A Novel Traceback Scheme of Malicious Nodes in Wireless Sensor Networks*

ZENG Meimei, JIANG Hua, WANG Xin*

(*Guilin University of Electronic Technology, GuiLin Guangxi* 541004, *China*)

Abstract: For wireless sensor networks lacking of single reliable routing device, the packet markings will be tampered by forwarding nodes. In order to solve this problem, this paper proposes an improved node sampling packet marking method. The method generates the watermark with the ID and data packet by hash function, and then probabilistic watermark marking (PWM) marks into the marked area. The Sink node can trace the malicious node using the markings. This algorithm effectively prevents the colluded nodes from changing marking, and locates the malicious node in a hop. The theoretical analysis and simulations show that the improved algorithm can effectively track the malicious nodes. Compared to the methods of based on edge marking traceback, the success rate rapidly increases.

Key words: malicious node; colluded node; probabilistic watermark marking (PWM); packet marking

EEACC: 6150P; 7230 **doi**: 10.3969/j.issn.1004-1699.2013.01.025

一种新的无线传感器网络恶意节点追踪方法*

曾梅梅, 蒋 华*, 王 鑫

(桂林电子科技大学计算机科学与工程学院, 广西 桂林 541004)

摘 要: 无线传感器网络中缺少单一可信的路由设备, 存在中间节点篡改包标记的问题, 为解决这一问题, 提出一种改进的节点采样包标记算法。该算法通过对 ID 和数据包进行 HASH 运算来产生水印, 并把水印概率性标记到相应的标记区中, Sink 节点根据标记信息来实现对恶意节点的追踪。该算法能够有效地抵抗串通节点更改标记, 把恶意节点定位在一跳范围之内。实验表明, 改进后的算法可以有效地追踪到恶意节点, 并将该方法与基于边标记的追踪方法进行对比, 定位成功率得到提高。

关键词: 恶意节点; 串通节点; 概率性水印标记; 包标记

中图分类号: TP393 **文献标识码**: A **文章编号**: 1004-1699(2013)01-0122-06

无线传感器网络广泛地应用于生活、军事、农业、环境监测、智能家居等领域。通常, 无线传感器网络工作环境比较恶劣, 存在严重的安全威胁[1]。此外, 无线传感器网络的无人照管操作使得传感器节点易于被敌方物理性地控制, 从而成为恶意节点, 并获得节点自身存储的信息, 包括密钥等机密信息[2]。这些恶意节点将会对网络产生巨大的危害, 比如虚假信息注入[3], 就是一种由恶意节点发起的严重攻击。恶意节点可以注入大量的虚假流量, 并随着路径前进发送到 Sink 节点, 将导致应用程序失败、能量和带宽耗费等严重的问题。对于 DOS 攻击, 目前主要解决方案是在节点上进行过滤虚假数据包来减缓危害, 但无法在攻击后进行主动防御。

针对数据包过滤的不足, 本文重点研究主动防御问题, 即如何在传感器网络中定位到恶意节点, 进而采取相应的主动防御策略。如果能够获知恶意节点的位置, 就可以把它们从网络中隔离或移除, 从根本上消除了攻击发生的可能性。然而, 在无线传感器网络中, 准确定位恶意节点存在很大的困难。一方面, 无线传感器网络的架构不同于互联网, 节点既是主机又是路由器, 而且每个节点都是平等的, 缺少可信任的路由设施。另一方面, 存在串通节点配合源恶意节点进行攻击, 它们不但共享密钥, 而且可以应用合理的方法操纵数据包来掩盖它们的路径, 这

项目来源: 国家自然科学基金重点项目(61262074)
收稿日期: 2012-09-15 **修改日期**: 2012-12-10

些篡改攻击比起简单增加虚假流量更复杂。由于互联网下的 IP 追踪技术较少考虑到串通节点配合情况[3-5],不能直接应用于无线传感器网络上。针对这一问题,本文在包标记框架的基础上,提出一种适用于无线传感网络下恶意节点溯源追踪的算法。

