doi: 10.3969/j.issn.1006-1576.2012.09.012

基于多路由传输的无线传感器网络安全数据汇聚机制

罗永健，史德阳，陈涛，张卫东
（西安通信学院电子工程系，西安 710106）

摘要：针对无线传感器网络数据汇聚中存在的安全威胁问题，提出一种基于多路由传输的安全数据汇聚机制。该机制将传感器节点感知数据分解到不同的维数上，在数据传输过程中采用多路由传输，且在数据传输过程中不必执行解密–加密操作，并从外部攻击和内部攻击对新机制的安全性进行了分析。分析结果表明，该机制能有效抵御侦听、数据分组丢弃、路由分组丢弃等类型的攻击。

关键词：无线传感器网络；安全数据汇聚；多路由传输
中图分类号：TP393.08　　**文献标志码**：A

Secure Data Aggregation Mechanism of Wireless Sensor Networks Based on Multi-Routing Transmission

Luo Yongjian, Shi Deyang, Chen Tao, Zhang Weidong
(*Dept. of Electronic Engineering*, *Xi'an Communications Institute*, *Xi'an* 710106, *China*)

Abstract: Aiming at the threats in the process of data aggregation, a secure data aggregation mechanism based on multi-routing transmission for wireless sensor networks is proposed. The data is divided into different dimensions before transmission, and then the divided data are transmitted by means of multi-routing. Meanwhile, the encrypted data do not need to be decrypted in the process of data transmission. The security of the new mechanism is analysed from the aspects of external attacks and insidious attacks. Analysis results show that the wireless sensor networks by means of the new mechanism can effectively protect against eavesdropping, routing packet discarding and data packet discarding.

Key words: wireless sensor networks; secure data aggregation; multi-routing transmission

0　引言

无线传感器网络是由部署在监测区域内的大量廉价微型传感器节点组成，并通过无线通信方式形成的多跳自组织网络系统[1]。目前，针对无线传感器网络的研究主要从路由、能量、跨层设计以及安全等方面开展[2]，其中能量问题和安全问题是很重要的研究内容。由于无线传感器网络节点通常采用微型电池供电，并且在很多情况下其能量无法进行补给，故降低网络能耗成为无线传感器网络的研究热点之一。由于数据汇聚技术可以消除数据冗余、降低网络能耗，因此数据汇聚在无线传感器网络中得到了广泛应用[3-4]。然而，由于无线传感器网络节点通常部署在敌后或者条件恶劣的环境中，传感器节点极易受到恶意攻击，使得数据汇聚安全问题严重限制了数据汇聚技术的应用[5]。

针对数据汇聚过程中存在的安全威胁，目前相关研究人员已经开展了大量的研究。传统的数据机密性保护主要采用逐跳加密的方式[6]，但此方案不能保证数据的端到端机密性，并且由于需要在中间节点执行解密–加密操作，增加了数据汇聚的成本。针对该问题，Westhoff 等人首先采用同态加密技术对节点感知数据进行加密，该方案不需要对密文数据进行解密，从而保证了数据的端到端机密性[7]。遗憾的是，该方案无法有效防御攻击者施加的选择性转发攻击。为了克服以上不足，文献[8]提出一种基于信息重构的多路由数据传输算法，该算法允许网络中存在妥协节点，能有效抵御侦听、数据篡改和拒绝服务攻击，但该算法信息重构的过程较为复杂，且计算量较大。Shu Qin Ren 等提出一种基于数据挖掘的数据汇聚算法[9]，该算法采用同态加密技术保证数据的机密性，并采用信息挖掘技术，对节点感知数据进行过滤，可以实现相对精确的平均值汇聚，但是当无线传感器网络中不存在攻击时该算法仍会剔除边缘数据。基于此，笔者提出一种基于多路由传输的安全数据汇聚机制。

