第44卷第4期 中国科学技术大学学报 Vol. 44, No. 4
2014年4月 JOURNAL OF UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA Apr. 2014

文章编号:0253-2778(2014)04-0317-08

无线传感器网络中基于邻居节点监听的虚假数据过滤策略

章曙光[1,2],周学海[1],杨 峰[1],徐 军[1]

(1. 中国科学技术大学计算机科学与技术学院,安徽合肥 230027;
2. 安徽建筑大学电子与信息工程学院,安徽合肥 230601)

摘要:提出了一种基于邻居节点监听的虚假数据过滤策略(false reports filtering scheme based on neighbor watch,NWFFS).在NWFFS策略中,每个节点保存两跳邻居节点信息,每个数据包必须包含T个来自不同密钥分区节点的ID及其生成的MAC.除生成数据包的簇头节点外,每个中间节点向其下游节点转发数据包后,还需向自己的上游节点发送ACK包,通过对ACK包的监听,恶意节点利用其他区域俘获节点信息伪造的虚假数据包将被其一跳邻居识别出来,同时中间节点和Sink节点利用自身携带的密钥对少部分逃脱的虚假数据包进行进一步验证.理论分析和实验表明,该策略有效地避免了恶意节点利用任意区域已被其俘获的节点伪造虚假数据而不被识别出来,提高了途中过滤效率,从而降低了恶意节点对网络的影响,延长了网络生存期.

关键词:无线传感器网络;邻居节点监听;两跳邻居节点信息;虚假数据过滤

中图分类号:TP393 **文献标识码**:A doi:10.3969/j.issn.0253-2778.2014.04.009

引用格式:Zhang Shuguang, Zhou Xuehai, Yang Feng, et al. A false report filtering scheme based on neighbor watch for wireless sensor networks[J]. Journal of University of Science and Technology of China, 2014,44(4):317-324.

章曙光,周学海,杨峰,等. 无线传感器网络中基于邻居节点监听的虚假数据过滤策略[J]. 中国科学技术大学学报,2014,44(4):317-324.

A false report filtering scheme based on neighbor watch for wireless sensor networks

ZHANG Shuguang[1,2], ZHOU Xuehai[1], YANG Feng[1], XU Jun[1]

(1. *School of Computer Science and Technology, University of Science and Technology of China, Hefei* 230027, *China*;
2. *School of Electronics and Information Engineering, Anhui JianZhu University, Hefei* 230601, *China*)

Abstract: A false report filtering scheme based on neighbor watch was proposed, in which information from two-hop neighboring nodes was stored, which included IDs and MACs of T nodes from different zones. Each forwarding node sent an ACK message to its upstream node after sending a report to its downstream node. False reports generated with keys from other zones would be detected by the one-hop neighbors of the malicious node. Meanwhile, forwarding nodes and the Sink would verify the authenticity

收稿日期:2013-04-03;**修回日期**:2013-07-16

基金项目:国家自然科学基金(60873221),安徽省教育厅自然科学重点项目(KJ2008A103)资助.

作者简介:章曙光,男,1970年生,博士生/副教授. 研究方向:无线传感器网络和网络安全. E-mail: zhangsg@mail.ustc.edu.cn

通讯作者:周学海,博士/教授. E-mail: xhzhou@ustc.edu.cn

of other reports. Analysis and experimental results show that this scheme improves filtering efficiency significantly, thus reducing the impact of malicious nodes and extending the life of the sensor network.
Key words: wireless sensor networks; neighbor watch; two-hop node information; false data filtering

0 引言

随着嵌入式计算技术、传感器技术和通信技术的迅猛发展,无线传感器网络(wireless sensor networks,WSN)在许多领域得到了广泛应用[1-2].传感器网络节点通常部署在野外或者是敌方区域,由于价格低廉、抗捕获的能力较弱,攻击者可以通过俘获若干节点向网络注入虚假数据、恶意篡改或丢弃转发的数据包,若不加以防范,这些虚假的数据将会消耗有限的网络资源,造成部分网络临时或永久瘫痪,同时引发错误警报,影响用户决策.为避免上述问题,目前已提出了许多途中过滤策略用于解决上述问题[3-9].其基本思想是当事件发生时,事件周围的多个节点侦查到事件发生,簇头节点收集 T 个以上数据,融合数据后,选择在待发送的数据包后额外附加 T 个 MAC(message authentication code),转发节点利用共享密钥对数据包进行认证,从而实现对虚假数据的识别和过滤.上述策略不能有效防止一个恶意节点利用已被其俘获的节点信息伪造一个发生在网络中任何区域的虚假事件.

