(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 104219661 A
(43)申请公布日 2014.12.17

(21)申请号 201410440553.9

(22)申请日 2014.09.01

(71)申请人 北京邮电大学
地址 100876 北京市海淀区西土城路 10 号
申请人 无锡北邮感知技术产业研究院有限公司

(72)发明人 芦效峰 鲁鹏 李睿凡 李蕾 袁彩霞 刘咏彬 曲昭伟 李晖

(51)Int.Cl.
H04W 12/02(2009.01)
H04W 40/02(2009.01)

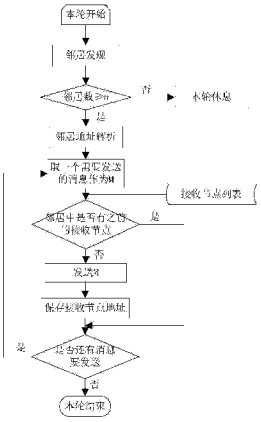
权利要求书1页 说明书6页 附图2页

(54)发明名称

抗 TDOA 定位追踪的源位置隐私保护路由方法

(57)摘要

本发明公开了一种抗 TDOA 定位追踪的源位置隐私保护路由方法，包括：源节点将一个完整的信息加密后分成 k-1 个信息分段，并把解密密钥包含在第 k 个分段中。源节点和转发节点在发送某信息分段时首先检测其邻居节点数量，如果邻居节点数量少于参数 n，则不发送信息分段，否则检测当前的邻居节点中是否有节点是之前该信息的其他分段的接收节点，如果当前邻居节点中有节点是之前该信息的其他分段的接收节点，则不发送当前信息分段，否则发送该信息分段。根据本发明的方法，当源节点在发送最后一个信息分段时，即使有攻击节点伪装成普通节点收到了最后一个分段，如果它没有接收到前面全部的 k-1 个信息分段，攻击节点也不会对源节点进行定位追踪，从而提高了源节点的抗定位能力，保护了源节点的位置隐私。



CN 104219661 A

1. 抗 TDOA 定位追踪的源位置隐私保护路由方法，其特征在于消息生成时包括有下列处理步骤：

步骤一、源节点初始化参数 n 和 k。源节点统计一段时间内平均连接节点个数 x，如果 $x \leqslant 2$，则设置 $n = 2$，否则设置 $n = x$；之后确定参数 k：如果 $n \geqslant 4$，则 $k = 3$；否则 $k = 2$；

步骤二、源节点将原始信息加密，密钥由源节点随机生成，加密算法为节点内置的加密算法，然后把加密后信息分成 k-1 段，把解密密钥保存在第 k 个信息分段中，第 k 个信息分段不加密。

步骤三、开始消息转发，转发消息节点 N_i 每隔时间 T 周期性地检测其周围连接节点数 x；

步骤四、当节点 N_i 周围连接节点数 x 大于等于 n 时，节点 N_i 根据消息 M 的历史接收节点和当前连接节点判断是否可以转发消息 M，判断依据是：当前的连接节点和 M 的历史接收节点集合之间没有交集则可以转发。

2. 根据权利要求 1 所述的抗 TDOA 定位追踪的源位置隐私保护路由方法，其特征在于：将原始信息加密后分为 k 段分别发送给不同的接收节点。

3. 根据权利要求 1 所述的抗 TDOA 定位追踪的源位置隐私保护路由方法，其特征在于：当连接节点数数大于等于阈值 n 时才发送消息。

4. 根据权利要求 1 所述的抗 TDOA 定位追踪的源位置隐私保护路由方法，其特征在于：参数 n 和 k 都是根据平均连接节点个数情况而设置的。

5. 根据权利要求 1 所述的抗 TDOA 定位追踪的源位置隐私保护路由方法，其特征在于：原始信息的解密密钥放在最后一个分段中，并且不加密。

6. 根据权利要求 1 所述的抗 TDOA 定位追踪的源位置隐私保护路由方法，其特征在于：源节点将信息 M 的目标 IP 地址设置为广播地址，目标 MAC 地 址设置为目标节点的 MAC 地址。

