无线传感器网络中虚假数据过滤方案*

朱凌志[1]，赵巾帼[1]，刘志雄[2]，黄俊杰[2]，梁俊斌[3]
(1. 湖南工学院 计算机与信息科学学院，湖南 衡阳 421002；2. 中南大学 信息科学与工程学院，长沙 410083；3. 广西大学 计算机与电子信息学院，南宁 530004)

摘　要：传统虚假数据过滤算法不能有效地应用于无线传感器网络，因而需要研究适合无线传感器网络的虚假数据过滤方案。在介绍无线传感器网络与虚假数据过滤的概念和特点后，提出了虚假数据过滤方案的分类方法，探讨了各种虚假数据过滤策略，着重分析了当前一些较为重要的虚假数据过滤策略，并指出了这些策略的优缺点。最后分析了当前亟待解决的问题，展望了其未来的发展趋势。

关键词：无线传感器网络；网络安全；虚假数据过滤；密钥技术
中图分类号：TP393　　**文献标志码**：A　　**文章编号**：1001-3695(2012)12-4426-06
doi:10.3969/j.issn.1001-3695.2012.12.005

False data filtering scheme in wireless sensor networks

ZHU Ling-zhi[1], ZHAO Jin-guo[1], LIU Zhi-xiong[2], HUANG Jun-jie[2], LIANG Jun-bin[3]
(1. *School of Computer & Information Science, Hunan Institute of Techology, Hengyang Hunan* 421002, *China*; 2. *School of Information Science & Engineering, Central South University, Changsha* 410083, *China*; 3. *School of Computer & Electronics Information, Guangxi University, Nanning* 530004, *China*)

Abstract: Traditional false data filtering cannot be applied efficiently to wireless sensor networks. Therefore false data filtering for WSN should be studied. After describing the concepts and characteristics of wireless sensor networks and false data filtering in the networks, this paper presented the classification standards for false data filtering. Then it analyzed the key mechanisms of the existing representative false data filtering, and pointed out the merits and demerits of them in detailed. In particular, this paper summarized the current research progresses. Finally, it also pointed out the open research problems.

Key words: wireless sensor networks(WSN); network security; filtering of false data; encryption technology

无线传感器网络在国防军事、环境监测、医疗卫生和人体监控等领域具有广泛的应用前景[1]，因此，WSN 是一个非常活跃的研究领域。传感器节点通常是部署在恶劣环境、野外、大型广场、甚至敌方区域等不方便人工处理的地方，簇头一般需要经过多跳才能将数据传送给基站，且节点容易被俘获，攻击者可以利用存储在节点内的密钥伪造事实上并不存在的虚假事件，恶意窜改正在传送的数据包，发送重复数据包等[2]。若不加防范，虚假数据会引发错误警报，干扰用户决策、消耗有限的网络资源。此外，一旦节点被俘，攻击者很容易获取并利用存储在节点内的密钥信息伪造虚假数据，并通过妥协节点发送给邻居节点，其邻居节点将难以判断数据包的真假。因此，如何识别并过滤 WSN 中的虚假数据是一个具有挑战性的难题[1~4]。

1　无线传感器网络的特点

尽管在传统网络中虚假数据过滤方案已经有了很多成熟、有效、复杂的应用，但 WSN 和传统网络相比仍有一些差距，这主要表现在传感器节点拥有较低的计算能力、较小的存储空间、较短的通信半径以及有限的电量。因此，许多传统网络的方案不适合应用于 WSN，使得 WSN 的虚假数据过滤方案面临巨大考验[5~9]。

a)有限的电量。传感器节点体积微小，为降低成本，通常采用一次性电池供电且电池电量有限，一旦用尽很难更换。故虚假数据过滤方案应充分考虑能量高效、在不明显增加系统任何代价的前提下，能够及时有效地过滤假数据。

b)较小的存储空间和较低的计算能力。通常认为基于公开密钥技术的虚假数据过滤具有更高的安全性，但由于其过于复杂，计算和存储开销过大，无法适用于 WSN。

c)较短的通信半径。由于 WSN 节点通信范围十分有限，一般只能与周围的邻居节点进行通信，故通常使用多跳路由的方式将数据传给汇聚节点或 sink 节点，节点既是数据的发送者，也是数据的转发者。

d)缺乏后期节点部署的先验知识。为了能顺利完成监测任务，WSN 通常随机布撒成千上万个节点在监测区域。任意两个节点之间是否能直接相连在 WSN 部署之前是未知的。

e)无法保证监测区域节点的物理安全。由于节点数量众

收稿日期：2012-05-01；**修回日期**：2012-06-14　　**基金项目**：国家自然科学基金资助项目(61103245)；广西自然科学基金资助项目(2012GXNSFBA053163，2012GXNSFAA053222)；湖南省科技厅计划科学研究资助项目(2010SK3057)

作者简介：朱凌志(1979-)，男，湖南邵阳人，讲师，硕士，主要研究方向为无线传感器网络、物联网技术(lingzhi0825@163.com)；赵巾帼(1965-)，女，湖南邵阳人，副教授，硕士，主要研究方向为无线传感器网络、网络安全；刘志雄(1982-)，男，湖南娄底人，博士，主要研究方向为无线传感器网络；黄俊杰(1979-)，男，湖北大冶人，讲师，硕士，主要研究方向为无线传感器网络；梁俊斌(1979-)，男，广西南宁人，副教授，博士，主要研究方向为无线传感器网络.