为解决上述问题,本文提出了一种基于邻居节点监听的虚假数据过滤策略,该策略通过监听上游节点是否发送 ACK 包来判断上游节点是生成数据包的节点还是中间转发节点,若恶意节点利用其他区域被俘获节点信息伪造虚假数据包,则将被其一跳邻居节点识别出来,因此提高了途中过滤效率,降低了恶意节点对网络的影响,延长了网络生存期.

1 相关工作

文献[3]最早提出了 SEF 策略,其基本策略是通过在发送的数据包后附加 T 个 MAC 来实施认证,每个节点随机地在密钥库中选择少部分密钥存储,转发节点利用其存储密钥对数据进行认证,并过滤掉虚假数据.为提高网络的安全性,该策略进一步要求一个合法的数据报告必须要用来自 T 个不同密钥分区中的探测节点来标记,但若攻击者俘获大约 $2T$ 个节点,便可能以极高的概率伪造任何区域的事件而不被识别出来.文献[4]提出了一种逐步交叉认证的策略,确保虚假数据能在一定跳数内被发现并被过滤掉.文献[5]提出一种不受阈值 T 限制的虚假数据过滤策略,网络中除布置普通节点外,还布置了能量比普通节点强得多的簇头节点,簇头节点完成数据聚合,聚合结果必须附加簇内各普通节点产生的 MAC,Sink 节点收到汇聚结果后,对聚合结果及附加 MAC 进行校验,进而实现对虚假数据的过滤.文献[6-7]提出了一种利用单向哈希链认证对数据进行过滤的技术,保证中间节点只能校验数据但不能修改数据.文献[8]提出了一种基于地理位置信息的密钥分配方案 LBRS,即便攻击者俘获一定数目的节点,这些节点也只能伪造对应网格所发生的事件,转发节点的过滤方法与传统方法类似.在 LBRS 之前的传统解决方案,被俘获节点超过一定数目后,都可以伪造一个任意区域发生的事件而不被识别出来,LBRS 中虽然节点只能伪造本区域内发生的事件,但虚假数据包仍然能够在网络中传播.文献[9]提出了一种基于分组的 GRSEF 策略,该策略将节点仅分为 T 组,而不是 SEF 策略中的 n 组($n>T$),确保了网络中任何位置都能被来自不同组的 T 个节点以较高的概率所覆盖,此外提出了一种多坐标轴的密钥生成方法与 Cell 划分方法.

上述策略不能有效防止一个恶意节点利用已被俘获的其他区域节点信息伪造一个系统难以识别的虚假事件,其根本原因在于接收数据包的节点无法判断该数据包是由其上游节点生成还是转发的,本文将解决这一问题,确保被俘获节点不能成功伪造其他区域发生的事件,并且在绝大多数情况下,虚假数据包将在一跳之内被过滤.

2 基于邻居节点监听的虚假数据过滤策略

2.1 网络模型和相关假设

假定传感器网络由数千个价格低廉且抗俘获能力较弱的传感器节点构成,节点分布密集,节点的通信半径相同且保持不变.节点在传送数据的过程中,通过监听狗技术[10]确保数据不被篡改或任意丢弃.假定传感器节点和 Sink 节点布置后不再移动,Sink 节点具有较强的安全性,不会被俘获,同时具有较强的计算能力、较高的存储性能和电源供给能力.假定