7. 根据权利要求 1 所述的抗 TDOA 定位追踪的源位置隐私保护路由方法，其特征在于：源节点为信息生成信息识别码 ID_M，信息的 k 个分段具有一样的信息识别码 ID_M。

8. 抗 TDOA 定位追踪的源位置隐私保护路由方法，其特征在于接收节点接收信息时包括有下列处理步骤：接收节点收到 HeartBeat 心跳信号后发送 HeartBeat 心跳信号，如果发送节点发送消息 M，接收节点则接收消息 M，之后接收节点检查信息 M 的目标 MAC 地址，如果目标 MAC 地址是接收节点的 MAC 地址，节点将该信息提交该上层应用协议处理，该消息不再转发；否则把 M 保存在存储单元中，提取 M 的信息识别码 ID_M，建立空集合 $List_{history}(ID\_M)$。

9. 根据权利要求 8 所述的抗 TDOA 定位追踪的源位置隐私保护路由方法，其特征在于：接收节点提取接收到的信息 M 的信息识别码 ID_M，根据信息识别码 ID_M 建立一个 $List_{history}(ID\_M)$ 集合，$List_{history}(ID\_M)$ 保存消息 ID_M 的全部接收节点。

抗 TDOA 定位追踪的源位置隐私保护路由方法

技术领域

[0001] 本发明涉及一种网络路由技术领域，更特别地说，是指一种基于消息分段和限定转发实现抗 TDOA 定位追踪的源节点位置隐私保护方法。

背景技术

[0002] MANET(mobile ad hoc net) 是由可移动无线节点组成的能够进行相互通信的无线自组织网络。该网络常常用于环境监测、灾难恢复、幸存者搜救等无法使用有线网络或是有线网络难以发挥作用的环境中。在无线通信中，由于信号在共享的通信介质中传播，电磁信号不可避免地能够被非目标节点接收。在一些情况下，这些非目标节点中存在攻击者，攻击者可能对源节点造成危害和伤害。一方面，攻击者希望获取源节点发送的内容，另一方面，攻击者也希望得到源节点的位置，从而直接捕获或破坏源节点。

[0003] 例如，在战术环境下由车辆所携带的无线电台组成的无线自组织网络中，节点通信的安全性和隐蔽性是至关重要的。但是，由于无线通讯采用共享通信介质的方式通信，使得无线信号很容易被其他无线接收装置所接收，如果这些无线接收装置被攻击者使用，则会给发送节点，乃至整个网络带来巨大的安全问题。一旦攻击者发现并识别了发送节点的有用信号，则可以窃听通信内容，此外，攻击者更可以对源节点发起定位攻击，即通过定位算法获得发送节点的位置。获得发送节点的位置后，攻击者既可以通过无线电方式干扰其正常通信，也可以直接捕获和破坏发送节点。

[0004] 本发明针对无线网络中存在普通节点和攻击节点情况，攻击节点伪装成普通节点，攻击节点不对每个普通节点定位，攻击节点只对发送含有重要或敏感内容的源节点进行 TDOA 定位。

[0005] TDOA 定位方法测量不同的接收节点接收到同一个源节点发出的信号的时间差来计算源节点的位置。根据 TDOA 定位方法，如果有 3 个节点接收到了一个源节点发出的信号，则可以计算出源节点的位置。不同于依靠无线信号强度的 RSSI 定位方法和依靠绝对时间的 TOA 定位方法，时间差是一个健壮的指标，它降低了对发送节点和接收节点时间同步的要求，仅要求接收节点之间时间同步。由于攻击者之间可以实现时间同步，因此攻击者会使用 TDOA 定位方法来发现源节点的位置。

[0006] 现有的防源节点被定位的方法是在无线网络中设置一些欺骗节点，这些用于欺骗攻击者的节点也会发出无线信号。攻击者可以接收到由欺骗节点发出欺骗报文，由于欺骗报文和真实报文完全一致，攻击者无法区别出欺骗节点和真实节点，则攻击者会对欺骗节点定位，从而保护了真实源节点的位置。但是这种方法的缺陷是其只能欺骗攻击者一次，即使部署多个固定的欺骗节点，攻击者可以通过记录这些欺骗节点的位置而不被再次欺骗，因此这种方法不能长期保护源节点的位置隐私。

