(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 101820618 A
(43)申请公布日 2010.09.01

(21)申请号 201010145480.2

(22)申请日 2010.04.13

(71)申请人 中国科学技术大学
地址 230026 安徽省合肥市金寨路 96 号

(72)发明人 王行甫 钱雷 曹仁之

(74)专利代理机构 北京市立方律师事务所 11330
代理人 张磊

(51)Int.Cl.
H04W 12/00(2009.01)
H04W 64/00(2009.01)
H04W 84/18(2009.01)

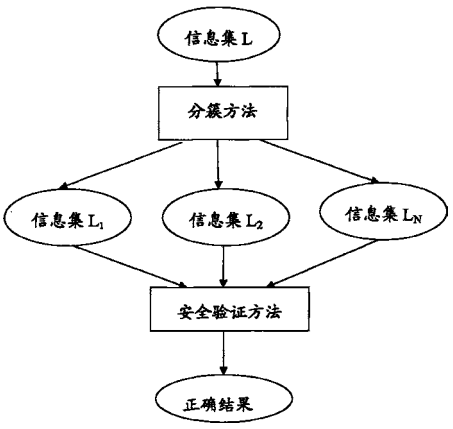
权利要求书 3 页 说明书 8 页 附图 3 页

(54)发明名称

一种抗多数合谋攻击的无线传感器安全定位方法及装置

(57)摘要

本发明的实施例提出了一种抗多数合谋攻击的无线传感器安全定位方法，包括如下步骤：待定位节点向其通信范围内的信标节点发送定位请求，接收返回的定位信息；根据定位信息生成定位信息集L，利用分簇算法得到N个簇，计算得到N个定位结果；待定位节点向其通信范围内的已定位非信标邻居节点发送定位验证请求，接收返回的定位验证信息，将其与N个定位结果进行定位验证，得到安全定位结果。本发明的实施例还提出了一种抗多数合谋攻击的无线传感器安全定位装置，该装置位于待定位节点上，包括接收模块、分簇模块和验证模块。根据本发明提供的方法及装置，通过一致性检测和安全验证技术，移除受攻击信标节点发送的恶意信息，获得高精度的定位结果。



CN 101820618 A

1. 一种抗多数合谋攻击的无线传感器安全定位方法，其特征在于，所述方法包括如下步骤：

待定位节点向其通信范围内的信标节点发送定位请求，接收所述信标节点返回的定位信息；

所述待定位节点根据所述定位信息生成定位信息集 L，利用分簇算法得到 N 个簇，根据所述 N 个簇计算得到 N 个定位结果；

所述待定位节点向其通信范围内的已定位非信标邻居节点发送定位验证请求，接收所述已定位非信标邻居节点返回的定位验证信息，将所述定位验证信息和所述 N 个定位结果进行定位验证，得到安全定位结果。

2. 如权利要求 1 所述的方法，其特征在于，所述待定位节点利用分簇算法得到 N 个簇，根据所述 N 个簇计算得到 N 个定位结果，包括如下步骤：

A1：所述待定位节点从所述定位信息集 L 中抽取 K 个元素形成集合 L_1，对到所述集合 L_1 进行一致性检测，其中，$K \geq 3$；

A2：所述待定位节点从剩余的 $L-L_1$ 中取出元素放入 L_1 中，对 L_1 进行一致性检测，若满足一致性检测条件，则将该元素取出 L_1，放入 L_3；否则将该元素取出 L_1，放入 L_2；直到 $L-L_1$ 中元素取完，将 L_3 中元素放入 L_1；

A3：对 L_2 进行一致性检测，

当 $|L_2| < 3$ 时，即 L_2 中信标节点数量小于 3 时，生成新簇 L_1，执行步骤 A2，

当 $|L_2| \geq 3$ 时，即 L_2 中信标节点数量大于或等于 3 时，对 L_2 做一致性检测，若 L_2 满足一致性检测条件，生成新簇 L_2，执行步骤 A2；否则执行步骤 A1，对 L_2 执行分簇算法，继续分簇；

A4：当生成新簇 L_N 时，得到 N 个定位结果。

3. 如权利要求 2 所述的方法，其特征在于，所述一致性检测包括如下步骤：

所述待定位节点根据所述定位信息集 L，通过极大似然估计算法求出待定位节点坐标 $(\tilde{x}_s, \tilde{y}_s)$，

其中，该估计的均方差为 $\delta^2 = \frac{1}{|L|}\sum_{i=1}^{|L|}\left(d_i - \sqrt{(x_i-\tilde{x}_s)^2+(y_i-\tilde{y}_s)^2}\right)^2$，

当均方差 $\delta^2 < \tau$ 时，则表示 L 满足一致性检测条件，通过一致性检测，其中，τ 为一致性检测的阈值。

4. 如权利要求 2 所述的方法，其特征在于，

当 $N = 1$ 时，该簇 L_1 为安全的定位信息集，计算位置信息，算法结束；

当 $N \geq 2$ 时，根据所述 N 个簇计算 N 个不同的定位结果 (x_i, y_i)，其中，$i = 1, 2 \ldots\ldots N$，N 为正整数。

5. 如权利要求 4 所述的方法，其特征在于，所述待定位节点从所述邻居节点信息集 L^* 中随机取出一个定位信息 $p = (x_p, y_p, d_p)$ 进行测试，所述测试包括如下步骤：

根据所述定位结果 (x_i, y_i)，计算 $u_i = |d_i - d_p|$，

其中 $d_i = \sqrt{(x-x_i)^2+(y-y_i)^2}$，$d_p = \sqrt{(x-x_p)^2+(y-y_p)^2}$，$i = 1, 2 \ldots\ldots N$，

对所述计算得到的 u_i 进行比较，得到当 $i = q$ 时，u_i 取最小值，

则 (x_q, y_q) 为安全定位结果。

6. 一种抗多数合谋攻击的无线传感器安全定位装置，其特征在于，所述安全定位装置位于待定位节点上，

所述安全定位装置包括接收模块、分簇模块和验证模块，

所述接收模块，用于向所述待定位节点的通信范围内的信标节点发送定位请求，接收所述信标节点返回的定位信息；

所述分簇模块，用于根据所述定位信息生成定位信息集 L，利用分簇算法得到 N 个簇，根据所述 N 个簇计算得到 N 个定位结果；

所述验证模块，用于向所述待定位节点的通信范围内的已定位非信标邻居节点发送定位验证请求，接收所述已定位非信标邻居节点返回的定位验证信息，将所述定位验证信息和所述 N 个定位结果进行定位验证，得到安全定位结果。