1　相关工作

在无线传感器网络中,虚假信息注入攻击是一种重要的安全威胁,该领域的研究主要集中于途中过滤和广播认证的方法[3,7-10]。途中过滤[3,7-8],即在虚假数据包到达 Sink 节点之前进行路由过滤,该方法只能暂时地减轻危害,不能够定位并隔离恶意节点,从而无法阻止恶意节点继续注入虚假信息,甚至这些数据包可能经过多跳后才被发现,此时虽可以对其进行过滤,但它们已经消耗合法节点的能量。文献[9]提出一种叫做 CAPTRA 的广播认证方法,通过充分利用节点发送分组信息时的广播特性来进行追踪。节点利用布隆过滤器(Bloom Filter)的数据结构来节约存储分组信息所要消耗的内存。当转发节点接收到分组时,附近的监听节点也会收到该分组信息,都对分组信息进行提取,把所提取出来的部分信息作为分组摘要,并把上一跳转发节点的标志等信息一起存储在过滤器中。这种方法不足在于追踪过程需要反复迭代,消耗大量通信和内存。文献[10]提出一种基于公钥密码体系的广播认证方法,将恶意节点定位在两步范围内,但是传感器节点的能量和计算能力的限制,它所采用的公钥体系方法将不适用于传感器网络。近年来,开始有研究提出基于包标记[11-13]的方法。文献[12]提出了一种概率性嵌套包标记方法(PNM),为了保护上游节点在数据包上的标记,每个转发节点以嵌套方式标记数据包,防止串通节点掩盖数据包经过节点的位置,或者是串通节点自身的位置。但是,随着节点不断地被加密标记,数据包越来越大,将明显的加重网络通信负载。文献[13]提出一种基于边采样追踪方法,通过对节点的 ID 进行两次加密,防止泄露包标记的信息。由于仅对 ID 加密,随着多个数据包的传送,将造成串通节点可以复制数据包中加密节点的信息,从而伪造其他无辜节点,而不能精确定位到恶意节点,甚至可能误定位到无辜节点。

根据以上情况,本文提出一种适用于无线传感器网络的溯源追踪方案。该方案采用对称密钥方法,利用包头中的两个节点域,根据某一概率对数据包和 ID 进行 HASH 产生水印,然后把水印标记到节点域中,实现恶意节点地溯源追踪。实验结果表明,基于水印的追踪方法的计算量和网络通信量较小,同时具有较高的安全性和恶意节点定位准确率。

2　解决方案

2.1　基础概念

假设每个传感器节点都有一个唯一的 ID 标识符,节点的位置在传感器网络部署后相对固定不再移动,节点之间的通信是通过多跳无线通道来完成信息传递。同时,假定数据包传输的路径相对稳定,即在短时间内是不会频繁改变,每个节点都只有唯一的下一跳节点。

