应对虚假数据注入结合途中过滤与溯源追踪方法①

谢 婧[1]，李 曦[1,2]，杨 峰[1,2]

[1](中国科学技术大学 计算机科学与技术学院，合肥 230026)
[2](中国科学技术大学 苏州研究院，苏州 215123)

摘 要：对无线传感器网络中的虚假数据注入攻击问题进行了深入研究，并提出了切实可行的解决方案。本方案结合了途中过滤与溯源追踪的优点，它的核心思想是在数据报告中添加部分标记信息，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，收集到足够多数据报告后，便可以进行溯源追踪操作。同时，我们提出了一种更加均衡的分组方法及概率标记方法，实现了更好的性能。

关键词：途中过滤；溯源追踪；无线传感器网络；启发式分组

Filtering and Traceback in the False DataInjection Based on Combing En-Route

XIE Jing[1], LI Xi[1,2], YANG Feng[1,2]

[1](University of Technology and Science of China, Hefei 230026, China)
[2](Suzhou Institute for Advanced Study, University of Technology and Science of China, Suzhou 215123, China)

Abstract: We propose a practical solution- combining the en-route filtering and traceback method to solve the false data injection attack in the wireless sensor networks. The solution combining the advantages of the en-route and traceback schemes. Its core idea is to add some marking information to the data reports, and the sink node will add the unverified data reports to the traceback set. When collecting enough reports, it will execuate the traceback operation. Meanwhile, we propose a more balanced group scheme and a probabilistic marking method to improve the performance.

Key words: en-route filtering; traceback; wireless sensor networks; Heuristic group

无线传感器网络是下一代的信息技术，它综合了传感技术、无线通信技术、数据处理与分析技术等多个科学领域的最新进展，广泛应用于军事、科研、工业等多个领域[1-4]。随着无线传感器网络的普及，它所承担的任务也越来越重要，它所面临的安全威胁问题也越来越突出[5]，并已经引起了学术界与工业界的普遍重视。因为其具有一些独特的性质，导致在传统互联网中的安全解决方案并不能直接移植。首先，为了使无线传感器网络更加实用，传感器节点的能量、计算能力、存储空间等都比较有限；其次，不同于传统的网络，传感器节点通常被部署于室外，这就增大了其被物理俘获的风险；第三，传感器节点与物理环境或者人群直接接触，这也给传感器网络带来了新的风险。本文将研究无线传感器网络所面临的主要安全威胁——虚假数据注入攻击（False Data Injection）[6-10]，并提出有效的应对方案，为无线传感器网络中的大规模应用提供基础的安全保障。

1 系统模型与安全威胁分析

本文所考虑的系统模型与传统的途中过滤模型相似[6-10]，具体如图 1 所示：网络覆盖区域被划分为等大小的网格（cell），每个传感器节点都有一定的监测范围，在监测范围内发生的事件可以被传感器节点所感知，而在监测范围内的网格便被称为监测网格（detecting cell）。同时每个节点还需要按照一定概率随机选取若干个不在它监测范围内的网格，作为认证网格（verifying cell），节点可以对其认证网格内发生的事件所对应的数据报告进行验证。