收稿日期：2012-04-01；**修回日期**：2012-05-02
基金项目：国家自然科学基金“基于攻击检测的无线传感器网络复原汇聚技术研究”（61179002）；陕西省自然科学基础研究计划资助项目“无线传感器网络分簇数据复原汇聚方法及其应用研究”（2011JM8030）
作者简介：罗永健(1971—)，男，湖北人，博士，教授，从事阵列信号处理、雷达目标识别及多用户通信研究。

1　数据汇聚存在的安全威胁

针对数据汇聚的攻击通常分为外部攻击和内部攻击 2 种。外部攻击[10]是指非授权用户利用无线信道的开放性，在数据从源节点到汇聚节点的传输过程中进行监听，通过分析监听到的关键信息获得节点感知信息，进而实施侦听、篡改等类型的攻击，基于密码学的安全体制可有效防范外部攻击。

内部攻击[11]是指攻击者已经突破身份认证等依托现代密码技术而设置的第一层安全防护，并掌握了相应的安全密钥，以所拥有的合法身份，从网络内部主动地发起有针对性的、蓄意的、串谋的攻击行为。攻击者获得的合法身份通过物理俘获网络节点或者操控节点感知环境的方式获得，拥有合法身份的节点可参与数据收集、数据传输等网络关键服务，从而实现对转发数据的篡改、注入和丢弃等。根据无线传感器网络提供的数据汇聚和分组转发这 2 种关键服务，可将内部攻击行为分为路由分组丢弃、数据分组丢弃和数据篡改 3 种[12]。

2　系统模型假设

文中数据汇聚机制建立在分簇式无线传感器网络的基础上，分簇式的无线传感网络模型如图 1。利用分簇算法将无线传感器网络划分为若干个簇，每个簇含有若干个传感器节点并选择其中一个节点充当簇头。簇头收集该簇节点的感知数据并进行汇聚处理，然后将汇聚结果传送至基站，基站根据用户需求提供一个关于节点监测环境的全局信息。

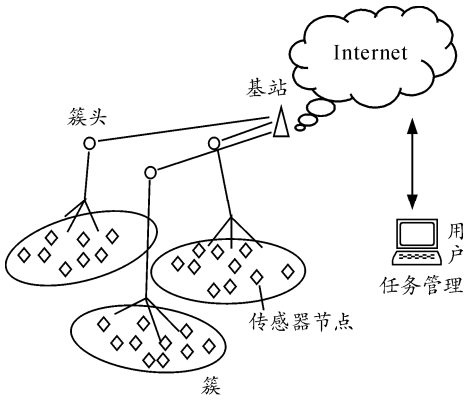

图 1　分簇式无线传感器网络模型

在分簇式无线传感器网络的基础上，笔者假设无线传感器网络具有以下性质：

1) 无线传感器网络为静态网络，传感器节点部署后不再移动；

2) 节点具有一定的存储空间，用来存储密钥和感知数据等信息；

3) 邻居节点之间的通信是双向的；

4) 传感器节点具有相同的信息处理能力以及通信能力，且每个节点具有唯一的身份标识；

5) 初始网络中不存在恶意攻击节点。

3　安全数据汇聚新机制的基本原理

在上述系统模型假设的基础上，笔者提出一种基于多路由传输的安全数据汇聚机制。该机制的工作流程可分为簇形成阶段、数据加密阶段、簇头处汇聚阶段、多路由传输阶段和基站处汇聚阶段。

1) 簇形成阶段。

在网络部署之初，在每个传感器节点上预置一个密钥环[9]，密钥环由密钥环生成器产生，如图 2 所示。密钥环包含 2 部分的内容，即密钥 $R_i=\{K_{i1},K_{i2},\cdots,K_{im}\}$ 和索引 $I_i=\{I_{K_{i1}},I_{K_{i2}},\cdots,I_{K_{im}}\}$，其中 $I_{K_{ij}}=\mathrm{index}(K_{ij})$。簇头节点随机选取一个密钥 K_{ij} 作为该簇的共享密钥，并将该密钥对应的密钥索引 $I_{K_{ij}}$ 告知该簇的成员节点。