多,随机分布且监测区域多位于恶劣的环境,本身就存在一些不安全因素,节点很可能被冒充或被捕获。因此,设计虚假数据过滤方案应该考虑如何有效地检测发现并丢弃伪造的数据包、如何及时溯源追踪到发送虚假数据的被俘节点,将被俘节点隔离,以及如何应对被俘节点导致的安全隐患。

f)动态拓扑结构。部署在户外环境的节点可能会因为电量用尽,被捕获或其他故障等原因而离开 WSN;也可能因为工作需要而加入 WSN。因此,为了避免节点离开或加入后 WSN 无法工作,设计的虚假数据过滤方案应该具备较高的灵活性和容错性。

2　虚假数据过滤方案

攻击者可以通过部署传感器节点冒充网络节点,窃取机密信息,发动虚假数据注入攻击;攻击者还可以通过直接俘获无线传感器网络中的节点,窃取它们所存储的所有信息,并利用它们发送大量虚假数据,迅速耗尽网络资源,如能量、带宽、计算能力、存储空间等。若不加防范,虚假数据会引发错误警报,干扰用户决策,消耗有限的网络资源。将通过冒充或俘获节点向网络中注入虚假数据、捏造事实上不存在的虚假事件、恶意窜改正在传送的数据包、发送重复的数据包等行为统称为 WSN 的虚假数据问题。

针对虚假数据问题,国内外学者提出了一些过滤、识别 WSN 中虚假数据的策略。这些策略主要针对虚假数据报告注入攻击和重放攻击两种情形。虚假数据报告注入攻击,是指中间人俘获节点后,进行虚报修改或者重播路由信息、污水池(sinkhole)攻击、选择性转发(selective forwarding)攻击、女巫(sybil)攻击或者 Hello 泛洪攻击以及 Ask 攻击;重放攻击是指中间人将截获的合法消息再次或反复发送给目标节点。防范重放攻击只需在 report 中加入时间戳即可实现,目前研究主要集中于防范虚假数据报告注入攻击这方面。

近年来,国内外学者对于防范虚假数据报告注入攻击已经取得了一定的成果,陆续提出了许多过滤、识别 WSN 中虚假数据的方案。不同的过滤方案也有不同的侧重点,根据这些方案的特点可以进行适当分类。

2.1　途中过滤和溯源追踪方案

按照对虚假数据包预处理的方式,可将虚假数据过滤方案分为途中过滤方案和溯源追踪方案。

在途中过滤方案中,每个转发节点在转发数据包时,验证数据包中的担保证明来被动地检测及丢弃源节点所发送的虚假数据。该方案的优点是有效过滤了绝大部分的虚假数据,减小了虚假数据在 WSN 中传输所带来的能量和带宽的开销,延长网络的生命期,是目前防范虚假数据报告注入攻击的主流研究方向;该方案缺点是仅仅被动地过滤数据包,攻击者仍然可以通过源节点不断发送虚假数据包,耗尽节点能量和网络带宽。

在溯源追踪方案中,每个转发节点都按照一定概率标记它所转发的数据包,汇聚节点收集到足够多的数据包便能够重建攻击路径找出并排除发送伪造数据的源节点。该方案的优点是从根本上解决问题,隔离排除发送虚假数据的攻击节点或被捕获节点;缺点是存储开销较大,对数据包头大小有一定要求,这对较小的存储空间、能量有限的 WSN 来说不现实,有待进一步的研究与优化。

2.2　基于对称密钥过滤和基于公开密钥过滤方案

按照所使用的密码技术的不同,可以将虚假数据过滤方案分为基于对称密钥过滤方案和基于公开密钥过滤方案。其中基于对称密钥的过滤方案是利用相同的密钥和加/解密算法对数据进行加/解密和转发认证,该方案具有计算复杂性低、实现简单的特点,从能量有效及实用性等角度来说,为资源有限的传感器网络所青睐。基于公开密钥的过滤方案,利用不同的密钥和加/解密算法对数据进行加/解密和转发认证的优点,该方案具有安全性极高、使用较灵活、易于实现信息认证,但是其安全操作需要执行大量的计算,这对较小的存储空间、较低的计算能力和有限能量的 WSN 来说是个沉重负担。虽然部分学者对其进行了适当的优化,但开销还是过大,有待进一步的研究与优化。

2.3　概率性过滤和确定性过滤方案

按照共享密钥节点对的选定方式,可将虚假数据过滤方案分为概率性过滤方案和确定性过滤方案。在概率性过滤方案中,每个节点按照一定概率随机选择一个密钥组加入。这种方法的优点是过滤耗费较少能量便可以取得较好的过滤效果;缺点是在最坏情况下,可能某一区域的节点都选择同一密钥组加入,使事件不能够形成合法的数据报告[8]。在确定性过滤方案中,其汇聚节点掌握所有节点的分布,并为每个节点分配一个密钥组,使得所有密钥组的节点达到均匀分布,这种方法的优势是性能较高,但缺点是需要的计算时间较长,代价较大[8]。

3　传感器网络中虚假数据过滤方案

目前 WSN 的技术、应用还不是很成熟,尤其是虚假数据过滤方案的研究才刚刚起步,国内研究水平与国际还存在一定的差距。由于 WSN 自身的特性与特定的应用环境,适用于传统网络的虚假数据过滤机制无法直接移植;再者,为了减少网络负载和节省能耗,WSN 通常采用网内处理数据的方法,不便采用传统网络中的端到端数据认证机制,因此必须研究适合 WSN 特点的虚假数据过滤方案[10]。

3.1　途中过滤方案

文献[4]提出的途中过滤方案的主要框架包括四个部分:密钥分发管理、数据报告生成、转发过滤以及 sink 验证。密钥分发管理是指在节点间建立密钥关联,形成密钥共享关系。密钥分发管理是过滤机制的核心部分,节点间的密钥共享度决定了中转过滤的能力。提高密钥共享度能提高中转过滤的能力,同时也使得每个节点所存储的密钥信息较多。因此,密钥分发机制在提高密钥共享度的同时应该保证密钥的安全性。

数据报告生成是指有事件发生时,每个检测节点(源节点)利用存储的密钥对数据进行加密,得到消息认证码;接下来,多个检测节点利用 MAC 以及相应的密钥索引联合生成数据报告。一个合法的数据报告必须携带 $t(t>1)$ 个不同检测节点的 MAC。

中转过滤是指当节点接收到数据包时,首先检查数据包是否附带 t 个来自不同检测节点的 MAC;若存储了与数据包中相匹配的密钥,则利用存储的密钥重新产生一个 MAC,并比较是否与数据包中待验证的 MAC 相同。如果其中任何一个步骤的检测没有通过,直接丢弃数据包。若节点没有存储相匹配的密钥,则直接转发数据包。

