doi:10.3969/j.issn.1000-436x.2012.z1.023

无线传感器网络复件攻击的移动检测方法

陈向益，王良民，詹永照
(江苏大学 计算机科学与通信工程学院，江苏 镇江 212013)

摘 要：无线传感器网络无人值守的特性使得它易于遭受复件攻击从而造成严重的安全隐患。提出了一个移动检测复件攻击的方法，通过检测节点的移动使得网络内的每个节点都能直接与检测节点通信，从而使得检测节点与一跳范围内的传感器节点能够直接通信，从而全局地检测到网络中的复件攻击节点，并采用更新网络对称密钥的方法防御逃避检测的节点。实验表明该方法能够检测到网络内的所有复件攻击节点，和其他方法相比，本方法不需要检测消息的转发，检测开销小并且实现了开销在网络中的均衡。
关键词：无线传感器网络；复件攻击；移动检测
中图分类号：TP393 **文献标识码**：B **文章编号**：1000-436X(2012)Z1-0178-08

Mobile detection of replication attacks in wireless sensor network

CHEN Xiang-yi, WANG Liang-min, ZHAN Yong-zhao
(School of Computer Science and Telecommunication Engineering, Jiangsu University, Zhenjiang 212013, China)

Abstract: The detection schemes proposed so far are not satisfactory because they are energy and memory demanding, not suit for use in resource-constrained wireless sensor networks. the detection of replica attack was focused on in WSN. from the intuition that mobility, in conjunction with the one-hop sensor node's communication, helps detect the replica attack globally. Then, propose a mobile detection method to detect the replica attack. Analysis and simulations result show that the our method helps to detect replica attacks effectively and efficiently, with a small and well-balanced overhead in the network.
Key words: wireless sensor network; replica attack; mobile detection

1 引言

无线传感器网络（WSN, wireless sensor network）节点通常部署在无人照看的环境中，通过自组织的方式形成网络进行环境监测、敌情勘察等重要工作。由于 WSN 的无人照看的特性使得无线传感器网络特别容易遭受各种攻击，而来自于 WSN 内部的安全威胁[1]严重影响了 WSN 的正常运转。

在这些内部攻击中，复件攻击是一种较为隐蔽的潜在的安全威胁，指的是攻击者通过物理俘获无线传感器网络内部的合法节点，破解而获得节点的身份 ID、密钥等重要信息，接着克隆出使用同样身份 ID 和密钥等信息的复件节点，偷偷地将这些复件节点部署在网络中，随后利用这些复件节点发起诸如数据注入、选择性转发、制造路由环路甚至拓扑分割等恶劣的攻击活动。如图 1 所示，黑色节点代表正常节点，自组织地形成了网络，攻击者俘获了的节点用灰色表示，白色的节点代表攻击者克隆

收稿日期：2012-07-10
基金项目：国家自然科学基金资助项目（61272074）；江苏省自然科学基金资助项目（BK2011464）；安徽大学计算智能与信号处理教育部重点实验室开放基金资助项目
Foundation Items: The National Natural Science Fundation of China (61272074); The Natural Science Fundation of Jiangsu Province (BK2011464); The Open Fundation of Key Laboratory of Intelligent Computing & Signal Processing, Ministry of Education, Anhui University

并部署的复件节点。

由于复件节点对无线传感器网络的正常运行构成了严重的潜在安全威胁，因此，复件节点的检测和撤销成为无线传感器网络安全的一个重要研究内容[1]。好的检测方案要求检测率高、误检率低、检测方案造成的计算、存储和通信开销低，并且要求检测开销要能够在网内节点间均衡不致于使得个别节点过早能量耗尽而死亡。

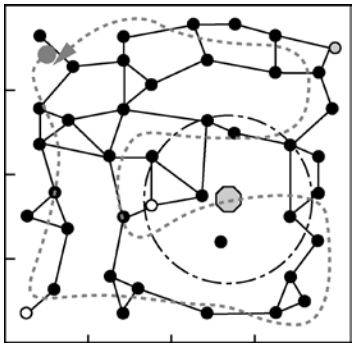

图 1　基于移动 sink 的复件节点检测方案

现有的复件节点的检测方案可以分为中心式检测[2]、局部检测[3~5]和广播检测[6]。中心式检测方案[2]采用所有的节点将自己的邻居节点列表上传到中心基站进行节点 ID 的比对和判断，这种方案较为有效，能够检测出网内所有的复件节点，但是中心基站的模式存在能耗严重不均的问题，越靠近基站的节点能量消耗越高，容易能量过早耗尽而死亡；局部检测方案[3~5]采用本地节点间的投票来检测出复件节点，能够有效地检测出本地复件节点，缺点是不能检测到分散距离较远的复件节点；广播式的检测方案[6]让所有节点广播自己 ID 和所在位置的声明消息，那些收到同个 ID 在不同位置的证人节点就成功检测到复件节点，然后向网络内节点广播撤销该 ID 所对应节点的消息，该方案能够有效地进行分布式地检测，主要缺点是每个节点都要进行声明消息的广播，并且要存储和比较收到的其他节点的声明消息，存储和通信开销较大。