源恶意节点:发送大量虚假数据包的节点,如图 1 中的节点 S。

串通节点:在前转路径上,通过伪造标记或删除标记,协同源恶意节点注入虚假信息等,如图 1 中的节点 X。

恶意节点:包括串通节点和源恶意节点。

定位节点:溯源追踪方案定位到的节点。

定位成功:即定位节点是恶意节点或者是在恶意节点的下游一步邻居范围内。

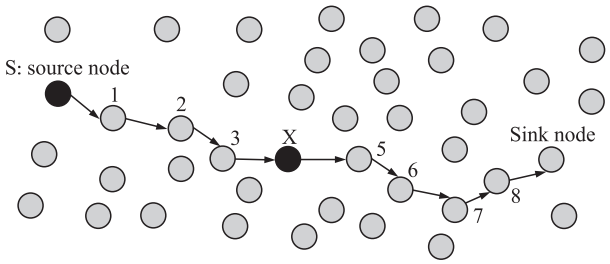


图 1　攻击示意图,节点 S 与 X 是被俘获节点

2.2　标记算法

每个数据包都含有两个节点(node)区域,如图 2 所示。其中,node1 区域用于记录靠近源节点的节点信息,node2 区域用于记录靠近 Sink 节点的节点信息。设原始数据包为 M,节点域初始值为 null;任意节点 n 与 Sink 节点共享一个密钥 K 和一个单向函数 H,H 用于产生节点 ID 和数据包的水印。当节点 i 收到数据包时,首先根据概率 p 来确定是否标记此数据包。如果确定要标记,则产生节点相应的水印 W=H(id|key|M)并进行标记。标记

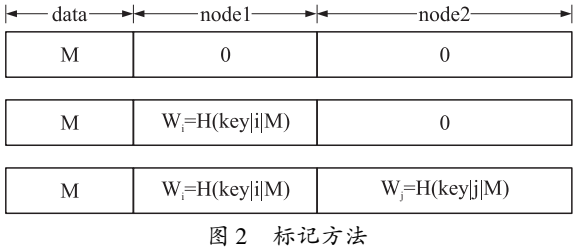


图 2　标记方法

过程如下:

检查 node1 域是否为空:①若(node1)为空,将 W_i 标记在 node1 域中;②若不为空,则检查 node2 域是否为空;③若(node2)为空,则把 W_i 标记在此 node2 域中;④若不为空,则节点覆盖 node1 域进行标记,并把 node2 域置为 null,算法伪代码如表 1 所示。

表 1 标记算法

算法 1:基于水印的标记算法
输入:M //原始数据包 P //标记数据包的概率 i //节点的 ID(唯一标识符) key //节点与 Sink 节点共享的密钥 输出:数据包标记 步骤:节点 i 随机产生一个小于 1 的数据 x 如果 x<p 那么 提取数据包 M,产生节点相应水印 W_i = H(key|i|M) 如果 M. node1 = = null and M. node2 = = null 那么 W_i = H(key|i|M)→M. node1 否则 M. node2 = = null 那么 W_i = H(key|i|M)→M. node2 否则 W_i = H(key|i|M)→M. node1 M. node2 = null

2.3 追踪算法

Sink 节点维护一张表,表项为{id,key},其中,id 是节点唯一标识符,key 是节点与 Sink 节点对应的密钥,以及一个安全单向函数 F1,用于提取水印中的节点 ID。在追踪节点算法中,Sink 节点存储四个集合 un_set,dn_set,e_set,s_set。当节点收到一个标记包时,分别提取数据包的 node1 和 node2 区域,通过解密函数 F1 获取标记节点的 ID,分别记为 id_u 和 id_d,其中 id_u 这类节点称为上游节点,并存入 un_set 集合里;id_d 这类节点称为下游节点,并存入 dn_set 集合里;同时把(id_u,id_d)存放在 e_set 集合里,当收集到足够多的数据包时,就可以构建出攻击的路径;s_set 初始为空,收到标记包后进行存放 id_u,当 id_u 节点出现在 dn_set 集合里或者 id_d 节点出现在 s_set 集合里,则把它从 s_set 中移除,不断地进行更新,存放的唯一节点就追踪到的目标节点,具体算法伪代码如表 2 所示。