① 收稿时间:2011-04-23;收到修改稿时间 2011-07-04

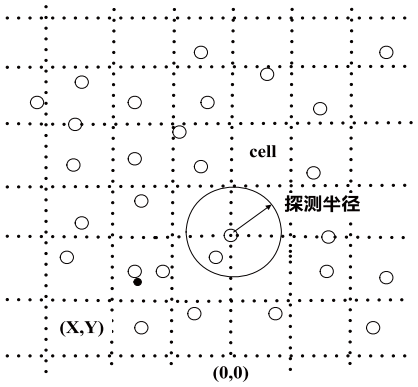

图 1　系统模型

在本系统中，共有 L 个主密钥组。每个节点需要选择一个主密钥组加入，然后它便可以利用这个主密钥组中的密钥生成对应于监测网格以及认证网格的密钥。当一个事件发生时，由探测到这一事件的节点共同生成一条数据报告（应包含事件发生的位置）；然后每个节点都利用其所掌握的对应事件发生地点的密钥为这条数据报告添加一个消息认证码（MAC, Message Authentication Code）。一条合法的数据报告必须包含 T 个消息认证码，并且产生这 T 个消息认证码的节点需要来自于不同的主密钥组(L 与 T 都是事先设定的参数)。途中节点收到一条数据报告后，首先查看事件发生的地点，然后根据事件发生的地点以及自己掌握的密钥来决定是否对数据报告进行检测认证与过滤，如果不进行检测认证，则按照一定概率对此数据包进行标记，然后转发此数据报告，否则，如果检测认证通过，同样按照一定概率对其进行标记，然后转发此数据报告，如果检测认证失败，则直接丢弃此数据报告，检测认证即利用自己所掌握的密钥重新计算消息认证码，并与数据报告所携带的消息认证码进行比对，如果相同则认证成功，否则便失败；最终认证通过或者未被认证的数据报告都发送到汇聚节点，汇聚节点对所有收到的数据报告进行检测认证，并将所有虚假数据报告加入溯源追踪集合，收集到足够多数据报告后便利用我们提出的溯源追踪算法定位攻击节点位置。，大大降低了驱动开发的复杂度。

2　解决方案的基本流程

传统的途中过滤方案中汇聚节点对收集到的所有数据报告进行最终验证，如果验证不通过便直接丢弃。我们考虑在数据报告中添加部分标记信息，汇聚节点将验证不通过的数据报告加入溯源追踪集合中，收集到足够多数据报告后，便可以进行溯源追踪操作。

2.1 方案概述

在转发的过程中，有一些虚假数据报告会被中间节点过滤掉，转发节点以一定概率标记它没有过滤掉的数据报告。当汇聚节点收到数据报告后，会验证所有的消息认证码，如果数据报告是正常信息，则进入下一步处理，如果数据报告是虚假信息，汇聚节点便将其加入到回溯集合中供定位攻击节点使用；若集合中的数据报告超过预先设定的参数极限，汇聚节点则执行回溯过程，最终定位攻击节点。

2.2 预设值与数据报告生成

在图 1 所示的系统模型中，传感器网络所覆盖的区域将被分为同等大小的正方形网格（Cell）。在传感器节点部署之前，每个节点预先加载网格的大小、原点的位置参数、单程哈希函数 H()、消息认证码生成函数、以及 L 个主密钥，它们的作用将在下文介绍。节点部署后，通过选择的定位方法[41]，确定它所处的位置以及所处的网格。然后每个节点确定它所能监测的网格并按照所设定的概率随机选择它能够验证的网格。全局性密钥池被分为 L 组，每个节点借助于我们所提出的启发式分组方法来选择其中的一个组加入。例如，节点 i 加入其主密钥为 Ki 的第 i 组，通过预先加载的安全的单程哈希函数 H()，得到对应于网格(Xi，Yi)的密钥 $K(X_i,Y_i) = H(K_i,(X_i,Y_i))$，通过这种方式，节点 i 获得了它所能监测以及验证网格的密钥，然后节点将所有主密钥及用于生成认证密钥的哈希函数清除。

当一个有效事件发生时，所有的监测节点将临时组成为一个簇（cluster），这些节点将就本次报告的内容达成一致（包括事件发生地点、时间、性质等），并利用[42]所提出的选举算法来选举簇头（cluster head），每个节点利用其所拥有的对应于事件发生网格的认证密钥和相应的生成函数生成一个消息认证码（MAC），这个消息认证码也包含节点所加入的主密钥组序号，完成后便将其发送给簇头，最后当簇头收集到来自 T 个不同组的消息认证码后，便将消息认证码附加于原始数据报告之后，发送至汇聚节点。

2.3 途中节点的转发、过滤与标记

中间节点在收到数据报告后，首先检验该数据报

告是否包含有 T 个消息认证码，若少于 T 个，则丢弃此数据报告，否则便从数据报中获取事件位置，再检验其是否存储了对应于该网格的密钥。若有密钥，则查看该数据报告是否携带有该密钥对应的消息认证码，如果没有，则按照下文所要介绍的标记方法对数据报告进行标记，并转发此数据报告，如果数据报告携带有相应的消息认证码，则验算消息认证码，并将其和附带的信息认证码进行比较，验证若失败，则数据报告被丢弃；若成功，则仍然使用下文所要介绍的标记方法进行概率性标记并转发数据报告。

