第 34 卷 第 7 期 计 算 机 工 程 2008 年 4 月
Vol.34 No.7 Computer Engineering April 2008
·安全技术· 文章编号：1000—3428(2008)07—0145—03 文献标识码：A 中图分类号：TP393.08

传感器网络的报文攻击检测技术研究

陈国旗，黄 俊
(中国计量学院信息工程学院，杭州 310018)

摘 要：提出以基站(BS)为基础的基于一致性检查的代理报文方法，该方法通过代理报文方式验证从 CH 到 BS 中的数据报文的正确性，由于代理报文是通过非主路径周期性发送的，BS 可接收传感器网络中不同路径传送的 2 个不同来源的数据报文，并通过比较实现数据的检查，有效地解决了传感器网络的报文在主路径中被丢弃和篡改问题。

关键词：传感器网络；报文攻击；恶意簇头；安全检测

Research on Report Attack Detection in Sensor Networks

CHEN Guo-qi, HUANG Jun
(Department of Information Engineering, China Jiliang University, Hangzhou 310018)

【Abstract】 A consistency checking-based proxy-report schemes rooted at the BS is introduced, which uses proxy reports to verify the accuracy of data reports sent by a CH to the BS. Proxy reports are periodically sent along non-primary paths, enabling the BS to detect any tampering or dropping of the data reports by malicious nodes on the primary paths.

【Key words】 sensor networks; report attack; malicious cluster heads; security detection

无线传感器网络的安全问题正在成为制约无线传感器网络技术发展的瓶颈。目前对无线传感器网络的安全问题研究主要集中在密钥管理、女巫(sybil)攻击和非法信息注入等方面，这些研究主要强调密钥管理和重置密钥相关协议[1]。大部分传感器网络安全方法是建立在到基站(Base Station, BS)的报文是经簇头进行过端-端加密的假设上，但传输的报文可能被恶意簇头篡改而在大型传感器网络环境中很难被检测到，也可能被恶意簇头或路径上的中间节点进行有选择的丢弃。由于目前传感器网络技术缺少BS对接收报文的应答确认机制，因此传感器网络的报文丢弃和篡改检测问题一直无法得到解决。本文通过采用对主报文和代理报文间的一致性检查和周期性确认从簇头发送到BS的数据报文方法提出了一种基于BS的轻量级检测方法，该方法与其他防虚假数据注入方法[2]结合可有效解决传感器网络数据通信的可信性和可靠性问题。

1 方法概要

本文提出的传感器网络报文丢弃和篡改检测方法是通过传统的数据一致性检查方法加以实现的，BS 接收传感器网络中不同传感器传送的不同来源的数据报文并通过比较进行数据一致性检查，即除簇头通过簇内节点数据收集形成一主报文，簇内的备份节点通过收集它的信号范围内节点数据另外形成一代理报文，并将该报文转发到簇外一称为代理节点的节点上，代理节点又将该代理报文作为特殊标记数据传输到自己的簇头，簇头通过主路径将该代理报文发送到 BS，BS 在接收到传感器网络中不同节点传送的不同来源的数据报文后，通过比较检查验证主报文数据的完整性和可靠性，原理如图 1 所示。根据不同的应用，报文的格式可以是数值格式或非数值字符串格式，簇的范围可大可小。小簇中，发送到 BS 的报文包含期望消息认证码(XMAC)值用于校验。大簇中的数值报文格式的报文，基于非交互相关函数证明(non-interactive function-specific proof)的 Merkle 哈希树随同报文一起发送到 BS。对于非数值字符串格式，发送到 BS 的报文中含有基于散列消息鉴别码(HMAC)。BS 采用 XMAC 值或附在主报文的非交互证明以保证所接收的报文是无任何错误或被篡改的正确可靠报文。