发明内容

[0007] 本发明目的在于至少解决上述技术缺陷之一。

[0008] 为此，本发明的目的在于提供一种抗 TDOA 定位追踪的源位置隐私保护路由方法。该方法可以提高源节点的抗定位能力，保护源节点的位置隐私。

[0009] 为实现上述目的，本发明采取如下技术方案 ：

[0010] (1) 源节点初始化阶段。源节点将一个完整的信息加密，然后分成 k-1 个信息分段 (segment)，也称分段，并把解密密钥包含在第 k 个分段中，第 k 个信息分段不加密，源节点将每一分段都发给不同的接收节点。只有接到了全部 k 个分段的节点才能先组合前 k-1 个信息分段，然后再使用保存在第 k 个分段中的密钥解密前 k-1 个信息段，得到完整的信息的内容。

[0011] (2) 信息转发阶段。每个节点在发送某信息分段时首先检测其邻居节点数量，如果邻居节点数量少于参数 n，则不发送信息分段 ；如果邻居节点数大于等于 n，则检测当前的邻居节点中是否有节点是之前该信息的其他分段接收节点，如果当前邻居节点中有节点是之前该信息其他分段的接收节点，则不发送当前信息分段。根据本发明的方法，当发送节点在发送最后一个信息分段时，即使有攻击节点伪装成普通节点收到了最后一个分段，如果它没有接收到前面全部的 k-1 个信息分段，攻击节点也不会对源节点进行定位追踪，从而提高了源节点的抗定位能力，保护了源节点的位置隐私。

[0012] 本发明中，攻击节点伪装成普通节点，发送节点无法知道其邻居节点中是否存在着攻击节点 ；攻击节点通过 TDOA 定位方法对源节点定位。

[0013] 本发明中，邻居节点是指两个节点都在双方的通信范围内，可以相互通信的节点。

[0014] 本发明中，普通节点在接收到一个信息分段后，如果该信息分段不是发送给自己的，根据本发明规定的转发条件继续转发该信息分段给其他的普通节点 ；目标节点接收到发送给自己的信息分段后，不再继续转发。

[0015] 本发明中，所有普通节点都有相同的加解密算法，每个源节点在有信息需要发送之前，随机产生一个新的加解密密钥。

[0016] 本发明的抗 TDOA 定位追踪的源位置隐私保护路由方法的优点在于 ：

[0017] (1) 通过将重要信息分段加密后发送的方式，增加了攻击节点解密的难度。如果一个节点接收了前 k-1 个信息分段，而没有接收到包含解密密钥的最后一个分段，该节点无法解密数据的内容 ；同样如果收到最后一个信息分段的节点没有接收前面全部的 k-1 个信息分段，它也无法知道原始信息的内容。由于攻击节点不知道该信息的内容，攻击节点不会对发送节点进行定位。

[0018] (2) 通过检查邻居节点，保证一个信息的不同的信息分段发送给了不同的接收节点，这样增加了一个节点获得全部 k 个信息分段的时间，从而让源节点有时间移动到较远的位置，保证源节点的安全。

[0019] (3) 节点在发送或转发信息时，首先检查邻居节点的数量，当数量小于 n 个节点时不发送信息，通过提高每次广播信息时接收节点的数量使整个参与发送的节点能够使用较少的能量将信息发送到目的地。

附图说明

[0020] 图 1 是本发明源节点初始化工作流程图。

[0021] 图 2 是本发明中源节点和转发节点发送消息的工作流程图。

[0022] 图 3 是本发明中节点接收消息的工作流程图。

具体实施方式

[0023] 下面将结合附图对本发明做进一步的详细说明。本发明包括两个工作阶段，第一阶段是源节点初始化阶段，第二阶段是信息转发阶段。图 1 是本发明源节点初始化的工作流程图，图 2 是本发明中源节点和普通节点发送消息的工作流程图，图 3 是本发明中节点接收消息的工作流程图。