算法 4.1. 溯源追踪算法

```
//Initialization
    S= Ø, T= Ø;
//Traceback
    When the sink receives a packet with no mark
        does nothing;
    When the sink receives a packet with 1 valid mark
        if the packet's first two domains are marked by node s
            if s∉T
                S=S∪{s};
                T=T∪{s};
        if the packet's last two domains are marked by node t
            if t∉T
                T=T∪{t};
            if t∈S
                S=S-{t};
    When the sink receives a packet with 2 valid marks from nodes s&t
        if s∉T
            S=S∪{s};
            T=T∪{s};
        if t∉T
            T=T∪{t};
        if t∈S
            S=S-{t};
```

图 2 溯源追踪算法

2.4 汇聚节点处理与溯源追踪方法

当汇聚节点接收到数据报告后，因其存储所有分组的所有密钥，可执行最终的全局性验证。如果验证通过，数据报将被正常处理。否则此数据报被视为虚假数据报，并被加入到回溯池中。当池中存储的数据报告数量超过预设值的参数值时，汇聚节点开始进行回溯过程。在汇聚节点存储的信息中，有 2 张信息表，分别存储有(id(i), hi(i))及(id(i), hi(i)’),也就是将节点 id 与加密后的字段和用于生成标记认证信息的哈希函数一一对应。当汇聚节点收到数据报告后，首先提取最后一个节点的标记信息，读取其中的 hi (i)域，然后通过查找第一张信息表确定标记节点的 id，再通过查找第二张表确定本 id 对应的哈希函数，通过这个哈希函数计算消息认证码的数值，并与数据报告所携带的数值相比对，如果成功，则继续提出第一个标记节点的信息，重复以上过程，如果都成功的话，则确定了第一个节点与第二个节点的偏序关系。有了偏序关系之后，汇聚节点需要对其进行处理。具体来说，汇聚节点维护有 S 节点集合与 T 节点集合，S 节点集合是所有可能定位到的节点集合；T 节点集合是所有标记过虚假数据报告的节点集合。汇聚节点记录所有被验证过的节点，再将节点插入到 S 和 T 集合中；或者从 S 中删除某些节点，当收集到足够多的信息时，S 集合内的元素便是本方案所定位的节点，而攻击节点也来自 S 集合的单跳邻居节点中。算法 4.1 显示了溯源追踪方法的具体执行过程。本文所采用的溯源追踪方法与文献[31]类似，其有效性证明也可以参见文献[31]。

3 解决方案的实现细节

为了实现本方案，节点需要选择一个主密钥组加入，同时节点需要按照一定的概率标记它所转发的数据报告，因此，我们将介绍在实现本方案中所采用的启发式分组加入方法与均衡的概率标记方法。

3.1 启发式分组加入方法

由上文的介绍可以知道，从理论上看，加入同一密钥组的节点需要在网络区域内均匀分布，也就是希望加入同一组的节点尽量覆盖整个网络区域。目前针对这一问题有两类较为通行的解决方案：（1）随机化方法[46,48]，每个节点按照一定概率随机选择一个密钥组加入，这种方法的优点是效率较高，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，使事件不能够形成的合法数据报告；（2）确定性方法[47]，汇聚节点掌握有所有节点的分布，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，但是缺陷是需要的计算时间较长，代价较大。

以上两类情况都没有考虑执行此算法的时间可能是不固定的，即系统部署后留给分组选择的时间有可能长也有可能很短，如果可以进行分组选择的时间较长，显然可以提出一个较优的分组算法，而如果分组选择时间极短，则随机化方法就是一种较好的选择。针对以上情况，我们提出一种启发式的分组加入方法，

它采用了逐步求精的方法。所有节点在部署之前都被载入一个计时器（Timer），它表示节点有多长的时间用来运行分组选择算法，当部署完成后，每个节点通过随机数生成器随机选择一个密钥组加入，如果计时器耗尽，则程序结束，该算法退化为完全随机的算法，否则，在计时器未耗尽的时间内，每个传感器节点按照如下方式决定其最终加入哪一组，同样假设共有 L 个密钥组供节点选择加入。