中转过滤是一种概率性过滤,无法确保将所有假数据包检测出来并丢弃,故将 sink 节点作为最后一道屏障,识别并丢弃所有最终到达的虚假数据。Sink 拥有全局密钥信息,能量充足,具备强大的计算能力,能够验证数据包中所有的 MAC。如果所有 MAC 都校验正确,则 sink 将接收数据包,否则将数据包丢弃。

密钥分发管理是途中过滤方案的核心,已有途中过滤方案研究主要是从对称密钥技术、公开密钥技术和组密钥技术等方面进行的;此外还采用了诸如多项式、数字水印等技术手段进行了研究。

3.1.1 基于对称密钥的途中过滤方案

文献[4,11~18]借助数字签名的思想,基于对称密钥技术提出了一些 WSN 中虚假数据过滤的解决方案。该方案采取概率性和确定性两种方式在网络中部署对称密钥,数据加密和认证开销较低。

1) SEF 方案

文献[4]首次基于数字签名的思想提出了用于过滤虚假数据的统计中途过滤方案(statistical en-route filtering,SEF),该方案将一个全局密钥池分成多个密钥分区,给每个节点预置随机选取的一个密钥分区中的部分密钥。有事件发生时,多个检测节点联合产生一个包含 t 个 MAC 的数据报告,确保生成这些 MAC 的密钥来自不同的密钥分区。在转发过滤阶段,若拥有与检测节点相同的密钥,则中间节点利用该密钥重新产生一个 MAC,并验证数据包中所携带的 MAC 的正确性。最后,由于 sink 拥有全局密钥信息并配备强大的计算、通信和存储能力,从而能将所有假包过滤掉。但 SEF 方案存在以下缺点:a)中转节点只能按一定概率过滤虚假数据,因此不能保证中转节点一定能将虚假数据过滤掉,虚假数据总是以一定的概率存在,并从源节点传输到基站;b)虚假数据一般需要传输一定的跳数才能被过滤,不利于节省网络资源;c)由于没有将密钥与检测区域进行绑定,一旦攻击者俘获了 t 个不同的密钥分区,即可任意伪造假数据包而不被中转节点识别。

文献[11]提出了对 SEF[4] 的改进方案,将节点密钥信息和节点自身的位置进行绑定,由此来限制攻击者的串谋攻击。改进的方案比 SEF 在安全性上有所加强 ,但仍然存在与 SEF 算法相似的两个问题,即过滤效率不高及不利于节省网络能量。

2)基于地理位置的虚假数据过滤方案

文献[12]针对阈值 t 限制问题,提出了一种基于地理位置的虚假数据过滤方案。在传感器网络部署后,节点把地理信息预分发给部分邻居节点存储,每个数据报告必须包含 t 个具有不同密钥分区检测节点的 MAC 以及地理位置,转发节点既对数据分组中包含的 MAC 和地理位置的正确性进行验证,还对地理位置的合法性进行验证,可以有效地过滤不同地理区域的多个妥协节点协同伪造的虚假数据,但该方案需要给节点配备昂贵的 GPS 定位工具。

3)IHA 方案

文献[13]率先提出了在路由时进行交叉的逐步认证机制 IHA。节点部署后成簇,每个簇头建立一条到 sink 的路径,路径中相距 $t+1$ 跳的节点建立协作关系。事件发生时,每个检测节点利用与 sink 共享的私钥以及与下游协作节点共享的对偶密钥分别产生两个 MAC,簇头收集 $t+1$ 个检测节点的 MAC 信息生成数据报告。在转发过程中,各节点对上游协作节点产生的 MAC 进行校验。验证成功后,再利用与下游协作节点共享的密钥重新产生一个 MAC 替换掉验证过的 MAC。IHA 能在 t 跳内将假包过滤,但其密钥分发方式不适合于动态的 WSN 路由,从而需要较大的维护开销。

文献[14]针对 IHA[13] 方案进行了改进,认为 IHA 不适于动态的 WSN 环境,提出了一种适合 WSN 动态拓扑结构的数据认证机制,并利用爬山策略预先对最可能要经过的中间节点进行认证密钥预分配。采用了爬山策略,即有 l 条不同的单向散列链,每个节点随机从每条散列链中选一个 key 装载,在认证过程中,只有 key-index 较大的 key 能对 key-index 较小的 key 进行认证。爬山策略保证靠近基站的节点含有的密钥数量不会太多,有利于均衡网络负载,延长网络寿命;其不足是会导致密钥共享度太低,认证效率低。

文献[15]认为,IHA 方案在多路径路由中开销太大且无法抵制串谋攻击,提出一种适于多路径路由的过滤机制,多路径路由容错性好。但是多协作节点的建立和维护需要节点之间发生多次通信,开销太大。

4)不受门限值限制的过滤机制 RSFS

文献[16]认为 SEF、IHA 等受门限值的限制,提出了一种不受门限值限制的机制,节点与 sink 之间形成星型拓扑。假设存在一种比普通节点能量强得多的节点作为簇头完成数据聚合,聚合结果必须附加簇内各个普通节点产生的 MAC 信息才算合法,目的节点在收到汇聚结果时通过对聚合结果及附加 MAC 信息的校验,实现对虚假数据的过滤。该方案虽然不受门限值限制,但必须假设存在一种比普通节点能量高的节点作为簇头完成数据聚合,其假设过高。

5)基于哈希函数的虚假数据过滤方案 FFRF

文献[17]提出了一种基于哈希函数的虚假数据过滤方案 FFRF。FFRF 将节点分为探测节点和校验节点,并给每个节点预载相同的单向函数,然后生成一条单向哈希链 $c_1, c_2, \cdots, c_t$。每个源节点将初始哈希值公开,转发节点利用预存储的验证哈希值对哈希值的正确性进行验证,还利用共享的对称密钥对数据包中的 MAC 进行验证,以过滤虚假数据。Sink 节点可以通过重新验证哈希值进一步过滤虚假数据,还可以通过校验各个 MAC 的异或值来判断出妥协节点的大致位置。由于 FFRF 没有将节点密钥和哈希值进行绑定,故攻击者很容易从合法包中获取合法哈希值而攻破安全机制。

