文章编号:1001 - 9081(2006)12 - 2897 - 03

无线传感器网络中的 Sybil 攻击检测

余 群[1,2],张建明[1]
(1. 江苏大学 计算机科学与通信工程学院,江苏 镇江 212013;
2. 盐城师范学院 计算机系,江苏 盐城 224002)
(yuqun_2007@yahoo.com)

摘 要:对 Sybil 攻击进行了研究,提出了一种基于地理位置信息的检测方法。利用基站和节点间传输的数据包信息检测部分 Sybil 攻击,构造多条路径,定义查询包,对通过不同路径到达目标节点的查询包中的字段值进行比较,再结合多跳确认机制,检测网络中的 Sybil 攻击。这种方法避免了传统的加密、身份认证等方法带来的高计算量和通信量,节省了节点能量。

关键词:Sybil 攻击;地理位置;多路径;多跳确认机制
中图分类号: TP393.08 **文献标识码**:A

Sybil attacks detecting in wireless sensor networks

YU Qun[1,2], ZHANG Jian-ming[1]
1. *Department of Computer Science and Communication Technology, Jiangsu University, Zhenjiang Jiangsu* 212013, *China*;
2. *Computer Department, Yancheng Teachers College, Yancheng Jiangsu* 224002, *China*

Abstract: To study Sybil attacks, a light-weight method to detect Sybil attacks was proposed. The method detected part of Sybil attacks through the transmission of packets between base station and nodes, formed multi-path, and defined query packets. Finally the fields in the query packets, which came to destination node from different routes, were compared. Also the method used multi-hop acknowledgement to generate alarm packets to detect the Sybil attacks. Different from some other methods that use encryption, identity certification and so on, this method reduces communication overhead and computations, and saves the energy of sensor nodes.

Key words: Sybil attacks; geographical location; multi-path; multi-hop acknowledgement technique

0 引言

无线传感器网络中的 Sybil 攻击会破坏多路径和地理位置路由、数据融合、投票、公平资源分配、非法行为检测[1]等机制,对网络构成严重的威胁。它是网络层容易出现的一种攻击,在这种攻击中,单个节点以多个身份出现在网络其他节点面前,使其更易于成为路由路径中的节点。我们定义,Sybil 攻击中的一个节点呈现出来的其他某个身份为 Sybil 节点。目前检测 Sybil 攻击的方法都是基于密钥分配、加密和身份认证的方法,对于电源能量、通信能力、计算能力均有限的传感器节点来说,通信量、计算量过大,缩短了无线传感器的寿命。

本文针对上面方法的不足,提出了一种检测 Sybil 攻击的新方法。首先利用基站和节点间传输的三种数据包信息来检测部分 Sybil 攻击,然后根据地理能量有效路由(Geographical and Energy Aware Routing, GEAR)协议[2]中建立路径的方法构造多条路径,从初始节点发出查询数据包,分别经过这多条路径发往目标节点,查询数据包中携带经过的不同路径中的节点身份和位置信息,目标节点比较这些信息,再结合多跳确认机制[3]检测 Sybil 攻击。本文提出的方法与加密、身份认证的方法相比,降低了通信量和计算量,节省了节点能量。

1 网络模型

本文中用到的网络由一千个传感器节点构成,网络配置好后节点静止不动。节点之间进行无线通信,每个节点和固定的有限数量的邻节点通信,且保存节点信息表和邻节点信息表。

首先作出如下四个假设:

假设一 已知目标节点的位置信息,每个传感器节点都知道自己的位置、身份和剩余能量信息,并通过一个简单的 Hello 消息交换机制知道所有邻节点的位置、身份和剩余能量信息。

假设二 网络在配置阶段是安全的,只有在邻节点间交换身份、位置和剩余能量信息时才会受到 Sybil 攻击。

假设三 传感器节点间的链接是双向的。

假设四 网络只受到 Sybil 攻击,数据包内容是安全的,Sybil 攻击只会从合法节点那里获取整个数据包的内容,使得数据包内容泄密。

根据 Sybil 攻击中单个节点占据多个身份的特点将 Sybil 攻击的表现形式总结为:一个身份多个地理位置、多个身份一个地理位置和多个身份多个地理位置。本文主要研究前两种表现形式的 Sybil 攻击,最后一种表现形式的 Sybil 攻击作为以后的研究工作。

2 攻击检测协议

2.1 节点结构的定义

在检测过程中,节点需要提供它及其邻节点表的信息,为

收稿日期:2006 - 06 - 19;**修订日期**:2006 - 08 - 23 **基金项目**:江苏大学高级专业人才科研启动基金资助项目(05JDG020)
作者简介:余群(1982 -),女,江苏盐城人,硕士研究生,主要研究方向:无线传感器网络安全协议; 张建明(1964 -),男,江苏镇江人,教授,博士,主要研究方向:无线传感器网络安全协议、虚拟现实.