首先，所有节点都向邻居节点广播其节点号、位置及所加入的密钥组,我们采用 CSMA/CA 广播协议[49]以便避免冲突，保证在某一时刻只有一个节点占用广播信道，每个节点收到其他某个节点的广播后，便读取广播节点的节点号、位置及加入的密钥组，然后按照如下原则调整自身所加入的组：（1）根据所收到的所有广播信息判断，如果它的邻居节点们共加入了（L-1）个不同的密钥组，则本节点加入剩余的唯一一个密钥组；（2）如果他的邻居节点加入了少于（L-1）个密钥组，则本节点在剩余的密钥组中随机选择一个组加入；（3）如果它的邻居节点加入了所有密钥组，则本节点加入包含最少节点的密钥组；（4）如果包含最少节点的密钥组超过一个，则本节点计算其与这些密钥组节点的最短距离，并选择最短距离最大的密钥组加入；（5）如果经过以上步骤，仍然存在多个密钥组可以加入，则本节点在剩余的密钥组中随机选择一个加入。

节点选定了其所加入密钥组之后，便重复以上所述步骤，向其邻居节点广播其节点号、位置及所加入的密钥组，直至计时器耗尽为止。可以看出本方法的目的就是使得在一个区域内的节点尽可能均匀地分布到多个密钥组中。

很明显，我们所提出的方法是可以自适应的。不论 Timer 周期有多长，每个节点都可以选择一个组加入，而随着 Timer 时间周期的增加，节点分布的也将更加均匀。我们将在后续章节进行实验，验证所提出的分组算法的覆盖性能。

3.2 均衡的概率标记方法

所有不过滤数据报告的中间节点都将以一定概率标记传输来的数据报告，数据报告最多可被 m（m≥1）个节点标记，m 为系统设置的参数，本文仅考虑 m=2 的情况，m 为其他值的情况与此类似，图 3 显示的是当 m = 2 时的标记方法。

简单来说，我们让 M 表示数据报和监测节点的信息。每个节点 i 和汇聚节点共享两个哈希函数(hi, hi’)。其中 hi 表示加密其 ID，hi’生成数据报告所携带的标记认证信息，对 id 也进行加密是为了保证本方法的安全性。

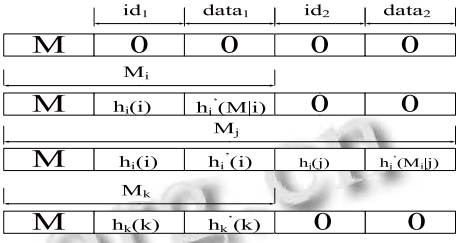

图 3　标记方法

简单来说，我们让 M 表示数据报和监测节点的信息。每个节点 i 和汇聚节点共享两个哈希函数(hi, hi’)。其中 hi 表示加密其 ID，hi’生成数据报告所携带的标记认证信息，对 id 也进行加密是为了保证本方法的安全性。

当节点要对数据报告进行标记时，会检查有多少节点已经标记过此数据报。如果比 m 小则从第一个空白区域标记此数据报告，标记的格式如图 4.1 所示，既对节点 id 进行加密标记，也对所转发的整体数据进行标记，所施行的仍然是链式标记，图 3 中的节点 i 与节点 j 便进行了这项工作；如果数据报告的标记域已经被全部占用，则它会在清除先前标记后再重新标记，图 3 中的节点 k 便是采用的这种操作方法。

在传统的回溯方案[30,31]中，所有的节点一般是以确定相等的概率来决定是否标记数据报，这样情况下，上游节点所标记的 id 信息很有可能会被下游节点清除，并且数据报告的传输路径越长，这种情况发生的可能性越大，因此上游节点的标记将只能被汇聚节点以很小的概率收集到，故回溯方案的效率会大幅度降低；另外，通常靠近汇聚节点的传感器节点需要转发大量的数据，消耗较多的能量、网络带宽、存储容量等，很容易失效，这就容易造成连锁反应，一个节点失效后，它的周围节点又要承担更多的转发任务，加速了失效的过程，最终造成汇聚节点的邻居节点大量失效，使得汇聚节点成为信息孤岛。为了解决以上两项缺陷，我们提出了一种均衡性的概率标记方法。