在广播式方案的基础上，为降低检测开销，相应的改进方案[6~8]被提出。其中，文献[6]提出了 RM 和 LSM 方案，RM 方案中，节点将使用基于身份的公钥机制签名的身份和位置绑定的声明信息广播给自己的邻居节点，邻居节点再以一定的概率将该声明消息发送到随机选择的网络内节点进行见证，按照生日悖论，相同 ID 的节点将以较大的概率拥有相同的证人节点，从而被证人节点检测到；为了进一步提高 RM 方案的检测概率，LSM 方案让转发声明消息的路径上的节点也存储和比较声明消息，从而一个声明消息从源节点到目的地节点形成了由线段形成的验证线，而相同 ID 节点的验证线将有较大的概率相交于网络内的某些节点，从而这些节点成为证人节点，检测到复件节点并发起撤销过程，LSM 方案相对 RM 方案提高了检测率，但也增加了节点的存储开销，同时也存在验证现在网络中心交叉概率大的中心拥挤问题。文献[7]针对 LSM 检测方案存在的中心拥挤问题提出了 RED 检测方案，提出使用一个全网共享并更新的随机数种子，使得复件节点和变节节点通过相同的伪随机函数计算得到同样的位置声明消息发送的目的地节点，从而被这些证人节点检测到，但是该方案要实现随机数种子的全网共享和更新，多数情况下不易实现。文献[8]则在概率选取的基础上，利用群部署（group deployment）的先验知识进一步降低安全代价并提高检测率。总之，这些检测方案的成功率和精度依赖于生日悖论和随机概率，检测的开销依然较大。

在无线传感器网络的推广应用过程中，移动节点的出现则扩充了无线传感器网络的使用范围。文献[9]研究了由移动节点组成的 WSN 的复件节点攻击检测方法，提出使用 SQRT 方法，以移动节点的移动速度不能超过系统设置的最大值为标准进行检测，但是仅适用于由移动节点构成的无线传感器网络。文献[10]借用节点移动的思想到静态传感器网络，提出使用移动 Patroller 作为检测者，进行网络复件节点的检测，能够有效地检测出网络的复件节点，通过使用移动 Patroller 降低了网络内部静态节点的能耗，能够有效地延长网络的寿命，但是，方案中静态节点仍旧需要执行节点定位算法和时间同步算法从而增加了节点的计算和通信开销。复件节点的检测问题远没有有效地解决，仍旧是一个需要继续深入研究的开放性问题。

受移动节点这一思想的启发，本文设计了使用移动 sink 来进行复件节点检测的方法，不需要使用节点定位机制和节点间的时间同步算法，通过移动 sink 在网络中进行数据收集和巡视，来检测网络中的复件节点。本文后续内容组织如下：第 2 节给出网络和攻击者的模型；第 3 节提出基于移动 sink 的复件节点检测和撤销方案；第 4 节针对提出的协议进行分析并给出仿真实验结果；第 5 节对本方案和现有的相关方案进行比较；第 6 节对文中的提出的方案进行总结。

2 网络模型和假设

假设无线传感器网络 WSN 由静态传感器节点和一个移动 sink 组成，移动 sink 在网络部署区域移动巡视，假设移动 sink 是可信的管理者，计算、存储、通信能力较强，能量充足。另外，假设网络中的所有的通信是双向的，这也是多数复件检测方案的假设。

移动 sink 熟悉网络的拓扑和节点部署的大致地理位置，并且移动 sink 带有定位装置（如 GPS 设备）知道自身当前的地理位置，静态传感器节点不需要知道自己的位置信息。

网络中移动 sink 和静态节点之间的通信采用基于身份的公钥方案(ID-based public key schema)进行加密和签名，类似于文献[6~10]，只有节点知道自己的私钥，节点的私钥由网络部署者采用秘密的信息和节点的 ID 通过计算得到，而这个秘密的信息不存储在节点中，因此攻击者不可能获得这个秘密。节点的公钥由它的身份标识 ID 通过函数 $f(ID)$ 计算得到，节点不需要存储对方的公钥或者证书信息。表 1 列出了本文提出的方案描述中使用到的相关的符号和对应的含义。