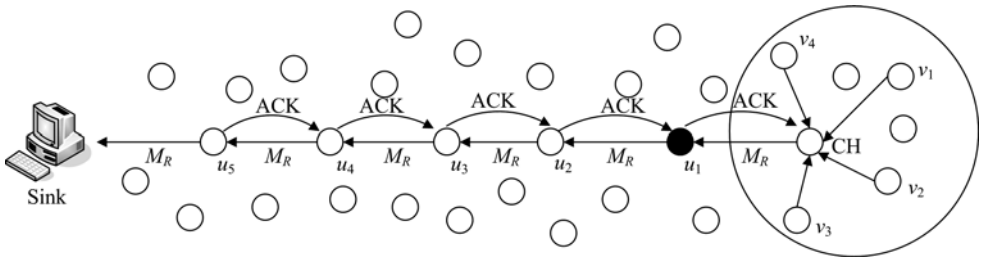

图 1　系统模型示意图

Fig. 1　System model

一个事件发生时能被周围的 T 个以上不同密钥组的节点所感知并生成相应的融合数据.

2.2　NWFFS 策略的基本思想

在传统途中过滤解决方案中,如果攻击者俘获了来自网络中不同区域的 T 个节点,其中一个被俘获节点便可以利用这些节点所存储的密钥伪造来自任意区域的虚假数据包,下游节点无法区分该数据包是由上游节点生成还是转发的,所以只能被动验证转发,因此如果能够识别数据包是由上游节点生成的,则下游节点可以了解到远处的节点不是该节点的邻居,从而判断出该数据包是其伪造的.

NWFFS 策略规定:每个节点都保存其两跳邻居节点信息,除生成数据包的簇头节点外,每个中间节点向其下游节点转发数据包后,还需向自己的上游节点发送 ACK 包.模型如图 1 所示,当网络中某节点如 u_2 收到上游节点 u_1 发送的数据包 M_R 后,u_2 通过监听 u_1 是否发送 ACK 包来判断其是生成数据包的簇头节点还是转发节点.若某节点判断其上一跳节点为簇头节点,可利用其保存的 2 跳邻居节点信息判断数据包中各 ID 是否都为上一跳节点的邻居节点,若不是则判定该数据包为虚假数据包;若恶意节点利用其邻居节点生成虚假数据包,则该邻居节点将识别此情况,并发送警告信息至下游节点.若某节点(如 u_2)监听到上一跳节点 u_1 回送 ACK 包给节点 u_0,可判断节点 u_1 为转发节点,此时,u_1 和 u_0 的共同邻居节点也监听到 ACK 包,检查各自缓冲区中保存的数据包中的 Packet_ID,判断是否存在与 ACK 包中一致的 Packet_ID,如存在则可判断该 ACK 消息为合法消息,否则可判断为异常,将监听的异常结果通过 alarm 包的形式发送给节点 u_2. 当节点 u_2 收到数据包中节点发送的 alarm 包或来自不同节点发送 alarm 包的数目超过系统规定的阈值 w 时,认定接收到的数据包为虚假数据包.在发送 alarm 包过程中,我们采用单向链技术保证节点身份的真实性. Sink 节点拥有所有节点的相关密钥,少部分逃脱的虚假数据包到达 Sink 节点后,将被 Sink 节点检测出来.由此可以看出,在绝大多数情况下,虚假数据包将在一步之内被过滤掉.

数据包 M_R,ACK 包及 alarm 包格式如图 2 所示. alarm 包中包含虚假数据包的编号(Packet_ID)、自身的最新单向链密钥和可疑节点的 ID 等相关信息,假设 u_1 向下一跳节点 u_2 发送虚假数据包,则二者共同邻居 u'通过监控 ACK 包判定数据包虚假后,通过查找自己保存的 2 跳之内邻居节点信息向 u_2 发送 alarm 包,若 u_2 为 u'的直接邻居,将 alarm 包直接发送至节点 u_2,若节点 u_2 为节点 u'的 2 跳邻居,则需要通过其他节点转发至 u_2,否则不发送任何数据包. 节点 u_2 收到 alarm 包后,利用其存储的节点 u'的单向链密钥 $K^i_{u_i}$ 验证 alarm 包中密钥的合法性,若通过验证,u_2 统计发送 alarm 包的不同节点个数,并更新其存储的节点 u'对应的单向链密钥.