在这里我们设计了一个简单有效的标记概率计算方法。节点将会以概率 p = d/D 来标记数据报，其中 d 表示本转发节点与汇聚节点间的距离，而 D 则表示整

个网络区域中传感器节点与汇聚节点间的最大距离。此标记方法有两大优势：1)节点标记数据报告的概率随着其与汇聚节点之间距离的增加而增加，因此按比例地增大了上游节点的标记信息被汇聚节点收集到信息的概率，并且这一概率仅依赖于节点间的相对距离，简单有效，不容易被篡改。在这种情况下，源节点也可以更高效的被定位；2)因为靠近汇聚节点的传感器节点标记概率显著下降，也就降低了靠近汇聚节点的传感器节点运算量，节约了较多的计算资源。本方案的性能将在下一节通过实验进行详细验证。

4 仿真实验结果与分析

我们首先用实验验证 3.1 节提出的分组选择算法的性能，我们在一个 2Km×2Km 的平坦区域内均匀随机部署 500,1000,2000 个传感器节点，主密钥的数目被设置为 4 个，运行 3.1 节所提算法 1000 次后，计算加入每个密钥组的节点数目平均值，其中分组算法时间周期被设置为 1 分钟，传感器节点进行计算与传输所需要的时间依据 CrossBow 公司生产 MicaZ 节点[12]。

表 1 分组选择算法性能

N	SET			
	G1	G2	G3	G4
500	122.7	128.5	125.3	123.5
1000	251.3	252.1	247.6	249
2000	501.1	498.1	502.7	498.1

可以看出，本算法在 1 分钟的时间内，可以使节点达到较为均匀地分布，即加入每个密钥组的节点数目约为总节点数目的 1/4。

接下来，我们继续衡量本章所提出方案的覆盖性能、过滤效率及溯源追踪的性能。我们所做仿真实验的参数设置如下：传感器节点被均匀散布了一个 2Km×2Km 的平坦区域内，网格大小为 25 米，汇聚节点位于网络区域的中央，每个节点的探测半径设置为 25 米，传输半径设置为 50 米，网络主密钥分为 8 组，一个合法数据报告携带来自 4 个不同组的消息认证码。

(1) 覆盖性能

我们将本方案的覆盖性能与成熟的途中过滤解决方案 SEF[6], LBRS[8]和 GRSEF[9]进行对比，部署于网络区域的传感器节点数依次设为 500,1000,2000。对每种情况，进行 1000 次实验，在每次实验中，我们在网络区域中随机选择一个位置，然后考察在事件发生后能否形成一个合法数据报告。表 2 显示了在不同的网络节点数目下，每种途中过滤方案的覆盖性能。

表 2 覆盖性能对比

N	Coverage Percentage(%)		
	OUR SCHEME	SEF&LBRS	GRSEF
500	89.2	70.4	71.2
1000	97.4	90.1	91.3
2000	99.2	93.5	94.2

（2）抗俘获性、过滤性能与回溯性能

抗俘获性是指随着攻击者俘获节点数目的增多，攻击者可以伪造多大区域内发生事件所对应的合法数据报告，良好的抗俘获性是指虽然攻击者俘获了较多的传感器节点，但仍然仅能伪造较小区域内发生的事件所对应的数据报告；过滤性能一般用伪造的数据报告被传输的平均数目来衡量，良好的过滤性能是指虚假数据报告仅仅被传输较短的跳数；回溯性能是指汇聚节点需要收集到多少虚假数据报告才能定位攻击节点。因为以上三项性能指标相互影响，所以我们统一对其进行考虑。

在本次实验中，我们在上文所示的网络区域内部署 2000 个传感器节点，在三种传统的途中过滤方法中，每个节点以 0.1 的概率获得其他区域的共享密钥，在 LBRS 中，光柱宽度（beam width）被设置为 100 米，网格大小被设置为 25 米，GRSEF 中的设置与文献[9]相同，网格大小同样被设置为 25 米，在我们所提出的方案中，为提高抗俘获性，节点获得其他区域共享密钥的概率为 0.02。