表 1 文中使用到的符号和对应的含义

符号	含义
n	网络中节点的总数
$ID_{\sin k}$	移动 sink 的身份标识
ID_i	传感器节点 S_i 的身份标识
S_i	第 i 个传感器节点
$K_{ID_{\sin k}}^{pk}$	移动 sink 的公钥
$K_{ID_{\sin k}}^{sk}$	移动 sink 的私钥
$K_{ID_i}^{pk}$	节点 s_i 的公钥
$K_{ID_i}^{sk}$	节点 s_i 的私钥
Req	要求节点应答巡视的命令
Revoc	撤销复件节点的命令
No	巡视周期编号
N_i	节点自己的待巡视周期编号
$f(\cdot)$	公钥计算函数 $K^{pk}=f(ID)$
$DATA_i^{Ni}$	传感器节点 S_i 在巡视周期 N_i 采集的数据
$RandNum^{No}$	在巡视周期 No，移动 sink 收到节点应答 $Message_2$ 后，更新节点的对称密钥
$Message_1$	发送到节点的巡视请求消息
$Message_2$	传感器节点对 $Message_1$ 的应答
$Message_3$	移动 sink 更新对称密钥的消息
$Message_4$	移动 sink 撤销复件节点的消息
Evidence	移动 sink 撤销消息中的证据

攻击者由于不可能获得网络部署者的秘密信息，不可能任意地创造节点的身份 ID，除非通过物理俘获已有的网络内静态节点、破解从而获得它的私钥，这就限制了攻击者只能通过变节节点而进行克隆来制作复件节点。

3 移动 sink 检测方案

在网络部署之后，网络部署者将网络的部署区域按照移动 sink 的通信覆盖能力分割成一系列的子区域，使得每个子区域保证移动 sink 的通信半径能够完全的覆盖到，将这些子区域按照方便巡视的方式进行编号，移动 sink 按照编号的顺序依次巡视这些小区域，完成节点数据汇集和复件节点的检测和撤销过程，如图 1 所示，细虚线表示区域划分，粗虚曲线表示可能的巡视路径。

移动 sink 在 WSN 部署的区域中按照一定的周期进行巡视，到达一个区域之后，进行数据的收集、复件节点的检测，然后移动进入下一个区域，执行同样的工作，直到网络的所有部署区域巡视结束，完成一个巡视周期。然后，移动 sink 查看检测到的复件节点表格，如果检测到新的复件节点，则向网络广播撤销消息，之后进入下一个巡视周期。

静态节点的待巡视周期编号为 N_i，网络初始部署之后，每个节点都将自己存储的待巡视周期初始化为零，该编号在节点被巡视过之后加一表示等待下一个巡视周期；移动 sink 也将巡视周期 No 初始化为零。在开始一个新的巡视周期的时候，移动 sink 将该编号加一，表示开始一个新的巡视周期。

3.1 协议描述

在本检测方案中，移动 sink 和传感器网络内部节点间的通信交互的时间顺序如图 2 所示，移动 sink 执行如图 3 所示的算法；无线传感器网络内的静态节点执行如图 4 所示的算法。

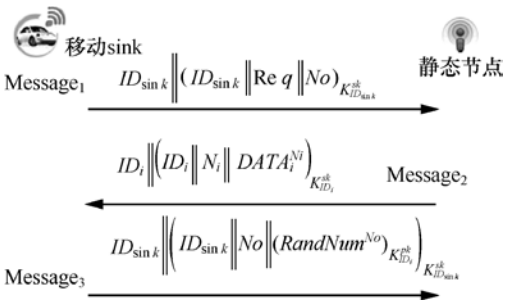

图 2 移动 sink 和节点间的通信过程

```
算法 1：移动 sink 执行
计算下一个巡视子区域 Ai;
if(Ai ≠ A1) then
    移动到子区域 Ai;
    向子区域广播 Message1;
    接收静态节点的应答 Message2
    从 Message2 获得节点身份记为 ID1=IDi
    计算该节点的公钥 K_IDi^pk = f(ID1)
    验证消息 Message2 的数字签名
    从验证过签名的消息中得到 IDi、Ni
    记 ID2=IDi，N1=Ni
    if ID2 = = ID1 && No = = N1 then
        if ID1 不在 ReplicaTable 中 then
            if ID1 已经在 IDTable 中 then
                存储 ID1 到 ReplicaTable
            else
                存储 ID1 到 IDTable
            Endif
            发送 Message3 给静态节点 IDi
        endif
    endif
else
    if ReplicaTable 为非空 then
        广播撤销消息 Message4
    endif
    No=No+1
    计算和产生新的对称密钥 RandNum^No
endif
```