6)基于簇组织和投票机制的虚假数据过滤方案 PVFS

文献[18]提出 PVFS 机制,将节点组织成簇,各簇头建立到 sink 的最短路径,转发节点均为簇头,以概率 d_i/d_0 存储源簇内一个节点的密钥,其中 d_0 和 d_i 表示源簇和转发簇离 sink 的跳数。当事件发生时,检测节点产生一个投票(vote,其作用类似 MAC),簇头收集簇内 t 个节点产生的投票产生数据报告。在转发过程中,转发簇头以一定概率对数据进行验证。然而,簇头之间需要以比普通节点大得多的通信半径进行数据转发,簇头很容易耗尽能量。

7)基于簇组织的虚假数据过滤方案 CCFS

文献[19]针对 SEF 和 PVFS 方案没有考虑到各个节点计算、通信负荷的不同,使得靠近 sink 的节点容易因负荷太重而过早死亡的情况进行改进,提出了一种基于簇结构的虚假数据过滤方案。

文献[20]在文献[19]的基础上进行改进,提出一种依据网络中节点能量的不均衡性构造成簇,通过节点的负载计算和密钥分发实现虚假数据过滤。

8)STEF 方案

文献[21]提出了基于 request-response 方式的 STEF 机制,其 ticket 基于单向函数。该算法利用一种入场券的模型来识别和过滤虚假数据,提高了虚假数据的过滤概率。STEF 机制由于忽略了中转节点也能伪造数据的事实,只针对源节点伪造数据的虚假数据过滤率较高。

综上所述,对称密钥技术具有开销低、加/解密速度快以及能耗低等特性,但不适合一些对安全性要求比较高的情况。针对这类情形,需要做进一步的研究工作。

3.1.2　基于公开密钥的途中过滤方案

公开密钥由于其安全性较高,易于实现数据认证,被广泛地应用于传统网络中。文献[22~25]等认为基于对称密钥的虚假数据过滤方案安全性过低,故需要引入安全级别更高的公开密钥技术。

文献[22]提出了一种基于密码交换(commutative cipher)的路由过滤机制。该机制假设各节点与 BS 共享同一会话密钥,基于公钥模型,采用 query-response 会话模型,每个会话有一个 session key(用于产生报告)、witness key(用于验证密钥),session key 相当于私钥,witness key 相当于公钥。但是这种公钥机制开销太大。

文献[23]提出基于位置的密钥(将节点位置、节点 ID 及节点私钥绑定)和基于位置密钥的邻居认证方案,在此基础上进一步提出了基于位置的门限数字签名的方法过滤虚假数据。邻居节点之间基于位置密钥建立对偶密钥,将妥协节点的破坏性限制在本地,防止串谋攻击,其引入带 GPS 功能的 robots,为节点提供位置信息。该机制的不足之处就是需要 GPS 和机器人的支持,以及对偶密钥的建立和维护等,开销太大。

文献[24]利用椭圆曲线密钥技术来改进已有的基于对偶密钥虚假数据过滤算法,采用了随机网络编码和公开密钥技术,将整个网络划分成不重叠的单元(cell),采用线性网络编码(linear network coding),以单元块(cell by cell)的方式传递数据,采用了门限共享技术和公开密钥技术保证数据的安全。相邻 cell 之间用 cell key(公钥认证)。此方案虽然提高了安全性,但其开销相对较大,不适用于密度较小和移动性较大的网络。文献[25]提出的网络拓扑和 LNCS[22]一致,将网络划分成不重叠单元,在一个特定的路由上进行传输。

综上所述,基于公开密钥技术提出的虚假数据过滤策略具备较高的安全性,抗妥协能力更强,但是其安全操作需要执行大量的计算,建立和维护公开密钥机制,能量开销大,这对较小的存储空间、较低的计算能力和有限能量的 WSN 来说是个沉重负担。

3.1.3　基于组密钥的途中过滤方案

1)基于邻居协商的组密钥更新方案

文献[26]首次提出组密钥的概念,其核心思想是将节点分成组,从组密钥的角度来抵抗虚假数据注入攻击,提出了一种基于邻居协商的组密钥更新方案。将当前和未来要使用的组密钥的相关信息预置在一些可信节点中,当组密钥需要更新时,通过邻居节点之间的协商进行更新。该方案假设过高,通信和存储开销大,若有节点发生故障或暂时无法通信,将会造成多个节点无法更新组密钥而成为孤立节点。

2)基于分布式更新权限的组密钥管理方案 DRA

文献[27]提出了一种基于分布式更新权限的组密钥管理方案 DRA,在组密钥更新过程中引入广播机制,并构造权限分布函数(即每一个节点根据权限分布函数只有一个权限值,而只有获得足够权限值的节点才能成为合法 BC 发起更新,由此实现了对更新权限的保护,防止少数妥协节点发起组密钥更新,进而控制整个网络)、组密钥隐藏函数(即基于私有密钥分发技术构造组密钥隐藏函数,利用权限分布函数实现了对组密钥的隐藏)及广播认证函数(即采取广播方式进行更新)以实现对妥协节点的剔除及更新信息的完整性鉴别。DRA 方案是一种比较适合 WSN 特征的组密钥管理方案,更新密钥时不需要任何网络拓扑信息,对妥协信息能够作出实时反应。在保证安全性的同时具有较小的存储开销和通信开销,并能够有效地避免孤立节点的问题。但是,其存在更新时延随着网络规模的增大而增大的不足。

综上所述,目前组密钥过滤还存在一些问题,如侧重于具有固定节点或可靠连接的 WSN,对所有节点均可移动的 WSN 有待进一步完善;组密钥更新算法的性能有待提高;密钥不一致问题;不适用于大规模移动 WSN 安全问题。