此定义了节点的结构,包括节点本身的信息和它所维护的邻节点表的信息。

定义 1 节点信息。如表 1 所示,各字段分别表示节点的身份、位置、剩余能量、发送包到目标节点的实际代价、是否是 Sybil 节点、具有的邻节点数、接收 Ack 包的规定时间以及指向此节点维护的邻节点表。

定义 2 邻节点表信息。如表 1 所示,字段分别表示邻节点的身份、位置、剩余能量、发送包到目标节点的实际代价、是否是 Sybil 节点及实际代价的大小顺序。

表 1 节点信息表格式

节点类型	信息表内容
节点	nID nLoc nRemainEngy nLearnedCost isSybilNode neighnum T_{ack} ptneigh
邻节点	neighID neighLoc neighRemainEngy neighLearnedCost isSybilNode neighCostOrder

2.2 几种包的定义和初始化工作

在检测过程,需要用到一系列的数据包,为此定义了下面六种包和其中的两个参数,并对它们进行了初始化。

1) Req 包、Rep 包和 Info 包的定义

表 2 中 Req 包中字段 feedback 表示是否要求其他节点返回 Rep 包;Rep 包中字段 node 表示返回节点信息,feedback 表示是否已向目标节点返回 Rep 包;Info 包中字段 sybilnodeID[sybilnodenum]存放是 Sybil 节点的节点身份。

2) Query 包、Ack 包、Alarm 包和参数 Ack_Span、Ack_TTL 的定义

本文借鉴了文献[3]中的使用三种数据包及多跳确认机制来检测攻击的方法,下面定义了三种本文中所要用到的数据包。表 2 中 Query 包中字段 nID_nLoc[passnodenum]存放 Query 包经过的路径上的节点的身份和位置信息,后面三个字段分别表示初始节点发送包、目标节点接收包和理论上查询数据包平均每跳传输的时间,Ack_Cnt 是一个递减计数器;Ack 包中字段 TTL 表示 Ack 包丢失前传输的跳数;Alarm 包中字段 Time_Stamp 表示检测出 Sybil 节点丢弃 Query 包的时间;Ack_Span 决定哪个节点需要发送 Ack 包,Ack_TTL 表示 Ack 包在被丢弃前能够传输的跳数。设定 Ack_TTL = t * Ack_Cnt ($t \geq 2$),因此一个中间节点可能接收来自下游节点的 t 个 Ack 包。t 表示中间节点需接收到的 Ack 包个数的最小值。

表 2 报文类型与格式

报文类型	报文格式
Req 包	SrcID feedback
Rep 包	DstID node feedback
Info 包	DstID sybilnodenum SybilnodeID[sybilnodenum]
Query 包	DstID SrcID nID_nLoc[passnodenum] Tsrcnode Tdstnode Ttheory Ack_Cnt
Ack 包	nID TTL
Alarm 包	DstID Time_Stamp Sybil_Node_ID

3) 初始化工作

在基站中设置一个最小能量值 E_{min},将节点和邻节点的标记 isSybilNode = FALSE。置 Ack_Cnt = Ack_Span,TTL = Ack_TTL。规定事件区域内首先收到 Query 包的节点为目标节点,Query 包从基站发往目标节点,对于中间节点,基站是其上游节点,目标节点是其下游节点。

2.3 检测协议

Sybil 攻击的检测协议分为以下三个部分:

2.3.1 基站检测 Sybil 攻击

协议 1 是在网络未通信之前,基站和节点通过 Req 包、Rep 包和 Info 包的传输实现互相检测,检测出网络里部分或全部表现为一个身份多个位置的 Sybil 攻击的存在。

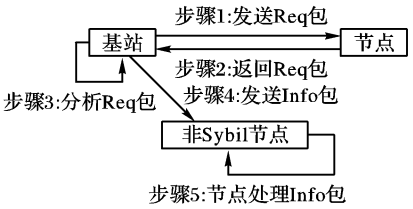

图 1 协议 1 过程

步骤 1:基站向网络内的节点泛洪一个 Req 包,将包中的字段 SrcID 赋值为其自身的身份,字段 feedback = TRUE。

步骤 2:节点接收基站发送过来的 Req 包,判断其中的字段 feedback 的值。如果 feedback = TRUE,则置 Rep_Msg. DstID = Req_Msg. SrcID 且 feedback = FALSE,向基站返回 Rep 包。

