两层传感器网络中安全 Top-k 查询处理技术综述

戴 华[1,2] 叶庆群[1] 杨 庚[1,2] 肖 甫[1,2] 何瑞良[1]
(南京邮电大学计算机学院 南京 210013)[1]
(南京邮电大学宽带无线通信与传感网络技术教育部重点实验室 南京 210013)[2]

摘 要 无线传感网中安全数据查询技术的研究已引起了广泛的关注,其中以存储节点为中间层的两层传感器网络中安全 Top-k 查询技术的研究具有重要的现实意义。现有的安全 Top-k 查询技术主要针对查询过程中数据的隐私保护和查询结果的完整性验证等问题开展研究工作。从安全性能和通信性能两个维度出发对现有的两层传感器网络中的安全 Top-k 查询技术进行了总结,介绍了网络模型查询模型,以及查询过程中存在的安全性问题;同时分析和总结了现有的各协议所采用的关键技术以及其主要优点和不足,最后指出了未来可能的研究方向。

关键词 两层传感器网络,Top-k 查询,隐私保护,完整性验证
中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2017.05.002

Overview of Secure Top-k Query Processing in Two-tiered Wireless Sensor Networks

DAI Hua[1,2] YE Qing-qun[1] YANG Geng[1,2] XIAO Fu[1,2] HE Rui-liang[1]
(College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210013, China)[1]
(Key Laboratory of Broadband Wireless Communication & Sensor Network Technology (Nanjing University of Posts and Telecommunications), Ministry of Education, Nanjing 210013, China)[2]

Abstract The research of secure data query in wireless sensor networks has attracted more and more attentions, and it is important to research secure Top-k query in two-tiered wireless sensor networks, in which storage nodes is intermediate layer of networks. The present research about secure Top-k queries in two-tiered sensor networks is mainly concentrated on solutions of data privacy preservation and query result verification. This paper surveyed the current state of the art of secure Top-k query techniques in two-tiered sensor network according to two dimensions, which are security and communication performance, and introduced the network model, query model and security questions in query process. This paper summarized the key techniques of current protocols and the main advantages and disadvantages of these protocols. At last, this paper pointed out possible research direction in the future.

Keywords Two-tiered wireless sensor networks, Top-k query, Privacy preservation, Completeness verification

1 引言

无线传感网络(Wireless Sensor Networks, WSNs)是由大量具有微小计算能力的感知元件以无线连接的方式组成的一种大规模、多跳、无线、自组织性网络。该网络作为物联网的重要组成部分,在军事安全、环境监测、森林防火、目标定位等方面具有广阔的应用前景。由于网络部署环境不容易控制,通常将传感网络分布在无人值守的环境中,因此对传感器网络安全问题的研究具有重要的现实意义。两层传感网络[1](以下简称两层 WSNs)作为无线传感网络的一个发展方向,其在传统的多跳无线传感网络的基础上引入了资源丰富的存储节点作为网络中间层;网络下层为感知节点(Sensor node),是由大量体积小、价格便宜、具有无线通信和监测能力的电子元件组成。具体如图1所示。

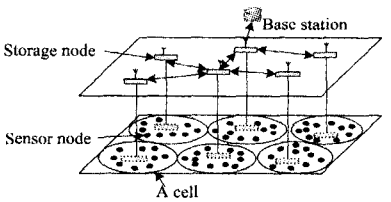

图1 两层传感器网络模型

在两层 WSNs 中,存储节点的引入使得基站无需与网络

到稿日期:2016-04-20 返修日期:2016-06-05 本文受国家自然科学基金项目(61300240, 61572263, 61402014, 61472193, 61202004, 61373138),江苏省自然科学项目(BK20151511, BK20130096),江苏省高校自然科学研究项目(14KJB520027)资助。

戴 华(1982—),男,博士,副教授,CCF 会员,主要研究方向为无线传感器网络数据管理与安全、数据库安全技术等,E-mail:daihua@njupt.edu.cn;叶庆群(1992—),女,硕士,主要研究方向为无线传感器网络数据管理与安全;杨 庚(1961—),男,博士,教授,主要研究方向为网络与信息安全、分布与并行计算、大数据隐私保护;肖 甫(1980—),男,博士,教授,主要研究方向为无线传感网络、信息网络、多媒体技术等;何瑞良(1988—),男,硕士,主要研究方向为无线传感器网络数据管理与安全。

中的感知节点进行直接通信,而是通过存储节点进行间接通信。相对于传统的无线传感网络,该网络结构具有明显优势:首先,两层 WSNs 的网络拓扑简单;其次,存储节点的引入降低了网络通信代价,同时极大地提高了查询处理的效率,并且改善了存储资源不足的问题。

然而,由于存储节点中存储着大量的数据信息,一旦存储节点被俘获,则必然会导致网络内数据的安全性受到威胁。当攻击者通过被俘获的存储节点窥探存储在存储节点上的数据信息时,会导致网络中的数据隐私性遭到破坏;当攻击者对被俘获的存储节点上的数据信息进行插入、篡改、删除时,会导致网络数据的完整性遭到破坏。鉴于存储节点的特殊性,研究和解决两层 WSNs 中的数据安全性问题对促进传感器网络的大规模应用具有重要的现实意义。

近年来,两层 WSNs 的安全查询处理技术已引起广泛的关注并成为研究的热点,如安全 Top-k 查询、范围(Range)查询[33-43]、最值(MAX/MIN)查询[44]以及数据聚集[2]查询处理技术等。Top-k 查询作为两层 WSNs 中一种重要的操作,本文对其研究成果进行了回顾和总结,并从数据的安全性能和通信代价两个维度对现有的技术进行了分类,分析和比较了各个协议的主要性能和优缺点,并指出了未来的研究方向。

本文第 2 节为相关模型介绍以及相关问题描述;第 3 节对现有的安全 Top-k 查询技术进行比较与分析;第 4 节总结全文并对未来该领域的研究方向进行展望。

2　相关模型及问题描述

2.1　网络模型

与传统无线传感网络相似,两层 WSNs 同样是由大量相似节点以无线连接的形式构成的自组织网络。不同之处在于,两层 WSNs 中节点分为两类(见图 1):一类是少量的高资源节点,即存储节点 M;另一类是大量的资源受限节点,即感知节点 s。在网络中,M 作为网络中间层,与邻近的下层感知节点共同构成一个个网络单元 $Cell$,每个 $Cell$ 包含一个 M 和大量的感知节点 $S=\{s_1,s_2,\cdots,s_n\}$,可记为 $Cell=(M,\{s_1,s_2,\cdots,s_n\})$。其中感知节点负责采集感知数据;$M$ 负责接收并存储同一个 $Cell$ 中感知节点上传的数据,响应并执行来自基站的查询指令。

这种通过无线链接(如卫星链接)方式进行的节点间的通信通常具有不稳定性,且具有代价高、效率低等特点,因此要求 Top-k 查询过程中产生的通信代价尽可能低。而两层 WSNs 具有网络拓扑简单、易扩展等优点,因此具有良好的发展空间。

2.2　查询模型

两层 WSNs 中的 Top-k 查询即获取特定范围和特定时间周期内感知节点采集到的最大(或最小)的 k 个数据,因此可将 Top-k 查询模型形式化地表示为:

$Q_t=(c,t,k)$

其中,c 为所查询网络单元,t 为查询时间周期,k 为需要查询的数据项数。例如 $Q_t=(\{s_1,s_2,\cdots,s_{10}\},t_0,8)$,表示查询感知节点 s_1-s_{10} 在时间周期 t_0 内所采集的最大(小)的 8 个数据。

如图 2 所示,查询过程分为两个阶段:第一阶段为感知数据上传阶段,即感知节点将时间周期 t 内的感知数据上传至邻近的 M;第二阶段为查询处理阶段,即接收到来自基站的查询指令后,M 对感知数据进行处理,并将处理后的查询结果反馈给基站。