图 3　移动 sink 执行的检测算法

```
算法 2：静态节点执行
接收消息
计算公钥 K_IDsink^pk = f(IDsink)
验证消息签名
获得 IDsink , No，并分析得到消息类型
switch(消息类型) do
  case Message1:
    if ID == IDsink and No = = Ni then
        发送 Message2 给移动 sink
    Endif
  case Message3:
        验证签名
        解密获得对称密钥 RandNum^No
        Ni=Ni+1
  case Message4:
    if ID == IDsink and No == Ni then
        foreach(撤销请求中的 IDi) do
        if IDi 不在复件黑名单中 then
            if 撤销证据得到验证 then
                将 IDi 存储复件黑名单
            endif
        endif
        end
    endif
end
```

图 4　网内静态节点执行的算法

3.2　复件节点的检测过程

第 1 步：移动 sink 向所在的子区域内广播数据收集请求消息 $Message_1$，内容如式(1)所示，

$$Message_1 = \left\{ ID_{\sin k} \left\| (ID_{\sin k} \left\| Req \right\| No)_{K_{ID_{\sin k}}^{sk}} \right. \right\} \quad (1)$$

其中，Req 是数据收集的请求，No 是巡视周期编号，$(ID_{\sin k} \left\| \mathrm{Re}q \right\| No)_{K_{ID_{\sin k}}^{sk}}$ 表示移动 sink 进行数字签名。

第 2 步：节点应答移动 sink。

网络内处于移动 sink 通信覆盖区域的节点收到 $Message_1$ 之后，根据 $ID_{\sin k}$ 计算出移动 sink 的公钥 $K_{ID_{\sin k}}^{pk} = f(ID_{\sin k})$，使用该公钥验证签名过的内容 $(ID_{\sin k} \left\| \mathrm{Re}q \right\| No)_{K_{ID_{\sin k}}^{sk}}$ 得到 $ID_{\sin k}$，Req 和 No，对比 $ID_{\sin k}$，比对 No 和节点内存储的待巡视周期 N_i，并据 Req 判断是否是收集数据的请求，验证不通过则忽略该消息，否则构造并向移动 sink 发送应答消息 $Message_2$，如式(2)所示。

$$Message_2 = \left\{ ID_i \left\| \left(ID_i \left\| N_i \right\| DATA_i^{Ni} \right)_{K_{ID_i}^{sk}} \right. \right\} \quad (2)$$

$Message_2$ 中包含节点自己的身份标识 ID_i 和节点私钥 $K_{ID_i}^{sk}$ 签名的内容 $\left(ID_i \left\| N_i \right\| DATA_i^{Ni} \right)$，将标识再次包含进去是为了给对方进一步验证。

第 3 步：移动 sink 发送对称密钥给“忠实”应答的节点。

移动 sink 收到消息 $Message_2$ 之后，首先根据 ID_i 检查已经检测到的复件节点列表 ReplicaTable，如果该身份标识已经在该列表中，说明该身份 ID 对应的节点是已知的复件节点，则处理结束；否则，根据 ID_i 计算得到节点 S_i 的公钥 $K_{ID_i}^{pk} = f(ID_i)$，验证签名内容 $\left(ID_i \left\| N_i \right\| DATA_i^{Ni} \right)_{K_{ID_i}^{sk}}$ 得到 $ID_i \left\| N_i \right\| DATA_i^{Ni}$，比对 ID_i 确认身份，比对 N_i 确认巡视周期，验证通过，将 $Message_2$ 存储起来以备撤销时候使用。接着检查本检测周期中已经巡视过的节点列表 IDTable，如果该 ID 已经在该列表中说明该节点是复件节点，移动 sink 一个巡视周期 No 内收到 2 个来自同一个 ID 的 $Message_2$，则发现复件节点，将该 ID 存储到复件节点列表，并将矛盾的 $Message_2$ 作为证据，在撤销时使用。

对于正常应答的节点，在处理结束之后更新对称密钥 $RandNum^{No}$ 给该 ID_i 对应的节点，消息内容如 $Message_3$ 所示，其中要更新的对称密钥 $RandNum^{No}$ 使用节点的公钥进行加密，并随同移动

sink 的身份表示和巡视周期编号一起被移动 sink 数字签名，如式(3)所示。

$$Message_3 = \left\{ ID_{\sin k} \left\| \left(ID_{\sin k} \left\| No \right\| (RandNum^{No})_{K_{ID_i}^{pk}} \right)_{K_{ID_{\sin k}}^{sk}} \right. \right\} \tag{3}$$

为了防范复件节点在第 2 步不应答移动 sink 从而躲避检查，移动 sink 针对“忠实”应答的节点的回复更新传感器网络内静态节点间通信使用的对称密钥 $RandNum^{No}$，该对称密钥在每个巡视周期 No 由移动 sink 进行更新。通过该机制将使得复件节点除非在第 2 步进行应答，否则，将得不到移动 sink 更新的对称密钥，从而不能参与后续的网络内活动。