7. 如权利要求 6 所述的装置，其特征在于，所述分簇模块利用分簇算法得到 N 个簇，根据所述 N 个簇计算得到 N 个定位结果，包括如下步骤：

A1：从所述定位信息集 L 中抽取 K 个元素形成集合 L_1，对到所述集合 L_1 进行一致性检测，其中，$K \geqslant 3$；

A2：从剩余的 $L-L_1$ 中取出元素放入 L_1 中，对 L_1 进行一致性检测，若满足一致性检测条件，则将该元素取出 L_1，放入 L_1；否则将该元素取出 L_1，放入 L_2；直到 $L-L_1$ 中元素取完，将 L_3 中元素放入 L_1；

A3：对 L_2 进行一致性检测，

当 $|L_2| < 3$ 时，即 L_2 中信标节点数量小于 3 时，生成新簇 L_1，执行步骤 A2；

当 $|L_2| \geqslant 3$ 时，即 L_2 中信标节点数量大于或等于 3 时，对 L_2 做一致性检测，若 L_2 满足一致性检测条件，生成新簇 L_2，执行步骤 A2；否则执行步骤 A1，对 L_2 执行分簇算法，继续分簇；

A4：当生成新簇 L_N 时，得到 N 个定位结果。

8. 如权利要求 7 所述的装置，其特征在于，所述分簇模块进行一致性检测包括如下步骤：

根据所述定位信息集 L，通过极大似然估计算法求出待定位节点坐标 $(\tilde{x}_s, \tilde{y}_s)$，

其中，该估计的均方差为 $\delta^2 = \frac{1}{|L|}\sum_{i=1}^{|L|}\left(d_i - \sqrt{(x_i-\tilde{x}_s)^2+(y_i-\tilde{y}_s)^2}\right)^2$，

当均方差 $\delta^2 < \tau$ 时，则表示 L 满足一致性检测条件，通过一致性检测，其中，τ 为一致性检测的阈值。

9. 如权利要求 7 所述的装置，其特征在于，

当 $N = 1$ 时，该簇 L_1 为安全的定位信息集，计算位置信息，算法结束；

当 $N \geqslant 2$ 时根据所述 N 个簇计算 N 个不同的定位结果 (x_i, y_i)，其中，$i = 1, 2 \ldots\ldots N$，N 为正整数。

10. 如权利要求 9 所在的装置，其特征在于，所述验证模块从所述邻居节点信息集 L^* 中随机取出一个定位信息 $l = (x_i, y_i, d_i)$ 进行测试，所述测试包括：

所述验证模块根据所述定位结果 (x_i, y_i)，计算 $u_i = |d_i - d_p|$，其中

$d_i=\sqrt{(x-x_i)^2+(y-y_i)^2}$,$d_p=\sqrt{(x-x_p)^2+(y-y_p)^2}$ ，i ＝ 1,2.....N,

对所述计算得到的 u_i 进行比较，得到当 i ＝ q 时，u_i 取最小值，则 (x_q, y_q) 为安全定位结果。

一种抗多数合谋攻击的无线传感器安全定位方法及装置

技术领域

[0001] 本发明涉及网络信息安全领域，具体而言，本发明涉及一种抗多数合谋攻击的无线传感器安全定位方法及装置。

背景技术

[0002] 无线传感器网络是由部署在监测区域内大量的廉价微型传感器节点组成，通过无线通信方式形成的一个多跳自组织网络。无线传感器网络是一种全新的信息获取平台，能够实时监测和采集网络分布区域内的各种检测对象的信息，并将这些信息发送到网关节点，以实现复杂的指定范围内目标检测与跟踪，具有快速展开、抗毁性强等特点，有着广阔的应用前景。

[0003] 目前的大多数无线传感器网络节点安全定位机制研究分为基于测距安全定位和无需测距安全定位两类。在基于测距安全定位，现有的典型安全定位系统如基于距离界定协议的VM(Verifiable Multilateration)机制，借助授权节点和若干信标节点协作实现对未知节点定位以及结果验证。此外，还包括SLS(Secure Localization Scheme)方案以及SLA(Secure Localization Algorithm)方案。无需测距安全定位机制，目前已知的SeRLoc协议，它是一种完全分布式、局部化的安全定位协议，通过质心算法计算坐标。此外，还包括有ROPE(Robust Position Estimation)协议、HiRLoc协议是SeRLoc进一步的改进协议。以及适用于高密度随机传感器网络的PLV(Probabilistic LocationVerification)算法。

[0004] 但是，通过研究发现以上算法尚存在以下几个问题需要解决，包括：

[0005] (1)需要具有特定的定向天线，成本较高；

[0006] (2)计算复杂度、通信开销较高不适合于低成本的传感器网络；

[0007] (3)对于恶意节点超过半数以上的合谋攻击无效。

发明内容

[0008] 本发明的目的旨在至少解决上述技术缺陷之一，特别针对解决恶意节点超过半数以上的合谋攻击，获得高精度的定位结果，提出了一种抗多数合谋攻击的无线传感器安全定位方法及装置。

[0009] 为实现上述目的，本发明的实施例的一个方面提出了一种抗多数合谋攻击的无线传感器安全定位方法，包括如下步骤：

[0010] 待定位节点向其通信范围内的信标节点发送定位请求，接收所述信标节点返回的定位信息；

[0011] 所述待定位节点根据所述定位信息生成定位信息集L，利用分簇算法得到N个定位结果；

[0012] 所述待定位节点向其通信范围内的已定位非信标邻居节点发送验证请求，接收所述已定位非信标邻居节点返回的验证信息，将所述验证信息和所述N个定位结果进行验证，得到安全结果。

