,Henan* 450046,*China*;
3. *School of Computer and Electronic Information,Guangxi University,Nanning,Guangxi* 530004,*China*)

**Abstract:** Spatio-temporal Top-$k$ query results in TMWSNs (Two-tiered Mobile Wireless Sensor Networks) are facing threats. To preserve the integrity of the Top-$k$ query results in TMWSNs, a novel integrity-ensured protocol named VIP-TQ is proposed for spatio-temporal Top-$k$ queries in TMWSNs in this paper. VIP-TQ achieves integrity preserving for spatio-temporal Top-$k$ queries by using several novel techniques such as node virtualization and binding encryption, and some novel methods such as the method of data pre-processing on the sensor nodes, the method of spatio-temporal Top-$k$ query processing on the data storage node and the method of completeness verification on the Sink node. Theoretical analysis and simulation results show that VIP-TQ can detect the incomplete Top-$k$ query results with probability 100% with high energy efficiency.

**Key words:** two-tiered mobile wireless sensor networks; spatio-temporal Top-$k$ queries; integrity preservation; location correlation; multilayer cooperation

## 1 引言

双层可移动无线传感器网络(Two-tiered Mobile Wireless Sensor Networks,TMWSNs)是下层存在可移动传感器节点[1,2]的双层传感器网络[3],其结构模型如图1所示.在TMWSNs中,存在一类重要的查询类型,即时空Top-$k$查询[4~7].它是指对某一指定区域内的传感器节点在指定时间周期内产生的数据项进行Top-$k$查询.然而,这类查询正面临一定的安全威胁.由于位于TMWSNs结构模型上层的数据存储节点是网络的关键节点,在不安全环境中,易被攻击者捕获而成为妥协节点.利用妥协的数据存储节点,攻击者可通过篡改、丢弃

收稿日期:2017-01-21;修回日期:2017-10-01;责任编辑:孙瑶
基金项目:国家自然科学基金(No.61702438,No.61501393,No.61562005);河南省自然科学基金面上项目(No.162300410234);信阳师范学院南湖学者奖励计划;信阳师范学院校青年骨干教师资助计划(No.2015GGJS—06)

保存在数据存储节点上的合法 Top-$k$ 数据项等多种攻击方式来破坏时空 Top-$k$ 查询结果的数据完整性[3].

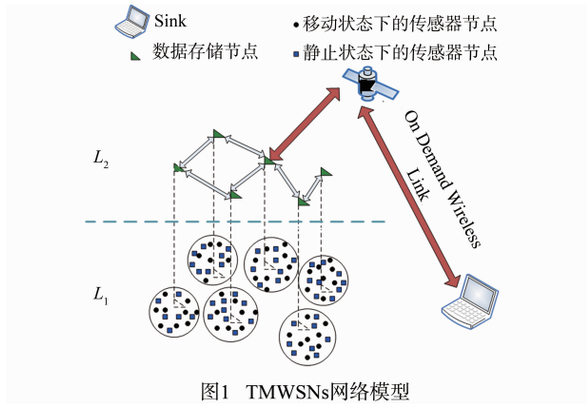


图1　TMWSNs网络模型

针对这一问题,研究人员提出的解决方法主要包括:基于消息验证码的验证方法[3,8~10]、基于数据汇聚树的验证方法[11,12]、基于数据项加密链的验证方法[13]、基于概率空间的邻居验证方法[14]、基于水印嵌入的链式验证方法[15,16]、基于仿造感知数据(Dummy Readings)的验证方法[17]等. 然而,这些方法都基于一个共同前提,即假设传感器节点是静止的,每个节点产生的数据项都对应相同的数据产生位置[18]. 然而,由于已有方法主要面向静态网络,所研究的 Top-$k$ 查询类型也都属于时间域上的,因而不能防止恶意化的数据存储节点将传感器节点在不同区域内产生的感知数据之间相互替代. 虽然目前有极少数学者针对这一问题提出了一些解决方案[19,20],但这些方案仍存在一些问题,比如,用于安全验证的冗余信息过多,增大了网络的额外通信开销.

为了提高 TMWSNs 中时空 Top-$k$ 查询的安全性和能效性,弥补已有方案的不足,本文提出了一种新的时空 Top-$k$ 查询数据完整性保护协议 VIP-TQ(Verifiable Integrity Protection for Top-$k$ Queries). VIP-TQ 主要通过虚拟化动态节点,建立虚拟化节点的感知数据项与感知数据项、感知数据项与位置信息之间的绑定关系,并设计特定的时空 Top-$k$ 查询数据完整性验证算法来实现时空 Top-$k$ 查询的完整性保护,所包含的主要机制和算法有:传感器节点上的感知数据与位置信息预处理机制,数据存储节点上的查询处理机制以及 Sink 端的时空 Top-$k$ 查询数据完整性验证算法.