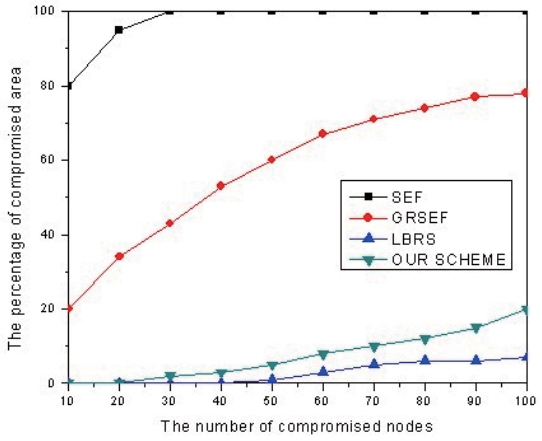

图 4 各类方案的抗俘获性能比较

我们通过考察攻击者能够伪造合法数据报告的网络区域占整体网络区域的百分比来衡量方案的抗俘获性，可以看出：本方案的抗俘获性明显高于 SEF 与 GRSEF，略微高于 LBRS。但 LBRS 要求汇聚节点固定以及静态的路由协议，而本方案并没有这些限制。

为衡量每种方案的过滤性能，我们考察数据报告在被过滤前传输的平均跳数，在仿真实验中，随机选择的被俘获节点数目依次设置为 10、50、100，对每种情形，我们重复 1000 次实验，然后计算虚假数据报告被转发的平均跳数，表 3 显示了实验结果，可以看出，本方案的过滤性能低于其他的途中过滤解决方案，因为在本方案中，节点获得其他区域密钥的概率较低，但是未被途中过滤的虚假数据报告被汇聚节点收到并发现后可以用于溯源追踪，并尽快定位攻击节点。

表 3　各类方案的过滤性能比较

N_c	Average of the number of forwarding hops			
	OUR SCHEME	SEF	LBRS	GRSEF
10	6.5	4.1	3.9	3.8
50	9.8	6.5	5.1	4.9
100	14.3	10.7	8.3	8.9

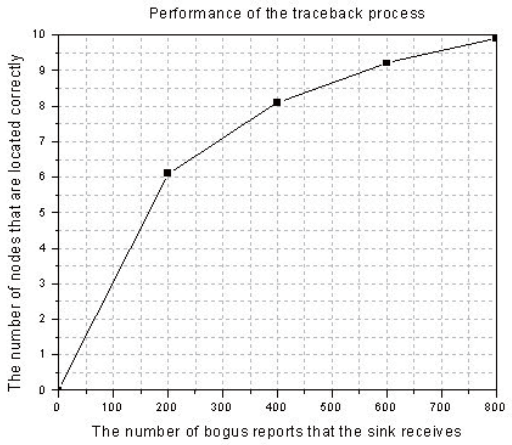

图 5　溯源追踪性能示意图

接下来我们便考察本方案的溯源追踪性能，在我们的仿真实验设置中，当汇聚节点收集到 50 个虚假数据报告后便运行溯源追踪过程，我们随机设置 10 个传感器节点被攻击节点俘获并在发送虚假数据报告，然后依次考虑汇聚节点收集到 200、400、600、800 个虚假数据报告的情况，并分别考察可以定位攻击节点的数目，对于每种情形，我们运行 100 次实验，并计算被定位的被俘获节点的平均数目，实验结果如图 5 所示。由图 5 可以看出，当汇聚节点收到 600 个虚假数据报告后，便可以成功定位超过 90%的攻击节点。

由以上仿真实验可以看出，本方案平衡了抗俘获性、过滤性能与溯源追踪性能，使得在应对虚假数据攻击的过程中，以上三项性能都可以取得较好的结果，而且用户也可以根据网络特性调整参数设置，增强或者削弱某一项特定性能，以取得优化的综合效果。

参考文献

1 Estrin D, Culler D, Pister K, Suk-hatme G. Connecting the Physical World with Pervasive Networks. IEEE Pervasive Computing, 2002.

2 孙利民,李建中,陈渝,等.无线传感器网络.北京:清华大学出版社,2005.