3.1.4　基于其他技术的途中过滤方案

1)基于多项式的虚假数据过滤方案

这类机制的主要思想是采用一次和二次多项式代替密钥进行数据加/解密,可抵抗多妥协节点发动串谋攻击。文献[28,29]在多项式中引入干扰数,提出了基于干扰数和干扰多项式的虚假数据过滤方案,该类方案可抵抗多妥协节点发动串谋攻击。文献[30]提出了基于前者的技术,并采用了基于有限域上的干扰多项式对数据进行加密和认证。文献[31]采用虚拟证人簇的思想,提出了一种基于云团模型的多项式虚假数据过滤方案。该方案由源节点结合多个云团认证码,构造出系统认证多项式,采用多项式技术,通过云团内部节点协作认证,突破了 t 门限值的限制。文献[32,33]针对抗捕获性差的特点,提出了一种基于簇的分布式预分配密钥管理机制,采用分布式管理策略,通过更新多项式的方式把被捕获节点隔离,使网络具有一定的抗捕获能力;其缺点是需要其他方案检测伪造、不安全节点或簇头。

综上所述,虽然多项式的计算比 MAC 计算开销低,但是存储要求较高,且传输多项式的开销也较大,因此,与 MAC 认证方案相比,并不能显著地降低算法开销。

2)基于时间同步的虚假数据过滤方案

时间同步技术是指在时间高度同步的基础上,利用时间戳为主要识别手段对数据包进行认证。绝大多数节点都需要根据时间同步机制交换同步消息,与网络中的其他传感器节点保持时间同步[30]。由于其扩展性、稳定性、鲁棒性、收敛性、能量感知等特点决定了网络时间同步机制。

文献[34]认为,在大量妥协节点存在的条件下,假设节点之间保持时间同步,同时,报告产生者和认证者之间共享密钥,能提供一种“推迟的”认证。这类机制的缺点是认证和网络延迟之间的一个网络规模太大时,很难确定延迟的下界。此外,邻居节点在时间上保持高度同步能量消耗过大。

3)基于数字水印的虚假数据过滤方案

数字水印技术是指在数据包中嵌入传感器节点的身份等

认证信息,替代密钥进行数据加密。

文献[35]针对基于 MAC 认证的机制存在附加在数据包后的 MAC 易压缩受损并易受窜改攻击的安全隐患,提出了一种基于多重半脆弱水印的虚假数据过滤算法,利用水印对数据包进行相关认证,无须依赖 MAC 认证。该方案提出了新颖的认证节点委派策略,能由用户动态调控认证节点的认证概率,有利于节省网路资料,既能够识别虚假数据,又能抵抗重放攻击的双重目标,但是对其他攻击则很难识别。

文献[36]提出了一种适用于无线传感器网络的数字水印技术,并设计了水印的生成、嵌入和检测算法。该算法通过水印信息标志发送节点的身份,将水印信息嵌入到节点采集的数据中进行发送,并在数据融合的过程中保留这种信息。该算法能较有效地验证数据的可靠性,具有较好的可行性和实用性。但分布式数字水印的生成和提取都需要多个节点协作,开销较大,此外,一旦参与认证的节点睡眠甚至死亡后,机制的维护代价也很大。

文献[37]提出一种 WSN 中基于协作水印的虚假数据过滤算法,该算法以时间戳和簇头节点的身份信息作为鲁棒性水印,以证人节点认证信息为半脆弱水印,然后将这多个水印以协同方式嵌入到聚合后的数据中,从而达到对发送节点身份与发送数据内容双重认证的目的。该算法需要多个节点协作,开销较大。在数据转发过程中,只能过滤绝大部分的虚假数据包和重复数据包,需要 sink 节点作为最后一道屏障,识别并丢弃所有最终到达的虚假数据。

3.2 溯源追踪方案

途中过滤方案虽然能有效检测和过滤虚假数据,但并不能找到隔离发送虚假数据的源节点,使得其仍然可以通过源节点不断向 WSN 中注入大量虚假数据,直到耗尽节点能量和网络带宽为止。为了保证 WSN 正常运行,需要采用更为主动的安全措施,检测并排除发送虚假数据的源节点[8]。

文献[38]最早就 WSN 中源节点定位问题展开研究,提出了一种基于链式标记方法的溯源追踪方案,即每个转发节点都按照一定概率标记它所转发的数据包,汇聚节点收集到足够多的数据包便能够重构一条到源节点的路径。但该方案的缺点是假设数据包头的空间足够大,而在真实的网络环境中,数据包的空间是有限的,节点不可能无限制地标记数据包,因此该方法仅具有理论意义。

文献[39]提出一种基于概率包标记方法的溯源追踪方案,在该方案中每一个数据包最多可以被两个节点标记,当节点收到数据包时,首先按照一定概率决定是否标记此包。如果决定标记,再检查此包被几个节点标记过,如果已经有两个节点标记此包,则用本节点标记信息覆盖第一个标记节点信息,同时将第二个节点标记信息清空,否则将本节点标记信息写入正确位置。每个被标记过的包都保存了部分路径信息,因此汇聚节点只需要收集到足够数量的包,就可以溯源追踪到源节点。该方案的缺陷是上游节点标记可能被下游节点标记覆盖,因此距离汇聚节点越远的节点,其标记被收集到的概率就越低,如果距离汇聚节点很远的节点被俘获并发动攻击,汇聚节点将需要收集大量的包才能够将其定位。

针对上述问题,文献[40]提出了等概率包标记方案。在该方案中,假设每个节点标记被收集到的概率都基本相等。在实际应用中并不存在一种计算函数可以适用于所有网络,因此需要根据不同网络拓扑来确定其计算函数[40]。该方案的缺点是攻击节点距离汇聚节点越远,汇聚节点就需要收集越多的包才能够将其定位。

针对这个问题,文献[40]又提出了等数目包标记方案。在该标记方案中,汇聚节点除了一跳邻居外都收集大致相等数目的包而将其定位。该方案具有较好的扩展性,但其不能完全解决 WSN 中发送虚假数据攻击问题,仍需要其他方案的配合。