## 2　网络模型

TMWSNs 的网络模型如图 1 所示,分为 $L_1$,$L_2$ 两层. 其中,$L_1$ 层是由资源有限、通讯半径较短的可移动传感器节点组成的多跳自组织网络,$L_2$ 层是由多个资源丰富、通讯半径较长的数据存储节点组成的 Mesh 网. 整个被监测区域被划分为 $M$ 个单元,任意单元内部署一个数据存储节点 $H_c(1\leqslant c\leqslant M)$ 和 $N$ 个传感器节点 $\{S_{1,c},S_{2,c},S_{3,c},\cdots,S_{N-1,c},S_{N,c}\}$(其中包含部分或全部可移动传感器节点). $S_{i,c}(1\leqslant i\leqslant N,1\leqslant c\leqslant M)$ 可通过单跳或多跳的方式与 $H_c$ 通讯,并能根据应用需要向目标位置移动,到达目标位置后停止移动并对目标环境展开监测. 假设 $S_{i,c}$ 仅在其所属单元内移动,并假设 $S_{i,c}$ 只在静止状态下才启动感知器件并对周围环境进行监测. 为便于描述,下文将 $S_{i,c}$ 简写为 $S_i$.

令 $T$ 表示 TMWSNs 网络的生命周期,$T$ 被均匀划分为 $x$ 个大小相等的时间区间 $T_t(1\leqslant t\leqslant x)$,即 $T=|T_1|+|T_2|+|T_3|+\cdots+|T_{x-1}|+|T_x|$($|T_1|=|T_2|=|T_3|=\cdots=|T_{x-1}|=|T_x|$). 其中,$T_t(1\leqslant t\leqslant x)$ 表示时间区间 $T_t$ 的宽度. 用 $\lambda_i$ 表示 $S_i$ 在 $T_t$ 内停留过的位置个数,$L_{i,j}$ 表示 $S_i$ 在 $T_t$ 内的第 $j$ 个停留位置,$\mu_{i,j}$ 表示 $S_i$ 在 $T_t$ 内在 $L_{i,j}$ 处产生的数据项的个数,$D^v_{L_{i,j}}$ 表示 $S_i$ 在 $T_t$ 内在 $L_{i,j}$ 处产生的大小排行第 $v$ 的感知数据项,则 $S_i$ 在 $T_t$ 内停留过的位置集合可表示为 $\{L_{i,1},L_{i,2},L_{i,3},\cdots,L_{i,\lambda_{i-1}},L_{i,\lambda_i}\}$,$S_i$ 在 $T_t$ 内在 $L_{i,j}$ 处产生的数据项集合可表示为 $\{D^1_{L_{i,j}},D^2_{L_{i,j}},D^3_{L_{i,j}},\cdots,D^{\mu_{i,j}-1}_{L_{i,j}},D^{\mu_{i,j}}_{L_{i,j}}\}$. 在任意时间区间 $T_t(1\leqslant t\leqslant x)$ 结束时,$S_i(1\leqslant i\leqslant N)$ 将其在 $T_t$ 内产生的感知数据项发送到 $H_c(1\leqslant c\leqslant M)$ 进行存储. Sink 节点可通过按需无线链路向 $H_c$ 发送查询请求,并从 $H_c$ 那里获取查询结果.

假设网络中存在一个公共权重评估函数 $f(\cdot)$[21],此评估函数主要用来计算各个数据项的重要程度(权重). 数据项 $D^v_{L_{i,j}}$ 的权重可表示为 $d^v_{L_{i,j}}=f(D^v_{L_{i,j}})$. 由于对涉及多个单元的时空 Top-$k$ 查询可以划分为多个仅涉及单个单元的时空 Top-$k$ 查询,因此,下文中提到的时空 Top-$k$ 查询主要是指仅涉及单个单元的细粒度(Fine-Grained)[3]时空 Top-$k$ 查询,并用 $H$ 表示所关注单元的数据存储节点. 一个细粒度时空 Top-$k$ 查询原语 $Q_t$ 可表示如下:

$$Q_t=<SR,c,t,k> \tag{1}$$

其中,$SR$(Sub-Region)表示被查询区域,$c$ 表示单元 ID 号,$t$ 表示时间区间序号,$k$ 即为 Top-$k$ 查询的 $k$ 值.

## 3　Top-$k$ 查询处理协议 VIP-TQ

分别从传感器节点的数据预处理、数据存储节点的时空 Top-$k$ 查询处理以及 Sink 节点对查询结果的完整性验证三个层次和阶段来介绍 VIP-TQ 协议的具体内容.

### 3.1　传感器节点的数据预处理

在当前时间区间 $T_t(1\leqslant t\leqslant x)$ 结束时,传感器节点 $S_i(1\leqslant i\leqslant N)$ 对其在当前时隙内的数据项进行预处理,并生成如下格式的数据报告:

$$< i, E_{k_{i,t}}\{L_{i,1}, 1, L_{i,2}, 2, \cdots, L_{\lambda_i}, \lambda_i\}, \quad (2)$$
$$DVI_{i,1}, DVI_{i,2}, \cdots, DVI_{i,\lambda_i} >$$

其中,$i$ 表示 $S_i$ 的 ID 号,$E_{k_{i,t}}\{*\}$表示利用对称密钥 $k_{i,t}$进行的加密操作,$<1,2,\cdots,\lambda_i>$表示 $S_i$ 在 $T_t$ 内所有停留过的位置顺序编号,$DVI_{i,j}(1\leqslant i\leqslant N, 1\leqslant j\leqslant\lambda_i)$的内容分情况讨论如下:

如果 $\mu_{i,j}=0$,则有

$$DVI_{i,j} = E_{k_{i,t}}\{j\} \quad (3)$$

如果 $\mu_{i,j}>0$,则有

$$\begin{aligned} DVI_{i,j} = <& L_{i,j}, E_{k_{i,t}}\{j, d^1_{L_{i,j}}\}, d^1_{L_{i,j}}, \\ & E_{k_{i,t}}\{j, D^1_{L_{i,j}}, d^2_{L_{i,j}}\}, d^2_{L_{i,j}}, \\ & E_{k_{i,t}}\{j, D^2_{L_{i,j}}, d^3_{L_{i,j}}\}, \\ & \cdots, \\ & d^{\mu_{i,j}}_{L_{i,j}}, E_{k_{i,t}}\{j, D^{\mu_{i,j}}_{L_{i,j}}\} > \end{aligned} \quad (4)$$

式(4)中的数据项$\{D^1_{L_{i,j}}, D^2_{L_{i,j}}, D^3_{L_{i,j}}, \cdots, D^{\mu_{i,j}-1}_{L_{i,j}}, D^{\mu_{i,j}}_{L_{i,j}}\}$为 $S_i$ 在 $L_{i,j}$上产生的 $\mu_{i,j}$个数据项,且已按对应权重由大到小进行了排列.

### 3.2 数据存储节点的 Top-$k$ 查询处理

假设数据存储节点 $H$ 收到的 Top-$k$ 查询请求为 $Q_t = <SR, c, t, k>$,$H$ 首先对单元 $c$ 内的传感器节点在 $T_t$、$SR$ 内产生的所有数据项按权重大小排序,然后选出权重最大(或最小)的前 $k$ 个数据项,并将这 $k$ 个数据项连同对应的验证信息一同发送给 Sink 节点.

令 $NR^{S_i}$表示 $H$ 经过查询处理后向 Sink 返回的由传感器节点 $S_i$ 产生的数据信息,$m_i(0\leqslant m_i\leqslant\lambda_i)$表示 $S_i$ 在时间 $T_t$、$SR$ 内停留过的位置个数,则 $NR^{S_i}$的内容讨论如下:

①如果 $m_i=0$,则 $S_i$ 需要通过 $H$ 向 Sink 发送 $S_i$在 $T_i$内的所有停留位置信息,有

$$NR^{S_i} = <i, E_{k_{i,t}}\{L_{i,1}, 1, L_{i,2}, 2, \cdots, L_{\lambda_i}, \lambda_i\}> \quad (5)$$

②如果 $m_i>0$,令$\{z_1, z_2, z_3, \cdots, z_{m_i}\}$表示 $S_i$ 在时间区间 $T_t$、在区域 $SR$ 内停留过的 $m_i$ 个位置序号

$$\begin{aligned} NR^{S_i} = <& E_{k_{i,t}}\{L_{i,1}, 1, L_{i,2}, 2, \cdots, L_{\lambda_i}, \lambda_i\}, \\ & DVI_{i,z_1}, DVI_{i,z_2}, \cdots, DVI_{i,z_{m_i}} > \end{aligned} \quad (6)$$

在式(6)中,$DVI_{i,z_j}(1\leqslant j\leqslant m_i)$表示 $S_i$ 在 $T_t$ 内、在 $L_{i,z_j}$上产生的 Top-$k$ 数据项及相关验证信息. 令 $\mu_{i,z_j}$表示 $S_i$ 在 $T_t$ 内、在 $L_{i,z_j}$上产生的感知数据项的总个数,$\gamma_{i,z_j}$表示 $S_i$ 在 $T_t$ 内、在 $L_{i,z_j}$上产生的 Top-$k$ 数据项的个数,则 $DVI_{i,z_j}$的具体内容分情况讨论如下:

③如果 $\mu_{i,z_j}=0$,根据式(3),有

$$DVI_{i,z_j} = E_{k_{i,t}}\{z_j\} \quad (7)$$

④如果 $\mu_{i,z_j}\neq 0$,$\gamma_{i,z_j}=0$,则 $DVI_{i,z_j}$仅包含 $S_i$ 在 $T_t$ 内、在 $L_{i,z_j}$上产生的所有数据项的最大权重与节点的停留点序号的绑定信息,即

$$DVI_{i,z_j} = E_{k_{i,t}}\{z_j, d^1_{L_{i,z_j}}\} \quad (8)$$

⑤如果 $0<\gamma_{i,z_j}<\mu_{i,z_j}$,则 $DVI_{i,z_j}$除包含式(8)中的内容外,还应包含 $\gamma_{i,z_j}$个 Top-$k$ 数据项以及相关的数据关联关系,因此有

$$\begin{aligned} DVI_{i,z_j} = \{& E_{k_{i,t}}\{z_j, d^1_{L_{i,z_j}}\}, E_{k_{i,t}}\{z_j, D^1_{L_{i,z_j}}, d^2_{L_{i,z_j}}\}, \\ & E_{k_{i,t}}\{z_j, D^2_{L_{i,z_j}}, d^3_{L_{i,z_j}}\}, \cdots, E_{k_{i,t}}\{z_j, D^{\gamma_{i,z_j}}_{L_{i,z_j}}, d^{\gamma_{i,z_j}+1}_{L_{i,z_j}}\}\} \end{aligned} \quad (9)$$