[0013] 本发明的实施例的另一方面提出了一种抗多数合谋攻击的无线传感器安全定位装置，该安全定位装置位于待定位节点上，包括接收模块、分簇模块和验证模块，

[0014] 所述接收模块，用于向所述待定位节点的通信范围内的信标节点发送定位请求，接收所述信标节点返回的定位信息；

[0015] 所述分簇模块，用于根据所述定位信息生成定位信息集 L，利用分簇算法得到 N 个定位结果；

[0016] 所述验证模块，用于向所述待定位节点的通信范围内的已定位非信标邻居节点发送验证请求，接收所述已定位非信标邻居节点返回的验证信息，将所述验证信息和所述 N 个定位结果进行验证，得到安全结果。

[0017] 根据本发明实施例的方法及装置，不需要使用定向天线特殊设备，通过一致性检测和安全验证技术，使得节点定位过程中，发生恶意节点超过半数以上的合谋攻击时定位算法可以检测到被攻击的信标节点，并移除受攻击信标节点发送的恶意信息。最终能够获得高精度的定位结果。从而可以使定位算法有效适应各种不安全的应用环境，使定位过程具备抗多数合谋攻击的能力。

[0018] 本发明提出的上述方案，对现有系统的改动很小，不会影响系统的兼容性，而且实现简单、高效。

[0019] 本发明附加的方面和优点将在下面的描述中部分给出，部分将从下面的描述中变得明显，或通过本发明的实践了解到。

附图说明

[0020] 本发明上述的和 / 或附加的方面和优点从下面结合附图对实施例的描述中将变得明显和容易理解，其中：

[0021] 图 1 为根据本发明实施例的安全定位方法的流程框图；

[0022] 图 2 为根据本发明实施的安全定位方法的算法示意图；

[0023] 图 3 为根据本发明实施例的待定位节点与信标节点进行安全定位的示意图；

[0024] 图 4 为根据本发明实施例的安全定位装置的结构框图；

[0025] 图 5 为恶意攻击节点数和定位误差关系示意图；

[0026] 图 6 为恶意攻击节点数和恶意节点检测率关系示意图。

具体实施方式

[0027] 下面详细描述本发明的实施例，所述实施例的示例在附图中示出，其中自始至终相同或类似的标号表示相同或类似的元件或具有相同或类似功能的元件。下面通过参考附图描述的实施例是示例性的，仅用于解释本发明，而不能解释为对本发明的限制。

[0028] 为实现本发明之目的，本发明实施例公开了一种抗多数合谋攻击的无线传感器安全定位方法，图 1 示出了该安全定位方法的流程框图。如图 1 中所示，该方法包括如下步骤：

[0029] S101：待定位节点向其通信范围内的信标节点发送定位请求，接收所述信标节点返回的定位信息。

[0030] 结合图 2 所示，待定位节点 S 利用基于测距的定位算法，向其通信范围内的信标节

点，即信标节点发出定位请求。信标节点 i 收到上述定位请求后，向待定位节点 S 返回其自身的位置信息 (x_i, y_i)，d_i 为该信标节点到 S 的距离。

[0031] 优选的，d_i 可以同 RSSI(Received Signal Strength Indication，接收的信号强度指示）获取，亦可以通过 TOA 获取

[0032] 由此，待定位节点 S 获得一个由多个三元组 (x_i, y_i, d_i) 组成的定位信息集 L。

[0033] 其中，(x_i, y_i) 为每个信标节点本身的坐标；d_i 为信标节点到待定位节点 S 之间的距离。

[0034] S102：待定位节点根据所述定位信息生成定位信息集 L，利用分簇算法 N 个簇，根据所述 N 个簇计算得到 N 个定位结果。

[0035] A1：根据步骤 101 中得到的定位信息集 L，利用蒙特卡罗方法从 L 中随机抽取 K 个元素形成集合 L_1，对到集合 L_1 进行一致性检测，直到集合 L_1 通过一致性检测结束。其中，$K \geqslant 3$。

[0036] A2：从剩余的 $L-L_1$ 中取出元素 (x_i, y_i, d_i) 放入 L_1 中，对 L_1 做一致性检测。

[0037] 若满足一致性检测条件则将元素 (x_i, y_i, d_i) 取出 L_1，放入 L_3；若不满足则将元素 (x_i, y_i, d_i) 取出 L_1，放入 L_2。直到 L 中所有剩余元素取完。将 L_3 元素并入 L_1 中，若 L_1 不满足一致性检测则转到 A1。

[0038] 上述一致性检测方法包括如下步骤：待定位节点获得的定位信息集合 $L = \{(x_1, y_1, d_1) \ldots (x_i, y_i, d_i) \ldots (x_N, y_N, d_N)\}$。通过极大似然估计算法求出待定位节点坐标$(\tilde{x}_s, \tilde{y}_s)$，此时该次估计的均方差为

[0039] $$\delta^2 = \frac{1}{|L|}\sum_{i=1}^{|L|}\left(d_i - \sqrt{(x_i - \tilde{x}_s)^2 + (y_i - \tilde{y}_s)^2}\right)^2 \quad 。$$

[0040] 当均方差 $\delta^2 < \tau$ 时，则表示 L 满足一致性检测条件，通过一致性检测。其中，τ 为一致性检测的阈值。

[0041] 最大似然估计算法对局外点特别敏感，单个干扰数据就足以导致参数估计严重偏差。因此估计均方差增大，说明计算结果精度较低，信息集 L 不一致；当计算精度精确时，均方差较小，信息集 L 一致。当均方差 δ^2 小于阈值 τ 时，我们称集合 L 通过一致性检验。

[0042] A3：对 L_2 进行一致性检测。

[0043] 当 $|L_2| < 3$ 时：生成一个新簇 L_1，执行步骤 A2，即 L_2 中的信标节点数量小于 3 时，生成一个新簇 L_1；

[0044] 当 $|L_2| \geqslant 3$ 时：即 L_2 中的信标节点数量大于 3 时，对 L_2 做一致性检测，若 L_2 满足一致性检测条件，生成一个新簇 L_2，执行步骤 A2；否则 L_2 算法执行步骤 A1，对 L_2 执行分簇算法，继续分簇。

[0045] A4：当生成新簇 L_N 时，可以得到 N 个定位结果。

[0046] 生成新簇 L_1 至 L_N，由于每个簇中的定位信息均满足一致性，因此在每个簇上执行最大似然估计定位计算，可以得到一个定位结果，即 N 个定位结果。具体的说，以由三元组 (x_i, y_i, d_i) 组成的定位信息集 Li 例，利用最大似然估计定位计算该节点的位置，定位算法表征下：