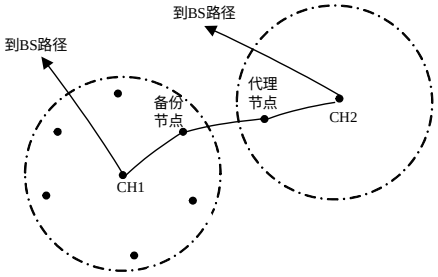

图 1 CH1 簇的备份和代理节点

簇的备份路径选择首先是由它的邻接簇簇头到 BS 的路径构成一组备份路径，称为侯选路径，如图 2 所示。再从这些侯选路径中选择其中一条作为备份路径。选择原则是如主路径的任何一个节点失效或受到威胁，对其备份路径产生的影响最小的路径为备份路径。文献[3]中证明了在移动 ad-hoc 网络中由于节点的移动性，节点数最少和节点间非相关性最大的多路径最健壮。笔者将该理论应用于本方法中，即一条最佳的备份路径是与主路径非相关性最大且节点数最少的路

基金项目：国家自然科学基金资助项目(60608009)；浙江省教育厅科研基金资助项目(20060520)
作者简介：陈国旗(1971－)，男，工程师，主研方向：网络安全技术及数据库技术；黄 俊，副教授
收稿日期：2007-04-10 **E-mail：**hjun@cjlu.edu.cn

径。而选择最佳备份路径的问题是 NP-hard 问题，通过文献[4]中所提出的启发法(Heuristic)进行备份路径的最佳选择，为了有效解决 BS-簇间的通信模型问题，笔者设计一个由 BS 计算的称为非相关度(Degree of Disjointedness, DD)的启发度量，簇内节点根据启发度量来进行备份节点和路径的选择，如图 3 所示。

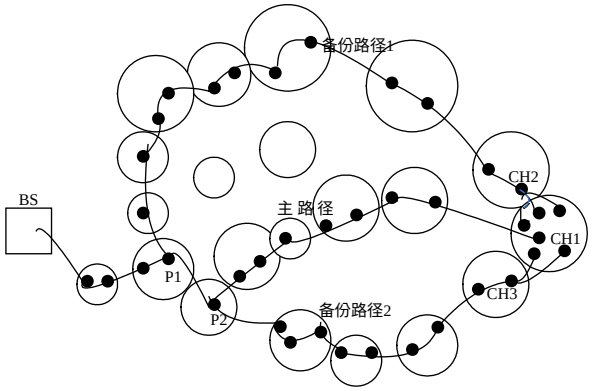

图 2　CH1 簇的主路径和备份路径

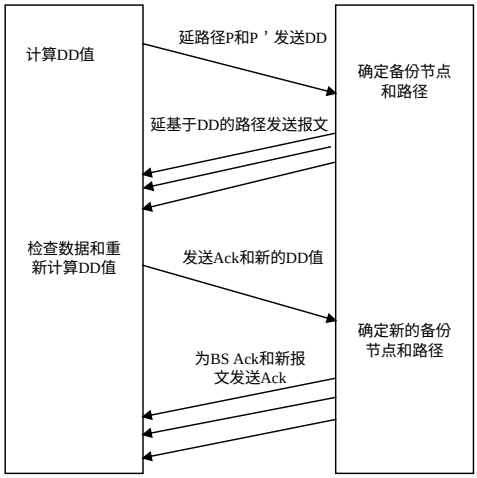

图 3　BS-簇间通信示意图

本方法中簇的备份和代理节点的选择同样关键。(1)簇头不能是备份节点。(2)在短时间内已连续向 BS 发送过一定数量的代理报文节点不能作为备份节点，避免由于恶意备份或代理节点发送的数据降低主数据报文的可信度。(3)备份节点的电池能量应大于某一阈值。具体选择备份和代理节点的方法如下：

(1)随机选择法。在簇内随机选择一节点为备份节点，其优点是实现简单，不足是恶意节点可能多次被选择作为备份节点。

(2)静态选择。侯选节点按顺序排列，然后按序指定为备份节点。该方法适用于节点在无需交换任何信息的情况下自己决定排列顺序[5]，优点是某一恶意节点连续被选择作为备份节点概率较小。