步骤 3:基站将从节点那接收到的 Rep 包信息存放在自己的内存中,判断其中携带的信息。如果 nRemainEngy < E_{min},则置 nRemainEngy = 0;如果节点 i 和节点 j 的身份相同位置不同,则置 node[i]. isSybilNode = TRUE, node[j]. isSybilNode = TRUE;如果 node[j]. isSybilNode = TRUE,且节点 j 是节点 i 的邻节点,则置 Info_Msg. sybilnodeID[s] = nID_j,且 sybilnodenum 加 1。

步骤 4:基站向网络里的非 Sybil 节点发送 Info 包,告知非 Sybil 节点存在哪些邻节点是 Sybil 节点。

步骤 5:节点 isSybilNode = FALSE 时接收来自基站的 Info 包时,通过 Info 包中的字段可知是 Sybil 节点的邻节点身份和个数,将相应的邻节点的字段赋值 isSybilNode = TRUE。

在协议 1 中,基站只能检测出部分或全部一个身份多个地理位置的 Sybil 节点,下面依据 GEAR 协议中建立路径的方法构造多条路径,并结合多跳确认机制对网络中未检测出来的一个身份多个地理位置的 Sybil 节点及多个身份一个地理位置的 Sybil 节点进行检测。

2.3.2 建立多路径转发 Query 包并实现多跳确认

协议 2 根据 GEAR 协议中建立路径的方法构造多条路径,在不同路径上转发 Query 包,同时利用 Ack 包实现多跳确认机制,在规定时间内未接收到 Ack 包时生成并传输 Alarm 包到目标节点。假设节点 N 转发 Query 包 P 到目标节点 T。

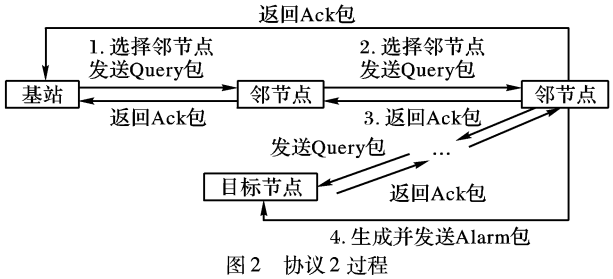

图 2 协议 2 过程

1) 基站 N 选择邻节点发送 Query 包

步骤 1:N 查看自己的邻节点表。如果邻节点 N_i 的 isSybilNode = FALSE,则 N_i 计算到 T 的距离,归一化得到 $d(N_i,T)$,将 N_i 的剩余能量归一化得到 $e(N_i)$,根据公式(1)计算 N_i 到 T 的估计代价 $c(N_i,T)$,且 N_i 的实际代价赋值 $h(N_i,T) = c(N_i,T)$。

$$c(N_i,T) = \alpha d(N_i,T) + (1-\alpha)e(N_i) \quad (1)$$

步骤2:如果节点N存在实际代价最小且比N的实际代价小的邻节点N_{min},则N将 Query 包转发给它,且将节点的身份和位置信息添加到 Query 包中的字段 nID _ nLoc[passnodenum]中,置$h(N,T) = h(N_{min},T) + C(N,N_{min})$。$C(N,N_{min})$是包从节点$N$发送到$N_{min}$的能量消耗,是两节点$N,N_{min}$关于位置和剩余能量的一个函数;如果节点$N$的邻节点的实际代价都比它的大,则出现路由空洞现象,转步骤3。

步骤3:节点N将包转发给邻节点N_j,N_j发现其所有邻节点的代价都比其大,若N_j具有邻节点N_{j1}、N_{j2},如果$h(N_j,T) < h(N_{j1},T)$且$h(N_j,T) < h(N_{j2},T)$且$h(N_{j1},T) \leqslant h(N_{j2},T)$,则$N_j$选择节点$N_{j1}$转发包,将 Query 包中的节点$N_j$的身份和位置信息换成节点$N_{j1}$的身份和位置信息,且$h(N_j,T) = h(N_{j1},T) + C(N_j,N_{j1})$。