[0047] $$(\tilde{x}_s,\tilde{y}_s)=\arg\min_{(x_s,y_s)}\sum_{i=1}^{n}\left(d_i-\sqrt{(x_i-x_s)^2+(y_i-y_s)^2}\right)^2,$$

[0048] 该方法使用使等式右边的求和表达式值最小的两元组作为待定位节点坐标 (x, y),即定位结果。由此,分别对 N 个簇的信息集进行最大似然估计,得到 N 个定位结果。

[0049] 当 N = 1 时,则该簇作为唯一的簇,是安全的定位信息集,计算位置信息,算法结束。

[0050] 当 N ≥ 2 时,说明发生了合谋攻击,根据 N 个簇计算得到 N 个不同的定位结果 (x_i, y_i),对其做进一步检测,其中,i = 1,2.....N,N 为正整数。

[0051] 分簇算法可以用于检测并处理独立攻击。对于少数和多数合谋攻击分簇算法检测出后,执行安全验证方法找出安全定位结果,解决许多算法无法解决的多数合谋攻击。

[0052] 分簇方法可以将定位信息集 L 分成若干个满足一致性的子集。由一致性检测定义可以得出定位信息集合越大,计算消耗越大。设计出一种复杂度低的分簇方法用以降低整体的复杂度。

[0053] S103 :待定位节点向其通信范围内的已定位非信标邻居节点发送定位验证请求,接收已定位非信标邻居节点返回的定位验证信息,将定位验证信息和 N 个定位结果进行定位验证,得到安全定位结果。

[0054] 具体的说,利用距离和和位置的约束性可以验证定位结果的安全性。待定位的节点 S 通信范围内存在某个已经安全定位的节点。待定位节点 S 发送定位验证请求给该已定位非信标邻居节点的邻居节点 S_p。S_p 节点在收到定位验证请求后,向待定位节点发送定位验证信息。当通过第一步分簇结束后,生成簇的数量大于或等于 2 时,即 N ≥ 2。此时,待定位 S 节点检测出合谋攻击。

[0055] 根据 N 个不同的簇,获得 N 个不同的定位结果 (x_i, y_i),其中,i = 1,2.....N,N 为正整数。S 节点可以向这些邻居节点 S_p 请求验证,从而找到安全定位结果。其验证过程如下 :

[0056] S 节点向 S_p 节点发送验证请求,S 收到已经定位的邻居节点信息集 L^*,随机取出一个定位信息 p = (x_p, y_p, d_p)。其中,(x_p, y_p) 为 S_p 节点的坐标,d_p 为 S_p 到 S 节点的距离。

[0057] 根据所述定位结果 (x_i, y_i) 以及 d_p,计算 $u_i = |d_i - d_p|$,其中 $d_i=\sqrt{(x-x_i)^2+(y-y_i)^2}$,$d_p=\sqrt{(x-x_p)^2+(y-y_p)^2}$,i = 1,2.....N。对所述计算得到的 u_i 进行比较,得到当 i = q 时,u_i 取最小值,则 (x_q, y_q) 为安全定位结果。

[0058] 下面以 N = 2 为例对本实施例进行详细说明。即当两个信息簇时,计算安全定位结果。根据两个不同的信息簇 L_A 和 L_B,S 节点可以计算得到两个不同的坐标 (x_1, y_1) 和 (x_2, y_2),S 节点可以向这些邻居节点 S_p 请求验证,从而找到正确的定位坐标。其验证过程如下 :

[0059] (1)S 节点向 S_p 节点发送验证请求,S 收到已经定位的邻居节点信息集 L^*,随机取出一个定位信息 p = (x_p, y_p, d_p)。其中,(x_p, y_p) 为 S_p 节点的坐标,d_p 为 S_p 到 S 节点的距离。

[0060] (2)S 节点分别使用坐标 (x_1, y_1),(x_2, y_2) 与 S_p 坐标计算 S 和 S_p 之间的计算距离 d_1 和 d_2。

[0061] 根据上述定位信息进行测试 :$u = |d_1 - d_p| - |d_2 - d_p|$,其中 $d_1=\sqrt{(x-x_1)^2+(y-y_1)^2}$

$d_2=\sqrt{(x-x_2)^2+(y-y_2)^2}$,$d_p=\sqrt{(x-x_p)^2+(y-y_p)^2}$

[0062] (3) 通过计算比较 $|d_1-d_p|$ 和 $|d_2-d_p|$，其中值较小的式子所代表的节点坐标为正确坐标。

[0063] 当 u ＜ 0 时，表示 (x1，y1) 为安全结果；

[0064] 当 u ≥ 0 时，表示 (x2，y2) 为安全结果。

[0065] 安全验证方法主要用于生成的所有信息簇中寻找安全信息簇，计算得到正确的定位结果。

[0066] 图 3 为待定位节点与信标节点进行安全定位的示意图。如图 3 中所示，中心的三角形标识为待定位节点，实心圆点为正常信标节点，空心圆点为受攻击信标节点。待定位节点向其通信范围内的信标节点发送定位请求，包括正常信标节点和受攻击信标节点。上述信标节点接收到定位请求后，向待定位节点返回定位信息。待定位节点收到所有定位信息三元组后，启动安全定位算法。首先进行分簇算法，若在分簇算法中检测出独立攻击那么直接处理并获得正确定位结果。图 3 示出的安全定位过程为发生少数合谋攻击的情况。若在分簇算法中检测出合谋攻击则启动安全验证方法处理合谋攻击。

[0067] 根据本发明实施例提供的方法不需要使用定向天线特殊设备，通过一致性检测和安全验证技术，使得节点定位过程中，发生恶意节点超过半数以上的合谋攻击时定位算法可以检测到被攻击的信标节点，并移除受攻击信标节点发送的恶意信息，最终能够获得高精度的定位结果。从而可以使定位算法有效适应各种不安全的应用环境，使定位过程具备抗多数合谋攻击的能力。

[0068] 本发明实施例还公开了一种抗多数合谋攻击的无线传感器安全定位装置，结合图 4 所示，该安全定位装置 400 位于待定位节点上，包括接收模块 410、分簇模块 420 和验证模块 430。