(3)基于评价法。每个侯选节点都有简单的评价值 N，N 是一个包含 DD、节点发送流量、节点的剩余能量和节点覆盖的簇区域大小等参数的函数。该方法精度高，但计算复杂。

2　BS-簇间的通信方式

BS 与簇间的通信步骤如图 3 所示。文中符号 P 表示簇的主路径；P’表示为簇的侯选路径；p’代表选择用来发送报文的备份路径。

BS 为 P’中的各条路径计算 DD 值。开始阶段，备份路径 p’是 P’中具有最大 DD 值的那条路径，计算的各条路径 DD 值通过路径 p 和 p’传输到簇，簇内全部节点将获得这些 DD 值。由于路径 p 或 P’中备份路径可能发生改变，因此 BS 将会对这些 DD 值随时进行更新。

BS 通过确认摘要(acknowledgement digest)方式应答簇的 last-t 报文，其中 t 是一实现相关(implementation-dependent)参数，具体的 t 值是 BS 根据过去收到正确报文数或根据簇的大小来确定，这与 TCP 协议中的流控制类似。开始时，BS 是同时延路径 p 和 p’发送确认摘要，再根据阈值选择发送确认摘要路径数，如果超过一半的 last-t 报文被正确接收，BS 将只选择路径 p 发送，否则仍然同时选择路径 p 和 p’发送。初始 p 是由 BS 选择的，后面则是由簇内节点根据 DD 值由簇内的本地计算来选择。

形成代理报文的备份节点以及传输代理报文的路径 p’也是由簇选择的。而备份节点通过收集它的信号覆盖范围内节点数据形成代理报文，并将它传输到代理节点，代理节点又将它作为特殊的标记数据发送到自己的簇头。

为保证系统的健壮性，簇在接收到 BS 确认摘要后应对 BS 进行应答，这种应答可和下一个报文一起通过路径 p 或和代理报文一起通过路径 p’发送。

3　BS 的报文验证和一致性检查

BS 需要对所接收的每个报文进行有效性验证并对主报文和代理报文进行一致性检查。小簇由于簇内每一个节点均在节点信号覆盖范围，其一致性检查相对简单，而对于大簇，除考虑备份节点的覆盖范围外，还需其他检查措施。

3.1　BS 端的报文检查

(1)小簇区域的字符串格式报文和数字格式报文

为验证主报文或代理报文的有效性，BS 重点检查的内容是：1)报文中的明文部分的序号、Nonce、簇的 ID 号、CH 的 ID 号需与报文中的加密部分相同。2)Nonce 值新鲜且以前没被使用。3)XMAC 值正确。

另外 BS 通过以下的确定检查主报文与代理报文间的一致性：1)两个报文中的序号和簇的 ID 号应相同。2)代理报文所报告的数据值应是主报文报告的值的一个子集。

(2)大簇数字格式报文

报文的有效性检查与小簇区域情况类似，但需要确定报文中的 proof 的合法性，即 BS 需要验证报文中的 proof 是否与所报告的数据值精确吻合。虽然 BS 不能直接检查所报告的代理报文数据值是否为主报文值的子集，但 BS 可通过对两报文的函数相关(function-specific)一致性检查来实现

(3)大簇字符串格式报文

报文的检查方式与小簇区域情况类似，但需增加对两个报文的压缩部分进行解压的步骤。

3.2　大簇节点覆盖区域计算

设传感器节点的信号范围为 r，簇的半径为 R，备份节点与簇心间的距离为 u，则备份节点所能覆盖的区域范围为

$$A = r^2\arccos\left(\frac{r^2+u^2+R^2}{2ru}\right) + R^2\arccos\left(\frac{R^2+u^2-r^2}{2Ru}\right) - 2\sqrt{(s-u)(s-r)(s-R)}$$