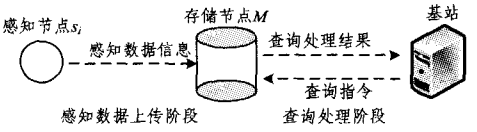

图 2　两层 WSNs 中的 Top-k 查询示意图

为方便描述,本文以查询最大的 k 个数据为例,讨论在单位时间周期 t 内一个 $Cell=(M,\{s_1,s_2,\cdots,s_n\})$ 中的 Top-k 查询。最小的 k 个数据查询与最大的 k 个数据查询的方法类似。对于多时间周期和(或)多个单元的查询,只需通过简单的分解与合并即可获得所需的查询结果。

2.3　问题描述

两层 WSNs 中,与现有文献[6-18]类似,通常认为 M 为不可信节点,而基站可信。虽然被攻击的感知节点也会导致敏感数据泄露,但是感知节点的安全防范比较困难,且单个感知节点采集的数据仅占总体数据的极小一部分;而 M 上存储着大量的敏感信息,一旦 M 受到攻击,攻击者往往可以通过妥协的 M 直接或间接地窥探隐私数据信息,甚至篡改或删除存储在 M 上的数据信息,使得网络的安全性遭到破坏。因此两层 WSNs 中的 Top-k 安全查询研究主要针对 M。

两层 WSNs 中 Top-k 查询过程中的安全性问题可分为两种。

(1)隐私性问题:妥协的 M 意图通过直接或间接的方式窥探存储在 M 上的感知数据、查询结果和 k 的明文数值,使网络中数据的隐私性受到威胁。

(2)完整性问题:在 Top-k 查询过程中,被攻击的 M 意图对存储于该节点的数据信息进行篡改或删除,使最终返回的查询结果不完整。

针对这两类问题,现有研究主要在如下 3 个安全模型框架下开展。

(1)半诚实模型(Honest-but-curious model)[3-4]:在该模型下,M 能够遵循指定协议,并获取正确结果,但可能会窥探、泄露存储在 M 上的敏感信息。且基于该模型,文献[9,12]针对查询过程中的数据隐私保护问题进行了深入研究。

(2)完整性攻击模型(Integrity attack model)[6,13-14]:被俘获的 M 可能对查询结果进行伪造、篡改、丢弃,使得反馈给基站的查询结果不完整。在该模型框架下,针对 Top-k 查询结果的完整性验证问题,文献[6,13-14]给出了相应的解决方案。

(3)强安全模型(Strong security model)[7-8,10-11,16-18]:在该安全模型下,被俘获的 M 不仅会导致网络中的敏感数据泄露,而且会造成查询结果不完整。基于该安全模型,既具有隐私保护性又可验证查询结果完整性的查询处理方案见文献[7-8,10-11,16-18]。

2.4　性能指标

2.4.1　安全性指标

在两层 WSNs 中,设查询指令为 $Q_t=\{c,t,k\}$,在网络单

元 c 中，任一感知节点 s_i 在时间周期 t 内采集并向存储节点 M 上传的数据集为 $D_{i,t}=\{d_{i,1},d_{i,2},\cdots,d_{i,N}\}$；接收到的数据集为：

$$D_t=\bigcup_{s_i\in c}\{D_{i,t}\} \tag{1}$$

其中，D_t 中包含的数据个数记为 $|D_t|$，且 $|D_t|\geqslant k$；最终的查询结果为 R_t。

(1)数据的隐私保护。使 M 无法通过直接或间接的方式窃取感知数据、查询结果以及数值 k 的明文数值，即使下列数据的明文数值不被获取：

$$\forall d\in D_t\wedge\forall d\in R_t\wedge k \tag{2}$$

(2)查询结果的完整性验证。完整性验证包含 3 个方面：1)验证查询结果中的数据个数是否正好为 k；2)验证查询结果是否为最大的 k 个数据；3)验证查询结果中所有数据是否均为感知数据，即验证查询结果是否满足：

$$|R_t|=k\wedge\min(R_t)\geqslant\max(D_t\backslash R_t)\wedge\forall d\in R_t(d\in D_t) \tag{3}$$

2.4.2 通信性能指标

由于两层 WSNs 中感知节点的资源受限性，因此感知节点的通信代价大小直接决定传感网络的生命周期，即在一定能量的情况下，感知节点单位时间能量消耗越低，其可持续工作时间越长，网络生命周期越长。此外，在查询过程中，通常需要传输大量的数据信息，因此 M 与基站间的通信代价往往成为影响网络工作效率的重要因素。

(1)感知节点的通信代价：感知节点向 M 提交感知数据所产生的通信代价记为 S_Cost。设感知节点 $s_i\in c$ 到 M 的路径长度为 L_i，s_i 上传至 M 的数据量为 $DS(s_i)$，则 S_Cost 的通用计算公式为：

$$S\_Cost=\sum_{s_i\in c}DS(S_i)\cdot L_i \tag{4}$$

由式(4)可知，感知节点上传至 M 的数据量 $DS(s_i)$ 越小，则感知节点通信代价 S_Cost 越小。因此，现有研究工作的首要任务就是在满足安全需求条件下，尽可能地降低感知节点的数据传输量。

(2)存储节点与基站间的通信代价：基站发出查询指令和 M 响应执行基站的查询指令并将查询结果上传到基站共同产生的通信代价，记为 M_Cost。设基站向 M 发送查询指令的数据量为 $Cost(Q_t)$，M 向基站上传查询结果 R_t 中的感知数据量为 $RD(R_t)$，而上传的验证数据量为 $VD(R_t)$，则 M_Cost 的通用计算公式为：

$$M\_Cost=Cost(Q_t)+RD(R_t)+VD(R_t) \tag{5}$$

由式(5)可知，M 向基站上传的查询结果数据 $RD(R_t)$ 和验证数据数据量 $VD(R_t)$ 的大小以及基站向 M 发送的指令数据量 $Cost(Q_t)$ 都直接影响 M 与基站之间的通信代价 M_Cost 的大小。而与 $RD(R_t)$ 和 $VD(R_t)$ 相比，$Cost(Q_t)$ 的数据量相对较小，因此，现有研究工作的首要任务是通过尽可能地降低 $RD(R_t)$ 和 $VD(R_t)$ 实现安全 Top-k 查询通信性能的最优化。特别地，如文献[9,12]中只涉及数据的隐私保护时，M 则无需向基站上传额外的验证信息 $VD(R_t)$，即式(5)中的 $VD(R_t)=0$。

两层 WSNs 中的安全 Top-k 查询技术研究针对不同的应用环境，在实现安全性指标的前提下不断实现性能指标的优化。

3 安全 Top-k 查询处理技术

3.1 面向查询结果隐私性的查询处理方法

针对两层 WSNs 中的数据隐私性问题，基于半诚实模型，文献[9,12]对 Top-k 查询过程中的隐私保护问题进行了研究。

(1)OPESTQ

为保护 Top-k 查询过程中数据的隐私性，文献[9]基于保序加密[5]思想提出了一种具有隐私保护的 OPESTQ 查询处理方案。

该方案中，在数据上传阶段，为使被俘获的 M 无法获取感知数据的明文数值，感知节点 s_i 利用仅与基站共享的秘钥对感知数据 $D_{i,t}=\{d_{i,1},d_{i,2},\cdots,d_{i,N}\}$ 进行保序加密，然后将加密后的数据上传至相邻的 M。

在查询处理阶段，由于保序加密过程中明文数据和密文数据具有一一对应关系，即若假设 $d_{i,j}$ 对应的保序加密后的密文数据为 $E_K(d_{i,j})$，则当数据明文数值 $d_{i,j}>d_{i,j+1}(1\leqslant j<N)$ 时，加密后的数据也满足 $E_K(d_{i,j})>E_K(d_{i,j+1})$。因此 M 可根据该关系实现非明文数据的秘密比较，然后定位前 k 个数据，并将其上传至基站。最终由基站解密并计算出查询结果。