为了较高效地定位源节点,文献[41]提出了一种层次式溯源追踪解决方案,该方案将网络划分为不同的层次,每次运行能够将源节点定位在一个更小的层次内,经过次数较少的回溯后将定位源节点。

文献[42]提出一种将途中过滤方案与溯源追踪方案相结合的方法。它的核心思想是转发节点以一定概率标记它没有过滤掉的数据报告,汇聚节点将没有通过验证的数据报告加入溯源追踪集合中供定位源节点使用。若集合中的数据报告超过预先设定的参数极限,汇聚节点执行回溯过程,进行溯源追踪操作,最终定位源节点[42~44]。

4 结束语

从研究现状来看,基于对称密钥的途中过滤方案和策略被认为是最适用于 WSN[4,11~18]的。表 1 较为直观地展示了常见的虚假数据过滤方案的优劣。

表 1 过滤策略比较

技术分类	优点	缺点
MAC 认证机制	过滤率高,节约网络资源	需多跳才能过滤
单向哈希链技术	过滤较高,精确性较高	开销较大
PVFS 机制	抵抗 MAC 攻击,过滤率高,抵制修改数据	浪费能量
STEF 机制	加入入场券模型,过滤率高	忽略了中转节点也能伪造数据
位置密钥技术	防止串谋攻击,GPS 支持,机器人支持	开销太大
椭圆曲线密钥	随机网络编码,公开密钥技术,增大安全性	较大的开销
LEDS 机制	过滤率较高,不重复单元	假设条件高
DRA 机制	防串谋攻击,保证更新信息的完整性鉴别	维护代价高
干扰多项式技术	抵抗串谋攻击比 MAC 技术开销低	存储传输开销高
时间节点同步	节点时间同步,共享密钥,提供“推迟的”认证	很难确定大网络的延迟下界
DSF 机制	爬山策略,有利于均衡网络负载,延长网络寿命	密钥共享度太低,认证效率低
多路径路由过滤	过滤率较高,容错性好	开销太大
认证节点委派	不依赖 MAC 认证,过滤性高,开销低,可抵抗重放攻击	“拒绝服务”过滤不足

如何有效识别和过滤虚假数据包是无线传感器网络中一个具有挑战性的难题。虚假数据过滤研究成为无线传感器网络安全研究的重要问题,需要从以下几个方面进行深入探讨:

a)使用 WSN 对移动目标进行追踪和监测越来越成为关注的热点,此外,WSN 传输链路易碎的特点使得其性能很不稳定,而已有研究大都是在静态网络拓扑上进行。因此,研究适合动态环境和动态网络拓扑的虚假数据过滤策略,是一个值得进行深入研究的问题。

b)WSN 一个突出的特点就是能量极其有限,存储空间低。已有的通过加/解密操作实现的过滤机制都极大地增加了网络开销。对于 WSN 来说,能否完成指定期限的监控任务是一个很重的负担。因此,应更多地考虑采用比加/解密操作更节省

能量的手段来解决虚假数据过滤的问题。

c)为了节省传输能量,WSN 通常在网内进行数据压缩和聚集,这样往往会造成数据包尾部的破坏,在数据包后额外附加 T 个 MAC 的认证机制并不适合于这类网络。因此,研究不依赖 MAC 认证的过滤机制应成为下一步研究的方向。

d)目前,基于公开密码过滤方案的研究还很少,公开密钥技术适不适用于 WSN 还有待商榷。已有研究表明,利用中国剩余定理、Montgomery multiplication 和优化的 squaring 等优化方法可以让 RSA 的复杂度降低 25%。因此,基于上述思想有可能研究出适合 WSN 虚假数据过滤方案的公开密钥技术[9]。

e)已有途中过滤方案虽能有效检测和过滤虚假数据,但并不能找到并隔离发送虚假数据的源节点,使得大量虚假数据还是源源不断地注入 WSN,直到耗尽节点能量和网络带宽为止。应该考虑研究更为主动的溯源追踪方案,找出并排除发送虚假数据的源节点。

f)已有途中过滤方案大多没有考虑延迟问题,而 WSN 中多跳路由、网络阻塞和节点处理数据等往往会引起网络的延迟[9],攻击者可以利用延迟进行重放攻击。因此,研究时间同步或序列号机制来解决延迟问题也是一个值得深入的方向。

随着 WSN 虚假数据过滤问题的有效解决,将会极大地提高 WSN 的安全性,进一步促进更多的技术借助 WSN 平台。WSN 的应用将不断深入及广泛。

参考文献:

[1] 任丰原,黄海宁,林闯. 无线传感器网络[J]. 软件学报,2003,14(7):1282-1291.

[2] 苏忠,林闯,封富君,等. 无线传感器网络密钥管理的方案和协议[J]. 软件学报, 2007,18(5):1218-1231.

[3] CHONG C,KUMAR S. Sensor networks:evolution,opportunities,and challenges[J]. Proeeedings of IEEE,2003,91(8):1247-1256.

[4] YE Fan,LUO H Y,LU Song-wu,*et al*. Statistical en-route filtering of injected false data in sensor networks[J]. IEEE Journal on Selected Areas in Communication,2005,23(4):839-850.

[5] 马祖长,孙怡宁,梅涛. 无线传感器网络综述[J]. 通信学报,2004,25(4):114-124.

[6] 朱凌志,梁俊斌,刘志雄,等. 基于部署前密钥分配的虚假数据过滤方案[J]. 计算机工程与应用,2012,48(26):96-100.

[7] 朱凌志, 王建新, 马行坡. 基于代码片段的无线传感器网络密钥更新方案[J]. 计算机应用研究, 2011,28(6):2212-2214.

[8] 张启元. 无线传感器网络虚假数据检测排除机制研究[D]. 合肥:中国科技技术大学,2010.

[9] 米波,曹建秋,段书凯,等. 无线传感器网络密钥管理问题综述[J]. 计算机工程与应用,2011,47(6):77-82.

[10] 李平,林亚平,曾玮妮. 传感器网络安全研究[J]. 软件学报,2006,17(12):2577-2588.