[0069] 接收模块 410，用于向待定位节点的通信范围内的信标节点发送定位请求，接收所述信标节点返回的定位信息。

[0070] 具体的说，结合图 2 所示，接收模块 410 利用基于测距的定位算法，向待定位节点通信范围内的信标节点，即信标节点发出定位请求。信标节点 i 收到上述定位请求后，向接收模块 410 返回其自身的位置信息 (x_i, y_i)，d_i 为该信标节点到 S 的距离。

[0071] 优选的，d_i 可以同 RSSI(Received Signal Strength Indication，接收的信号强度指示）获取，亦可以通过 TOA 获取

[0072] 由此，接收模块 410 获得一个由三元组 (x_i, y_i, d_i) 组成的定位信息集 L。

[0073] 其中，(x_i, y_i) 为每个信标节点本身的坐标；d_i 为信标节点到待定位节点 S 之间的距离。

[0074] 根据步接收模块 410 中得到的定位信息集 L，采用分簇模块 420 对 L 进行分簇，得到 N 个定位结果。具体包括：

[0075] A1：分簇模块 420 利用蒙特卡罗方法从 L 中随机抽取 K 个元素形成集合 L_1，对到集合 L_1 进行一致性检测，直到集合 L_1 通过一致性检测结束。其中，K ≥ 3。

[0076] A2：分簇模块 420 从剩余的 $L-L_1$ 中取出元素 (x_i, y_i, d_i) 放入 L_1 中，对 L_1 做一致性检测。

[0077] 若满足一致性检测条件则将元素 (x_i, y_i, d_i) 取出 L_1，放入 L_3；若不满足则将元素 (x_i, y_i, d_i) 取出 L_1，放入 L_2。直到 L 中所有剩余元素取完。将 L_3 元素并入 L_1 中，若 L_1 不满足一致性检测则转到 A1。

[0078] 分簇模块 420 进行一致性检测，主要包括：将接收模块 410 获得的定位信息集合 $L = \{(x_1, y_1, d_1)\ldots(x_i, y_i, d_i)\ldots(x_N, y_N, d_N)\}$。通过极大似然估计算法求出待定位节点坐标 $(\tilde{x}_s, \tilde{y}_s)$，此时该次估计的均方差为

[0079] $$\delta^2 = \frac{1}{|L|}\sum_{i=1}^{|L|}\left(d_i - \sqrt{(x_i - \tilde{x}_s)^2 + (y_i - \tilde{y}_s)^2}\right)^2 \quad 。$$

[0080] 当均方差 $\delta^2 < \tau$ 时，则表示 L 满足一致性检测条件，通过一致性检测。其中，τ 为一致性检测的阈值。

[0081] 最大似然估计算法对局外点特别敏感，单个干扰数据就足以导致参数估计严重偏差。因此估计均方差增大，说明计算结果精度较低，信息集 L 不一致；当计算精度精确时，均方差较小，信息集 L 一致。当均方差 δ^2 小于阈值 τ 时，我们称集合 L 通过一致性检验。

[0082] A3：分簇模块 420 对 L_2 进行一致性检测。

[0083] 当 $|L_2| < 3$ 时：生成一个新簇 L_1，分簇模块 420 执行步骤 A2，即 L_2 中的信标节点数量小于 3 时，生成一个新簇 L_1；

[0084] 当 $|L_2| \geq 3$ 时：即 L_2 中的信标节点数量大于 3 时，对 L_2 做一致性检测，若 L_2 满足一致性检测条件，分簇模块 420 生成一个新簇 L_2，执行步骤 A2；否则 L_2 算法执行步骤 A1，分簇模块 420 对 L_2 执行分簇算法，继续分簇。

[0085] A4：当生成新簇 L_N 时，可以得到 N 个定位结果。

[0086] 生成新簇 L_1 至 L_N，由于每个簇中的定位信息均满足一致性，因此在每个簇上执行最大似然估计定位计算，可以得到一个定位结果，即 N 个定位结果。具体的说，以由三元组 (x_i, y_i, d_i) 组成的定位信息集 L_i 例，利用最大似然估计定位计算该节点的位置，定位算法表征下：

[0087] $$(\tilde{x}_s, \tilde{y}_s) = \arg\min_{(x_s, y_s)} \sum_{i=1}^{n}\left(d_i - \sqrt{(x_i - x_s)^2 + (y_i - y_s)^2}\right)^2 ,$$

[0088] 该方法使用使等式右边的求和表达式值最小的两元组作为待定位节点坐标 (x, y)，即定位结果。由此，分别对 N 个簇的信息集进行最大似然估计，得到 N 个定位结果。

[0089] 当 $N = 1$ 时，则该簇作为唯一的簇，是安全的定位信息集，计算位置信息，算法结束。

[0090] 当 $N \geq 2$ 时，说明发生了合谋攻击，根据 N 个簇计算得到 N 个不同的定位结果 (x_i, y_i)，对其做进一步检测，其中，$i = 1, 2.....N$，N 为正整数。

[0091] 分簇算法可以用于检测并处理独立攻击和少数合谋攻击。对于多数合谋攻击分簇算法检测出后，执行安全验证方法找出安全定位结果，解决许多算法无法解决的多数合谋攻击。

[0092] 分簇模块 420 可以将定位信息集 L 分成若干个满足一致性的子集。由一致性检测定义可以得出定位信息集合越大，计算消耗越大。设计出一种复杂度低的分簇方法用以降低整体的复杂度。

[0093] 安全定位装置 400 还包括验证模块 430，用于向待定位节点的通信范围内的已定位非信标邻居节点发送定位验证请求，接收已定位非信标邻居节点返回的定位验证信息，将验证信息和所述 N 个定位结果进行定位验证，得到安全定位结果。

[0094] 具体的说，利用距离和和位置的约束性可以验证定位结果的安全性。待定位的节点 S 通信范围内存在某个已经安全定位的节点。验证模块 430 发送定位验证请求给该已定位非信标邻居节点的邻居节点 S_p。S_p 节点在收到定位验证请求后，向验证模块 430 发送定位验证信息。当通过第一步分簇结束后，生成簇的数量大于或等于 2 时，即 $N \geq 2$。此时，待定位 S 节点检测出合谋攻击。