OPESTQ 在一定程度上可以确保被攻击的 M 无法直接获取网络中敏感数据的明文数值，然而 M 可通过保序加密过程中明文数据与密文的顺序对应关系来推测感知数据的顺序信息，因此通过保序加密实现 Top-k 查询过程中的数据隐私保护仍有不足之处。

(2)PPTQ

为进一步提高两层 WSNs 中具有隐私保护的安全 Top-k 的查询效率，文献[12]提出了查询处理方案 PPTQ，即引入前缀成员验证(Prefix Membership Verification，PMV)[19-20]机制以实现 M 对密文数据的比较，并结合 Hash 身份验证编码机制(HMAC)[21]和对称加密技术实现对数据的隐私性进行保护。

在数据上传阶段，首先，感知节点 s_i 对在时间 t 内采集的感知数据 $D_{i,t}=\{d_{i,1},d_{i,2},\cdots,d_{i,N}\}$ 进行排序，使得 $d_{i,1}\geqslant d_{i,2}\geqslant\cdots\geqslant d_{i,N}$。然后分别计算 $d_{i,1}$ 和 $[d_{i,1},\bar{x}]$ 的数值化[43]前缀编码集合 $N(F(d_{i,1}))$ 和 $N(Se([d_{i,1},\bar{x}]))$，并对其进行 HMAC 编码处理得到 $HMAC_gN(F(d_{i,1}))$ 和 $HMAC_gN(Se([d_{i,1},\bar{x}]))$，其中 g 为 HMAC 函数的秘钥，$\bar{x}$ 为感知数据的上界；再利用仅与基站共享的秘钥 k_i 对感知数据进行加密，即计算 $(d_{i,j})_{k_i}$。最后 s_i 将如下数据上传至 M。

$$s_i\rightarrow M:i,t,\{(d_{i,1})_{k_i},(d_{i,2})_{k_i},\cdots,(d_{i,N})_{k_i}\},HMAC_g(N(F(d_{i,1}))),HMAC_g(N(Se([d_{i,1},\bar{x}])))$$

在查询处理阶段，由于利用前缀编码可将任意两个数据 p 和 q 之间的数值比较问题转换成判断 p 与 $[q,\bar{x}]$ 的前缀编码集合之间是否存在交集的问题，因此，接收到查询指令后，M 可通过感知节点上传的编码信息来比较并计算出满足查询结果的最小感知节点集合 MCS，然后通过 MCS 计算出包含查询结果的最小密文数据集合 Msg，并将其上传至基站。基站利用与感知节点共享的秘钥对其进行解密，并获得最终的查询结果。

PPTQ 查询协议的关键在于:在查询过程中,M 根据前缀编码集合性质确定出 MCS,从而最终确定 Msg,而不是直接对感知数据进行比较;且在数据上传过程中对数据进行加密的秘钥仅在感知节点和基站之间共享。因此被攻击的 M 很难获取网络中敏感数据的明文信息,即可有效地实现数据的隐私保护。

3.2　面向查询结果完整性的 Top-k 查询

针对 Top-k 查询过程中存在的查询结果完整性问题,文献[6,13-15]给出了相应的解决方案。

(1) VFTop-k

文献[6]提出了面向两层 WSNs 的可验证 Top-k 查询协议 VFTop-k 并对其进行优化,包含如下 3 个方案。

方案 1　数据上传阶段,在时间周期 t 内,感知节点 s_i 对采集到的感知数据集 $D_{i,t}=\{d_{i,1},d_{i,2},\cdots,d_{i,N}\}$ 进行排序,然后将相邻数据进行捆绑并加密形成加密数据链,同时将其上传至 M。设 $h_k(*)$ 为 HMAC 编码函数[21],$\overline{x}$ 和 $\underline{x}$ 分别为感知数据的上边界值和下边界值,同时 $\underline{x}\notin D_{i,t}\wedge\overline{x}\notin D_{i,t}$。则 s_i 向 M 上传的数据为:

$$s_i\rightarrow M:i,\ t,\ d_{i,1},h_{k_i}(\underline{x}\parallel d_{i,1}\parallel d_{i,2}),\cdots,d_{i,N},h_{k_i}(d_{i,N-1}\parallel d_{i,N}\parallel\overline{x})$$

在查询处理阶段,M 首先定位 $D_{i,t}$ 中满足查询指令 Q_t 的 γ_i 个数据项,然后将其与第 γ_i+1 个数据进行相邻数据捆绑,再将捆绑后的数据上传至基站,其中第 γ_i+1 个数据不满足查询指令。最后,基站通过与感知节点共享的秘钥对接收到的数据信息进行解密。若上传的验证信息均能被解密,且 $D_{i,t}$ 中数据均满足 $d_{i,y_i}>d_{i,y_i+1}$,则判定查询结果是完整的;否则认为查询结果不完整。

方案 2　由于方案 1 中 M 需要向基站交付大量的 MAC 信息和不满足查询指令的边界信息,查询过程中产生的通信代价较大,因此方案 2 在方案 1 基础上进行改进,并提出交叉验证方案。在该方案中,同一个 $Cell$ 中的感知节点之间将时间周期 t 内采集到的最大感知数据进行广播。然后,感知节点 s_i 将接收到广播数据嵌入到 $D_{i,t}$ 中,并得到 $D'_{i,t}$,再将 $D'_{i,t}$ 中的数据以加密数据链的方式上传至 M。因此基站可通过交叉验证感知节点上传的数据来判断查询结果的完整性。

方案 2 中,当感知节点中的数据不满足 Q_t 时,M 无需向基站上传不合格的边界数据,因此有效地降低了 M_Cost。然而,感知节点不仅需要向 M 上传当前节点采集的感知数据,而且需要上传接收到的广播数据以及其对应的感知节点信息,因此通过该方案得到的 S_Cost 比方案 1 的更高。

方案 3　为平衡方案 1 和方案 2 中的 M_Cost 和 S_Cost,在 VFTop-k 中提出第 3 种优化方案,即混合交叉验证方案。该方案综合了前两个方案的优点,并将每个网络单元虚拟地划分为若干个子区域。在数据上传阶段,与交叉验证方案相似,首先将感知数据在网络单元内进行广播,然后将感知数据和辅助验证信息上传至 M。不同的是,混合交叉验证方案中每个感知节点仅拥有所在子单元的数据信息。最后,基站根据交叉验证方案中的验证方法对查询结果的完整性进行验证。

(2) VSFTQ

为降低 Top-k 查询过程中产生的通信代价,文献[13]提出了 VSFTQ 查询协议。

在数据上传阶段,为使感知数据之间均可比较,感知节点 s_i 首先通过与文献[14]中相似的公共打分函数对在 t 内采集的感知数据 $D_{i,t}=\{d_{i,1},d_{i,2},\cdots,d_{i,N}\}$ 进行打分,例如 $d_{i,j}(1\leqslant j\leqslant N)$ 对应的分值为 $Score(d_{i,j})$,然后用与基站共享的对称加密密钥 k_i 对 $Score(d_{i,j})$ 和时间周期进行捆绑加密,并将其作为验证信息与感知数据一起上传至 M。假设对称加密函数为 $h_k(*)$,则 s_i 向 M 上传的信息为:

$$s_i\rightarrow M:i,h_{k_i}\{N,t\},d_{i,j},h_{k_i}(1,t,Score(d_{i,1})),\cdots,d_{i,N},h_{k_i}(N,t,Score(d_{i,N}))$$