[11] YANG Hao,YE Fan,YUAN Yuan,*et al*. Toward resilient security in wireless sensor networks[C]//Proc of the 6th ACM International Symposium on Mobile Ad hoc Networking and Computing. New York:ACM Press,2005:34-45.

[12] 刘志雄,王建新. 传感器网络中一种基于地理位置的虚假数据过滤方案[J]. 通信学报,2012,33(2):156-162.

[13] ZHU Sen-cun,SETIA S J,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. 2004:259-271.

[14] YU Zhen,GUAN Yong. A dynamic en-route scheme for filtering false data injection in wireless sensor networks[C]//Proc of the 3rd International Conference on Embedded Networked Sensor Systems. New York:ACM Press,2005:294-295.

[15] ZHANG You-tao,YANG Jun,VU H T. The interleaved authentication for filtering false reports in multipath routing based sensor networks[C]//Proc of the 20th International Parallel and Distributed Processing Symposium. Washington DC:IEEE Computer Society,2006:112-121.

[16] MA Miao. Resilience of sink filtering scheme in wireless sensor networks[J]. Computer Communications,2006,30(1):55-65.

[17] ZHOU Li,RAVISHANKAR C V. A fault localized scheme for false report filtering in sensor networks[C]//Proc of the 2nd International Conference on Pervasive Services. 2005:59-68.

[18] LI Feng,WU Jie. A probabilistic voting-based filtering scheme[C]//Proc of International Conference on Wireless Communications and Mobile Computing. New York:ACM Press,2006:27-32.

[19] LIU Zhi-xiong,WANG Jian-xin,ZHANG Xi. A false data filtering scheme using cluster-based organization in sensor networks[C]//Proc of IEEE International Conference on Communications. 2011:1-5.

[20] 祝青,郭赛球. 一种改进的虚假数据过滤方法[J]. 计算机工程,2012,38(5):158-160.

[21] CHRISTOPH K,MARKUS S,KPATCHA B,*et al*. STEF:a secure ticket-based en-route filtering scheme for wireless sensor networks[C]//Proc of the 2nd International Conference on Availability,Reliability and Security. 2007:310-317.

[22] YANG Hao,LU Song-wu. Commutative cipher based en-route filtering in wireless sensor networks[C]//Proc of the 60th Vehicular Technology Conference. 2004:1223-1227.

[23] ZHANG Yan-chao,LIU Wei,LOU Wen-jing,*et al*. Location-based compromise-tolerant security mechanisms for wireless sensor networks[J]. IEEE Journal on Selected Areas in Communications,2006,24(2):247-260.

[24] WANG Hao-dong,LI Qun. PDF:a public-key based false data filtering scheme in sensor networks[C]//Proc of IEEE International Conference on Wireless Algorithms,Systems and Applications. 2007:129-138.

[25] REN Kui,LOU Wen-jing,ZHANG Yan-chao. LEDS:providing location-aware end-to-end data security in wireless sensor networks[C]//Proc of the 25th IEEE Conference on Computing and Communicating. 2006:585-598.

[26] ZHANG Wen-sheng,CAO Guo-hong. Group rekeying for filtering false data in sensor networks[C]//Proc of the 24th IEEE Conference on Computing and Communicating. 2005:503-514.

[27] 曾玮妮,林亚平,胡玉鹏,等. 传感器网络中一种基于分布式更新权限的组密钥管理方案[J]. 计算机研究与发展,2007,44(4):606-614.

[28] SUBRAMANIAN N,YANG Chan-jun,ZHANG Wen-sheng. Securing distributed data storage and retrieval in sensor networks[C]//Proc of the 5th IEEE International Conference on Pervasive Computing and Communications. Washington DC:IEEE Computer Society,2007:191-200.

[29] ZHANG Wen-sheng,TRAN M,ZHU Sen-cun,*et al*. A random perturbation-based pairwise key establishment scheme for sensor networks[C]//Proc of the 8th ACM International Symposium on Mobile Ad hoc Networking and Computing. 2007:90-99.

[30] ZHANG Wen-sheng,SUBRAMANIAN N,WANG Gui-ling. Lightweight and compromise-resilient message authentication in sensor networks[C]//Proc of the 27th IEEE Computer and Communications Societies. Washington DC:IEEE Computer Society,2008:1418-1426.

[31] 彭舸,林亚平,易叶青. 无线传感器网络基于云团认证的虚假数据过滤机制[J]. 软件学报,2009,20(zk):239-248.

(下转第 4440 页)