其中，$s=\dfrac{R+r+u}{2}$。

由上式可知，不能被备份节点覆盖的区域范围为 $\pi R^2 - A$。如取 R=1 且 r 值固定，则备份节点不能覆盖的区

域范围为将为 $\int_0^1 (1-A/\pi)\mathrm{d}u$ 。如取 R=1 和 r=1，则备份节点不能覆盖范围为 0.978 6，大约占簇区域的 31.15%。最坏情况是备份节点位于簇的边缘，备份节点覆盖区域仅为 39.1%，也就表示备份节点只能接收到簇内 39.1%节点的数据。

图 4 表示了备份节点不能覆盖的区域范围的百分比，即 $1-A/\pi$(代表)在 R =1，不同 p 和 r 情况下的值。从图 4 中可以看出，不能被备份节点覆盖的区域范围比例与单个节点的信号范围成反比，当备份节点与 CH 间的距离小于簇半径的 0.8 倍时，备份节点不能覆盖的区域范围小于半个簇区域。

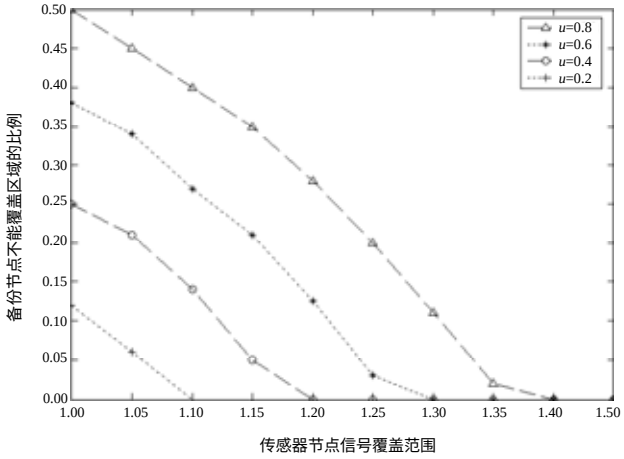

图 4　簇覆盖区域百分比

4　安全分析

4.1　外部攻击分析

如果 CH 和 BS 间的对称密钥未被泄露，报文中的数据值的内容就不可能被外部所解密。由于笔者使用 Nonce 和报文序号，外部也不可能发起重放攻击；另外由于报文中所有公共部分都未被加密(如序号、Nonce、簇的 ID 和节点 ID 等)，在加密部分中可被验证，避免了虚假数据注入式攻击。因此其方法可以抵御任何外部的攻击。

4.2　最小代价阻塞问题的完全性问题

设有m个簇：C_1,C_2,⋯,C_m。每个簇C_i使用主路径P_i和k轮不同的备份路径P_{i1}，P_{i2},⋯，P_{ik}。攻击者攻击的目的之一是阻塞某些簇的主路径和所有备份路径，使得从这些簇发出的报文无法抵达BS。设传感器节点总数为N=nm(n为簇的节点数)，每个节点均有一被危害的相伴代价c_i(i=1,2,⋯,N)，攻击者的目的转化成用最小总代价发现节点子集以达到通过阻塞这节点子集实现阻塞簇的子集与BS间的全部数据流量的目的。该问题是一个NP-hard问题，等价于用最小总代价发现节点一子集实现阻塞某些具体簇的所有主路径和备份路径。将每条路径作为一个元素，每个节点为包含某些元素的集合，如节点在一条路径中，则该路径包含在相应节点的集合中，问题就变为加权集合覆盖问题，该问题是一般性的集合覆盖问题和NP-hard问题。