在查询处理阶段,M 首先定位前 k 个数据,然后将其与对应的验证信息一起上传至基站。基站利用与感知节点共享的秘钥解密查询结果。由于任一 $d_{i,j}$ 与 $Score(d_{i,j})$ 具有一一对应的关系,被攻击的 M 若想篡改 $d_{i,j}$ 的信息,就必须同时篡改 $Score(d_{i,j})$;而在数据上传过程,s_i 对 $Score(d_{i,j})$ 进行加密的秘钥仅与基站共享,因此 M 无法获取秘钥,故很难同时篡改 $d_{i,j}$ 和 $Score(d_{i,j})$ 的信息。基站可根据这一对应关系检测查询结果的完整性。

与 VFTop-k 相比,在 VSFTQ 的执行 Top-k 查询的过程中既无需上传额外边界数据项,也无需将感知数据进行广播,因此有效地降低了查询过程的通信代价。

(3)EVTQ

文献[14]在 VFTop-k 中方案 1 的基础上进行改进,并提出了一种能量高效的可验证 Top-k 查询处理方法 EVTQ。

在感知数据上传阶段,与 VFTop-k 相似,感知节点 s_i 对 t 内采集的感知数据 $D_{i,j}=\{d_{i,1},d_{i,2},\cdots,d_{i,N}\}$ 进行排序,并利用 HMAC 加密函数对相邻数据进行捆绑加密,然后将其与感知数据一起上传至 M。同样假设 $\underline{x}$ 和 $\overline{x}$ 分别为感知数据的下边界值和上边界值,$h_{k_i}(*)$ 为加密函数,则 s_i 向 M 上传的信息为:

$$s_i\rightarrow M:i,t,d_{i,1},h_{k_i}(t\parallel d_{i,1}),d_{i,2},h_{k_i}(t\parallel d_{i,1}\parallel d_{i,2}),\cdots,d_{i,N},h_{k_i}(t\parallel d_{i,1}\parallel d_{i,2}\parallel\cdots\parallel d_{i,N}\parallel\overline{x})$$

与 VFTop-k 的不同之处在于查询处理阶段。在 EVTQ 中,当接收到查询指令 Q_t 后,M 将满足 Q_t 的 γ_i 个感知数据以及边界数据 d_{i,y_i+1} 与验证信息进行整体捆绑并上传至基站,即 M 以如下形式向基站上传查询结果。

$$M\rightarrow\text{基站}:i,d_{i,1},d_{i,2},\cdots,d_{i,y_i},d_{i,y_i+1},h_{k_i}(t\parallel d_{i,1}\parallel d_{i,2}\parallel\cdots\parallel d_{i,y_i+1})$$

最后,基站接收并计算出查询结果,与 VFTop-k 相似,基站可通过边界数据信息的性质对查询结果的完整性进行验证。

文献[15]对 EVTQ 做进一步优化,在数据上传阶段对上传的验证信息进行 Hash 压缩处理;同时,在查询处理阶段,M 将需要反馈给基站的验证信息进行融合处理,从而完成整个查询处理过程的通信性能优化。

3.3　面向可验证的隐私保护查询处理方法

当两层 WSNs 中数据的隐私性和完整性均受到威胁时,基于强安全模型,实现可验证的隐私保护 Top-k 查询处理方案的有文献[7-8,10-11,16-18]。

(1)SafeTQ

文献[7]首次在两层 WSNs 中提出可验证的隐私保护安全 Top-k 查询协议 SafeTQ,其中 SafeTQ 由隐私保护 Top-k 查询协议和两种不同的验证模式组成。

在 SafeTQ 中,为保护数据的隐私性,在数据上传过程中感知节点 s_i 产生随机数 r_i,并将其与排序后的感知数据 $D_{i,t}=\{d_{i,1}, d_{i,2},\cdots,d_{i,N}\}$ 中的前 k 个进行求和,并将求和结果记为 $d_{r_i,j}=d_{i,j}+r_i$。然后将求和后的数据上传至 M,同时将 r_i 上传至辅助计算节点:

$s_i \rightarrow M: i, \{d_{r_i,1}, d_{r_i,2},\cdots,d_{r_i,k}\}$

查询处理阶段,M 通过文献[23]中的安全比较算法计算出 $D_t=\bigcup_{s_i\in c}\{D_{i,t}\}$ 中的第 k 个数据值 v_{kth},并将 v_{kth} 发送至网络单元内的所有感知节点。感知节点 s_i 利用 v_{kth} 与 $D_{i,t}$ 中的数据进行比较,利用大于或等于 v_{kth} 的数据形成查询结果候选集合 $R_{s_i}=\{d_{i,j}\mid d_{i,j}\in D_{i,j}\wedge d_{i,j}\geqslant v_{kth}\}$。然后采用不同的完整性验证方案对其进行处理,并上传至基站。

在 SafeTQ 中,通过引入数据项加密链验证和概率空间邻居验证两种完整性验证模式,提出两种可验证隐私保护 Top-k 查询方案:SafeTQ-L 和 SafeTQ-N。

SafeTQ-L 方案:s_i 首先将感知数据的上、下界 $\bar{x}$ 和 $\underline{x}$ 加入到排序后的 $R_{s_i}=\{d_{i,1}, d_{i,2},\cdots,d_{i,w}\}$ 中,并利用与基站共享的秘钥 $k_{i,t}$ 将其加密,形成数据项加密链:

$$\{(\underline{x}\parallel d_{i,1})_{k_{i,t}}, (d_{i,1}\parallel d_{i,2})_{k_{i,t}},\cdots,(d_{i,w}\parallel \bar{x})_{k_{i,t}}\}$$

然后将其经过 M 上传至基站。基站接收到数据信息后,对其进行解密,并通过检测数据项加密链的完整性以验证查询结果的完整性。

SafeTQ-N 方案:与 SafeTQ-L 方案的不同之处在于 R_{s_i} 的上传阶段,感知节点 s_i 对 R_{s_i} 中的数据进行整体加密,并将整体加密后的数据经过 M 上传至基站,即上传的数据为:

$s_i \rightarrow M \rightarrow$ 基站$: i, \{R_{s_i}\}_{k_{i,t}}$

且通过 Top-k 节点的邻居节点以给定概率向基站发送验证信息,从而有效地减少了查询过程中的通信代价。

(2) SecTQ

针对 VFTop-k 方案中未涉及的数据隐私保护问题和通信代价较大的问题,文献[10]提出了 SecTQ,并在 SecTQ 中提出了一种基于多项式扰动函数的隐私保护方案,同时在原有的水印技术[28-31]的基础上提出了一种新的水印链方案来实现查询结果的完整性验证。

在数据上传阶段,感知节点 s_i 首先利用与基站共享的秘钥 $k_{i,t}$ 对排序后的感知数据 $D_{i,t}=\{d_{i,1}, d_{i,2},\cdots,d_{i,N}\}$ 进行加密,并对其进行编码,设编码函数记为 $pf_i(*)$,$d_{i,j}$ 加密后的编码数据可记为 $pf_i(d_{i,j})_{k_{i,t}}$;同时计算 $D_{i,t}$ 中的数据以及感知数据下界 $\underline{x}$ 的水印,记 $d_{i,j}$ 的水印为 $E(d_{i,j})$;然后将 $d_{i,j}$ 的水印嵌入到 $d_{i,j+1}$ 中,即计算 $h(d_{i,j+1}, E(d_{i,j}))$,其中 $h(*)$ 为嵌入函数。最后,s_i 将编码数据与嵌入水印后的数据一同发送至 M。

查询处理阶段,基站根据 k 值和 $D_t=\bigcup_{s_i\in c}\{D_{i,t}\}$ 中的数据计算查询比较值 V_k,然后对 V_k 进行扰动加密处理,并将其发送至指定 M。M 将感知数据与基站提供的 V_k 进行比较,从而定位前 k 个数据,并将其上传至基站。基站解密接收到的数据,并从水印中提取出原始数据与水印,然后将水印与数据进行匹配,若存在数据与其水印不匹配,则可判定查询结果不完整。

(3)PriSec

文献[8]基于保序对称加密技术[32]提出了基础的 PriSec 安全 Top-k 查询协议以实现数据的隐私性保护,并不断对其进行优化,最终达到既可正确执行 Top-k 查询指令又可保护数据隐私性的目标。因此 PriSec 中包含了 3 个安全查询方案。