节点收到 $Message_3$ 之后，验证签名并解密得到对称密钥 $RandNum^{No}$，在网内通信时用于消息的加密和解密。

移动 sink 在一个子区域处理完毕，进入下一个子区域执行以上过程，直到网络的所有子区域都处理完毕回到起点，从而完成整个巡视周期。在一个巡视周期结束之后，如果复件节点列表为空，说明经过检测没有发现复件节点，则不需要执行撤销过程；如果复件节点列表非空，则说明检测到了复件节点，则随之执行 3.3 节的复件节点撤销过程。

3.3 复件节点的撤销过程

撤销过程由 2 步构成。

第 1 步：移动 sink 向网络中的节点广播撤销消息 $Message_4$，如式(4)所示。

$$Message_4 = \left\{ ID_{\sin k} \left\| \left(ID_{\sin k} \left\| No \right\| \mathrm{Re}voc \right\| Evidence \right)_{K_{ID_{\sin k}}^{sk}} \right\} \tag{4}$$

Revoc 是撤销请求的命令，Evidence 包含被撤销的节点标识 ID_i 和撤销证据信息，内容如式(5)所示。

$$Evidence = \{ ID_i \| Message_2 \| Message_2' \} \tag{5}$$

$Message_2$ 和 $Message_2'$ 是移动 sink 在一个巡视周期 No 内收到的身份标识都是 ID_i 的 2 条应答消息，在此作为证据，在撤销消息中附带，发送给网络中的节点进行验证。

第 2 步：静态节点收到撤销消息之后将节点加入复件节点黑名单。

静态节点在收到 $Message_4$ 之后，根据 $ID_{\sin k}$ 计算移动 sink 公钥 $K_{ID_{\sin k}}^{pk} = f(ID_{\sin k})$，验证签名内容 $\left(ID_{\sin k} \left\| No \right\| \mathrm{Re}voc \right\| Evidence)_{K_{ID_{\sin k}}^{sk}}$ 得到 $ID_{\sin k}$、No、$Revoc$ 和 $Evidence$，比对身份标识 $ID_{\sin k}$ 和巡视周期 No，验证 $Revoc$ 确认是撤销消息，这些验证任何一个没有通过则忽略该消息。验证通过则查看证据 $Evidence$ 的内容，根据证据中的身份标识 ID_i，首先检查复件节点黑名单，如果该节点已经在黑名单中，则结束处理；否则，依次验证证据消息 $Message_2$ 和 $Message_2'$，验证通过则信任该证据，将身份标识 ID_i 存入复件节点黑名单，拒绝该身份 ID 所对应节点的所有通信。

4 协议分析和仿真实验

4.1 协议分析

4.1.1 漏检

本方案中，通过引入移动 sink，使得网络内静态节点获得和移动 sink 的直接通信机会，而移动 sink 在收集节点的传感器数据的同时通过判别节点的 ID 来检测复件节点。理论上只要复件节点应答移动 sink 的消息，则移动 sink 最后将找到网络内的所有复件节点。由于一轮检测周期中，每个 ID 对应的节点只会发送一个消息给移动 sink，则重 复 ID 的节点一定是复件节点，使得本方案不存在漏检的问题。

4.1.2 虚警

由于在移动 sink 的检测过程中，采用了数字签名的方案，保证了消息的可信性；撤销消息中采用节点签过名的身份作为证据，保证了撤销过程的可信性；因而，网内节点不会被错误地检测和撤销掉，不存在虚警的问题。

4.1.3 检测开销的均衡

移动 sink 在网络内巡视，将检测过程的开销平均分配到网络中的节点，实现了检测开销的均衡。

4.1.4 通信次数

在一个巡视周期中，如果没有检测到复件节点，正常节点只需要接收 2 条移动 sink 的消息，发送一条消息给移动 sink；如果检测到复件节点，则除了以上的开销之外，还将接收移动 sink 的一条撤销消息。

4.1.5 计算开销

1) 静态节点计算开销

网络中不存在复件节点时，在收到移动 sink 的

Message1 后，验证签名要用到公钥算法，发送消息 Message2 给移动 sink 时，需要用公钥算法进行签名，收到移动 sink 发送的 Message3 时，需要使用公钥算法验证签名、解密移动 sink 更新的对称密钥，网络内的静态传感器节点需要执行 4 次公钥算法。

如果复件节点被移动 sink 检测到，在撤销时，需要执行 3 次公钥算法，一次是对撤销消息的验证，另外 2 次用于检验证据。

2) 移动 sink 计算开销

在一轮巡视周期中，移动 sink 发送 2 个消息给节点要签名两次，从节点接收一个消息，要验证签名一次，在传送秘密给节点时要加密一次，对于一个区域中的节点要执行一次公钥算法，与网络内的每个节点通信总共需要执行 3 次公钥算法。对于存在撤销消息的情况，发送撤销消息将需要执行一次公钥签名算法。