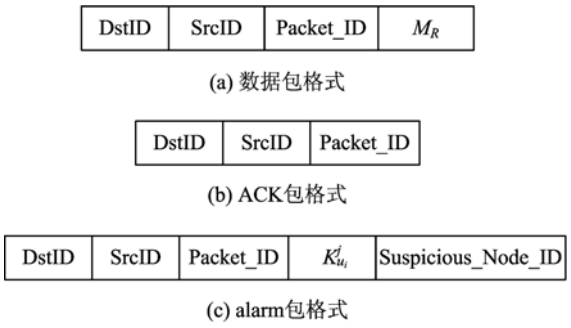

图 2　各数据包格式

Fig. 2　Data packet format

为解决以上认证过程导致的数据包传输延迟问题,本策略中各节点记录了其邻居节点的信任度值,当上游节点的信任度值大于系统规定的阈值上限 ub 时,节点 u 对数据包所携带的 MAC 进行简单验证后直接转发给自己的下游节点,之后再对数据包

进行认证，如认定该数据包为虚假数据包，将上游节点的信任度值降为原来的1/2，若上游节点的信任度值低于 ub 但大于阈值下限 lb 时，节点先等待上游节点各邻居节点的监听结果后再认证转发，阈值低于 lb 时，直接丢弃该数据包.

2.3 密钥分配和网络初始化

与SEF策略类似，设存在一个空间大小为 N 的公共密钥池 G，$G=\{K_i:0\leqslant i\leqslant N-1\}$，$i$ 为密钥索引，将密钥池分为 n 个不重叠的密钥分区 $\{N_i:0\leqslant i\leqslant n-1\}$，每个分区包含 m 个密钥，则 $N=n*m$，每个密钥分区可按 $N_i=\{K_j\mid im\leqslant j\leqslant(i+1)m-1\}$ 进行划分.

部署前，每个节点分发一个标志身份的唯一ID，一个全局的单向密钥生成函数 $F(x)$，参数 ub，lb，w 和 T_{wait}. 其中 ub 和 lb 表示节点信任度阈值，w 表示认证某节点为可疑节点所需的来自不同邻居节点的alarm包数目的阈值，T_{wait} 表示节点收到数据包后监听信息等待的时间. 每个节点随机选择一个密钥分区，并随机选取其中 L 个密钥存储.

借鉴LEAP策略[11]，假定节点在分发和网络初始化过程中的一段时间内，邻居节点的发现等过程是安全的.

当节点通过飞行器投放等方式部署到某一区域后，每个节点(如 u)利用随机数 R_u 及节点ID生成密钥 $K_u^m=F(R_u,\mathrm{ID}_u)$，然后利用函数 $K_u^j=F(K_u^{j+1})$ 生成每个节点对应的 $m+1$ 个单向链密钥$\langle K_u^0,K_u^1,\cdots,K_u^m\rangle$. 每个节点保存由自身ID计算出来的 $\lceil m/d_1\rceil+d_2$ 个单向链密钥. 其中，$\lceil m/d_1\rceil$ 表示间隔为 d_1 的若干个密钥 $K_u^{d_1}$，$K_u^{2d_1}$，…，$K_u^{kd_1}$，…，K_u^m，保存 d_2 个待使用的单向链密钥，初始化为 K_u^0，K_u^1，…，$K_u^{d_2-2}$，$K_u^{d_2-1}$；第1组密钥使用完毕后，利用邻近的单向链密钥生成第2组密钥并保存到 d_2 个单元中，依次类推. 每个节点广播包含自身 ID_u 和 K_u^0 信息的数据包，邻居节点收到后，将其邻居节点的 ID_u 和 K_u^0 记录下来，同时将各邻居节点的信任度置为1，再将其各邻居节点的 ID_u 和 K_u^0 发送给其各邻居节点保存，通过该方式，网络中每个节点不仅记录了其邻居节点的 ID_u，K_u^0 和信任度值，同时也记录了其两跳邻居节点的 ID_u 和 K_u^0.