PriSec_1:在数据上传阶段,感知节点 s_i 利用与基站共享的密钥 k_i 对时间周期 t 内采集的感知数据 $D_{i,t}=\{d_{i,1}, d_{i,2},\cdots,d_{i,N}\}$ 进行保序加密;然后分别对保序加密后的感知数据和节点信息进行对称加密,同时将感知数据与节点信息进行捆绑对称加密并计算其 MAC 值;最后,s_i 将加密后的数据和节点信息以及捆绑加密后的 MAC 值一起上传至 M。在查询处理阶段,M 定位前 k 个密文数据,并将其与对应的 MAC 值一起上传至基站。接收到来自 M 节点的查询结果信息后,基站对查询结果进行解密并计算出最终的查询结果。

PriSec_2:由于 PriSec_1 中采用保序加密技术实现数据的隐私性保护仍可能会导致感知数据的顺序信息泄露,因此,在 PriSec_2 中提出通过秘密扰动技术对 PriSec_1 进行改进,进一步实现对感知数据顺序信息的保护。数据上传阶段与 PriSec_1 类似,s_i 计算感知数据和节点 ID 的密文数据,以及其对应的 MAC 值,并将密文数据与其 MAC 一起上传至 M。不同的是,在 PriSec_2 中,s_i 与基站共享一个随机阈值 P,并通过 P 判断是否需要对感知数据 $d_{i,j}$ 进行扰动。在查询处理阶段,与 PriSec_1 类似,M 定位前 k 个密文数据,并将其与对应 MAC 一起上传至基站。最后由基站解密并计算出最终的查询结果。

PriSec_3:与 PriSec_1 相比,PriSec_2 虽进一步提高了数据的隐私保护能力,然而仍未考虑查询结果的完整性保护,因此 PriSec_3 在 PriSec_2 的基础上进行了改进,以保护查询结果的完整性。在数据上传阶段,与 PriSec_2 相似,s_i 将密文感知数据和节点 ID 信息以及与其对应的 MAC 信息一起上传至 M。在查询处理阶段,M 将查询结果上传至基站,并需同时上传 $key[*]=\{i, G_{k'}, t\}$ 作为验证信息,其中 $G_{k'}$ 为 M 从保序加密数据中选出的第 k' 个值。基站接收到查询结果,对其进行解密并计算出最终的查询结果 R。

在 Prisec 方案中,上传数据时,同样需要伴随上传大量 MAC 信息,因此通信代价仍然相对较高。

(4)SVTQ

文献[11]提出了 SVTQ 协议,SVTQ 提出了素数聚集方案以保护两层 WSNs 中 Top-k 查询过程中的数据隐私,并提出了一种差异链的数据结构以实现查询结果的完整性验证。

在数据上传阶段,在时间周期 t 内感知节点 s_i 首先将排序后的感知数据 $D_{i,t}=\{d_{i,1}, d_{i,2},\cdots, d_{i,N}\}$ 转换成差异链的形式,$d_{i,j}$ $(1\leqslant j\leqslant N)$ 对应的差异链为 $d'_{i,j}=d_{i,j}\parallel(d_{i,j}-d_{i,j+1})$。设 $\bar{x}$ 为感知数据的上边界,然后计算 $d'_{i,j}$ 和 $[d'_{i,j},\bar{x}]$ 素数聚集后 PMV 编码对应的素数,得到对应的素数分别记

$PF_{i,j}$和$PR_{i,j}$；再利用与基站共享的秘钥$k_{i,t}$对感知数据的差异链进行加密，即计算$d'_{i,j}$的密文数据$(d'_{i,j})_{k_{i,t}}$；最后，s_i将密文数据与其对应的编码数据一起上传至M，即s_i向M上传：

$$s_i \rightarrow M: i, [(d'_{i,1})_{k_{i,t}}, PF_{i,1}, PR_{i,1}], \cdots, [(d'_{i,N})_{k_{i,t}}, PF_{i,N}, PR_{i,N}]$$

在查询处理阶段，M通过对感知数据对应的素数进行比较，定位前k个数据，并将其上传至基站。基站对接收到的数据进行解密并计算出最终结果。

由于查询过程中M可通过对素数聚集后的感知数据进行比较，因此可保证网络中的敏感数据明文信息不被泄露；而感知数据以差异链的形式经M上传至基站，使得基站可通过检测接收到的任一感知数据与其前一个数据的差是否与差异链中的数据差相等，从而判断查询结果中的数据是否被篡改或删除。

(5)VQ

文献[16-17]提出可验证隐私保护 Top-k 查询方案 VQ。该方案在传统保序加密技术的基础上提出了随机分布式保序加密(rdOPE)，即对保序加密后的数据进行随机分布，以进一步保护网络中数据的隐私性；并提出了基于虚拟匿名框架和 HMAC 编码技术，以实现查询结果的完整性验证。

GD-VQ：在数据上传阶段，感知节点s_i采用秘钥为$k_{i,t}$的 rdOPE 对感知数据$D_{i,t}=\{d_{i,1}, d_{i,2}, \cdots, d_{i,N}\}$进行加密，得到密文数据$(d_{i,1})_{k_{i,t}} > (d_{i,2})_{k_{i,t}} > \cdots > (d_{i,N})_{k_{i,t}}$，并随机产生$\alpha$个虚拟感知数据，然后将其加入$D_{i,t}$中得到$(d'_{i,1})_{k_{i,t}} > (d'_{i,2})_{k_{i,t}} > \cdots > (d'_{i,N+\alpha})_{k_{i,t}}$，其中$N$个数据为真实感知数据，$\alpha$个数据为虚拟感知数据。最后，$s_i$将真实感知数据和虚拟感知数据一起上传至$M$。设$h_{\tilde{k}}(*)$为加密哈希函数，其秘钥为$\tilde{k}$，即$s_i$向$M$上传：

$$s_i \rightarrow M: i, (d'_{i,1})_{k_{i,t}}, h_{\tilde{k}_i}((d'_{i,1})_{k_{i,t}} \| \Lambda_{i,1}), \cdots, (d'_{i,N+\alpha})_{k_{i,t}}, h_{\tilde{k}_i}((d'_{i,N+\alpha})_{k_{i,t}} \| \Lambda_{i,N+\alpha})$$

其中，若$(d'_{i,j})_{k_{i,t}}$为虚拟感知数据，则$\Lambda_{i,j}=\emptyset$；否则$\Lambda_{i,j}=\tilde{k}_i$。

在查询处理阶段，基站向M发送 Top-1 查询指令，M则将最大的数据上传至基站。基站对接收到的数据$d'_{i,j}$进行判断，若$d'_{i,j}$为虚拟感知数据，则继续向M发送 Top-1 查询指令，直到获取到k个非虚拟感知结果；若$d'_{i,j}$既不是虚拟数据也不是原始感知数据，则可判定查询结果不完整。

AD-VQ：在 GD-VQ 中，M向基站上传的$k'(k' \geqslant k)$个数据中可能包含虚拟感知数据，为降低M与基站之间的通信代价，在 AD-VQ 中提出可通过虚拟线段来取代 AD-VQ 中的原始感知数据和虚拟感知数据，其中虚拟线段可用两个端点数据来表示。