4.1.6 存储开销

1) 静态节点存储开销

由于静态节点不需要存储检测过程中其他节点的信息，只需要存储待检测周期，由 *ID* 计算公钥的函数，移动 sink 更新的对称密钥，复件节点身份标识黑名单等数据，节点的存储空间需求正比于复件节点的身份标识 *ID* 的数目。

2) 移动 sink 存储开销

移动 sink 需要将每个节点的应答 Message2 都存储起来以便于比对以及作为撤销时的证据，所以存储能力要求较高，跟网络中的节点数目 *n* 成线性关系。另外，移动 sink 要存储已经检测过的节点身份标识列表，复件节点身份标识列表信息。

4.2 仿真实验结果

为了检验本文提出的基于移动 sink 的检测方案，在 NS2 仿真环境中进行了大量的不同场景下的仿真实验。

仿真的设置为：场地为 500m×500m 的平面区域，即场地为二维平面坐标 *XY* 中坐标为（0，0），（0,499），（499，499），（499,0）4 个顶点构成的方形区域；无线通信节点物理层的射频通信模型采用 TwoWayGround，MAC 层的协议采用 IEEE 802.11，由于本文只考虑让移动 sink 和通信范围内的邻居节点直接通信，不考虑路由，所以将路由协议设置为 DumbAgent，即不带路由功能；移动 sink 的移动路径依次为位置坐标(124,124)，(124,374)，(374,374)，(374,124)，这样将方形区域划分为大小相等的 4 个小方块，这样设计的依据是让移动 sink 的通信范围能够覆盖到划分的小区域，在仿真工具 NS2 中默认的无线节点的通信半径是 250m，因此采用如上的子区域划分能够保证移动 sink 对子区域完全的通信覆盖。

1) 检测结果以及节点数目对结果的影响

首先，为了检验本文设计的方案的检测结果，进行了一个复件节点的检测仿真。设定只有一个复件节点，但是改变节点个数 *n*，让这 *n* 个节点被随机撒播在场地中，随机分布采用均一分布，检查本协议在不同节点数目情况下对唯一一个复件节点的检测结果。仿真的结果显示，在存在一个复件节点的情况下，本文提出的协议能够成功地检测到该复件节点，检测所需要的时间以巡视轮数来衡量的话，该时间随着场地内节点的数目增多而延长，图 5 是依据仿真结果而绘制的曲线。

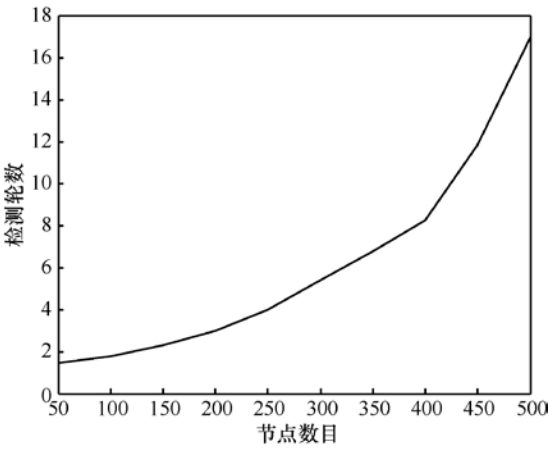

图 5　节点数目对检测的影响(存在 1 个复制节点的检测场景)

仿真实验中，节点数目分别设置为 50、100、150、200、250、300、350、400、450、500，为了消除节点随机分布对检测结果的影响，针对每个节点数目进行 20 次仿真实验求出平均的结果。由图 5 可见，随着节点数目的增加，检测该复件节点所需要的时间也随之增加，但该复件节点总能被本文提出的协议所检测到，时间的变化是由于节点数目增加之后，场地内节点的密度增大，无线通信的干扰也随之增大，导致移动 sink 和场地内节点之间的通信成功率降低，从而使得移动 sink 要通过多次巡视才能完成对网络内所有节点的遍历访问，并找到复件节点，因此造成了检测时间的增加。

从仿真结果看，实际的传感器网络在部署的时候，节点的密度对于检测过程具有较大的影响，因

为本检测协议在执行过程中，要通过移动 sink 广播检测请求信息，收到检测请求的节点在进行应答的时候的随机性使得通信冲突随着节点的部署密度增加而增大。

2) 复件节点数目对检测过程的影响

固定节点个数，增加某个身份 ID 被复制的节点的数目，考察复件节点数目的改变对检测过程和结果的影响。

实验中，固定节点数目 n=500，将一个身份 ID 被复制多个复件随机部署在网络中，同样进行多次仿真实验求出平均的结果。如图 6 所示是仿真结果，在节点数目固定之后，移动 sink 巡视网络内所有节点所需要的总的时间基本固定，在被复制节点的数目增多后，移动 sink 找到复件节点的机会也增大。检测所需要的时间（以巡视轮数来表示）随着复件节点的数目增加而减小，至少需要一轮的时间。