[0024] 本发明的抗 TDOA 定位追踪的源位置隐私保护路由方法针对源节点和转发节点有下列处理步骤：

[0025] 步骤一、源节点初始化参数 n 和 k；

[0026] 步骤二、源节点将一个原始信息加密，分成 k-1 段 (segment)，解密密钥放在第 k 段，第 k 个信息分段不加密；

[0027] 步骤三、开始消息转发，转发信息节点 N_i 每隔时间 T 周期性地检测其周围连接节点数 x；

[0028] 步骤四、当节点 N_i 周围连接节点数 x 大于等于 n 时，节点 N_i 根据消息 M 的历史接收节点和当前连接节点判断是否可以转发消息 M，判断依据是：当前的连接节点和 M 的历史接收节点集合之间没有交集。

[0029] 在本发明中，所述步骤一源节点初始化参数 n 和 k 的具体处理为：

[0030] S 表示产生一个新消息的源节点，N_i 表示普通节点。

[0031] 步骤 101：源节点 S 发送心跳信号 HeartBeat；心跳信号包含节点 S 的 IP 和 MAC 地址。当一个节点收到其他节点的心跳信号时，可以确认存在一个邻居节点及该邻居的地址。

[0032] 步骤 102：节点 S 的邻居节点 N_i 收到 HeartBeat；

[0033] 步骤 103：节点 S 的邻居节点 N_i 产生一个随机退避时间 t，退避时间范围在 1 秒内，节点 N_i 在等待退避时间 t 之后发送一个心跳信号 $HeartBeat_i$ 给节点 S，节点 S 统计在其发出心跳信号 HeartBeat 后 1 秒内接收到的 $HeartBeat_i$ 信号的个数 x，x 就是源节点 S 当前连接的节点个数，简称为连接节点个数；

[0034] 步骤 104：节点 S 每隔时间 T 周期性重复步骤 101 至步骤 103 共十次，10 次中连接节点个数 x 的平均值记为 average；

[0035] 步骤 105：确定参数 n：

[0036] 如果 average $\leqslant$ 2，则设置 n = 2；

[0037] 否则设置 n = average；

[0038] 步骤 103：确定参数 k：

[0039] 如果 n $\geqslant$ 4，则 k = 3；

[0040] 否则 k = 2；

[0041] 在本发明中，所述步骤二源节点将一个原始信息加密，分成 k-1 段，解密密钥放在第 k 段的具体处理为：

[0042] M 表示源节点需要发送的消息或信息。

[0043] 步骤 201：源节点 S 生成一个随机密钥 Key；

[0044] 步骤 202：如果 k = 2，源节点 S 将信息 M 加密，加密算法为节点内置的加密算法，

加密密钥是步骤 201 产生的密钥 Key，到步骤 204 ；

[0045] 步骤 203 ：如果 k ＝ 3，源节点 S 将信息 M 加密，加密算法为节点内置的加密算法，加密密钥是步骤 201 产生的密钥 Key，然后将加密后内容分成 2 段 ；

[0046] 步骤 204 ：把解密密钥 key2 保存在第 k 个信息分段中，第 k 个信息分段不加密 ；

[0047] 步骤 205 ：将 k 个消息分段的目标 IP 地址设为广播地址 255.255.255.255，目标 MAC 地址是接收节点的 MAC 地址。

[0048] 步骤 206 ：生成 M 的信息识别码 ID_M，在 k 个消息分段的 IP 报文头部存放信息识别码 ID_M 和参数 k，信息识别码 ID_M 为源节点随机产生，该信息识别码不加密。

[0049] 在本发明中，所述步骤三转发消息节点 N_s 每隔时间 T 周期性地更新其周围连接节点数的具体处理为 ：

[0050] 源节点 S 和接收了其他节点信息分段的节点都称为发送节点或转发节点，用 N_s 表示 ；

[0051] 步骤 301 ：节点 N_s 发送心跳信号 HeartBeat ；

[0052] 步骤 302 ：节点 N_s 的邻居节点 N_i 收到心跳信号 HeartBeat ；

[0053] 步骤 303 ：节点 N_i 产生一个随机退避时间 t，退避时间范围在 1 秒内，节点 N_i 在等待退避时间 t 之后返回一个心跳信号 $HeartBeat_i$ 给节点 N_s，节点 N_s 统计在其发出心跳信号 HeartBeat 后 1 秒内接收到的 $HeartBeat_i$ 信号的个数 x，并且记录每个连接节点的 MAC 地址 ；