[0095] 根据 N 个不同的簇，获得 N 个不同的定位结果 (x_i, y_i)，其中，$i = 1,2.....N$，N 为正整数。S 节点可以向这些邻居节点 S_p 请求验证，从而找到安全定位结果。其验证过程如下：

[0096] S 节点向 S_p 节点发送验证请求，S 收到已经定位的邻居节点信息集 L^*，随机取出一个定位信息 $p = (x_p, y_p, d_p)$。其中，(x_p, y_p) 为 S_p 节点的坐标，d_p 为 S_p 到 S 节点的距离。

[0097] 根据所述定位结果 (x_i, y_i) 以及 d_p，计算 $u_i = |d_i - d_p|$，其中 $d_i = \sqrt{(x-x_i)^2+(y-y_i)^2}$，$d_p = \sqrt{(x-x_p)^2+(y-y_p)^2}$，$i = 1,2.....N$。对所述计算得到的 u_i 进行比较，得到当 $i = q$ 时，u_i 取最小值，则 (x_q, y_q) 为安全定位结果。

[0098] 下面以 $N = 2$ 为例对本实施例进行详细说明。即当两个信息簇时，计算安全定位结果。根据两个不同的信息簇 L_A 和 L_B，验证模块 430 可以计算得到两个不同的坐标 (x_1, y_1) 和 (x_2, y_2)，验证模块 430 可以向这些邻居节点 S_p 请求验证，从而找到正确的定位坐标。其验证过程如下：

[0099] 验证模块 430 向 S_p 节点发送定位验证请求，验证模块 430 收到已经定位的邻居节点信息集 L^*，随机取出一个定位信息 $p = (x_p, y_p, d_p)$。其中，(x_p, y_p) 为 S_p 节点的坐标，d_p 为 S_p 到 S 节点的距离。

[0100] 验证模块 430 分别使用坐标 (x_1, y_1)，(x_2, y_2) 与 S_p 坐标计算 S 和 S_p 之间的计算距离 d_1 和 d_2。

[0101] 验证模块 430 根据上述定位信息进行测试：$u = |d_1 - d_p| - |d_2 - d_p|$，其中 $d_1 = \sqrt{(x-x_1)^2+(y-y_1)^2}$ $d_2 = \sqrt{(x-x_2)^2+(y-y_2)^2}$，$d_p = \sqrt{(x-x_p)^2+(y-y_p)^2}$

[0102] 验证模块 430 通过计算比较 $|d_1 - d_p|$ 和 $|d_2 - d_p|$，其中值较小的式子所代表的节点坐标为正确坐标。

[0103] 当 $u < 0$ 时，表示 (x1, y1) 为安全结果；

[0104] 当 $u \geq 0$ 时，表示 (x2, y2) 为安全结果。

[0105] 验证模块 430 主要用于生成的所有信息簇中寻找安全信息簇，计算得到正确的定位结果。

[0106] 下面结合图 5 和图 6，说明不同攻击强度下不同算法对定位误差的影响。在本实施例中，在 30m*30m 的区域内，通信半径为 $R = 15m$，测距误差 ε 服从均匀分布。设定测距误差为通信半径的 5%，最大测距误差 $\varepsilon_1 = 0.818m$。信标节点数共 14 个，一个待定位节点，一个已定位节点。

[0107] 其中图 5 和图 6 中示出的算法包括本发明实施例提出的 ETMCA(EnhancedTolerate

Majority-Colluding Attacks) 算法以及 LMS-scheme(Least Median ofSquares scheme) 算法、EARMMSE(Enhanced Attack-Resistant Minimum MeanSquare Estimation) 算法、CMMSE(Minimum Mean Square Estimation) 算法、QMMCE(Quick Minimum Mean Square Estimation) 算法。

[0108] 在这种部署方式下，使用不同的恶意信标数，数量从 3 个到 11 个，共有 14 个信标，发动合谋攻击，攻击强度固定。

[0109] 在这些攻击模型下，研究了不同的攻击强度对上述算法定位误差的影响，以及对算法合谋攻击的检测效率。上述攻击强度是指攻击时加入的错误值。在试验中我们设定攻击强度从 3m-30m，步长为 3。为了避免偶然性，所有的试验数据取均值。

[0110] 如图 5 所示，攻击强度为 27m 且不变的情况下，定位误差和参与合谋攻击的信标节点数的关系：随着攻击节点数增加定位误差也越来越大，在攻击节点数在 6 个以内时除了 LMS 算法其余算法的误差都稳定在一定值范围内。当攻击节点数超过 8 以后，除了 ETMCA 算法其余的算法均已失效。当攻击数从 8 到 10 的过程中误差只有微小上升。当攻击节点数增至 11 后，正常节点只有 3 个因此很容易导致误判为独立攻击，由于攻击强度很大因此产生较大误差。

[0111] 如图 6 所示，在攻击强度为 27m 且不变的情况下，合谋攻击检测率和参与合谋攻击的信标节点数的关系。随着攻击节点数增加，ETMCA 算法的检测率一直在 95％浮动。当恶意节点数较少或较多的情况下，由于测距误差的存在会导致误判为独立攻击，因此检测率曲线中间较高，两边较低。而对于其他算法在攻击节点数为 7 或 8 时检测率骤降为 0。

[0112] 根据本发明实施例提供的安全定位方法及装置不需要使用定向天线特殊设备，通过一致性检测和安全验证技术，使得节点定位过程中，发生恶意节点超过半数以上的合谋攻击时定位算法可以检测到被攻击的信标节点，并移除受攻击信标节点发送的恶意信息，最终能够获得高精度的定位结果。从而可以使定位算法有效适应各种不安全的应用环境，使定位过程具备抗多数合谋攻击的能力。

[0113] 本领域普通技术人员可以理解实现上述实施例方法携带的全部或部分步骤是可以通过程序来指令相关的硬件完成，所述的程序可以存储于一种计算机可读存储介质中，该程序在执行时，包括方法实施例的步骤之一或其组合。

[0114] 另外，在本发明各个实施例中的各功能单元可以集成在一个处理模块中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个模块中。上述集成的模块既可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。所述集成的模块如果以软件功能模块的形式实现并作为独立的产品销售或使用时，也可以存储在一个计算机可读取存储介质中。

