无线传感器网络的数据安全与隐私保护*

宋建华，税光泽
（湖北大学 数学与计算机科学学院，湖北 武汉 430062）

摘 要：从数据隐私保护的角度研究了无线传感器网络（WSN）的数据安全问题，探讨了传感器节点可能面临的数据安全与隐私威胁，分析了无线传感器网络数据隐私保护的相关技术。

关键词：无线传感器网络；数据安全；隐私保护

中图分类号：TP393.08 **文献标识码**：A **文章编号**：1674-7720（2013）03-0004-03

Data security and privacy preservation in wireless sensor networks

Song Jianhua，Shui Guangze
（School of Mathematics and Computer Science，Hubei University，Wuhan 430062，China）

Abstract：Data security in wireless sensor networks（WSN）is presented by focusing on data privacy preservation. Data security and privacy threats of sensor nodes are addressed. Some relative researches on data privacy preservation in wireless sensor networks are analyzed.

Key words：WSN；data security；privacy preservation

无线传感器网络WSN（Wireless Sensor Networks）是由部署在感知区域的大量微型传感器节点通过无线通信方式形成的一个多跳的自组织网络。传感器节点可以协同地感知、处理和传输采集到的数据，使人们能够远程地获取需要的信息。WSN可广泛应用于军事、工业、医疗、科研等领域。

近年来，随着无线传感器网络的应用发展，特别是作为物联网的基本组成部分，随着物联网技术的发展，无线传感器网络的安全问题已受到普遍关注。对于以数据为中心的传感器网络，如何保护其数据安全与隐私，也成为业界研究的热点。本文将从数据隐私保护的角度来讨论无线传感器网络的数据安全问题。

1 无线传感器网络面临的数据安全及隐私威胁

无线传感器网络以数据为中心，网络中的传感器节点承担着数据采集、数据传输、数据查询、数据融合等任务。由于传感器节点工作在开放环境，极易遭受诸如传感信息的窃听、拒绝服务攻击、隐私信息的泄露等多种威胁和入侵[1-2]。下面分析传感器节点在所承担的任务过程中可能面临的数据安全及隐私威胁。

（1）数据采集

传感器节点工作在开放环境，攻击者可能在网络中加入仿冒节点，将伪造的数据或有害信息注入网络，造成敏感数据失真，影响数据的采集；攻击者也可能把非法节点或被俘节点隐藏在WSN中，改变路由行为，在非法节点或被俘节点伪装成为正常节点后，诱惑信息包并不正确地转发它们，甚至对所有的节点宣称通过自己的路径是最好的路径，造成数据泄露和篡改。

（2）数据传输

对应用于军事、安防等重要领域的WSN，需要传输极其敏感或涉密的数据。数据传输中可能存在窃听和流量分析等攻击，威胁数据安全及隐私。

监听和窃听：窃听是对隐私保护最明显的攻击，借助听到的数据，敌手容易发现通信内容。当通信流量携带着传感器网络配置的控制信息，这些通信流量包含的信息潜在地比通过特定服务器获得的信息更详细。

通信流量分析：通信流量分析与监听和窃听明显结合在一起。在某些节点间传送信息包数目的增加将揭示特定传感器的合法行为。通过流量分析，具有特殊角色或行为的节点将被有效识别，造成隐私的泄露。

（3）数据融合

在无线传感器网络中，节点感知周围环境数据，数

*基金项目：国家自然科学基金资助（61272033）

据传送到汇聚节点，经过数据融合去除冗余或无用数据后，把结果发送给终端用户。这种操作有效地降低了网络负载，从而可以延长网络生命期。但是，攻击环境的存在使聚集节点可能被俘获，从而泄露感知数据。因此，需要研究在聚集节点不能获得感知数据的情况下实现数据聚集，并对聚集结果进行完整性验证，实现基于隐私保护的数据融合。

(4)数据查询

在两层传感器网络中，高资源节点承担了数据收集和查询任务，而高资源节点也可能被俘获，使得攻击者可以通过查询获得信息。因此，需要研究在高资源节点不能获得感知数据和查询信息的情况下实现查询操作，并对查询结果进行完整性验证，实现基于隐私保护的数据查询。