[0054] 在本发明中，所述步骤四的具体处理为 ：

[0055] 步骤 401 ：如果 N_s 连接的节点个数 x 大于等于 n，进入下一步 402，否则本轮结束 ；

[0056] 步骤 402 ：对本周期接收到的 x 个连接节点的 MAC 地址进行提取，获得当前连接节点的地址列表 $List_{now}$ ；

[0057] 步骤 403 ：节点 N_s 从其存储单元取一个要转发的消息作为消息 M，提取 M 的识别码 ID_M，根据识别码 ID_M 提取消息历史接收节点的地址列表 $List_{history}(ID\_M)$，将当前连接节点的地址列表 $List_{now}$ 和 $List_{history}(ID\_M)$ 进行比较 ：如果在消息 M 的历史接收节点地址列表 $List_{history}(ID\_M)$ 有一个地址和当前连接节点的地址列表 $List_{now}$ 中的地址相同，则不发送消息 M，跳转至步骤 406 ；否则，如果在消息 M 的历史接收节点的地址列表 $List_{history}(ID\_M)$ 中没有当前连接节点的地址，则到步骤 404 ；

[0058] 步骤 404 ：节点 N_s 广播消息 M ；

[0059] 步骤 405 ：节点 N_s 将当前连接节点的地址列表 $List_{now}$ 加入到消息 M 识别码 ID_M 的历史接收节点的地址列表 $List_{history}(ID\_M)$ ；

[0060] 步骤 406：节点 N_s 从存储单元取出下一条消息，重复步骤 403 至步骤 406，直到检查完全部的消息。

[0061] 图 3 是本发明中节点接收消息的工作流程图。如图 3 所示，接收节点的工作流程是 ：

[0062] N_r 表示接收到 N_s 的 HeartBeat 信号的节点。

[0063] 步骤 501 ：节点 N_r 收到一个来自 N_s 的 HeartBeat ；

[0064] 步骤 502 ：节点 N_r 产生一个随机退避时间 t，退避时间范围在 1 秒内，节点 N_r 在等待退避时间 t 之后返回一个心跳信号给节点 N_s ；

[0065] 步骤 503：如果节点 N_s 发送信息分段 M，由于该分段的目标 IP 地址是广播地址 255.255.255.255，则节点 N_r 接收 N_s 发送的信息分段 M；

[0066] 步骤 504：节点 N_r 检查信息 M 的目标 MAC 地址，如果信息 M 的目标 MAC 地址是节点 N_r 的 MAC 地址，节点 N_r 将该信息提交该上层应用协议处理，该消息不再转发；如果信息分段 M 不是发送给自己的，则把 M 保存在存储单元中，提取 M 的信息识别码 ID_M；

[0067] 步骤 505：检查是否已经建立了集合 $List_{history}(ID\_M)$，如果已经建立了，则结束；否则根据 ID_M 建立空集合 $List_{history}(ID\_M)$。

[0068] 根据本发明的方法，源节点将一个完整的信息加密后分成 k-1 个信息分段，并把解密密钥包含在第 k 个分段中，源节点将每一分段都发给不同的接收节点。本发明增加了攻击节点解密的难度，只有接到了全部 k 个分段的节点才能先组合前 k-1 个信息分段，然后再使用保存在第 k 个分段中的密钥解密前 k-1 个信息段，得到完整的信息的内容。当发送节点在发送最后一个信息分段时，即使有攻击节点伪装成普通节点收到了最后一个分段，如果它没有接收到前面全部的 k-1 个信息分段，攻击节点也不会对源节点进行定位追踪，从而提高了源节点的抗定位能力，保护了源节点的位置隐私。

[0069] 尽管上面已经示出和描述了本发明的具体实施例，可以理解的是，上述实施例是示例性的，不能理解为对本发明的限制，本领域的普通技术人员在不脱离本发明的原理和宗旨的情况下在本发明的范围内可以对上述实施例进行化、修改、替换和变型。

[0070] 本发明中引用字母的物理意义如下表说明：

[0071]