在数据上传阶段，感知节点首先对采集到的感知数据进行加密，然后计算加密后感知数据的虚拟线段。设数据$(d_{i,1})_{k_{i,t}}$的虚拟线段记为$\eta_i=\langle \eta_{i,begin}, \eta_{i,end} \rangle$，其中$\eta_{i,begin}$和$\eta_{i,end}$分别表示$\eta_i$的起点和终点。再分别从$\eta_{i,begin}$前和$\eta_{i,end}$后随机选出两个数，分别作为虚拟线段$\eta_i'$的起点和终点，记为$\eta_i'=\langle \eta_{i,begin}', \eta_{i,end}' \rangle$，并用$\eta_i'$取代$\eta_i$。设$\mathbf{N}_i$和$\mathbf{Z}_i$分别为$s_i$的邻居节点集合和$s_i$采集的原始感知数据哈希值，则：$\mathbf{N}_i=\{s_{\mathbf{N}_i,1}, \cdots, s_{\mathbf{N}_i,|\mathbf{N}_i|}\}$，$\mathbf{Z}_i=\{h_{\tilde{k}_i}((d_{i,1})_{k_{i,t}}), \cdots, h_{\tilde{k}_i}((d_{i,N})_{k_{i,t}})\}$，感知节点$s_i$向$M$上传如下数据：

$$s_j \rightarrow M: i, \eta_i', N, \mathbf{N}_i, \mathbf{Z}_i, h_{\tilde{k}_i}(j \| \eta_i' \| N \| \mathbf{N}_{i,1} \| \cdots \| \mathbf{N}_{i,|\mathbf{N}_i|}), h_{\tilde{k}_i}(i \| \eta_i' \| N)$$

并向M上传s_i的邻居节点$s_j \in \mathbf{N}_i$数据作为验证信息，即上传：

$$s_j \rightarrow M: j, \eta_i', N, h_{\tilde{k}_i}(j \| \eta_i' \| N)$$

在查询处理阶段，由于虚拟感知数据的嵌入，原始感知数据中满足 Top-k 查询的数据可能比虚拟感知数据小，为减少虚拟数据的上传，基站将向M发送的 Top-k 查询指令转换成 Top-$(\ell-1+k)$查询指令，其中ℓ为最大感知数据与最小感知数据的差。则M定位前$\ell-1+k$个数据，并将其上传至基站。基站解密并计算出最终的查询结果，同时根据上传的邻居节点信息验证查询结果的完整性。

(6)PTK

为进一步降低 Top-k 查询过程中的通信代价，文献[18]提出通过结合 Bloom 过滤器[22]和混淆编码机制实现隐私保护 Top-k 查询的方法 PTK 和 OPTK；并通过引入有序数据关系，提出了兼顾完整性的可验证隐私保护 Top-k 查询方法 SPTK。

PTK：在数据上传阶段，感知节点s_i利用与基站共享的秘钥$k_{i,t}$对时间周期t内采集的数据$D_{i,t}=\{d_{i,1}, d_{i,2}, \cdots, d_{i,N}\}$进行加密，并计算$D_{i,t}$中数据对应的 Bloom 过滤码。假设数据$d_{i,j}$的密文数据记为$(d_{i,j})_{k_{i,t}}$，$d_{i,j}$的 Bloom 过滤码记为$BF_{d_{i,j}}$。$s_i$将密文感知数据和感知数据对应的 Bloom 过滤码一起上传至M，即上传：

$$s_i \rightarrow M: i, \{(d_{i,1})_{k_{i,t}}, (d_{i,2})_{k_{i,t}}, \cdots, (d_{i,N})_{k_{i,t}}\}, \{BF_{d_{i,1}}, BF_{d_{i,2}}, \cdots, BF_{d_{i,N}}\}$$

在查询处理阶段，基站首先通过与文献[24-27]中类似的方法估算出 Top-k 数据的边界阈值V_k，并将包含 Top-k 数据的值对应到一个范围域内，然后将该范围域划分成多个子域。假设划分后的包含 Top-k 数据和边界值V_k的子域记为$\{A, B, C, D, E\}$，基站计算$\{A, B, C, D, E\}$的 Bloom 过滤码$\{BF_A, BF_B, BF_C, BF_D, BF_E\}$，并将其作为查询指令发送至$M$。接收到查询指令后，$M$通过判断下式是否成立来确认$d_{i,j}$是否属于子域$\lambda$。

$$BF_\lambda \cap BF_{d_{i,j}} = BF_{d_{i,j}} \Rightarrow d_{i,j} \in \lambda$$

其中，$\lambda \in \{A, B, C, D, E\}$。若$d_{i,j} \in \lambda$，则将其密文数据和 Bloom 过滤码上传至基站。基站接收到来自M的数据后，解密并计算出最终的查询结果。

在 PTK 中通过将 Top-k 查询指令值转换成离散的查询范围域，并通过 Bloom 过滤机制将感知数据和查询指令转换成对应的编码数据，从而保证了M在无法获取 Bloom 编码秘钥和$k_{i,t}$的情况下很难获取查询过程中的明文数据值。

OPTK：由于 PTK 中基于范围阈值的查询可能会造成k值范围的泄露，且 PTK 中未涉及到查询结果的完整性验证，为保证 Top-k 查询过程中的k值范围的隐私性，OPTK 提出对查询范围值进行混淆编码。其感知数据上传阶段和查询处理阶段与 PTK 中相似，不同之处在于基站计算查询子域的 Bloom 编码前首先利用混淆函数对$\{A, B, C, D, E\}$进行重新选择以得到新的子域$\{\hat{A}, \overline{B}, \hat{C}, \hat{D}, \overline{E}\}$，使得$\hat{A} \cup \overline{B} \cup \hat{C} \cup \hat{D} \cup \overline{E} = A \cup B \cup C \cup D \cup E$，然后再计算新子域的 Bloom 编码，并将其

作为查询指令发送至 M。

SPTK:改进的 OPTK 方案虽能有效防止查询指令中 k 值范围的隐私泄露,但仍未涉及查询结果的完整性验证,因此,在 SPTK 中提出通过建立有序的数据关系使基站可检测出查询结果是否完整。与 OPTK 的不同之处在于,数据上传阶段需先对数据进行排序;然后将感知数据与其排序后的顺序值进行捆绑加密,并计算感知数据的 Bloom 过滤码;再将密文数据与编码数据一起上传至 M。在查询处理阶段,与 OPTK 相似,M 节点判断出属于查询子域的感知数据,然后将其密文数据和编码数据上传至基站。基站解密并计算出查询结果,同时根据解密后的数据与其对应顺序关系判断查询结果是否完整。

最后,从安全目标、安全模型以及主要实现技术角度对现有的 Top-k 查询方法进行总结,如表 1 所列。

表 1 现有安全 Top-k 查询技术

方法	安全目标		安全模型	主要技术
	隐私保护	完整性		
VFTop-k[6]	×	√	完整性攻击模型	链接关系嵌入技术、消息认证技术
SafeTQ[7]	√	√	强安全模型	随机扰动和安全比较技术
PriSec[8]	√	√	强安全模型	保序加密、消息认证技术、随机扰动技术
OPESTQ[9]	√	×	半诚实模型	保序加密技术
SecTQ[10]	√	√	强安全模型	随机扰动技术、水印链技术
SVTQ[11]	√	√	强安全模型	素数聚集技术、差异链技术
PPTQ[12]	√	×	半诚实模型	前缀成员验证技术、HMAC 编码技术
VSFTQ[13]	×	√	完整性攻击模型	对称加密技术、公共打分技术
EVTQ[14-15]	×	√	完整性攻击模型	HMAC 编码技术、相邻加密数据链技术
VQ[16-17]	√	√	强安全模型	随机分布式保序加密技术、虚拟匿名技术
PTK[18]	√	√	强安全模型	Bloom 过滤技术、混淆编码技术

综合上述安全 Top-k 查询处理方案,并由表 1 可知,现有的两层 WSNs 中的安全 Top-k 查询技术研究均是从网络中数据的隐私保护以及查询结果的完整性保护的角度展开的,并对查询性能进行不断优化。

结束语 Top-k 查询技术作为一种重要的数据处理技术,已被广泛应用于 WSNs 中。同时,查询过程中的安全问题已引起了广泛关注,如网络中的数据隐私安全问题、查询结果完整性问题等。现有的面向两层 WSNs 的安全 Top-k 查询技术研究均是以存储节点不可信为基础的,并实现对查询过程中的感知数据、查询指令以及查询结果隐私性的保护,或实现对查询结果完整性的验证。