2.4 数据包的生成

当传感器节点感兴趣的某事件发生时，事件周围的若干个传感器节点将会侦查到该事件，并把侦查到的数据、地理位置及事件的类型等信息发送给邻居节点，当某节点收到大于 T 个不同密钥分组节点发送的数据后，该节点向其邻居节点宣布自己是簇头节点，并根据一定融合策略形成融合数据包 M，将数据包 M 发送给簇中各节点，簇中节点依据应用要求及传感器精度判断该数据是否与自己检测的数据相符合，如符合，从自身携带的密钥中随机选取一个密钥 K_i，生成 M_i 并发送给簇头节点. 其中，$M_i=\mathrm{MAC}(K_i,M\parallel\mathrm{ID}_v\parallel i)$，$\parallel$ 表示数据的顺序连接，MAC表示用密钥 K_i 对消息生成认证码. 具体过程如下：

$$v\rightarrow \mathrm{CH}:\mathrm{ID}_v,i,\mathrm{MAC}(K_i,M\parallel\mathrm{ID}_v\parallel i).$$

簇头节点收到反馈的数据后，首先查找其邻居节点列表判断该ID是否是其邻居节点，若不是丢弃该数据包，然后选择 T 个来源于拥有不同密钥分区的数据生成数据包 M_R，并将数据包发送给Sink节点，数据包 M_R 格式如下：

$$\mathrm{CH}\xrightarrow{M_R}\mathrm{Sink}:M,\mathrm{ID}_{\mathrm{CH}},K_{\mathrm{CH}}^j,\mathrm{ID}_{v_1},\cdots,\mathrm{ID}_{v_t},i_1,\cdots,i_t,M_{i_1},\cdots,M_{i_t}.$$

其中，$\mathrm{ID}_{\mathrm{CH}}$ 表示发送节点的ID，K_{CH}^j 表示发送节点最新的单向链密钥.

2.5 途中过滤

节点收到上游节点发送的数据包后，其过滤的过程如下：

(Ⅰ) 若数据包中上游发送节点的信任度值小于阈值lb，判断上游节点为恶意节点，直接丢弃该数据包；

(Ⅱ) 检查数据包中发送节点的ID是否是自己的邻居节点，并用自己保存的发送节点的单向链密钥验证数据包中单向链密钥的合法性，如不是自己的邻居节点或单向链密钥不合法，则直接丢弃该数据包；

(Ⅲ) 检查数据包中的密钥索引、ID和MAC的个数是否都等于 T，若存在不等的情况，直接丢弃掉该数据包，并将上游节点的信任度更改为原来的1/2；

(Ⅳ) 判断 T 个密钥索引是否来源于不同密钥分区，若存在同一分区的密钥则丢弃数据包，并将上游节点的信任度更改为原来的1/2；

(Ⅴ) 检查其自身是否存在与数据包中相同的密钥索引，若存在相同的密钥索引，用该密钥验证其对应的MAC，验证不通过则丢弃该数据包；

(Ⅵ) 若数据包中上游发送节点的信任度值小

于阈值 ub，对数据包采用先认证再转发的方式，先执行(Ⅶ)再执行(Ⅷ)，若数据包中上游发送节点的信任度值大于等于阈值 ub，对接收的数据包采用先转发再认证的方式，先执行(Ⅷ)再执行(Ⅶ)；

(Ⅶ) 在时间 T_{wait} 内，监听上一跳节点是否发送 ACK 包，若没有监听到 ACK 包，根据自身保存的两跳邻居节点列表判断 ID_{v_1}，…，ID_{v_t} 是否是发送节点的邻居节点，若存在某 ID 不是发送节点的邻居节点，丢弃该数据包，并将上一跳节点的信任度更改为原来的 1/2. 若监听到 ACK 包，统计收到发送 alarm 包的不同节点个数值 count，若 ACK 包中目标节点 DstID 不是自己两跳邻居节点 ID，则丢弃该数据包，并将上一跳节点的信任度更改为原来的 1/2；若 ACK 包中目标节点 DstID 是自己两跳邻居节点 ID，如果收到数据包中节点发送的 alarm 包，丢弃该数据包，如果未收到数据包节点发送的 alarm 包且 count 大于阈值 w，则丢弃该数据包，并将上一跳节点的信任度更改为原来的 1/2. 若判断为合法数据包，则将上一跳节点的信任度值增加 0.1；

(Ⅷ) 将数据包中发送节点的 ID 及单向链密钥用自身的 ID 和自身新的单向链密钥替换后转发给下游节点，并向上游节点回复 ACK 包.