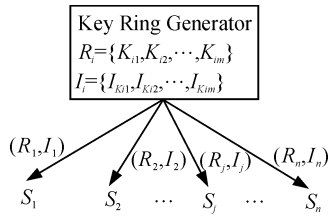

图 2　预置密钥的生成

2) 数据加密阶段。

节点将感知到的原始数据 X_{ij} 用密钥 K_{ij} 进行加密，得到加密后的数据 $e_{ij}=E_{K_{ij}}(X_{ij})$，然后节点将加密数据 e_{ij} 传输至簇头节点。

3) 簇头处汇聚阶段。

簇头节点收集到从该簇节点传来的数据后，对加密数据 e_{ij} 利用聚合函数进行聚合，得到该簇的汇聚结果 e_i，即

$$e_i=f(e_{i1},e_{i2},\cdots,e_{im_i}) \tag{1}$$

其中：m_i 为该簇传感器节点的数目；f 为聚合函数。

为进一步增加节点感知数据的安全性，将 e_i 转换数据格式。考虑将 e_i 转换成以 e_i 为半径的球上的任一点(也可将数据转换成二维、四维等，维数越高安全性越高，但相应的计算量也越大，文中以三维为例)，球的半径大小表示节点感知数据的不同，即

$$e_i\rightarrow(e_i\bullet\cos\phi\bullet\cos\theta,e_i\bullet\sin\phi\bullet\cos\theta,e_i\bullet\sin\theta) \tag{2}$$

4) 多路由传输阶段。

簇头节点将经过信息转换后的 3 个数据分量及该簇所用密钥索引 $I_{K_{ij}}$，通过不相交的 3 条路由向基站处转发，如图 3。

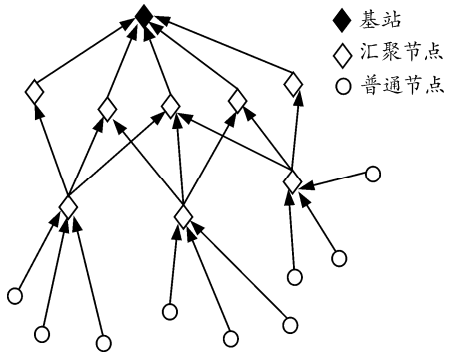

图 3 多路由数据传输示意图

5) 基站处汇聚阶段。

基站收集到来自簇头节点的信息后，首先将来自同一个簇头节点的信息进行重构

$$e_i = \sqrt{(e_i \cdot \cos\phi \cdot \cos\theta)^2 + (e_i \cdot \sin\phi \cdot \cos\theta)^2 + (e_i \cdot \sin\theta)^2} \quad (3)$$

基站利用相应的密钥索引 $I_{K_{ij}}$ 查询相应的密钥，对 e_i 进行解密。然后，对解密后的明文数据执行相应的数据汇聚算法，最终基站根据用户需求提供一个关于节点监测环境的全局信息。

4 安全性分析

假设攻击者不可能完全掌握网络的拓扑结构，且网络中不存在常规性的数据丢失，每条路由发送的数据在没有攻击的情况下都可以传递到基站。

1) 抵御外部攻击。

由于采用了多路由传输机制，若网络中的部分传感器节点被攻击者攻陷，那么攻击者只能获得节点感知信息的一部分。若攻击者想要得到一条完整信息，至少要获得来自 3 条不同路由且由同一个汇聚节点发出的信息。例如，假设攻击者在 3 条路由上攻陷了 3 个节点 X、Y 和 Z，每个节点收到来自不同节点的数据，若 X 收集的数据来自节点 a 和 b，Y 收集得到数据来自节点 c 和 d，Z 收集的数据来自节点 e 和 f，那么攻击者想要重构信息是不可能的，这样窃听攻击将难以实施。另一方面，该机制通过数据转换进一步增强了数据汇聚的安全性，即使攻击者获得了由同一个汇聚节点发出的 3 条不同路由的信息，若攻击者不知道信息重构方式和加密密钥，那么攻击者也将无法获得节点信息，从而保证了节点感知数据的机密性，也使得攻击者实施的侦听、数据篡改等攻击无法进行。