2 无线传感器网络数据隐私保护相关技术研究

近年来，无线传感器网络数据隐私保护技术成为研究热点，国内外都有相关研究成果[3-23]。

参考文献[4]从 WSN 的数据访问控制角度，采用盲签名技术对访问数据进行数据访问加密，同时通过令牌作为购买服务的等价物进行信息交换，在不改变数据原始形态的前提下，给出实现数据访问的隐私驱动型控制算法 DP2AC。DP2AC 能够在网络拥有者和传感器节点不能获知用户身份的情况下实现访问控制，保证合法用户的隐私安全问题；参考文献[5]提出基于簇的数据融合隐私保护算法 CPDA，通过安全多方通信技术对数据融合中的隐私信息进行保护，将随机噪音加入原始数据中。与数据挖掘中对数据的隐私加密技术不同，随机噪声的产生并非是独立无规则事件，而是根据邻居节点协调信息获取，进而避免产生过度泛化的数据结果，影响传输数据的正确表达。同时提出了一种基于数据切片的隐私保护算法 SMART。其中心思想是将所获取的数据分成若干片段(即切片)，将切片后的数据分别沿不同的传输路径进行传递。这样一来，除非隐私攻击者获得所有分片，否则无法得到最终的隐私信息；参考文献[6]改进了 SMART 方法，提出了一种新的低能耗无线传感器网络数据融合隐私保护算法 ESPART。一方面该算法依靠数据融合树型结构本身的特性，减少数据通信量；另一方面该算法分配随机时间片，以避免碰撞。同时限制串通数据范围，降低数据丢失对精确度的影响；参考文献[7]提出了一种将入侵检测与隐私保护相结合的数据融合算法。该算法针对两种隐私攻击类型——窃听和篡改融合结果，提出了一种基于直方图的信息隐藏方法，并在此基础上实现了对篡改攻击的入侵检测；参考文献[8]提出了一种通过注入伪造数据对真实数据进行隐藏的隐私保护算法 KIPDA。该算法中，首先假设每个节点发送的数据包中有 n 个数据，其中仅有一个真实数据，其余数据或者是按照一定规则伪造的数据，或者是随机生成的伪造数据。然后节点将所有数据按照预先与基站约定的顺序封装成包发送给基站节点，最后由基站节点负责将真实数据从不同节点发送来的数据包中提取出来；参考文献[9-11]提出了基于同态加密的数据融合隐私保护算法(CDA 系列算法)来解决数据融合操作中的隐私保护问题。由于同态加密算法的使用，中间节点在不需要解密数据的条件下就可以对数据实施有效的融合。CDA 系列算法存在的主要问题是该算法中基站节点仅能获取最后的融合结果，而不能推算出原始数据；参考文献[12]针对 CDA 算法中基站节点不能获取原始信息的问题，提出了可恢复原始数据的隐私保护算法 RCDA。参考文献[13]利用基于 2 轮融合的多维隐私保护算法进行信息隐藏，将加密后的隐私数据汇聚到基站节点，由基站节点进行相应计算后恢复出原始数据；参考文献[5,8,14]针对攻击者俘获聚集节点企图获取敏感信息的攻击模型，提出了具有保护隐私功能的 SUM、MIN、MAX、MEDIAN 等数据聚集算法；参考文献[15-17]在两层传感器网络中存储节点被俘获的情况下，研究范围查询隐私保护和可验证技术；参考文献[18]采用加随机数扰动和安全比较等技术在两层传感器网络中完成隐私保护精确 Top-k 查询，使用两种完整性验证模式使基站能够检测和拒绝不正确或不完整查询响应。

总的来说，无线传感器网络数据隐私保护相关技术研究在密码技术、密钥管理、安全路由、数据融合、数据查询、入侵检测等方向都有进展，但无线传感器网络中的节点通常是资源受限的。因此，能量消耗是无线传感器网络数据隐私保护技术需要进一步重点考虑的问题，这方面国内的研究还处于起步阶段，具有广阔的发展空间。

数据隐私保护技术作为新兴的研究热点，不论在无线传感器网络的理论研究还是实际应用方面，都具有非常重要的价值。现有的无线传感器网络数据隐私保护研究虽然已经提出了一些数据隐私保护方案，但是它们各自有自己的适用范围，而且部分解决方案还存在一些问题需要进一步解决，因此无线传感器网络数据隐私保护研究仍然任重道远。

参考文献

[1] CHAN H, PERRIG A. Security and privacy in sensor networks[J]. IEEE Computer Magazine,2003,36(10):103-105.

[2] PERRIG A, STANKOVIC J, WAGNER D. Security in wireless sensor networks [J]. Communication ACM,2004,47(6):53-57.