根据图 1 所示,假设源恶意节点和串通节点都不标记的情况,Sink 节点收到标记包经过解密后的标记 ID 和通过追踪算法得到四个集合的结果,如表 3所示。

表 2 追踪算法

算法 2:基于水印的追踪算法
输入:F1 //W = H(key|id|M)到 id 的解密函数 id_s //表示 Sink 节点的 ID 输出:s_set,e_set 步骤:初始化 s_set,e_set,un_set,dn_set 每收到一个数据包就进行下列循环 如果 M. node2 = = null and M. node1 ! = null 那么 id_u←F1(M. node1) 如果 id_u ∉ un_set 且 id_u ∉ dn_set 那么把 id_u 加入 un_set,s_set 把(id_u,id_s)加入 e_set 否则 M. node2 ! = null 那么 id_d←F1(M. node2) id_u←F1(M. node1) 把 id_u 加入 un_set 把 id_d 加入 dn_set 把(id_u,id_d)加入 e_set 如果 id_u ∉ dn_set 那么把 id_u 加入 s_set 否则 把 id_u 从 s_set 中移除 把 id_d 从 s_set 中移除 如果 id_d ∈ s_set 那么把 id_d 从 s_set 中移除 把 id_u 从 s_set 中移除

注:为简化伪代码,使其更通俗易懂,伪代码中的移除和加入操作都是先把节点 ID 和相应的集合进行比较,从而避免重复加入或者无值进行移除的情况。

表 3 Sink 节点追踪示例表

标记 ID	un_set	dn_set	s_set	e_set
(7,8)	7	8	7	(7,8)
(3,5)	3,7	5,8	3,7	(7,8)(3,5)
(5,7)	3,5,7	5,7,8	3	(3,5,7,8)
(2,3)	2,3,5,7	3,5,7,8	2	(2,3,5,7,8)
(3,6)	2,3,5,7	3,5,6,7,8	2	(3,6)(2,3,5,7,8)
(6,8)	2,3,5,6,8	3,5,6,7,8	2	(3,6,8)(2,3,5,7,8)
(8,null)	2,3,5,6,8	3,5,6,7,8	2	(3,6,8)(2,3,5,7,8)
(1,5)	1,2,3,5,6,8	3,5,6,7,8	1,2	(1,5)(3,6,8)(2,3,5,7,8)
(1,2)	1,2,3,5,6,8	3,5,6,7,8	1	(1,2,3,5,7,8)(3,6,8)

3 安全性分析

如图 1 所示,节点 S 和节点 X 是被俘获节点,源恶意节点 S 发送大量虚假数据,节点 X 串通节点 S 对数据包进行转发的同时,还可以对数据包中的标记进行修改或者删除。下面针对几种典型的攻击

模型,对本方案的安全性进行分析。

不标记:节点 S 对本身产生的数据包不进行标记,则 Sink 节点可以追踪到节点 S 的下游节点 1。

移除标记:节点 X 串通节点 S 发送虚假信息,并把在节点 S 与节点 X 之间所有标记进行随意删除的情况。本文方案将每个节点的 ID 标记和数据包进行 HASH 产生水印,假设节点每次传送的数据是随机的,则节点 X 不能选择性的对某一个特定的 ID 标记进行删除。如果节点 X 把所有的标记都删除掉,同时不进行标记或者错误标记节点 X 本身信息,则 Sink 节点也可以定位到 X 的下游节点 5;或者是正确标记,那么可以定位到串通节点 X。

更改标记:节点 X 更改上游节点的标记。因为节点的 ID 与数据包 M 进行 HASH 产生水印,不同的数据包 M,所产生的水印就是不同的,所以节点 X 无法获得上游节点的信息来进行更改标记,如果进行随机地更改标记,依然存在部分标记包能够到达 Sink 节点,从而追踪到节点 S 或者节点 1。如果节点 X 可能更改全部的数据包标记,并且自身不进行标记或者错误标记数据包,则可以追踪到节点 5;如果进行正确地标记,则可以追踪到节点 X。

选择性丢弃:节点 X 随机地选择丢弃上游节点的标记。节点 X 不知道所丢弃标记的 ID,所以不能针对性的去选择删除同一 ID 的标记,不能进行全丢弃,同样存在部分标记包能够到达 Sink 节点,从而追踪到节点 S 或者节点 1。