286.
[5] JUELS A, LUBY M, OSTROVSKY R. Security of blind digital signatures[C]//Proc of CRYPTO 1997. Berlin: Springer-Verlag, 1997: 150-164.
[6] WU Qian-hong, SUSILO W, MU Yi, *et al*. Efficient partially blind signatures with provable security[C]//Proc of International Conference on Computational Science and its Applications. Berlin: Springer-Verlag, 2007: 1096-1105.
[7] CAO Tian-jie, LIN Dong-dai, XUI Rui. A randomized RSA-based partially blind signature scheme for electronic cash[J]. Computers and Security, 2005, 24(1): 44-49.
[8] MARTINET G, POUPARD G, SOLA P. Cryptanalysis of a partially blind signature scheme or how to make $100 bills with $1 and $2 ones[C]//Proc of Financial Cryptography and Data Security. Berlin: Springer-Verlag, 2006: 171-176.
[9] HUANG Hui-feng, CHANG C C. A new design of efficient partially blind signature scheme[J]. Journal of Systems and Software, 2004, 73(3): 397-403.
[10] ZHANG Fang-guo, CHEN Xiao-feng. Cryptanalysis of Huang-Chang partially blind signature scheme[J]. Journal of Systems and Software, 2005, 76(3): 323-325.
[11] ZHANG Fang-guo, SAFAVI-NAINI R, SUSILO W. Efficient verifiably encrypted signature and partially blind signature from bilinear pairings [C]//Proc of INDOCRYPT 2003. Berlin: Springer-Verlag, 2003: 191-204.
[12] CHOW S S M, HUI L C K, YIU S M, *et al*. Two improved partially blind signature schemes from bilinear pairings[C]//Proc of the 10th Australasian Conference on Information Security and Privacy. Berlin: Springer-Verlag, 2005: 316-328.
[13] OKAMOTO T. Efficient blind and partially blind signatures without random oracles[C]//Proc of the 3rd Theory of Cryptography Conference. Berlin: Springer-Verlag, 2006: 80-99.
[14] SHAMIR A. Identity-based cryptosystems and signature schemes [C]//Proc of CRYPTO 1984. Berlin: Springer-Verlag, 1984: 47-53.
[15] 曾梦岐, 卿昱, 谭平璋, 等. 基于身份的加密体制研究综述[J]. 计算机应用研究, 2010, 27(1): 27-31.
[16] HU Xiao-ming, HUANG Shang-teng. An efficient ID-based partially blind signature scheme[C]//Proc of the 8th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing. Washington DC: IEEE Computer Society, 2007: 291-296.
[17] TSENG Y M, WU T Y, WU J D. Forgery attacks on an ID-based partially blind signature scheme[EB/OL]. (2008-08-21)[2012-04-19]. http://www.iaeng.org/IJCS/issues_v35/issue_3/IJCS_35_3_07.pdf.
[18] 张学军, 王育民. 高效的基于身份的部分盲签名方案[J]. 计算机工程与应用, 2007, 43(11): 211-213.
[19] 闫东升. 一个新的高效的基于身份的部分盲签名方案[J]. 计算机工程与应用, 2008, 44(2): 137-140.
[20] 崔巍, 辛阳, 胡程瑜, 等. 高效的基于身份的(受限)部分盲签名[J]. 北京邮电大学学报, 2008, 31(4): 53-57.
[21] 李明祥, 赵秀明, 王洪涛. 对一种部分盲签名方案的安全性分析与改进[J]. 计算机应用, 2010, 30(10): 2687-2690.
[22] 李明祥, 郑艳娟, 安文广. 一种高效的基于身份的部分盲签名方案[J]. 计算机应用研究, 2010, 27(11): 4299-4302.
[23] AL-RIYAMI S S, PATERSON K G. Certificateless public key cryptography[C]//Proc of the ASIACRYPT 2003. Berlin: Springer-Verlag, 2003: 452-473.
[24] 张福泰, 孙银霞, 张磊, 等. 无证书公钥密码体制研究[J]. 软件学报, 2011, 22(6): 1316-1332.
[25] 荣维坚. 无证书部分盲签名方案[J]. 漳州师范学院学报: 自然科学版, 2008, 62(4): 44-47.
[26] 苏万力, 谭示崇, 李艳平, 等. 无证书部分盲签名[J]. 吉林大学学报: 工学版, 2009, 39(4): 1094-1098.
[27] ZHANG Lei, ZHANG Fu-tai. Certificateless partially blind signatures [C]//Proc of the 1st International Conference on Information Science and Engineering. Washington DC: IEEE Computer Society, 2009: 2883-2886.
[28] SAHAI A, WATERS B. Fuzzy identity-based encryption[C]//Proc of EUROCRYPT 2005. Berlin: Springer-Verlag, 2005: 457-473.
[29] AGRAWAL S, BOYEN X, VAIKUNTANATHAN V, *et al*. Fuzzy identity based encryption from lattices[EB/OL]. (2011-08-01)[2012-04-19]. http://eprint.iacr.org/2011/414.
[30] CASH D, HOFHEINZ D, KILTZ E, *et al*. Bonsai tree, or how to delegate a lattice basis[C]//Proc of EUROCRYPT 2010. Berlin: Springer-Verlag, 2010: 523-552.
[31] MICCIANCIO D, PEIKERT C. Trapdoors for lattices: simpler, tighter, faster, smaller[EB/OL]. (2011-09-14)[2012-04-19]. http://eprint.iacr.org/2011/501.

(上接第 4431 页)

[32] 李明, 苗付友, 熊焰. 一种基于簇的 WSN 预分配密钥管理机制[J]. 计算机工程, 2011, 37(5): 1-4.
[33] 李明, 苗付友, 熊焰. 基于簇的无线传感器网络预分配密钥机制[J]. 计算机工程, 2011, 37(20): 127-132.
[34] PERRIG A, TYGAR J D, SONG D, *et al*. Efficient authentication and signing of multicast streams over lossy channels[C]//Proc of IEEE Symposium on Security and Privacy. Washington DC: IEEE Computer Society, 2000: 56-73.
[35] 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, 30(6): 53-63.
[36] 董晓梅, 赵枋, 李晓华, 等. 适用于无线传感器网络的数字水印技术[J]. 武汉大学学报: 理学版, 2009, 55(1): 125-128.
[37] 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.
[38] YE Fan, YANG Hao, LIU Zhen. Catching "moles" in sensor networks [C]//Proc of the 27th International Conference on Distributed Computing Systems. Washington DC: IEEE Computer Society, 2007: 69-77.
[39] 杨峰. 无线传感器网络恶意节点防范技术[D]. 合肥: 中国科技技术大学, 2009.
[40] 杨峰, 周学海, 张起元, 等. 无线传感器网络恶意节点溯源追踪方法研究[J]. 电子学报, 2009, 37(1): 202-206.
[41] YANG Feng, ZHOU Xue-hai, ZHANG Shu-guang. Hierarchical traceback in wireless sensor networks[C]//Proc of the 4th International Conference on Wireless Communications, Networking and Mobile Computing. 2008: 1-4.
[42] 谢婧, 李曦, 杨峰. 应对虚假数据注入结合途中过滤与溯源追踪方法[J]. 计算机系统应用, 2011, 20(12): 249-256.
[43] 杨峰, 周学海, 张起元. 无线传感器网络高覆盖、低延迟途中过滤方法研究[J]. 计算机工程与科学, 2010, 32(11): 20-24.
[44] 江长勇. 无线传感器网络中的攻击检测研究[D]. 镇江: 江苏大学, 2009.
[45] 孙利民, 李建中, 陈渝, 等. 无线传感器网络[M]. 北京: 清华大学出版社, 2005.