[0115] 上述提到的存储介质可以是只读存储器，磁盘或光盘等。

[0116] 以上所述仅是本发明的优选实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本发明原理的前提下，还可以做出若干改进和润饰，这些改进和润饰也应视为本发明的保护范围。

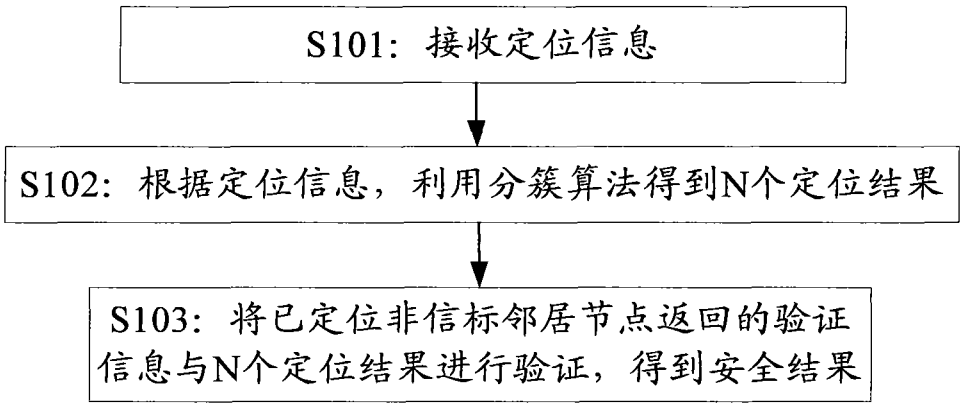

S101：接收定位信息
S102：根据定位信息，利用分簇算法得到N个定位结果
S103：将已定位非信标邻居节点返回的验证信息与N个定位结果进行验证，得到安全结果

图 1

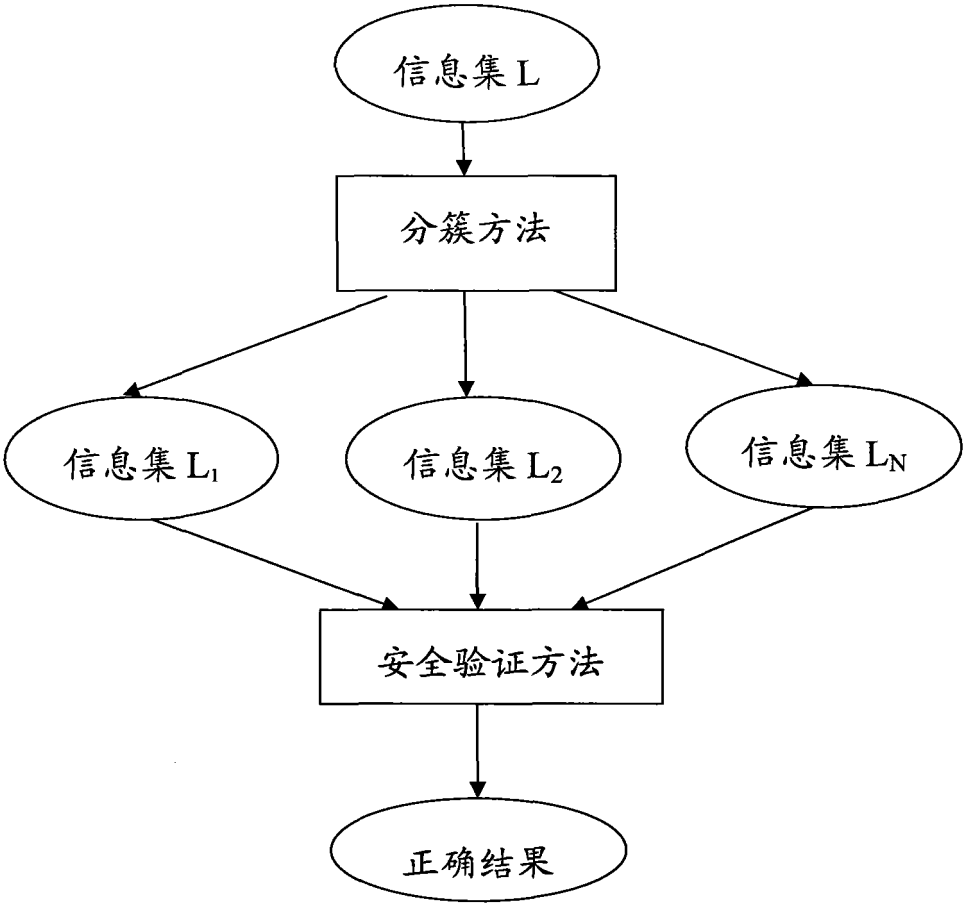

信息集 L
分簇方法