从以上分析可以得出,本文方案能够应对几乎全部的攻击类型,因此具有很强的实用性。

4　实验仿真与结果分析

根据赠券收集(Coupon Collector)问题[3],Sink 节点收到攻击路径上所有 d 个节点的不同标记包的期望为 $d\ln d+O(d)$。Sink 节点接收到一个距离攻击者 i 跳的节点标记的数据包的概率是 $p(1-p)^{d-i}$,当 $i=1$ 时概率最小,假设攻击路径上所有节点的标记包到达 Sink 节点的概率都为 $p(1-p)^{d-1}$,那么 Sink 节点收到一个标记包的概率是 $dp(1-p)^{d-1}$,Sink 节点完成路径重构需要的攻击包总个数 X 的期望值是 $E(X)<\dfrac{\ln d}{p(1-p)^{d-1}}$。假设路径长度已知,可以通过计算 $\dfrac{\ln d}{p(1-p)^{d-1}}$ 最小值来得出标记概率。假设 $f(p)=p(1-p)^{d-1}$,根据 $f(p)$ 的最大值与 $\dfrac{\ln d}{p(1-p)^{d-1}}$ 的最小值相等,本文通过求 $f(p)$ 的最大值来得出标记概率。

假设 $f(p)=p(1-p)^{d-1}$,所以对公式 $f(p)$ 求导如下:

$$\frac{\mathrm{d}}{\mathrm{d}p}(f(p))=(1-p)^{d-1}+(d-1)p(1-p)^{d-2}=(1-p)^{d-2}(1-dp) \tag{1}$$

因为 $p\in(0,1)$,由式(1)可知,当 $p=\dfrac{1}{d}$ 时,$f(p)$ 取得最大值,即 $dp=1$ 时,$\dfrac{\ln d}{p(1-p)^{d-1}}$ 取得最小值。

实验在 windows7 环境下,采用 CYGWIN+NS2 的仿真软件,对算法进行验证。实验采用随机图,为保证网络连通性,传感器网络模型的主要参数如下:有 400 个节点平均分布为 800 m×800 m 平坦区域 A 范围内,其中有一个是 Sink 节点在传感器区域 A 之外,如图 3 所示。根据不同跳数,由 $dp=1$ 来设定固定概率的大小,如图 4 所示,当节点跳数 $d<10$ 时,Sink 节点只要收到 17 个数据包,其中接收到含有标记的数据包可达 92%。同样,在 $d=20$ 跳或 30 跳,分别需要 46、55 个数据包就可以达到 90%,结果表明只需要较少的数据包,Sink 节点就可以收到所有节点的标记,尽可能少的耗费传感器节点能量和带宽。

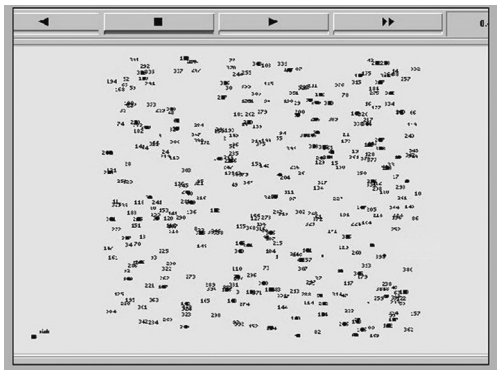


图 3　传感器节点随机分布图

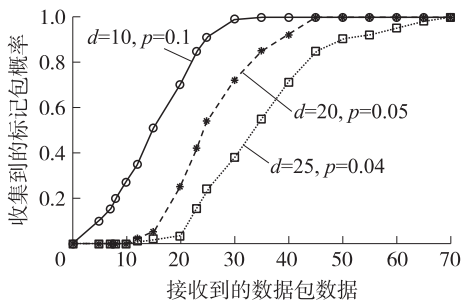


图 4　Sink 节点收集到标记的概率

源恶意节点随机产生的数据包 M,由中间节点根据概率 p 确定是否进行标记,确定标记的信息是通过 HASH 算法根据密钥不同对数据包产生一段长度为 64 bit 的水印,并根据标记算法进行相应地