2) 抵御内部攻击。

无线传感器网络的关键服务是环境感知并将感知数据传输至基站，这 2 类关键服务可分解为 2 类工作场景[12]：数据汇聚和分组转发服务。针对分组转发的内部攻击有数据分组丢弃和路由分组丢弃。路由分组丢弃是指恶意节点选择性转发路由数据分组；数据分组丢弃是指受攻击节点忠实地转发路由数据，而选择性地转发节点感知数据。由于文中汇聚机制采用多路由传输技术，在基站处需要对收集到的数据进行信息重构，而信息重构必须获得来自同一个节点的 3 个维数上的数据才能进行。当路由分组丢弃和数据分组丢弃攻击发生时，某些节点的感知数据也同时被丢弃，那么基站将无法重构信息，基站可根据收集到的信息来确定哪些节点的数据遭到丢弃。因此，新机制可有效抵御路由分组丢弃和数据分组丢弃等类型的攻击。

然而，新机制却无法有效抵御内部攻击行为中的数据篡改攻击。比如，当攻击者通过操控节点感知环境或者俘获网络中的部分节点时，将使节点感知的原始数据受到攻击。此时，可以利用相应的数据复原汇聚算法进行处理[13]。

5 计算开销分析

假定簇头选举的过程对每个节点是绝对公平的，下面笔者对新机制的计算开销进行了分析。下文表述中 r 为 WSN 中分簇的数目，n 为无线传感器网络中节点的总数目。

由于新机制在数据传输过程中对汇聚节点的聚合结果进行格式转换，且在基站处要进行信息重构，在一定程度上会增加汇聚节点和基站的计算量。与一般的数据汇聚机制(汇聚节点对收集到的数据进行聚合后直接传输至基站，不进行信息转换和多路由数据传输)相比，新机制在簇头节点处进行信息转换的过程中增加的计算量为 $5 \cdot r$ 次的乘积运算，由于簇头节点是通过簇头选择机制确定的，并要求尽可能保证每个节点充当簇头节点的公平性，所以在一次数据转换过程中，每个传感器节点增加的计算量平均为 $(5 \cdot r)/n$ 次的乘积运算。在基站处进行信息重构的过程中，基站增加的计算量为 3 次乘积运算和 1 次开平方运算。

鉴于基站的能量是不受限制的，在基站处增加的计算量所造成的能量消耗可以忽略不计。在一次数据汇聚过程中，每个节点增加的计算量平均为

$(5•r)/n$次的乘积运算。将 1 000 个传感器节点划分为 10 个簇时，每个节点增加的计算量平均仅为 0.05 次的乘积运算，这样的计算开销是很小的。一方面，随着无线传感器网络的不断发展，目前单个节点的存储和计算能力都有了很大提高，这样就放松了对单个节点计算量的限制；另一方面，无线传感器网络的能量主要消耗在数据传输、信号处理和硬件操作 3 个方面，而数据传输消耗的能量占节点总能量的 70%[14]，信号处理所造成的能量消耗只占其中的很小一部分(传输 1 bit 信息所需的能量大约可以执行 3 000 条计算指令)。鉴于以上原因，文中安全数据汇聚机制的计算开销不会影响网络的整体寿命。

6　结语

针对数据汇聚存在的安全威胁，笔者提出一种基于多路由传输的安全数据汇聚机制。该机制在数据传输过程中采用信息拆分和多路由传输，能够有效抵御窃听、数据分组丢弃、路由分组丢弃等类型的攻击，同时保证数据的端到端机密性。

参考文献：

[1] 秦晓良, 魏琴芳, 张双杰. WSNs 中高效且适应性强的安全数据融合[J]. 计算机应用研究, 2011, 28(11): 4299-4302.

[2] Buttyan L, Hubaux J P. Security and cooperation in wireless networks[M]. UK: Cambridge University Press, 2007.