⑥如果 $0<\gamma_{i,z_j}$,且 $\gamma_{i,z_j}=\mu_{i,z_j}$,则 $DVI_{i,z_j}$应包含 $S_i$ 在 $T_t$ 内、在 $L_{i,z_j}$上产生的所有数据项及相关数据关联关系,即:

$$\begin{aligned} DVI_{i,z_j} = \{& E_{k_{i,t}}\{z_j, d^1_{L_{i,z_j}}\}, E_{k_{i,t}}\{z_j, D^1_{L_{i,z_j}}, d^2_{L_{i,z_j}}\}, \\ & E_{k_{i,t}}\{z_j, D^2_{L_{i,z_j}}, d^3_{L_{i,z_j}}\}, \cdots, E_{k_{i,t}}\{z_j, D^{\gamma_{i,z_j}}_{L_{i,z_j}}\}\} \end{aligned} \quad (10)$$

针对查询请求 $Q_t$,数据存储节点向 Sink 节点返回的最终查询结果 $R_t$ 可表示为:

$$R_t = \{NR^{S_1}, NR^{S_2}, NR^{S_3}, \cdots, NR^{S_N}\} \quad (11)$$

### 3.3 Top-$k$ 查询结果的完整性验证

Sink 节点对 $R_t$ 进行数据完整性验证的过程如下:首先利用自身与各传感器之间共享的对称密钥对 $R_t$ 中的密文进行解密;然后,检查 $R_t$ 内是否包含被查询单元内的每个传感器节点在被查询时间和区间内停留过的所有位置信息;接着,检查 $R_t$ 中是否包含每个查询子点的 $DVI$;最后,逐个验证每个查询子点的 $DVI$ 的完整性. 只有当每个查询子点对应的 $DVI$ 都通过完整性验证时,$R_t$ 才能够被认为具备数据完整性. 具体如算法 1 所示.

**算法 1 细粒度时空 Top-$k$ 查询数据完整性验证算法**

输入:$Q_t = <SR, c, t, k>$,$R_t$
输出:*Integrity*
(1) 初始化变量:*Integrity* = true;
(2) 利用传感器节点与 Sink 之间的对称密钥对 $R_t$ 中的数据进行解密,并判断是否能够正常解密;
IF $R_t$ 内的数据不能被正常解密
  *Integrity* = false;
  RETURN *Integrity*;//返回变量 *Integrity* 的值
END IF;
(3)检查 $H_c$ 是否上报了其所在单元内每个传感器节点在时隙 $t$ 内的所有停留位置信息以及 $SR$ 内的所有 $DVI$:
FOR $i$ = 1,⋯,$N$ //循环 $N$ 次
  IF ($\{L_{i,1}, 1, L_{i,2}, 2, \cdots, L_{i,\lambda_i}, \lambda_i\} \not\subset R_t$)
    *Integrity* = false;
    RETURN *Integrity*;
  END IF;
FOR $j$ = 1,⋯,$\lambda_i$//内部循环 $\lambda_i$ 次
IF((($L_{i,j}\in SR$) && ($DVI_{i,j}\not\subset R_t$)) || (($L_{i,j}\notin SR$) && ($DVI_{i,j}\subset R_t$)))
    *Integrity* = false;
    RETURN *Integrity*;

```
  END IF;
END FOR
END FOR
```

(4) 依次检验单元内所有传感器节点在时隙 $t$ 内在 $SR$ 中产生的所有 $DVI$ 的数据完整性:

```
FOR i = 1,…,N
  FOR j = 1,…,m_i
    IF (γ_{i,z_j} = =0)
      IF ((\{z_j\}⊄DVI_{i,z_j}) && (\{z_j, d^1_{L_{i,z_j}}\}⊄DVI_{i,z_j}))
      Integrity = false;
      RETURN Integrity;
    END IF;
    IF ((\{z_j, d^1_{L_{i,z_j}}\}⊂DVI_{i,z_j}⊂) && (d^1_{L_{i,z_j}} > d_tail))
      Integrity = false;
      RETURN Integrity;
    END IF;
  END IF;//结束 IF(γ_{i,z_j} = =0)
  IF (γ_{i,z_j} >0)
    IF d^x_{i,z_j} ≠ f(D^x_{i,z_j})
      Integrity = false;
      RETURN Integrity;
    END IF;
    IF (\{z_j, D^{γ_{i,z_j}}_{L^1_{i,z_j}}, d^{γ_{i,z_j}+1}_{L^1_{i,z_j}}\}⊂DVI_{i,z_j})
    IF N_t < k
      Integrity = false;
      RETURN Integrity;
    END IF;
    IF ((N_t = =k) &&(d^{γ_{i,z_j}+1}_{L^1_{i,z_j}} > d_tail))
      Integrity = false;
      RETURN Integrity;
    END IF;
  END IF;
  END FOR //结束内部循环
END FOR //结束外部循环
RETURN Integrity;
```

## 4　VIP-TQ 协议在 Top-$k$ 查询的完整性保护方面的可靠性分析

**定理 1**　在传感器节点相对安全的情况下,如果攻击者捕获了 TMWSNs 中的数据存储节点并利用恶意化的数据存储节点来破坏时空 Top-$k$ 查询数据完整性,VIP-TQ 能够以 100% 的概率侦测出不完整的 Top-$k$ 查询结果. (下文中,$H$ 表示被恶意化的数据存储节点,$Q_t = <SR, c, t, k>$ 表示 $H$ 收到的 Top-$k$ 查询请求,$R_t$ 表示查询结果)