由于两层 WSNs 中 Top-k 查询的数据隐私保护和查询结果验证技术的研究和发展还处于起步阶段,一些挑战性问题仍有待进一步研究。

(1)查询过程中通信代价的进一步降低

WSNs 中感知节点的通信代价大小决定了网络生命周期的长短,且存储节点与基站之间的通信代价直接影响 Top-k 查询的效率。因此,在保证查询过程中的数据安全性的条件下,如何有效降低查询过程中通信代价的问题具有重要的研究意义。目前,部分工作通过设计或改进相关算法以减少查询过程中的通信代价。随着各项技术的发展与成熟,通过引入新的数据安全保护技术,不断实现查询的最优化仍具有很大的研究空间。

(2)共谋攻击的防范

通常,共谋攻击是指攻击者同时对多个节点进行攻击。在两层 WSNs 中,感知节点也可能被俘获,被俘获的感知节点同样会造成网络数据的隐私泄露。与现有工作类似,当网络中被俘获的感知节点之间发生共谋时,其对网络中数据安全造成的影响是有限的;然而,若感知节点与存储节点发生共谋时,即攻击者同时俘获存储节点和大量感知节点时,存储节点中与被俘获感知节点相关的所有信息的安全性均会受到威胁,从而造成更大程度上的网络数据泄露。目前安全 Top-k 查询中关于共谋攻击的研究基本还处于空白阶段,而两层 WSNs 中的安全范围查询等领域已涉及此类研究,例如文献[42]。因此,研究如何有效防范两层 WSNs 中 Top-k 查询过程中的共谋攻击对进一步提高查询过程中数据的安全性具有重要的现实意义。

(3)异常存储节点检测与排除

查询过程中还可能存在异常节点攻击,即在两层 WSNs 中存在被俘获的存储节点持续交付错误数据或不向基站交付数据信息,使基站始终无法获得正确的查询结果,从而导致网络资源利用率降低的情况。而现有工作中并未涉及对异常存储节点的研究,即检测并排除持续向基站交付错误信息甚至不交付信息的妥协存储节点。若能有效地根据上传的数据信息定位出异常存储节点,并将其从网络中排除,则可降低查询处理结果的不准确性,并有效地提高网络资源的利用率。因此,为进一步提高两层 WSNs 中的查询处理的可靠性,在未来安全查询处理方向还应关注异常节点的检测和排除。

参 考 文 献

[1] GNAWALI O, JANG K Y, PAEK J, et al. The tenet architecture for tiered sensor networks[C]// Proc of the ACM Conf on Embedded Networked Sensor Systems. New York: ACM, 2006: 153-166.

[2] YAO Y L, LIU J F, XIONG N N. Privacy-Preserving Data Aggregation in Two-Tiered Wireless Sensor Networks with Mobile Nodes [J]. Sensors, 2014, 14(11): 21174-21194.

[3] GOLDREICH O. Foundations of Cryptography: Volume 2, Basic Applications [M]. New York, NY, USA: Cambridge University Press, 2004.

[4] BOZOIC V, SOCEK D, STEINWANDT R, et al. Multi-authority attribute-based eneryption with honest-but-curious central authority[J]. International Journal of Computer Mathematics, 2012, 89(3): 268-283.

[5] AGRAWAL R, KIERNAN J, SRIKANT R, et al. Order preser-

ving encryption for numeric data [C]// Proc of the 2004 ACM SIGMOD International Conference on Management of Data. ACM, 2004: 563-574.

[6] ZHANG R, SHI J, LIU Y Z, et al. Verifiable fine-grained top-k queries in tiered sensor networks [C]// INFOCOM, 2010 Proceedings IEEE. IEEE, 2010: 1-9.

[7] 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. (in Chinese)
范永健,陈红. 两层传感器网络可验证 Top-k 查询处理协议[J]. 计算机学报, 2012, 35(3): 423-433.

[8] LIAO X J, LI J Z. Privacy-preserving and secure top-k query in two-tier wireless sensor network [C]// Proc of Global Communications Conference. CA, USA, IEEE, 2012: 335-341.

[9] YAO Y L, LI M, LIU J F. Privacy-preserving Top-K Query in Two-tiered Wireless Sensor Networks [J]. International Journal of Advancements in Computing Technology, 2012, 4(6): 226-235.

[10] LI R, LIN Y P, YI Y Q, et al. A Secure Top-k query protocol in two-tiered sensor networks [J]. Journal of Computer Research and Development, 2012, 49(9): 1947-1958. (in Chinese)
李睿,林亚平,易叶青,等. 两层传感网络中的安全 Top-k 查询协议[J]. 计算机研究与发展, 2012, 49(9): 1947-1958.

[11] ZHOU T, LIN Y P, ZHANG W, et al. Secure and Verifiable Top-K Query in Two-Tiered Sensor Networks [M]// Security and Privacy in Communication Networks. Springer International Publishing, 2013: 19-34.

[12] DAI H, YANG G, QIN X L, et al. Privacy-Preserving Top-k Query Processing in Two-Tiered Wireless Sensor Networks [J]. Journal of Computer Research and Development, 2015, 50(6): 1239-1252. (in Chinese)
戴华,杨庚,秦小麟,等. 面向隐私保护的两层传感网 Top-k 查询处理方法[J]. 计算机研究与发展, 2015, 50(6): 1239-1252.

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

[14] DAI H, YANG G, HUANG H P, et al. EVTQ: An Efficient Verifiable Top-k Query Processing in Two-tiered Wireless Sensor Networks [C]// Proc of 9th IEEE International Conference on Mobile Ad-hoc and Sensor Networks. 2013: 206-211.

[15] DAI H, YANG G, HUANG H P, et al. Efficient verifiable top-k queries in two-tiered wireless sensor networks [J]. KSII Transactions on Internet and Information Systems, 2015, 9(6): 2111-2131.

[16] YU C M, NI G K, CHEN Y, et al. Top-k query result completeness verification in sensor networks [C]// Proc of 2013 IEEE International Conference on Communications Workshops. IEEE, 2013: 1026-1030.

[17] YU C M, NI G K, CHEN Y, et al. Top-Query Result Completeness Verification in Tiered Sensor Networks [J]. IEEE Transactions on Information Forensics and Security, 2014, 9(1): 109-124.

[18] PENG H, ZHANG X, CHEN H, et al. Enable Privacy Preservation and Result Verification for Top-k Query in Two-Tiered Sensor Networks [C]// Proc of 2015 IEEE Trustcom/BigDataSE/ISPA. IEEE, 2015: 555-562.

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

[20] LIU A X, CHEN F. Collaborative enforcement of firewall policies in virtual private networks [C]// Proc of the Twenty-seventh ACM Symposium on Principles of Distributed Computing. ACM, 2008: 95-104.

[21] KRAWCYK H, CANETTI R, BELLARE M. HMAC: Keyed-hashing for message authentication, RFC 2104 [R]. Reston: Internet Society, 1997.

[22] BLOOM B H. Space/time trade-offs in hash coding with allowable errors [J]. Communications of the ACM, 1970, 13(7): 422-426.

[23] VAIDYA J, CLIFTON C W. Privacy-preserving kth element score over vertically partitioned data [J]. IEEE Transactions on Knowledge and Data Engineering, 2009, 21(2): 253-258.

[24] WU M, XU J, TANG X, et al. Top-k monitoring in wireless sensor networks [J]. IEEE Transactions on Knowledge and Data Engineering, 2007, 19(7): 962-976.

[25] MALHOTRA B, NASIMENTO M, NIKOLAIDIS I. Exact top-k queries in wireless sensor networks [J]. IEEE Transactions on Knowledge and Data Engineering, 2011, 23(10): 1513-1525.