信息集 L_1
信息集 L_2
信息集 L_N
安全验证方法
正确结果

图 2

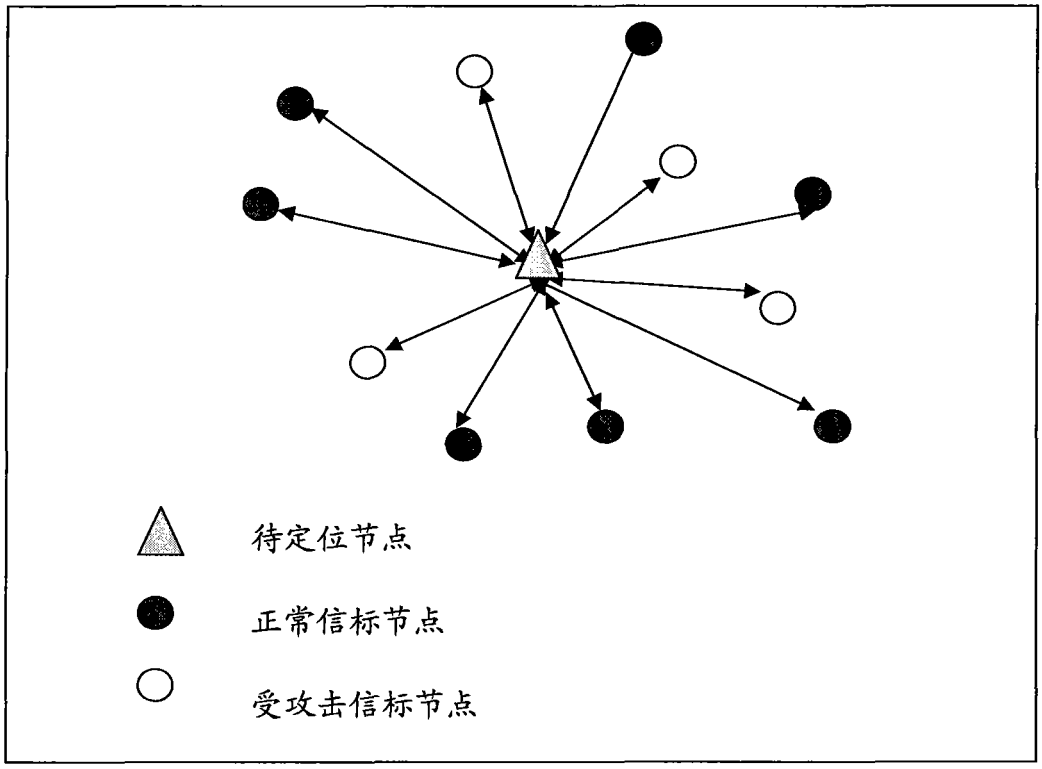


图 3

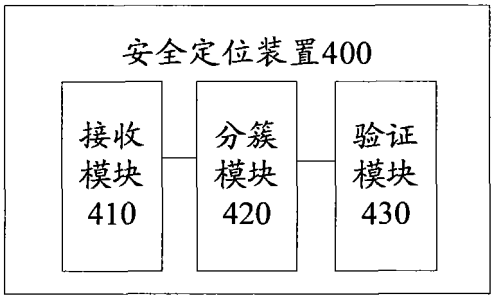


图 4

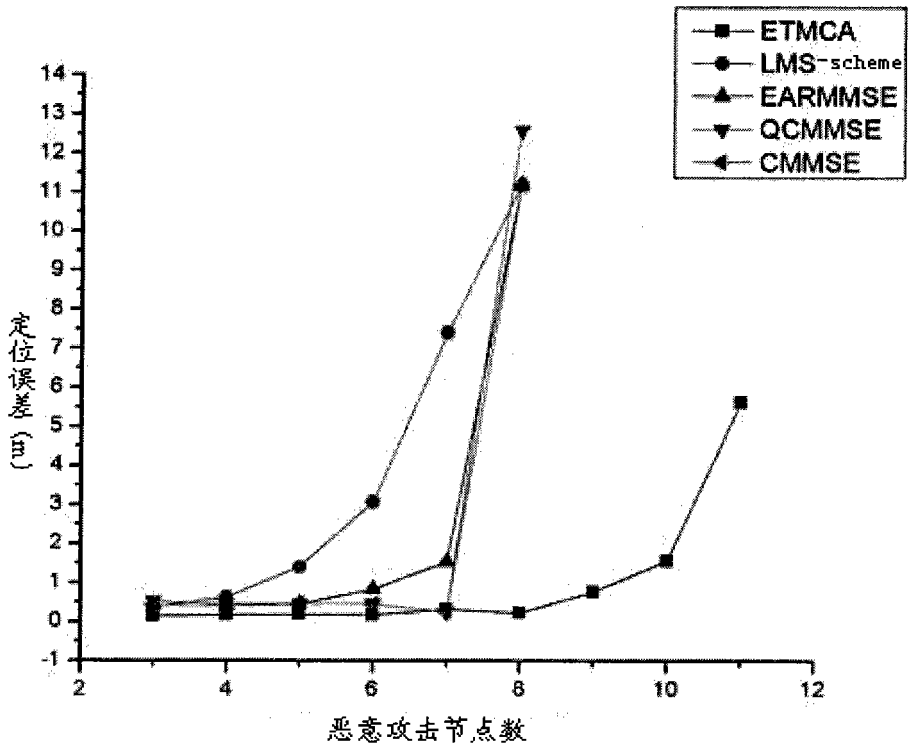

ETMCA
LMS-scheme
EARMMSE
QCMMSE
CMMSE
定位误差(m)
恶意攻击节点数

图 5

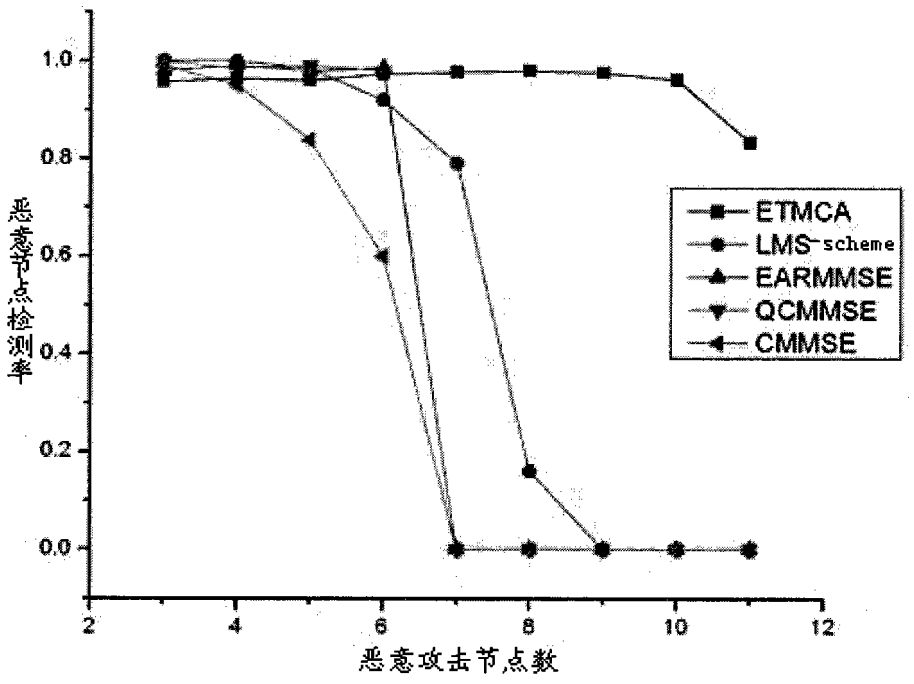

ETMCA
LMS-scheme
EARMMSE
QCMMSE
CMMSE
恶意节点检测率
恶意攻击节点数

图 6