**证明**　为达到破坏 Top-$k$ 查询数据完整性的目的,当攻击者捕获 TMWSNs 中的关键节点 – $H$ 节点时,攻击者可能发动的攻击方式有:数据造假、数据替换和数据丢弃.

首先,考虑数据造假的情况. 由于 $H$ 节点无法获得传感器节点与 Sink 之间的对称密钥,$H$ 向 $R_t$ 中加入虚假数据时无法产生合法的加密项,Sink 无法利用自身与传感器节点之间的对称秘钥对 $R_t$ 中的虚假数据加密项进行解密,根据算法 1,Sink 会认为 $R_t$ 不具备数据完整性. 因此,如果攻击者捕获 $H$ 节点并采用数据造假的方式来破坏 Top-$k$ 查询的数据完整性,VIP-TQ 能够以 100% 的概率侦测出不完整的 Top-$k$ 查询结果.

其次,考虑数据替换的情况. 数据替换有两种方式:(1)在不同传感器节点产生的数据项之间相互替换;(2)在同一传感器节点产生的数据项之间相互替换. 由于 $H$ 无法获得传感器节点与 Sink 之间的对称密钥,$H$ 只能选择在传感器节点加密后的数据项之间进行相互替换. 对于前一种替换方式,假设 $H$ 用任意传感器节点 $S_i(1 \leqslant i \leqslant N)$ 产生的数据项来替代 $S_j(1 \leqslant j \leqslant N, i \neq j)$ 产生的数据项,则必然会导致 Sink 节点用自身与 $S_j$ 的对称秘钥 $k_{j,t}$ 来解密用其与 $S_i$ 之间的对称密钥 $k_{i,t}$ 加密的数据项,使得 Sink 节点不能正常解密 $R_t$ 中的加密数据项. 根据算法 1,Sink 会认为 $R_t$ 不具备数据完整性. 对于后一种方式,根据本文的攻击模型,又可分三种情况考虑:

(1) $H$ 用 $S_i(1 \leqslant i \leqslant N)$ 在 $T_a(a \in \{1,2,3,\cdots,t-1\})$ 内产生的数据项来替换 $S_i$ 在 $T_t$ 内产生的数据项;

(2) $H$ 用 $S_i(1 \leqslant i \leqslant N)$ 在 $SR$(表示被查询区域)外产生的数据项来代替 $S_i$ 在 $SR$ 内产生的数据项;

(3) $H$ 用 $S_i(1 \leqslant i \leqslant N)$ 在 $SR$ 内产生的非 Top-$k$ 数据项来代替 $S_i$ 在 $SR$ 内产生的 Top-$k$ 数据项.

如果出现第一种情况,必然导致 Sink 节点利用对称密钥 $k_{i,t}$ 去解密经过 $k_{i,a}(a \in \{1,2,3,\cdots,t-1\})$ 加密的数据项,使得 Sink 节点不能正常解密,因而判定 $R_t$ 缺乏完整性;如果出现第二种情况,由于 VIP-TQ 中每个数据项都与其产生位置的对应 ID 号进行了加密绑定,Sink 可根据与数据项相绑定的位置 ID 号以及 $R_t$ 中所包含的位置信息找到对应的位置,然后通过与查询请求中的区域信息相互比对的方法侦测出产生于被查询区域外的数据项;如果出现第三种情况,必然有某一传感器节点在 $SR$ 中某一位置上产生的数据项之间的关联关系被打破,即 $R_t$ 中至少存在一个权重 $d^x_{i,j}$ 与其在 $R_t$ 内后继关联的数据项 $D^x_{i,j}$ 满足关系式 $d^x_{i,j} \neq f(D^x_{i,j})$,其中 $f(\cdot)$ 为权重评估函数. 根据算法 1,$R_t$ 同样会被 Sink 判定为不具备数据完整性. 因此,如果攻击者捕获了 $H$ 节点并通过数据替换的方式来破坏 Top-$k$ 查询的数据完整性,VIP-TQ 能够以 100% 的概率侦测出不完整的 Top-$k$ 查询结果.

最后,考虑数据丢弃的情况. 数据丢弃分为全部丢

弃和部分丢弃.

第一,考虑数据全部丢弃的情况. 假设 $H$ 丢弃了任意传感器节点 $S_i(1\leqslant i\leqslant N)$ 在某一查询子点处产生的全部数据项,并且被丢弃的数据项中包含 Top-$k$ 数据项. 在 $S_i$ 可信的情况下,由于 $H$ 无法获知传 $S_i$ 与 Sink 之间的对称密钥 $k_{i,t}$,无法伪造出加密项 $E_{k_{i,t}}\{j\}$,为了逃避完整性侦测,$H$ 只能在 $R_t$ 中保留 $S_i$ 产生的 $E_{k_{i,t}}\{j,d^1_{L_{i,j}}\}$ 项. 令 $d_{tail}$ 表示 $R_t$ 中所有数据项对应权重的最小值,必然有 $d^1_{L_{i,j}}>d_{tail}$(假设 Top-$k$ 查询选取的是前 $k$ 个权值最大的数据项),根据算法 1,$R_t$ 一定会被认为是不完整的.