标记。根据对基于边标记追踪算法的理论分析,它所采用的是仅对节点的 ID 进行两次加密的方法来进行追踪,存在标记信息能够被串通节点所获悉并进行篡改的情况,因此本文选用此算法与 PWM 进行对比。不同跳数下节点成功定位所需要的数据包数量不同,针对数据包数量是 200、400 分别从 5 跳到 50 跳进行实验,根据图 5 所示,200 个数据包在 20 跳范围内,定位成功率为 99%。根据图 6 所示,400 个数据包在 40 跳可以达到 90%,并与基于边标记的方法[12]进行对比,数据包数量为 200、400 定位的成功率分别提高了 11.7% 和 13.1%。

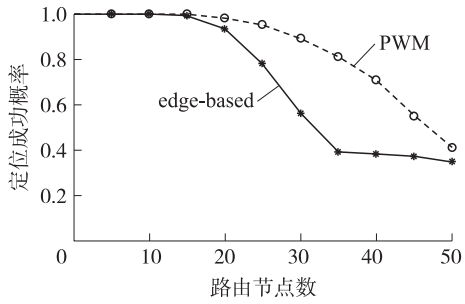


图 5 发送 200 个数据包,节点成功定位的概率

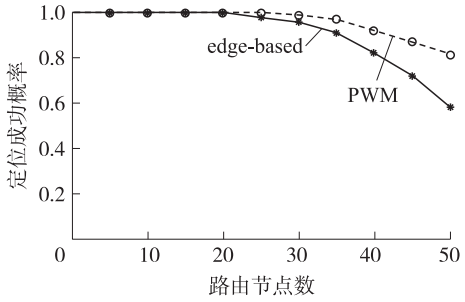


图 6 发送 400 个数据包,节点成功定位的概率

在提高网络的安全性同时,本文对提高安全性的代价进行分析如下:采用水印技术的追踪方法,节点在标记的算法中,时间复杂度为常数级;Sink 节点在重构路径的时间复杂度为 $O(n)$。由于节点的通信消耗远远大于计算能耗,而且本文采用是轻量级的水印技术,所以计算能耗可以忽略不计[1]。

根据无线传输能量模型[14],数据包在单跳传输/接收 1 bit 信息所需的能量:

$$E_b = E_t + E_r + \frac{E_{\text{dec}}}{l} \tag{2}$$

其中,E_b 表示节点的总能耗;E_t 和 E_r 分别表示传输和接收状态下的能量消耗,E_{dec} 表示数据包解码能量,可以忽略不计。l 表示有效负载。

由式(2)可得,

$$E_b = k_1 + k_1 \frac{(\alpha+\tau)}{l} + \frac{k_2}{l} \tag{3}$$

其中,k_1 表示传输 1 bit 有用信息所消耗的能量;k_2 表示无线电收发部件启动时所消耗的能量;α 表示数据包的头部;τ 表示数据包的尾部。两个节点域都标记,则数据包的能耗情况如式(4):

$$E'_b = k_1 + k_1 \frac{(128+\alpha+\tau)}{l} + \frac{k_2}{l} \tag{4}$$

标记数据包能耗最大增加 $k_1 \frac{128}{l}$,为了突出标记产生的能耗,本文针对考虑可靠性较好的网络,即数据包越长越好的情况。采用 RFM-TR1000 收发器时,可以计算出 $k_1 = 1.85$ μJ/bit,$k_2 = 24.86$ μJ/bit,取 $l = 128$ byte 进行计算。计算可得,$E'_b = E_b + \frac{k_1}{8}$,标记的数据包仅仅多消耗 0.02 μJ,为提高安全性所付出的能耗代价是可以承受的。