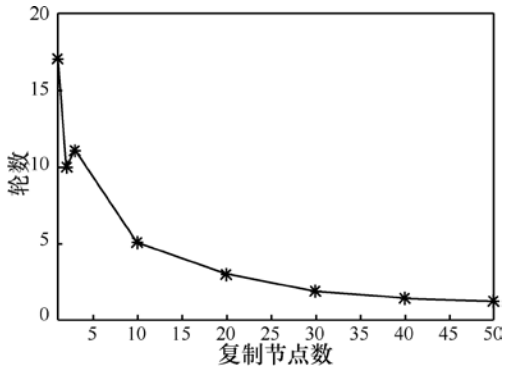

图 6　复件节点数目对检测时间的影响

3) 检测过程的通信开销

为了分析检测协议的检测开销，进行如下的仿真实验，固定节点数目为 n=100、复件节点数目 c 固定为 1。实验并分析为了检测到该复件节点网络内每个静态节点所需要的通信次数，仿真的结果如图 7 所示。从仿真结果分析，为了找到该复件节点，移动 sink 需要在网络的部署区域巡视大约两轮，在这两轮的巡视中网络内的静态节点需要平均发送 1.9 个数据分组给移动 sink，而平均需要从移动 sink 接收 6.17 个数据分组，平均总共需要 8.07 个数据分组与移动 sink 的收发。该结果包含了由于节点间的通信冲突而导致的数据分组重传的因素影响。这个结果与理论分析也是吻合的，因为从理论分析来看，本文提出的检测协议中，一轮检测过程，网络内每个静态节点需要从移动 sink 接收 2 个数据分组，静态节点需要发送 1 个数据分组给移动 sink，总共需要 3 个数据分组的通信过程。实际仿真的结果分析是由于执行两轮的检测才能遍历完整个网络内的所有静态节点，并包含了重传的因素。

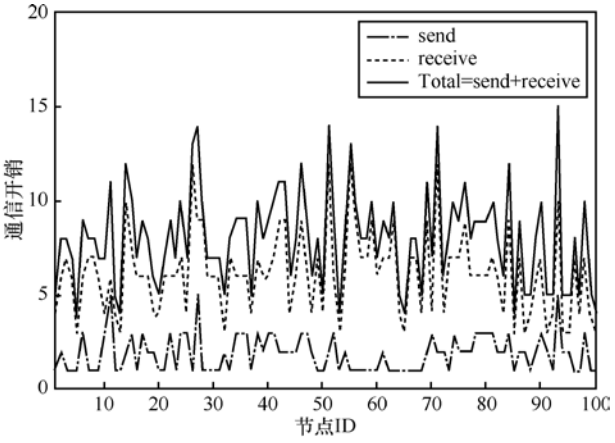

图 7　网内节点的通信开销

从以上的仿真结果来看，在不限制仿真时间的情况下，本文提出的检测协议能够有效地检测到网络内的复件节点，不存在误检和漏检的情况，并且当同一个身份 ID 的复件节点增加的情况下，检测出复件节点所需要的时间极大地降低；当网络内节点的数目增加从而使得节点的密度增大之后，节点之间的通信冲突增加从而导致较多的数据分组丢失和重传，使得仿真实验时检测出复件节点的时间相应地延长，通信的开销也相应地由于分组丢失和重传而增加，这也说明本方案不太适用于节点稠密的传感器网络部署环境。通常的实际应用环境中，基于成本的考虑，环境中节点的部署不会采用非常稠密的方式，所以本文提出的检测方案能够应用于多数实际的传感器网络。从通信的开销来看，本文提出的协议与理论分析的通信开销是基本吻合，但是由于通信冲突的原因稍高于理论分析值。

5　相关工作比较

本文提出使用移动 sink 检测和撤销方案，通过移动 sink 在网络中收集数据来判断复件节点，与现有的复件节点检测方案相比，节点不需要使用定位装置或者定位算法，并且不需要节点间的时间同步，降低了执行定位算法和时间同步算法的开销。表 2 列出了本文的方案和现有的方案在检测开销上的比较，其中，c 表示被复制的身份 ID 的数目。

表 2　　检测开销对比

方案	整个网络通信次数	公钥算法执行次数	存储开销
RM	$O(n^2)$	$O(\sqrt{n})$	$O(\sqrt{n})$
LSM	$O(n\sqrt{n})$	$O(\sqrt{n})$	$O(\sqrt{n})$
RED	$O(n\sqrt{n})$	$O(\sqrt{n})$	$O(\sqrt{n})$
本方案	$O(4n)$	$O(4+2c)$	$O(c)$