第二,考虑数据部分丢弃的情况. 假设 $H$ 丢弃了任意传感器节点 $S_i(1\leqslant i\leqslant N)$ 在某一查询子点 $L_{i,j}$ 处产生的部分数据项,且被丢弃的数据项中包含 Top-$k$ 数据项,为了保持 $S_i$ 在 $L_{i,j}$ 产生数据项的关联关系一致性,$H$ 只能选择丢弃这一数据链中从某一个数据项开始以后的所有数据项. 假设 $S_i$ 丢弃了数据项 $D^x_{i,j}(1\leqslant x\leqslant\mu_{i,j})$ 以及该数据项以后的所有数据项,根据 VIP-TQ 协议中数据关联关系的建立方法,数据项 $D^x_{i,j}$ 对应的权重 $d^x_{i,j}$ 仍会与数据项 $D^{x-1}_{i,j}$ 绑定并保留在 $R_t$ 中. 此时,如果 $R_t$ 中的数据项个数小于 $k$,则 $R_t$ 中应包含 $S_i$ 在 $L_{i,j}$ 处产生的所有数据项,这与上述假设相矛盾,根据算法 1,$R_t$ 被认为不具有数据完整性;如果 $R_t$ 中中的数据项个数等于 $k$,则一定会有 $d^x_{i,j}>d_{tail}$. 根据算法 1,$R_t$ 同样会被认为不具备完整性. 因此,如果攻击者捕获了 $H$ 节点并通过数据丢弃的方式来破坏 Top-$k$ 查询的数据完整性,VIP-TQ 同样能够以 100% 的概率侦测出不完整的 Top-$k$ 查询结果.

证毕

## 5 实验

TMWSNs 中安全 Top-$k$ 查询方案和协议的性能评价指标主要包括:Top-$k$ 查询数据完整性的正确侦测概率、单元内传感器节点传输安全验证信息的额外通信代价($C_{v\_sm}$)以及完成 Top-$k$ 查询完整性验证所需额外安全验证信息的冗余比($R_{vs\_sm}$)[15]. 令 $Amount_{d\_sm}$ 表示在不考虑安全性情况下单元内的所有传感器节点在一定时间内向数据存储节点传输必要数据时所发送和接收的数据总量,$Amount_{v\_sm}$ 表示在考虑安全性情况下单元内的所有传感器节点在一定时间内向数据存储节点传输验证信息过程中所发送和接收的验证信息总数据量,则 $C_{v\_sm}$ 即为单元内的所有传感器节点在参与发送和接收数据量为 $Amount_{v\_sm}$ 的验证信息的过程中所消耗的总能量,而对应的 $R_{vs\_sm}$ 又可表示为:

$$R_{v\_sm}=\frac{Amount_{v\_sm}}{Amount_{d\_sm}+Amount_{v\_sm}}\times 100\% \qquad (12)$$

显然,$R_{vs\_sm}$ 的值越小越能显示 Top-$k$ 安全查询协议的高效性.

由于本文已在上文中对 VIP-TQ 协议关于 Top-$k$ 查询数据完整性的正确侦测概率进行了证明,因此,下文主要给出 VIP-TQ 协议在 $C_{v\_sm}$ 和 $R_{vs\_sm}$ 方面的实验结果. 本文利用仿真工具 OMNET + + 对 VIP-TQ 协议进行模拟实验,并将其和 Wu 等人于 2016 年提出的 EVTopk 方案[20]进行对比. 默认的实验参数设置如表 1 所示.

**表 1 默认参数设置**

| 参数名 | 参数值 |
|---|---|
| 单个 Cell 面积 | 400 * 400 $m^2$ |
| 传感器节点的通讯半径 | 50 m |
| 可移动传感器节点所占比例 | 50% |
| 发送一个字节消耗的能量 | 1 J |
| 接收一个字节消耗的能量 | 0.5 J |
| 节点持续静止的时间($T_s$) | 10 s |
| 节点持续运动的时间($T_m$) | 5 s |
| 节点移动速度 | 2 m/s |
| 数据项对应权重的长度 | 20 bits |
| 数据项长度 | 400 bits |
| 哈希值字节长度 | 160 bits |
| 单个节点位置信息的长度 | 128 bits |
| 时间戳长度 | 10 bits |
| 节点 ID 号长度 | 10 bits |

图 2 给出了当其它参数保持不变,而 $r_d$(传感器节点的数据产生速率)和 $N$(单元内的传感器节点个数)发生变化时 VIP-TQ 协议和 EVTopk 方案在 $C_{v\_sm}$ 上的性能表现. 图 2 显示,两种方案所对应的 $C_{v\_sm}$ 都会随着 $r_d$ 和 $N$ 的增大而增大,但在相同参数设置情况下,VIP-TQ 所对应的 $C_{v\_sm}$ 值明显小于 EVTopk 所对应的 $C_{v\_sm}$ 值.