步骤4:基站N比较其邻节点表中邻节点$N_{i1},N_{i2},\cdots,N_{ik}$的实际代价值,如果$h(N_{i1},T) < h(N_{i2},T) < h(N_{i3},T) < \cdots < h(N_{ik},T)$,则分别给$k$个邻节点赋值,即置 neighnode[$N_{i1}$]. neighCostOrder = 1, neighnode[N_{i2}]. neighCostOrder = 2, …, neighnode[N_{ik}]. neighCostOrder = k。建立第一条路径时选择 neighCostOrder 值为 1 的邻节点,建立第二条路径选择 neighCostOrder 值为 2 的邻节点,依次类推。

2) 某一中间节点选择邻节点转发 Query 包

过程同上步骤 1 和步骤 2。节点依次选择邻节点转发 Query 包,直至将 Query 包转发给目标节点,基站选择不同的邻节点从而建立多条路径。

3) 邻节点向其上游节点返回 Ack 包

沿着上面建立的多条路径发送 Query 包给其邻节点,等待其邻节点返回 Ack 包。节点N_i接收到 Query 包后,如果 Ack_Cnt = 0,置 Ack_Cnt = Ack_Span 且 TTL = Ack_TTL,生成 Ack 包,沿着 Query 包传输的反方向路径将 Ack 包发送给向其传输 Query 包的上游节点;如果 Ack_Cnt≠0,则将 Ack_Cnt 值减 1,将 Query 包继续转发给下个节点,等待下游节点返回给它的 Ack 包。目标节点收到上游节点发送过来的 Query 包,向其上游节点返回 Ack 包。

4) 生成并发送 Alarm 包

如果在规定时间T_{ack}内未接收到指定数目的 Ack 包,则生成 Alarm 包,将其发送给目标节点。目标节点接收 Alarm 包。

2.3.3　目标节点检测 Sybil 攻击

目标节点判断接收到的 Query 包中携带的节点身份和位置信息,并判断 Alarm 包中的 Sybil_Node_ID 信息,检测 Sybil 攻击。算法步骤如下:

步骤1:建立的路径数为k,判断经过k条路径到达目标节点T的每个 Query 包中节点的身份和位置信息;如果存在两个或两个以上节点的身份相同位置不同,则分别将这些节点的 isSybilNode 置为 TRUE。

步骤2:判断k个 Query 包中节点的身份和位置信息,进行两两比较。如果建立的路径有共同节点,转选项 1;如果没有共同节点,转选项 2;

选项 1:判断分别经过k条路径到达目标节点T的 Query 包中的字段 nID_nLoc[passnodenum]值。如果存在两个或两个以上节点的身份相同位置不同,则分别将这些节点的 isSybilNode 置为 TRUE;如果存在两个或两个以上节点的位置相同身份不同,则分别将这些节点的 isSybilNode 置为 TRUE;如果不同路径上的节点身份不同位置也不同,则转步骤3;

选项 2:判断分别经过k条路径到达目标节点T的 Query 包中的字段 nID_nLoc[passnodenum]值。如果存在两个或两个以上身份相同位置相同的节点,则分别将这些节点的 isSybilNode 置为 TRUE;如果不同路径上的节点身份不同位置也不同,则转步骤3。

步骤3:置$T_{trans} = T_{dstnode} - T_{srcnode}$。如果$T_{trans} \ll T_{theory} * (n-1)$或$T_{trans} \gg T_{theory} * (n-1)$,则此路径中存在 Sybil 节点;如果$|T_{trans} - T_{theory}| < \theta$,则此路径中不存在 Sybil 节点;

步骤4:目标节点T判断接收到的 Alarm 包中的 Sybil_Node_ID。如果 Sybil_Node_ID == node[i]. nID,则此节点为 Sybil 节点。

步骤5:统计所有 Sybil 节点的身份和数量。

利用多路径转发 Query 包和多跳确认机制相结合的方法,网络中的数据包可避免被 Sybil 节点捕获。

3　实验及相关工作比较

目前检测 Sybil 攻击的方法有:文献[4]提出节点与基站共享一个对称密钥,节点间通过基站证实彼此身份建立共享密钥,用它去实现验证加密它们之间的连接;文献[5]提出的方法一种是射频测试,节点只能有一个射频收发器且不能同时在多个信道上发送和接收信息,当某个信道专门指定给某一邻节点时,节点以一定的概率检测 Sybil 节点。另一种是随机密钥预分布,通过验证节点拥有的部分或全部密钥来证明此节点身份的真伪性;文献[1]提出给节点分发身份证明书,任意两个节点通过 Merkle 哈希树加密方法认证彼此身份。本文从通信量、计算量和能量消耗这三个方面分别与文献[5]的第二种方法和文献[1]改进后方法进行性能比较。