[26] JIANG H, JIN S, WANG C. Parameter-based data aggregation for statistical information extraction in wireless sensor networks [J]. IEEE Transactions on Vehicular Technology, 2010, 59(8): 3992-4001.

[27] LI F, YI K, JESTES J. Ranking distributed probabilistic data [C]// Proc of the 2009 ACM SIGMOD International Conference on Management of Data. ACM, 2009: 361-374.

[28] FENG J, POTKONJAK M. Real-time watermarking techniques for sensor networks [C]// Proc of SPIE Security and Watermarking of Multimedia Contents. Bellingham, WA: SPIE Press, 2003: 391-402.

[29] ZHANG W, IU Y, DAS S K, et al. Secure data aggregation in wireless sensor networks. A watermark based authentication supportive approach [J]. Pervasive and Mobile Computing, 2008, 4(5): 658-680.

[30] YI Y Q, LIN Y P, LI X L, et al. False data filtering algorithm using cooperation watermarks for WSN [J]. Journal of Software, 2010, 21(1): 107-118. (in Chinese)
易叶青,林亚平,李小龙,等. WSN 中基于协作水印的虚假数据过滤算法[J]. 软件学报, 2010, 21(1): 107-118.

[31] YI Y Q, LIN Y P, PENG G, et al. False data filtering algorithm without relying on MAC authentication for wirelesss sensor networks [J]. Journal of Communication, 2009, 20(6): 53-63. (in Chinese)
易叶青,林亚平,彭舸,等. 无线传感器网络中不依赖 MAC 认证的虚假数据过滤算法[J]. 通信学报, 2009, 20(6): 53-63.

[32] BOLDYREVA A, CHENETTE N, O'NEILL A. Order-preserving encryption revisited: Improved security analysis and alternative solutions [M]. Advances in Cryptology-CRYPTO 2011. Springer Berlin Heidelberg, 2011: 578-595.

(下转第 47 页)

参 考 文 献

[1] XU B, CUI Y, ZHOU G Y, et al. Unsupervised Speckle Level Estimation of SAR Images Using Texture Analysis and AR Model [J]. IEICE Transactions on Communications, 2014, 97 (3): 691-698.

[2] ZHAO N, RICHARD Y F, SUN H J, et al. Interference alignment with delayed channel state information and dynamic AR model channel prediction in wireless networks[J]. Wireless Networks, 2015, 21(4): 1227-1242.

[3] INOUSSA G, PENG H, WU J. Nonlinear time series modeling and prediction using functional weights wavelet neural network-based state-dependent AR model[J]. Neurocomputing, 2012, 86 (1): 59-74.

[4] CHISCI L, MAVINO A, PERFERI G, et al. Real-time epileptic seizure prediction using AR models and support vector machines [J]. IEEE Transactions on Biomedical Engineering, 2010, 57 (5): 1124-1132.

[5] AKAIKE H. A Bayesian analysis of the minimum AIC procedure[J]. Annals of the Institute of Statistical Mathematics, 1978, 30(1): 9-14.

[6] KAY S M, MARPLE S L. Spectrum Analysis—a Modern Perspective[J]. IEEE Trans on Acoustics, Speech, and Signal Processing, 1981, 28(4): 441-445.

[7] BLU T, DRAGOTTI P L, VETTERLI M, et al. Sparse sampling of signal innovations [J]. Signal Processing Magazine IEEE, 2008, 25(2): 31-40.

[8] CHEN S S, DONOHO D L, SAUNDERS M A. Atomic decomposition by basis pursuit[J]. SIAM Review, 2001, 43(1): 129-159.

[9] RAO B D, KREUTZ-DELGADO K. An affine scaling methodology for best basis selection[J]. IEEE Transactions on Signal Processing, 1999, 47(1): 187-200.

[10] 张晓峒. 应用数量经济学[M]. 北京：机械工业出版社，2009：266-287.

[11] CHENG H, LIU G Q. A Modified Affine Scaling Methodology for Non-smooth optimization[J]. Numerical Mathematics A Journal of Chinese Universities, 2006, 28(1): 20-25. (in Chinese)
程浩，刘国庆. 求解一类非光滑优化问题的改进变尺度方法[J]. 高等学校计算数学学报，2006，28(1)：20-25.

[12] 解可新，韩健，林友联. 最优化方法(修订版)[M]. 天津：天津大学出版社，2004：114-123.

[13] LUENBREGER D G, YE Y Y. Linear and Nonlinear Programming[M]. New York: Spinger, 2008: 201-212.

[14] DING J D, LIU G Q. Covergence Analysis of an Affine Scaling Transformation for Best Basis Selection[J]. Numerical Mathematics A Journal of Chinese Universities, 2011, 33(4): 289-294. (in Chinese)
丁建东，刘国庆. 最优基选择变尺度变换方法收敛性分析[J]. 高等学校计算数学学报，2011，33(4)：289-294.

[15] HAGER W W, ZHANG H C. An affine scaling method for optimization problems with polyhedral constraints [J]. Comput Optim Appl, 2014, 59(1): 163-183.

[16] PANTULA S G, FULLER W A. A Comparison of Unit-Root Test Criteria[J]. Journal of Business & Economic Statistics, 1994, 12(4): 449-459.

[17] CHEN J L, ISLAM S, BISWAS P. Nonlinear dynamics of hourly ozone concentrations: nonparametric short term prediction[J]. Atmospheric Environment, 1998, 32(11): 1839-1848.

(上接第 13 页)

[33] YI Y, LI R, CHEN F, et al. A digital watermarking approach to secure and precise range query processing in sensor networks [C]// Proc of 2013 IEEE International Conference on Computer Communication. IEEE, 2013: 1950-1958.

[34] SHENG B, LI Q. Verifiable privacy-preserving range query in two-tiered sensor networks [C]// Proc of 27th IEEE International Conference on Computer Communications. NJ: IEEE. 2008: 46-50.

[35] SHI J, ZHANG R, ZHANG Y. Secure range queries in tiered sensor networks [C]// Proc of the 28th IEEE International Conference on Computer Communication. Piscataway, NJ: IEEE, 2009: 945-953.

[36] ZHANG R, SHI J, ZHANG Y. Secure multidimensional range queries in sensor networks [C]// Proc of the Tenth ACM International Symposium on Mobile Ad Hoc Networking and Computing. ACM, 2009: 197-206.

[37] CHEN F, LIU A X. SafeQ: Secure and efficient query processing in sensor networks [C]// Proc of the 28th IEEE International Conference on Computer Communication. Piscataway, NJ: IEEE, 2010: 1-9.

[38] CHEN F, LIU A X. Privacy and integrity-preserving range queries in sensor networks [J]. IEEE/ACM Transaction on Networks, 2012, 20(6): 1774-1787.

[39] TSOU Y T, LU C S, Kuo S Y. Privacy-and integrity-preserving range query in wireless sensor networks [C]// Proc of Global Communications Conference, 2012 IEEE. IEEE, 2012: 328-334.

[40] ZHANG X, DONG L, PENG H, et al. Achieving efficient and secure range query in two-tiered wireless sensor networks [C]// Proc of the 24nd IEEE International Symposium In Quality of Service (IWQoS). 2014: 380-388.

[41] NGUYEN T D, BUI T V, DANG V H, et al. Efficiently preserving data privacy range queries in two-tiered wireless sensor networks [C]// Proc of Ubiquitous Intelligence & Computing and 9th International Conference on Autonomic & Trusted Computing (UIC/ATC). IEEE, 2012: 973-978.

[42] ZHANG X, DONG L, PENG H, et al. Collusion-Aware Privacy-Preserving Range Query in Tiered Wireless Sensor Networks [J]. Sensors, 2014, 14(12): 23905-23932.

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

[44] YAO Y, XIONG N, et al. Privacy-preserving max/min query in two-tiered wireless sensor networks [J]. Computers & Mathematics with Applications, 2013, 65(9): 1318-1325.