移动 sink 的巡视在网络节点间均衡了检测开销。在每个巡视周期内，每个节点都会与移动 sink 通信一次，保证了复件节点一定会被检测到并撤销掉，不存在误检和漏检的问题，并且在撤销的广播消息中采用了节点签过名的证据，保证了撤销过程的可信性。

与中心式检测方案相比，本文中的基于移动 sink 的方案，改善了中心式检测方案存在的靠近中心基站的网络节点能耗较大的问题，同时通过移动 sink 主动式的分区域的访问，不会出现网络节点统一向中心基站汇报可能造成的拥塞问题。

与采用邻居间投票表决的方案相比，本方案能够检测出全局复件节点，即使复件节点不在共同的邻居域中，仍然能够被有效地检测到。

本方案和采用广播方式的检测方案相比，网络内节点不需要周期性地向网络中的证人节点发送消息，减少了检测报文的转发开销，使得每个节点的检测都不依赖于其他节点，不会增加其他节点的开销。

6　结束语

本文提出了一种基于移动 sink 的复件节点检测和撤销方案，能够有效地检测和撤销网络中的复件节点，与现有的检测方案相比，检测开销较小并且检测开销在网络内节点间实现了均衡。通过大量的仿真实验进一步验证了本方案的有效性。与现有的检测方案相比，本方案不需要定位装置或者算法；其次，本方案不需要执行时间同步算法。而这两项改进能够较大地降低节点的成本以及计算和通信方面的开销，延长传感器网络节点的寿命。本文提出的方案专注于复件攻击的检测，主要考虑了网络通信正常进行情况下复件攻击的检测，下一步的工作将从以下 2 个方面展开：首先，研究移动 sink 更新网络对称密钥存在的不同步问题，提出更加有效的网络对称密钥的更新方法；其次，研究通信失效的情形对检测协议和网络造成的影响，并给出更为有效的解决方案降低这种影响。

参考文献：

[1] 王良民, 李菲, 熊书明等. 无线传感器网络内部攻击检测方法研究[J]. 计算机科学. 2011, 38(4):97-129.
WANG L M, LI F, XIONG S M, *et al*. Research on detection methods for insidious attack of wireless sensor networks[J]. Computer Science. 2011, 38(4):97-129.

[2] ESCHENAUER L, GLIGOR V D. A key-management scheme for distributed sensor networks[A]. Proceedings of the ACM Conference on Computer and Communication Security (CCS)[C]. Washington, USA, 2002. 41-47.

[3] CHAN H, PERRIG A, SONG D. Random key predistribution schemes for sensor networks[A]. Proceedings of IEEE Symposium on Security and Privacy[C]. Berkeley, USA, 2003. 197-213.

[4] DOUCEUR J. R. The sybil attack[A]. Proceedings of the 1st International Workshop on Peer-to-Peer Systems (IPTPS’01)[C]. London, UK, 2002. 251–260.

[5] NEWSOME J, SHI E, SONG D, *et al*. The sybil attack in sensor networks: analysis & defenses[A]. Proceedings of ACM IPSN’04[C]. Berkeley, USA, 2004. 259-268.

[6] PARNO B, PERRIG A, GLIGOR V D. Distributed detection of node replication attacks in sensor networks[A]. Proceedings of 2005 IEEE Symposium on Security and Privacy (S&P ’05)[C]. Oakland, USA, 2005. 49-63.

[7] CONTI M, PIETRO R, MANCINI L. A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks[A]. Proceedings of the 8th ACM International Symposium on Mobile Ad Hoc Networking and Computing(MobiHoc’07) [C]. Quebec, Canada, 2007. 80-89.

[8] HO J W, LIU D G, WRIGHT M, *et al*. Distributed detection of replica node attacks with group deployment knowledge in wireless sensor networks[J]. Ad Hoc Networks, 2009(7):1476-1488.

[9] HO J W, WRIGHT M, DAS S K. Fast detection of replica node attacks in mobile sensor networks using sequential analysis[A]. IEEE INFOCOM 2009[C]. Rio de Janeiro, Brazil,2009. 1773-1781.

[10] WANG L M, SHI Y. Patrol detection for replica attacks on wireless sensor networks[J]. Sensors, 2011, 11(3):2496-2504.

作者简介：

陈向益（1978-），男，河南新安人，江苏大学博士生，主要研究方向为无线传感器网络。

王良民（1977-），男，安徽潜山人，博士，江苏大学副教授，主要研究方向为无线传感器网络及其安全。

詹永照（1962-），男，福建尤溪人，博士，江苏大学教授、博士生导师，主要研究方向模式识别、情感计算、分布式计算和无线网络。