[3] 范永健,陈红,张晓莹.无线传感器网络数据隐私保护技术[J]. 计算机学报,2012,35(6):1131-1146.

[4] ZHANG R, ZHANG Y, REN K. DP2AC: distributed privacy-preserving access control in sensor networks [C]. In Proceedings of 28th IEEE International Conference on Computer Communications(INFOCOM),2009:1298-1306.

[5] He Weibo, NGUYEN H. PDA: privacy-preserving data

aggregation in wireless sensor networks [C]. Proceedings of the 26th IEEE International Conference on Computer Communications. Washington D. C., USA: IEEE Computer Society Press, 2007:2045-2053.

[6] 杨庚,王安琪,陈正宇,等.一种低耗能的数据融合隐私保护算法[J].计算机学报,2011,34(5):792-800.

[7] Wang Chuang, Wang Guiling, Zhang Wensheng. Reconciling privacy preservation and intrusion detection in sensory data aggregation [C]. Proceedings of INFOCOM'11. IEEE Press, 2011:336-340.

[8] GROAT M M, He Wenbo, FORREST S. KIPDA: K-indistinguishable privacy-preserving data aggregation in wireless sensor networks [C]. Proceedings of INFOCOM'11. IEEE Press, 2011:2024-2032.

[9] GIRAO J, WESTHOFF D, SCHNEIDER M. CDA: Concealed data aggregation in wireless sensor networks [C]. Proceedings of ACM Workshop on Wireless Security. ACM Press, 2004.

[10] GIRAO J, WESTHOFF D, SCHNEIDER M. CDA: concealed data aggregation for reverse multicast traffic in wireless sensor networks [C]. Proceedings of IEEE International Conference on Communications. Seoul, Korea: IEEE Press, 2005: 3044-3049.

[11] WESTHOFF D, GIRAO J, ACHARYA M. Concealed data aggregation for reverse multicast traffic in sensor networks: encryption, key distribution, and routing adaptation [J]. IEEE Transactions on Mobile Computer, 2006, 5(10): 1417-1431.

[12] Sun Hungmin, Chen Chienming, Lin Yuehsun. RCDA: recoverable concealed data aggregation for data integrity in wireless sensor networks [J]. IEEE Transactions on Parallel and Distributed Systems, 2011, 22(4): 727-734.

[13] Yang Piyi, Cao Zhenfu, Dong Xiaolei. An efficient privacy preserving data aggregation scheme with constant communication overheads for wireless sensor networks [J]. IEEE Communications Letters, 2011, 15(1): 1205-1207.

[14] ZHANG W S, WANG C, FENG T M. GP2S: generic privacy-preserving solutions for approximate aggregation of sensor data [C]. Proceedings of the 6th Annual IEEE International Conference on Pervasive Computing and Communications. HongKong, China, 2008:179-184.

[15] Sheng Bo, Li Qun. Verifiable privacy-preserving range query in two-tiered sensor networks [C]. Proceedings of the 27th IEEE International Conference on Computer Communications (INFOCOM). Phoenix, USA, 2008:46-50.

[16] Shi Jing, Zhang Rui, Zhang Yanchao. Secure range queries in tiered sensor networks [C]. Proceedings of the 28th IEEE International Conference on Computer Communications (INFOCOM). Rio de Janeiro, Brazil, 2009:945-953.

[17] Chen Fei, LIU X. SafeQ: secure and efficient query processing in sensor networks [C]. Proceedings of the 29th IEEE International Conference on Computer Communications (INFOCOM). San Diego, USA, 2010:2642-2650.

[18] 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.

[19] 周贤伟,覃伯平,徐福华.无线传感器网络与安全[M].北京:国防工业出版社,2007.

[20] 肖湘蓉,无线传感器网络流式数据安全研究[D].长沙:湖南大学,2010.

[21] 王安琪.适用于WSN的数据融合隐私保护算法研究[D].南京:南京邮电大学,2012.

[22] 孙喜策.商用驱动的无线传感器网络分布式隐私保护技术研究[D].杭州:浙江大学,2010.

[23] 许建,杨庚,陈正宇,等.WSN数据融合中的隐私保护技术研究[J].计算机工程,2012,15(8):134-138.

(收稿日期:2012-11-06)

作者简介:

宋建华,女,1973年生,博士,硕士生导师,主要研究方向:信息安全,无线传感器网络。

税光泽,男,1988年生,硕士研究生,主要研究方向:信息安全,无线传感器网络,数据库。