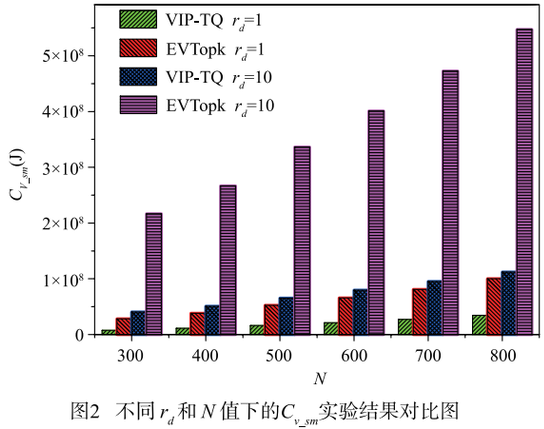



图2 不同 $r_d$ 和 $N$ 值下的 $C_{v\_sm}$ 实验结果对比图

图 3 给出了在其它参数保持不变而 $r_d$ 和 $N$ 发生变化时 VIP-TQ 协议和 EVTopk 方案在 $R_{vs\_sm}$ 上的性能表现. 图 3 显示,当 $r_d=10$ 时,VIP-TQ 协议中 $R_{vs\_sm}$ 的值被控制在 15% 以内;而对于 EVTopk 方案,无论 $r_d$ 取值为 1

还是取值为 10,其所对应的 $R_{vs\_sm}$ 的值都在 40% 以上. 由此可以看出,相对于 EVTopk 方案,VIP-TQ 协议在保证 TMWSNs 中 Top-$k$ 查询安全性的同时实现了更高的能效性.

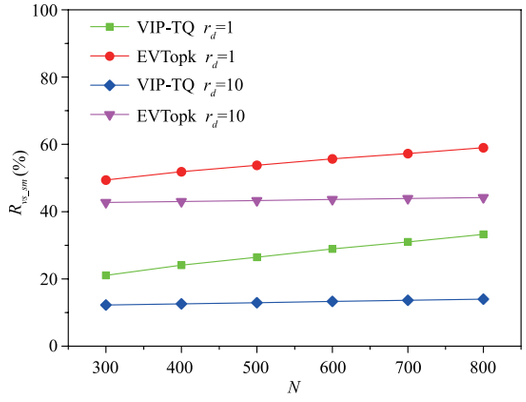



图3　不同 $r_d$ 和 $N$ 值下的 $R_{vs\_sm}$ 实验结果对比图

## 6　总结

为了实现 TMWSNs 中时空 Top-$k$ 查询的数据完整性保护,本文提出了一种新的安全时空 Top-$k$ 查询处理协议 VIP-TQ. VIP-TQ 包含“在传感器节点上的感知数据与节点动态位置信息预处理”、“在数据存储节点上的时空 Top-$k$ 查询处理”以及“在 Sink 节点上的时空 Top-$k$ 查询数据完整性验证”三个层次和阶段,利用虚拟化节点技术、位置信息与感知数据信息的间接加密绑定技术、感知数据之间基于权重加密的数据关联技术以及特定设计的时空 Top-$k$ 查询数据完整性验证方法来实现时空 Top-$k$ 查询的数据完整性保护. 本文在理论上证明了攻击者在采用数据丢弃、数据造假、数据替换等方式来破坏时空 Top-$k$ 查询结果数据完整性时均能被 VIP-TQ 侦测出来,证实了该协议的安全可靠性. 实验结果显示,VIP-TQ 所带来的验证信息冗余比远低于其它同类方案对应的验证信息冗余比,具有较高的能效性.

### 参考文献


[1] KE M,ZHANG YY,and Trappe W. Managing the mobility of a mobile sensor network using network dynamics[J]. IEEE Transactions on Parallel and Distributed Systems,2008,19(1):106 – 120.

[2] HATES T,ALI F H. Handbook of Research on Next Generation Mobile Communications Systems [M]. Hershey,Pennsylvania,USA:IGI Global,2016. 256 – 292.

[3] ZHANG R, SHI J, LIU Y, ZHANG Y. Verifiable fine-grained Top-$k$ queries in tiered sensor networks[A]. Proceedings of the 29th International Conference on Computer Communications[C]. San Diego,CA:IEEE,2010. 1 – 9.

[4] 陈志,王汝传,孙力娟. 无线传感器网络的自组织机制研究[J]. 电子学报,2007,35(5):854 – 857.
CHEN Zhi,WANG Ru-chuan,SUN Li-juan. Study on self-organization mechanism of wireless sensor networks[J]. Acta Electronica Sinica,2007,35(5):854 – 857. (in Chinese)

[5] 梁俊斌,马行坡,奎晓燕. 查询驱动模式下两层传感器网络 Top-$k$ 查询汇聚算法研究[J]. 电子学报,2014,42(10):2075 – 2080.
LIANG Jun-bin,MA Xing-po,KUI Xiao-yan. Research on Top-$k$ query aggregation algorithm of two layer sensor network based on query driven model[J]. Acta Electronica Sinica,2014,42(10):2075 – 2080. (in Chinese)

[6] 邬海琴,王良民. 基于连通支配集的无线传感网 Top-$k$ 查询最优支撑树研究[J]. 电子学报,2017,45(1):119 – 127.
WU Hai-qin,WANG Liang-min. Connected dominating set based support-tree for Top-$k$ query in wireless sensor networks[J]. Acta Electronica Sinica,2017,45(1):119 – 127. (in Chinese)

[7] ZHU C,YANG L,SHU L,LEUNG V,HARA N. Insights of Top-$k$ query in duty-cycled wireless sensor networks [J]. IEEE Transactions on Industrial Electronics,2015,62(2):1317 – 1328.

[8] 廖晓静,李建中,余磊. 一种能量有效的双层传感器网络 Top-$k$ 安全查询机制[J]. 计算机研究与发展,2013,50(3):490 – 497.
LIAO Xiao-jing,LI Jian-zhong,YU Lei. Secure and efficient Top-$k$ query processing in two-tiered sensor network [J]. Journal of Computer Research and Development,2013,50(3):490 – 497. (in Chinese)

[9] HE R,DAI H,YANG G,WANG T,BAO J. An efficient Top-$k$ query processing with result integrity verification in two-tiered wireless sensor networks [J]. Mathematical Problems in Engineering,2015,2015(1):1 – 8.