S	源节点，被输入了消息的某节点或者产生了消息需要发送的节点
N_i	网络中的普通节点
N_s	发送节点或转发节点，包括源节点 S 和接收了其他节点信息分段的节点
N_r	接收到节点
T	发送节点更新连接节点的周期时间
HeartBeat	心跳信号，转发节点在寻呼该区域其它节点的时候，发送的寻呼请求。

[0072]

M	需要转发的信息。
ID_M	信息识别码，一个信息的 k 个分段的信息识别码相同，不同信息的信息识别码不同
x	区域与转发节点保持连接状态的节点个数 x 。
$\mathrm{List}_{\mathrm{now}}$	当前连接节点的地址列表
$\mathrm{List}_{\mathrm{history}}(\mathrm{ID\_M})$	根据 M 的信息识别码 ID_M 建立的历史接收节点的地址列表
TTL	转发消息 M 的存活时间。
t	随机退避时间

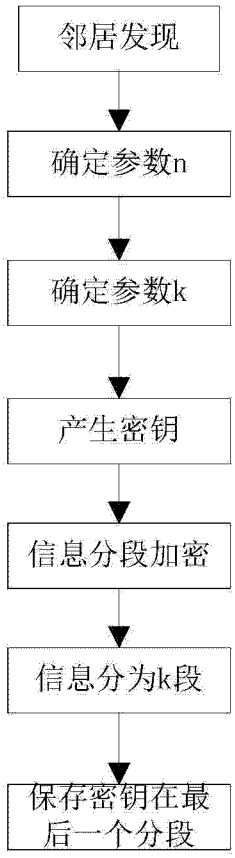

邻居发现
确定参数n
确定参数k
产生密钥
信息分段加密
信息分为k段
保存密钥在最后一个分段

图 1

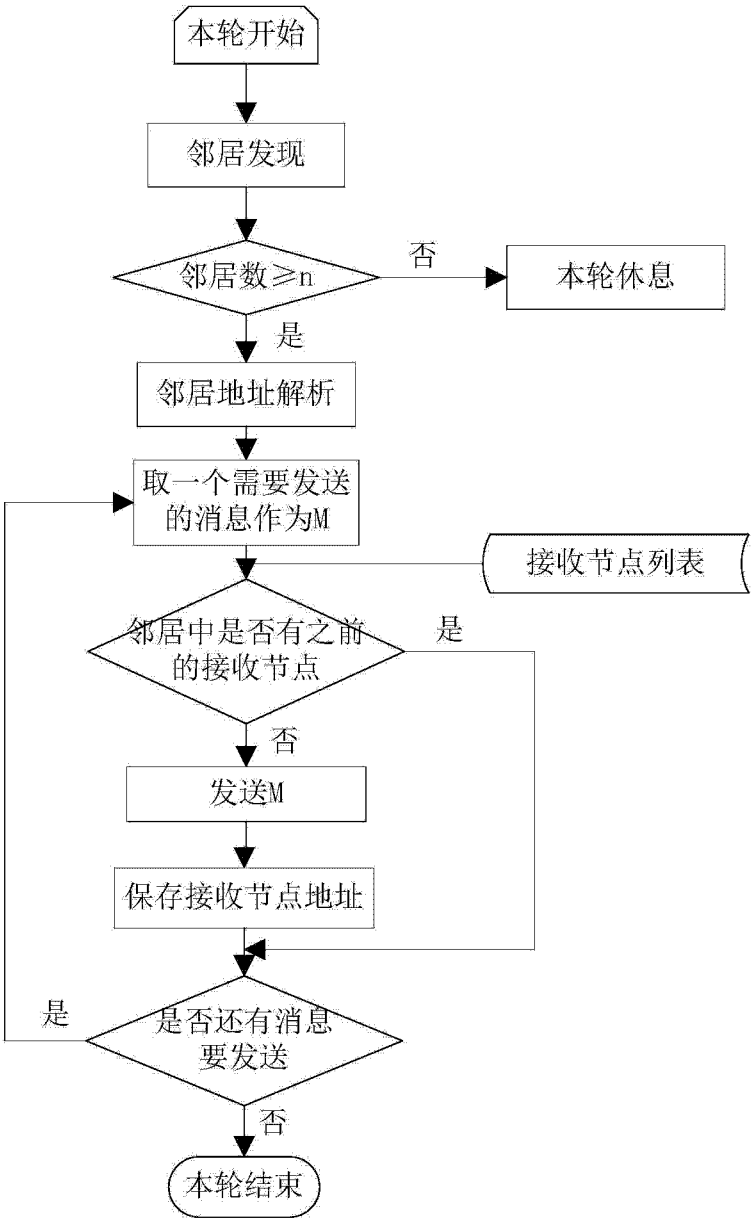

本轮开始
邻居发现
邻居数≥n
否
本轮休息
是
邻居地址解析
取一个需要发送的消息作为M
接收节点列表
邻居中是否有之前的接收节点
是
否
发送M
保存接收节点地址
是
是否还有消息要发送
否
本轮结束

图 2

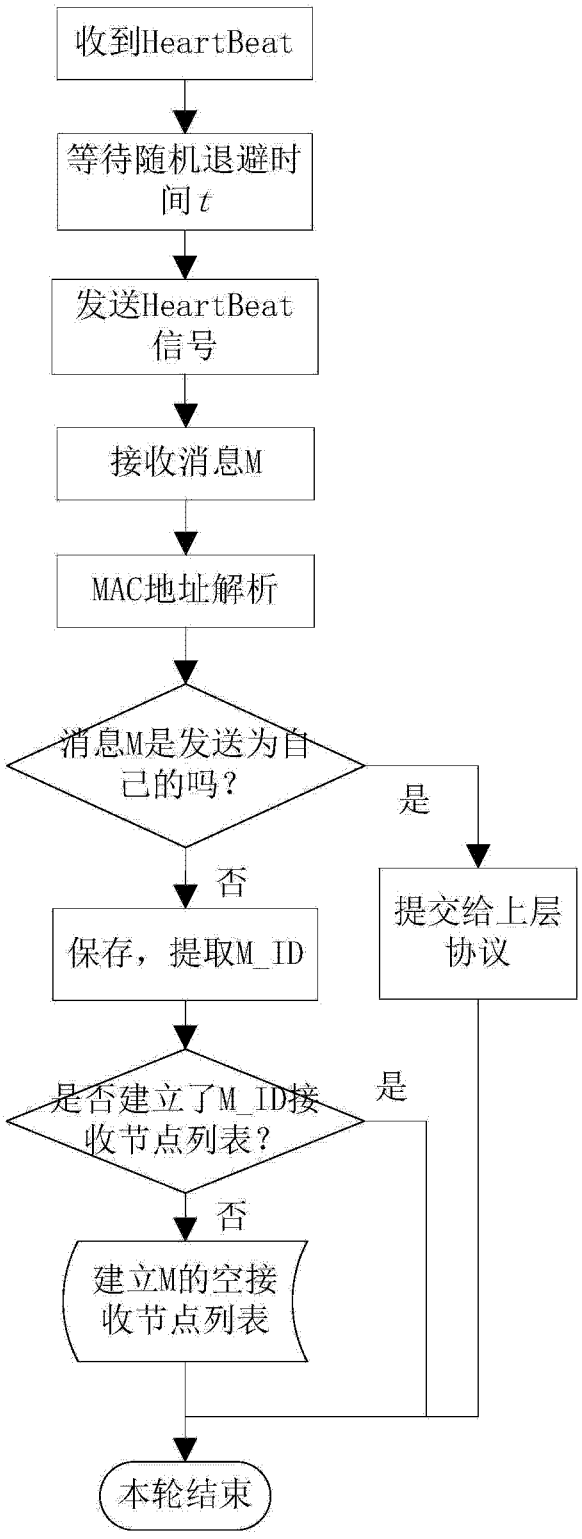

收到HeartBeat
等待随机退避时间t
发送HeartBeat信号
接收消息M
MAC地址解析
消息M是发送为自己的吗？
是
否
提交给上层协议
保存，提取M_ID
是否建立了M_ID接收节点列表？
是
否
建立M的空接收节点列表
本轮结束

图 3