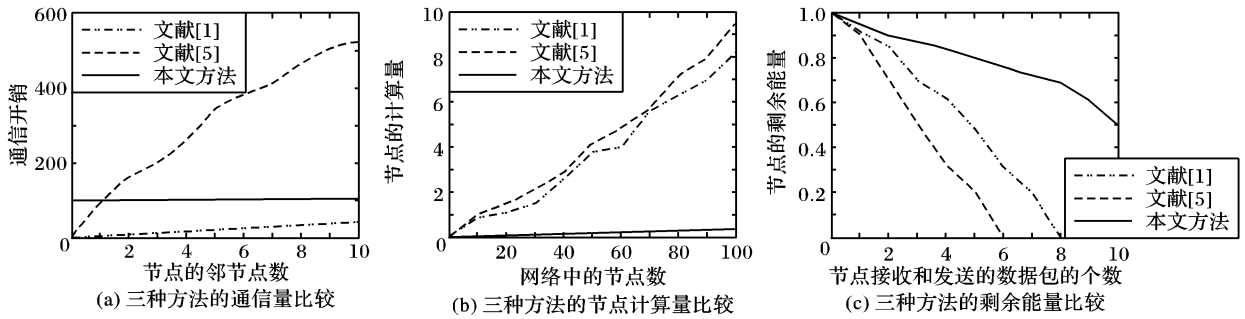

图3　三种方法的性能比较

在 TOSSIM 中实现下面的仿真,假设在$(2\,000 \times 2\,000)\,m^2$中均一地散布 400 个节点,包以 19.2Kbps 的速度逐跳传输。为了方便下面的分析,假设网络中有N个节点,每个节点有n个邻节点,文献[5]中网络通信量为$O(nkN)$,节点计算量为$O(k)$,k为给每个节点分配的密钥数。文献[1]中网络通信量为$O(n\log_2 N)$,节点计算量为$O(N)$。本文网络通信量为$O(N)$,除基站和目标节点计算量稍大外,每个节点只需接收

(下转第 2902 页)

身份,也不能进行地址哄骗。

2）每个节点以客户证书的形式本地存储自己的客户信息以供其他节点方便地查询。为防止实体篡改自己的信誉值或者因为不满其他节点对自己信誉值评价而报复评价节点,它的信誉值以信誉证书的形式存储于评价节点[6]。

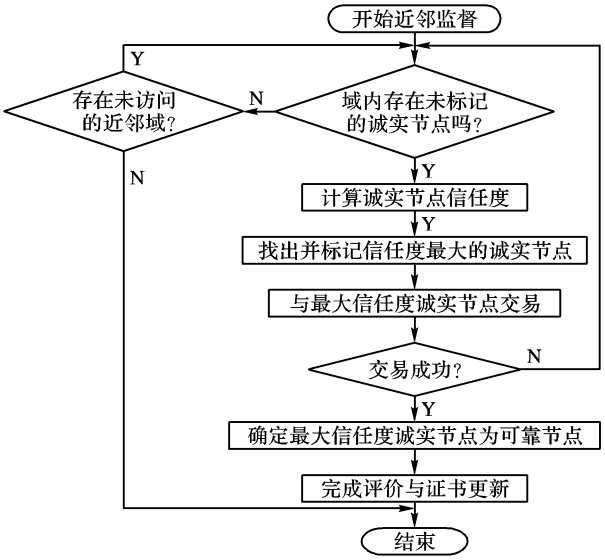

图2 可靠节点的搜索过程

3）网络内的每个节点执行近邻监督，按2.2节所述,计算本域内节点信任度,识别诚实节点、恶意节点、自私节点,并赋予一定的信任等级。

4）在本域的诚实节点中,利用冒泡排序等算法挑选信任度最大的节点,加以标记,同时与该节点进行交易。若节点交易成功,则将该节点作为本域内的可靠节点,退出冒泡排序循环,结束最大信任度节点的选择,转至5);否则,在未标记的节点中重复4),直到本域内的所有诚实节点都被访问过,此时转至6)。