[10] LIANG J,JIANG C,MA X,WANG G,KUI X. Secure data aggregation for Top-$k$ queries in tiered wireless sensor networks[J]. Adhoc & Sensor Wireless Networks,2016,32(1/2):51 – 78.

[11] Yu C M,TSOU Y T,LU C S,et al. Practical and secure multidimensional query framework in tiered sensor networks[J]. IEEE Transactions on Information Forensics and Security,2011,6(2):241 – 255.

[12] 陈伟,于乐,高迪. 一种支持完整性验证的隐私保护直方图融合算法[J]. 电子学报,2014,42(11):2268 – 2272.
CHEN Wei,YU Le,GAO Di. A Privacy Preserving histogram aggregation algorithm with integrity verification support[J]. Acta Electronica Sinica,2014,42(11):2268 – 2272. (in Chinese)

[13] 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[J]. 计算机学报,2012,35(3):423 – 433.
FAN Yong-jiang,CHEN Hong. Verifiable privacy- preserving Top-*k* query protocol in tiered sensor networks[J]. Chinese Journal of Computers,2012,35(3):423 – 433. (in Chinese)

[14] 陈伟,许若妹,李玉岭. 基于隐私保护和完整性验证的 Top-*k* 查询方法[J]. 计算机研究与发展,2014,51(12):2585 – 2592.
CHEN Wei,XU Ruo-mei,LI Yu-ling. A privacy- preserving integrity-verification-based Top-*k* query processing [J]. Journal of Computer Research and Development,2014,51(12):2585 – 2592. (in Chinese)

[15] MA X,SONG H,WANG J,GAO J,MIN G. A novel verification scheme for fine-grained Top-*k* queries in two-tiered sensor networks[J]. Wireless Personal Communications,2014,75(3):1809 – 1826.

[16] 李睿,林亚平,易叶青,熊帅,叶松涛. 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 Rui, LIN Ya-ping, YI Ye-qing, XIONG Shuai, YE Song-tao. Security Top-*k* query protocol in two layer sensor networks[J]. Journal of Computer Research and Development,2012,49(9):1947 – 1958. (in Chinese)

[17] YU C,NI G,CHEN Y,GELENB E,KUO S. Top-*k* query result completeness verification in tiered sensor networks [J]. IEEE Transactions on Information Forensics and Security,2014,9(1):109 – 124.

[18] 毛科技,邬锦彬,金洪波,苗春雨,夏明,陈庆章. 面向非视距环境的室内定位算法[J]. 电子学报,2016,44(5):1174 – 1179.
MAO Ke-ji,WU Jin-bin,JIN Hong-bo,MIAO Chun-yu,XIA Ming,CHEN Qing-zhang. Indoor localization algorithm for NLOS environment[J]. Acta Electronica Sinica,2016,44(5):1174 – 1179. (in Chinese)

[19] LIU F,MA X,LIANG J,LIN M. Verifiable Top-*k* query processing in tiered mobile sensor networks[J]. International Journal of Distributed Sensor Networks,2015,11(10):1 – 13.

[20] WU H,WANG L. Efficient and secure Top-*k* query processing on hybrid sensed data[J]. Mobile Information Systems,Article ID 1685054,2016. 1 – 10.

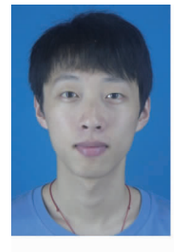
[21] DAS G,GUNOPULOS D,KOUDAS N,TSIROGIANNIS D. Answering Top-*k* queries using views[A]. Proceedings of the 32nd International Conference on Very Large Data Bases [C]. Seoul,Korea:VLDB Endowment,2006. 451 – 462.

## 作者简介

**马行坡(通信作者)** 男,1980 年 10 月出生,河南郑州人. 2013 年获得中南大学计算机应用技术专业博士学位. 现为信阳师范学院计算机与信息技术学院讲师,主要研究方向为物联网安全技术.
E-mail:maxingpo@ xynu. edu. cn

**危 锋** 男,1981 年 6 月出生,湖北天门人. 2005 年、2010 年分别在华中师范大学、解放军信息工程大学获得学士和硕士学位. 现为河南经贸职业学院计算机工程学院讲师,主要研究方向为网络信息安全.

**梁俊斌** 男,1979 年 3 月出生,广西南宁人. 2010 年获得中南大学计算机应用技术专业博士学位. 现为广西大学计算机与电子信息学院教授,主要研究方向为无线传感器网络数据收集.



**李 然** 男,1988 年 8 月出生. 2014 年获得南京邮电大学博士学位. 现为信阳师范学院计算机与信息技术学院讲师,主要研究方向为视频传输与压缩感知.

**马文鹏** 男,1986 年 11 月出生. 2015 年于中国科学院超级计算中心获得博士学位. 现为信阳师范学院计算机与信息技术学院讲师,主要研究方向为并行计算.

**祁传达** 男,1965 年 1 月出生,河南省固始县人. 现为信阳师范学院计算机与信息技术学院教授、院长,主要研究方向为密码学.