5 结论

目前虚假信息注入攻击越来越受关注,但是现有的方法绝大多数都是通过途中过滤来被动地减小攻击产生的危害。基于水印方法的追踪方法是一种在存在串通节点的情况下,采用主动防御定位到恶意节点的方法,最后可以结合物理性移动或者网络隔离,彻底解决恶意节点所产生的危害。本文通过安全性分析和仿真实验证明了 PWM 方法,在恶意节点危害到网络之前,能够定位到恶意节点,有效地防止虚假信息注入。下一步将进行如下的研究:①在当前的无线传感器网络平台上进行实验来评价 PWM 的性能;②研究如何在网络检测[15]和隔离追踪到的恶意节点。

参考文献:

[1] Sen J. A Survey on Wireless Sensor Network Security [J]. International Journal of Communication Networks and Information Security(IJCNIS),2009,1(2):55-76.

[2] 杨黎斌,慕德俊,蔡晓妍. 基于博弈理论的传感器网络拒绝服务攻击限制模型[J]. 传感技术学报,2009,20(1):90-94.

[3] Ye F, Luo H Y, Lu S W, et al. Statistical En-Route Filtering of Injected False Data in Sensor Networks [J]. IEEE Journal on Selected Areas in Communication,2005,23(4):839-850.

[4] Savage S, Wetherall D, Karlin A, et al. Practical Network Support for IP Traceback[C]//Proc. ACM SIGCOMM'00,2000:319-327.

[5] Snoeren A, Partridge C, Sanchez L, et al. Hash-Based IP Traceback [C]//ACM SIGCOMM'01,2001:27-31.

[6] Dong Q, Banerjee S, Adler M, et al. Efficient Probabilistic Packet Marking [J]. Proceedings of the 13th IEEE International Conference on Network Protocols,2005:368-377.

[7] Zhu S, Setia S, Jajodia S, et al. An Interleaved Hop-by-Hop Authentication Scheme for Filtering of Injected False Data in Sensor

Networks[C]//IEEE Symposium on Security and Privacy'04. Caliomia:Los Alamitos,Calif,2004.259-271.

[8] 谢婧,李曦,杨峰.应对虚假数据注入结合途中过滤与溯源追踪方法[J].计算机系统应用,2011,20(12):249-256.

[9] Sy D, Bao L. CAPTRA: Coordinated Packet Traceback[J]. The Fifth International Conference on Information Processing in Sensor Networks(IPSN),Nashville,TN,2006:19-21.

[10] Wang R, Du W, Ning P. Containing Denial-of-Service Attacks in Broadcast Authentication in Sensor Networks[C]//Proc. ACM Mobihoc'07. New York,USA:ACM N. Y. ,USA,2007.71-79.

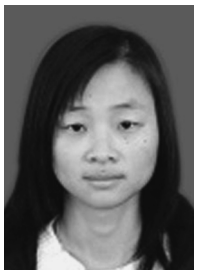
[11] 杨峰,周学海,张起元,等.无线传感器网络恶意节点溯源追踪方法研究[J].电子学报,2009,37(1):202-206.

[12] Ye F,Yang H,Liu Z. Catching Moles in Sensor Networks[J]. In Proc. IEEE ICDCS. Washington, DC, USA: IEEE Computer Society,2007:69-77.

[13] Xu J,Zhou X H,Yang F. Edge-Based Traceback in Sensor Networks[J]. 6th International Conference on Wireless Communications Networking and Mobile Computing(WiCOM),2010:1-4.

[14] 赵彤,杨文国.无线传感器网络中基于能效的最优数据包长[J].中国科学院研究生院学报,2008,25(2):161-166.

[15] 刘华博,崔建明,戴鸿君.基于多元分类的无线传感器网络恶意节点检测算法[J].传感技术学报,2011,24(5):771-777.



曾梅梅(1989-),女,汉族,福建莆田,硕士研究生,主要研究方向为无线传感器网络安全,zmmmmz123@163.com;

蒋　华(1963-),男(汉),河南信阳,教授、硕士生导师,博士,主要研究方向为网络信息安全,jianghua@guet.edu.cn。