3 Mainwaring A, Polastre J, Szewczyk R, Culler D, Anderson J. Wireless Sensor Networks for Habitat Monitoring. ACM WSNA'02, 2002.

4 Brooks R, Ramanathan P, Sayeed AM. Distributed Target Classification and Tracking in Sensor Networks. Proc. of IEEE, 2003,91(8).

5 Perrig A, Wagner D, Stankovic J. Security in Wireless Sensor Networks. Communications of the ACM, 2004, 47(6).

6 Ye F, Luo H, Lu S, Zhang L. Statistical en-route fIltering of injected false data in sensor networks. IEEE Journal on Selected Areas in Communication, 2005,23:839–850.

7 Zhu S, Jajodia S, Ning P, An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks. IEEE Symposium on Security and Privacy, 2004,259–271.

8 Yang H, Ye F, Yuan Y, Lu S, Arbaugh W. Toward resilient security in wireless sensor networks. IEEE MobiHoc, 2005,34–45.

9 Yu L. Li J, Grouping-based resilient statistical en-route filtering for sensor networks. IEEE INFOCOM, 2009, 1782–1790.

10 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.软件学报,2009,20:239–248.

11 Crossbow. www.xbow.com/Products/Product_pdf_files/ Wireless _pdf/MICAZ_Datasheet.pdf

12 Crossbow www. xbow. com/ Products/ Product_ pdf_ files/Wireless_pdf/Imote2_Datasheet.pdf.

13 Pister K, Kahn J, Boser B. http://eecs.berkeley.edu/~pister /SmartDust.

14 Beelinker Technology. http://www. beelinker. com/

15 深联科技. http://www. wsn. org. cn/cn/index.php

16 Arora A, Dutta P, Bapat S, S, et al. A line in sand:Awireless sensor network for target detection, classification,and tracking.Computer Networks Journal,Oct.2004.

17 阮殿旭,唐大方,张晓光,等.ZigBee 技术无线传感器网络在煤矿井下环境监测中的应用研究.煤矿机械,2008,(6):163–164.

18 杨维,周嗣勇,乔华.煤矿安全监测无线传感器网络节点定位技术.煤炭学报,2007,32(6):652–656.

19 Balogh G, et al. Wireless sensor network–based projectile trajectory estimation. Technical Report, ISIS– 05–601,Feb 2005. http://www.isis.vanderbilt.edu/projects/nests/applications.html

20 Eschenauer L, Gligor VD. A key–managem- ent scheme for distributed sensor networks. ACM Conference on Computer and Communications Security. Washington, DC, USA, 2005

21 Du W, Deng J, Han YS, et al. A pairwise key pre-distribution scheme for wireless sensor networks. ACM Conference on Computer and Communications Security. Washington, DC, USA, 2003.

22 Chan H, Perrig A, Song D. Random key predistribution schemes for sensor networks. Symposium on Security and Privacy, 2003. Berkeley, CA, USA, 2003.

23 Xiao Y, Rayi VK, Sun B, et al. A survey of key management schemes in wireless sensor networks. Computer Communications, 2007, 30(11-12):2314–2341.

24 Yang C, Xiao J. Location-Based Pairwise Key Establishment and Data Authentication for Wireless Sensor Networks. Information Assurance Workshop, 2006.

25 Basford P. Data authentication for sensor networks. School of Electronics and Computer Science, University of Southampton, 2008.

26 Zhang W, Subramanian N, Wang G. Lightweight and Compromise-Resilient Message Authentication in Sensor Networks. IEEE INFOCOM, Phoenix, AZ,USA. 2008.

27 Choi H, Zhu S, Laporta T. SET: Detecting node clones in Sensor Networks International Conference on Security and Privacy in Communication Networks, 2007.

28 Wang R, Du W, Ning P. Containing denial- of-service attacks in broadcast authentication in sensor networks. The 8th ACM International Symposium on Mobile Ad Hoc Networking and Computing Montreal. Quebec, Canada, 2007.

29 Shao M, Zhu S, Zhang W, et al. pDCS: Security and Privacy Support for Data-Centric Sensor Networks. INFOCOM, Anchorage, Alaska, USA, 2007.