5）上述节点在与可靠节点双方交易完成后,就作为评价者根据交互过程对可靠节点进行评价,以信誉证书形式存储评价的信誉值,并生成新的证书单元附加到被评价节点的客户证书之后,作为以后自己和其他节点判断的依据。可靠节点作为被评价节点向先前已在与之交互的其他评价节点发布证书已经成功更新的通知。如果这些评价节点没有更新证书或者更新的证书无效,则被评价节点向先前的客户端发出证书没有成功更新的通知,要求当前的客户端正确更新证书。转至7)。

6）访问相邻的其他域,执行4)。

7）结束节点间的访问过程。

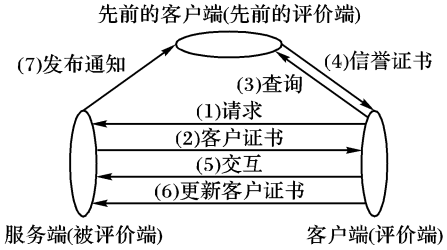

图3 节点间的认证、交互和证书修改过程

4 结语

基于信誉的信任机制的混合式P2P模型TBHPM可以加强节点间的合作,高效地实现节点间的交易,同时在一定程度上也很好地提高了系统的安全性。当然,随着与可靠节点通信量的增加,可靠节点可能成为网络内的瓶颈。在以后的研究中,需进一步完善这一方面的工作。但是总的说来,TBHPM在无线通信领域特别是那些对能量、效率要求比较苛刻的对等Ad hoc领域都有很好的应用前景。

参考文献:

[1] PAUL R, KUWABARA KO, ZECKHAUSER R, *et al*. Reputation systems[J]. Communications of the ACM, 2000, 43(12):45-48.

[2] 蔡晟,王泽兵,冯雁,等.基于Super-peer的对等网络研究[J].计算机应用研究,2004,21(6):258-260.

[3] WANG Y, VASSILEVA J. Trust and reputation model in peer-to-peer networks[A]. Proceedings of the 3rd IEEE Int'l Conference on Peer-to-Peer Computing[C]. Linköping: IEEE Computer Society, 2003. 150-158.

[4] SANKHLA V. SMART: A Small World based Reputation System for MANETs[D]. California: University Of Southern California, 2004.

[5] 窦文,王怀民,贾焰,等.构造基于推荐的Peer-to-Peer环境下的Trust模型[J].软件学报,2004,15(4):571-583.

[6] 赵恒,权义宁,胡予濮.对等网环境下一种安全有效的信誉体制[J].计算机应用,2005,25(3):551-553.

(上接第2899页)

和转发数据包,部分节点做简单的判断,因此计算量可忽略。根据三种方法的通信量和计算量可知本文方法节点的能量消耗最小。如图3(a),本文所用的检测方法在网络中多于一个节点时通信量远低于文献[5]的通信量,如图3(b)、(c),节点的计算量和能量消耗远小于文献[1,5]中的计算量和能量消耗。

4 结语

Sybil攻击是一个节点向网络中的其他节点呈现出多个身份,会破坏无线传感器网络的数据融合、资源分配等机制。本文提出了一种检测Sybil攻击的方法,能够有效地降低通信量和计算量,节省节点的能量。我们将在以后的工作中对多个身份多个地理位置的Sybil攻击形式进行研究,以完善对Sybil攻击的检测。

参考文献:

[1] ZHANG QH, PAN W, DOUGLAS S, *et al*. Defending against sybil attacks in sensor networks[A]. Proceedings of the 25th IEEE International Conference on Distributed Computing Systems Workshops (ICDCSW'05)[C]. 2005. 1545-0678.

[2] YU Y, GOVINDAN R, ESTRIN D. Geographical and energy aware routing: a recursive data dissemination protocol for wireless sensor networks[R]. Technical Report UCLA / CSD-TR-01-0023. UCLA Computer Science Department, 2001.

[3] YU B, XIAO B. Detecting selective forwarding attacks in wireless sensor networks[EB/OL]. http://www4.comp.polyu.edu.hk/~csbxiao/files/pub/SSN-06-Selective% 20forwarding% 20attacks.pdf, 2006.

[4] KARLOF C, WAGNER D. Secure routing in wireless sensor networks: attacks and counter-measures[A]. First IEEE Intl. Workshop on Sensor Network Protocols and Applications (SNPA 2003)[C]. Anchorage, AK, USA: IEEE computer Society, 2003. 113-127.

[5] NEWSOME J, SHI E, SONG D, *et al*. The sybil attack in sensor networks analysis & defenses[A]. Proceedings of Third Intl. Symposium on Information Processing in Sensor Networks (IPSN'04)[C]. Berkeley, California, USA: ACM Press, 2004. 259-268.