5　模拟实验分析

本文通过 Matlab 下的模拟实验环境来考察所提出方法的性能。考虑 100 个簇的传感器网络，每簇中有 10 个节点，所有节点随机分布在 1 000 m×1 000 m 的正方形区域内，该区域又划分为 10 个 100 m×100 m 的正方形小区域，每个簇都在一个小区域中，簇内节点随机分布在该小区域内，簇内随机选择一个节点作为 CH。不失一般性，假设网络中的节点为同构节点且节点的无线通信范围为 100 m。BS 位于区域的角落，最佳路由选择方法采用的是跳数最小的原则。

图 5 给出了当节点被破坏或失效时到达 BS 的报文的概率情况，从中可以看出当网络中点被破坏或失效节点增大时，到达 BS 的报文概率将呈线性下降，且至少有一个报文到达 BS 的概率也呈线性下降。

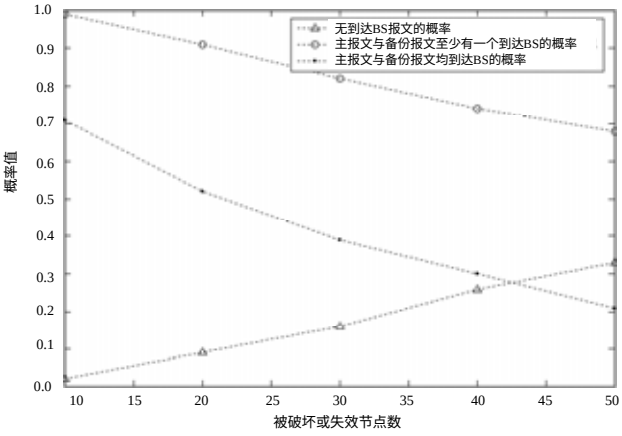

图 5　到达 BS 报文的概率

图 6 给出了在集中在某一点的 40 m×40 m 正方形区域模式节点失效时报文无法到达 BS 的簇比例情况，从中可以看出当受影响的区域靠近 BS 或受影响的区域在整个区域的对角线上时，所受影响的簇数目将急剧增加。通过模拟分析还可以发现由于大量的到 BS 的路由都是通过最接近 BS 的节点来实现的，破坏者只需要对这些关键点进行破坏就可以实现对整个网络产生巨大影响的目的，因此对这些节点需进行更好的安全防护措施。

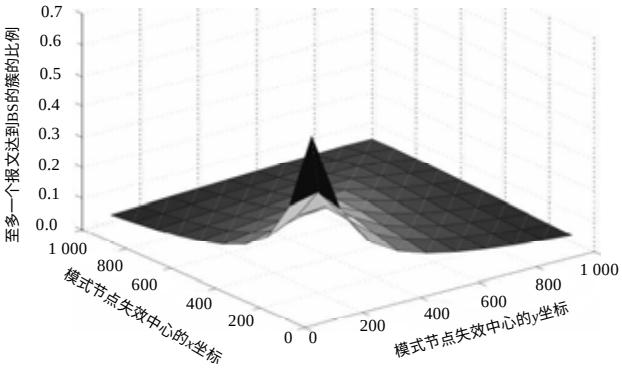

图 6　40 m×40 m 区域模式节点失效无报文到达 BS 的簇比例

6　结束语

本文所提出的方法在考虑不同簇的拓扑结构和不同报文格式情况下，以控制开销最小为前提，有效解决传感器网络的报文丢弃和篡改检测问题。通过与其他防止虚假数据注入的方法结合，可有效实现传感器网络的端到端的半可靠的数据传递。今后笔者将对如何通过定性分析和模拟验证对控制开销性能进行细致研究，以解决在不影响攻击检测精度前提下使代理报文的规模和内容最小问题。

参考文献

[1] 覃伯平, 周贤伟, 杨　军, 等. 无线传感器网络的安全路由技术研究[J]. 传感技术学报, 2006, 19(1): 16-19.

[2] Zhu Sencun, Setia S, Jajodia S, et al. An Interleaved Hop-by-Hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks[C]//Proc. of IEEE Symposium on Security and Privacy. [S. l.]: IEEE Press, 2004.

（下转第 170 页）