[3] Cayirei E. Data aggregation and dilution by modulus addressing in wireless sensor networks[J]. IEEE Communications Letters, 2003, 7(8): 355-358.

[4] 刘明, 龚海刚, 毛莺池, 等. 高效节能的传感器网络数据收集和聚合协议[J]. 软件学报, 2005, 16(12): 2106-2116.

[5] 张鹏, 喻建平, 刘宏伟. 传感器网络安全数据融合[J]. 计算机科学, 2011, 38(8): 106-108.

[6] 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.

[7] 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 Computing, 2006, 5(10): 1417-1431.

[8] 归奕红, 刘宁. 无线传感器网络安全数据汇聚算法[J]. 微电子学与计算机, 2011, 28(4): 115-121.

[9] Shu Q R, Jong S P. Density mining based resilient data aggregation for wireless sensor networks[C]//Fourth International Conference on Networked Computing and Advanced Information Management. USA: IEEE Computer Society, 2008: 261-266.

[10] Karlof C, Wanger D. Secure routing in wireless sensor networks: attacks and counter measures[J]. Elsevier's Ad Hoc Networks Journal, 2003, 1(2-3): 293-315.

[11] 王良民, 李菲, 熊书明. 无线传感器网络内部攻击检测方法研究[J]. 计算机科学, 2011, 38(4): 97-99.

[12] 王良民, 郭渊博, 詹永照. 容忍入侵的无线传感器网络模糊信任评估模型[J]. 通信学报, 2010, 31(12): 37-54.

[13] 罗永健, 丁小勇, 罗相根, 等. 一种有效的无线传感器网络数据复原汇聚方法[J]. 数据采集与处理, 2011, 26(1): 90-94.

[14] Perrig A, Szewczyk R, Wen V, et al. Security protocols for sensor network[J]. Wireless Networks, 2002, 8(5), 521-534.

****

(上接第 23 页)

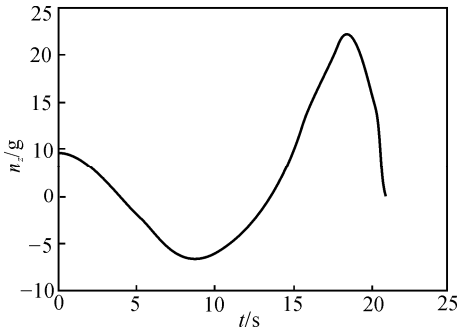

图 7　舰空导弹水平面上法向过载变化曲线

由式 (13) 可以看出，反舰导弹的法向过载与其速度的二次方成正比，与其机动半径成反比，而舰空导弹水平面上的需用法向过载随反舰导弹的法向过载增加而增加；因此，舰空导弹的需用法向过载随反舰导弹的速度增加而增加，随机动半径增加而减小，仿真结果也说明了这一点。

5　结束语

仿真结果表明，该模型可为舰空导弹对蛇行机动反舰导弹的拦截适宜性判断提供依据。

参考文献：

[1] 姚奕, 聂永芳. 提高反舰导弹突防能力措施研究[J]. 飞航导弹, 2008(8): 26-29.

[2] 张卫锋, 张中南, 熊小龙. 舰空导弹拦截“蛇行机动”反舰导弹的仿真研究[J]. 战术导弹技术, 2007(3): 82-85.

[3] 马良, 姜青山, 汪浩, 等. 反舰导弹对舰空导弹的机动突防模型研究[J]. 海军航空工程学院学报, 2008, 23(2): 185-188.

[4] 钱杏芳, 林瑞雄, 赵亚男. 导弹飞行力学[M]. 北京: 北京理工大学出版社, 2006: 90-112.

[5] 欧君瑜, 李刚, 高忠长. 基于 Matlab 的防空导弹三维弹道仿真[J]. 火力与指挥控制, 2010, 35(2): 166-168.

[6] 张建伟, 黄树彩, 韩朝超. 基于 Matlab 的比例导引弹道仿真分析[J]. 战术导弹技术, 2009(3): 60-64.