30 Ye F, Yang H, Liu Z. Catching “moles” in sensor networks. IEEE International Conference on Distributed Computing Systems(ICDCS). Toronto, ON, 2007.

31 杨峰,周学海,张起元,谢婧,章曙光.无线传感器网络恶意节点溯源追踪方法研究.电子学报,2009,37(1):202–206.

32 Zhang QY, Zhou XH, Yang F, Li X. Contact-based Traceback in Wireless Sensor Networks. The 3rd IEEE International Conference on Wireless Communications, Networking and Mobile Computing. Shanghai, China, 2007. 2487–2490.

33 Yang F, Zhou XH, Zhang QY, Xie J. On the performance of probabilistic packet marking for traceback in sensor networks. The 5th IEEE Consumer Communications and Networking Confer ence,2008:Las Vegas,US:682–686.

34 Lin ST, Chiueh C. A survey on solutions to distributed denial of service attacks Stony Brook University, Stony Brook,NY-11794. 2006.

35 Ren K, Lou W, Zhang Y. LEDS:Providing locationaware end-to-end data security in wireless sensor networks. IEEE Trans. on Mobile Computing,2007,7:585–598.

36 Yu Z, Guan Y. A dynamic scheme for en-route filtering false data. 3rd ACM International Conference on Embedded Networked Sensor Systems. New York: ACM Press, 2005. 294–295.

37 Sager G..Security fun with OCxmon and cflowd. Internet 2 Working Group Meeting, 1998.

38 Al–Duwairi B, Govindarasu M. Novel Hybrid Schemes Employing Packet Marking and Logging for IP Traceback. IEEE Trans. on Parallel and Distributed Systems, 2006, 17(5):403–418.

39 Priyantha NB, Chakraborty A, Balakrishnan H. The cricket

location-support system. International Conference on Mobile Computing and Networking, Boston, Massachusetts, United States, 2000.

40 Savvides A, Park H, Srivastava MB. The bits and flops of the n-hop multilateration primitive for node localization problems. International Workshop on Wireless Sensor Networks and Applications Atlanta, Georgia, USA. 2002.

41 Priyantha NB, Balakrishnan H, Demaine E, et al. Anchor-free distributed localization in sensor networks. MIT Lab for Computer Science, MIT Lab for Computer Science, 2003.

42 Heinzelman WB, Chandrakasan AP, BalakrIshnan H. An application-specific protocol architecture for wireless microsensor networks. IEEE Trans. on Wireless Communications, 2002,1(4):660–670.

43 Younis O, Fahmy S. Distributed clustering in ad-hoc sensor networks: A hybrid energy-efficient approach. INFOCOM Hong Kong, China, 2004.

44 Chen Q. General Clustering Framework in Wireless Sensor Networks.Computer Science and Engineering. Hong Kong: The Hong Kong UniversitySof Science and Technology. 2008.

45 Karp BTKH. GPSR: greedy perimeter stateless routing for wireless networks.MobiCom, Boston, USA, 2000.

46 Slijepcevic S, Potkonjak M. Power efficient organization of wireless sensor networks. ICC, 2001,2:472–476.

47 Hastad J. Some optimal inapproximability results. Journal of the ACM, 2001,48: 798–859.

48 Abrams Z, GOEL A, Plotkin SA. Set k-cover algorithms for energy efficient monitoring in wireless sensor networks. IPSN, 2004.424–432.

49 Editors of IEEE. IEEE 802.11,Wireless LAN MAC and Physical Layer Specifications, 1997.

50 Blake I, Seroussi G, Smart NP. Elliptic curves in cryptography, Cambridge Univ. Press, 2000.

51 Batina L, Mentens N, Sakiyama K, et al. Low-cost elliptic curve cryptography for wireless sensor networks. The 3rd European Workshop on Security and Privacy in Ad Hoc and Sensor Networks. Hamburg, Germany, (2006.

52 Gay D, Levis P, Culler D, et al. nesC 1.1 Language reference manual. http://nescc.sourceforge.net/papers/nesC-ref.pdf

53 Madden LS. TinyOS: An Operating System for Sensor Networks Ambient Intelligence. Springer Berlin Heidelberg, 2005. 115–148.