2.6　Sink 验证

Sink 节点收到数据包后，首先检查数据包中的密钥、ID 和 MAC 的个数是否都等于 T，若存在不等的情况，直接丢弃掉该数据包；其次判断 T 个密钥索引是否来源于不同密钥分区，若存在同一分区的密钥则丢弃数据包；最后由于其拥有所有节点 ID 及对应的密钥等信息，少部分逃脱中途节点过滤的虚假数据最终将被识别出来并被过滤掉.

2.7　NWFFS 策略应对恶意节点攻击形式分析

(Ⅰ) 恶意簇头节点中利用网络中俘获的非邻居节点伪造虚假数据包

当恶意节点利用网络中俘获的非邻居节点伪造虚假数据包发送给下游节点时，若没有向上游节点发送 ACK 包，下游节点可通过其保存的两跳邻居节点 ID 信息判断出该数据包为虚假数据包，直接丢弃该数据包；若向一个不存在的上游节点发送 ACK 包，下游节点通过其保存的两跳邻居节点 ID 信息判断该 ACK 包的合法性，从而判断出该数据包为虚假数据包；若向自己的某个邻居节点发送 ACK 包，收到 ACK 包的各共同邻居节点通过检查自己缓冲区中保存的数据包中的 Packet_ID，将发现不存在与 ACK 包中一致的 Packet_ID，从而判断出该 ACK 包为不合法数据包，并向下游节点发送 alarm 包. 当下游节点收到来自不同节点发送 alarm 包的个数超过 w 个时，可判断该数据包为虚假数据包. 该种情况的虚假数据可在第 1 跳便被过滤掉.

(Ⅱ) 恶意簇头节点利用自己的邻居节点伪造虚假数据包

途中过滤一般假定恶意簇头节点的被俘获的邻居节点来源于不同密钥分区的个数少于 $T-1$ 个，否则将生成系统难以识别的数据包. 当恶意簇头节点利用自己的邻居节点伪造虚假数据包时，若数据包中各 ID 都是已俘获的邻居节点的 ID，必然存在两个节点来自同一密钥分区，该数据包将被下游节点识别并过滤掉，若存在未被俘获的节点 ID，该数据包在发送过程中将被此节点识别出来，并向下游节点发送 alarm 包，当下游节点收到数据包中节点发送的 alarm 包时，丢弃该数据包，此时簇头节点也将收到 alarm 包，簇头节点将选择其他节点重新生成新的数据包，并发送给下游节点. 该种情况的虚假数据可在第 1 跳便被过滤掉.

(Ⅲ) 簇头节点和其俘获的下游节点发动合谋攻击

假设两个相邻的恶意节点发动合谋攻击，例如在图 1 中，u_1 和 u_2 两个节点为恶意节点，u_1 伪造数据包后发送给 u_2，u_2 不管收到多少 alarm 包，都转发该数据包. 在 u_2 收到 alarm 包的过程中，u_1 和 u_2 的公共邻居区域 C 中的各节点也将收到足够多的 alarm 包，当 u_2 转发该虚假数据包时，C 区域中相关节点将判断 u_2 可能为恶意节点，并向 u_2 的下游节点 u_3 发送 alarm 包，该虚假数据包将被过滤掉. 该种情况的虚假数据可在恶意节点的下 1 跳便被过滤掉.

3　性能分析与仿真实验

3.1　邻居节点的监听能力

(Ⅰ) 公共监听节点的个数分析

对于两个能直接相互通信的节点，其共同邻居节点的个数依赖于两个节点之间的距离，节点之间相隔越远，其共同的邻居节点越少，如图 3(a)和(b)所示. 当 u_1 和 u_2 节点之间的间隔距离为节点最大通信距离时，其共同的邻居节点最少，假设节点的最大通信距离为 r，C 区域为节点 u_1 和 u_2 的通信相交的公共区域，则 C 的最小公共区域面积为

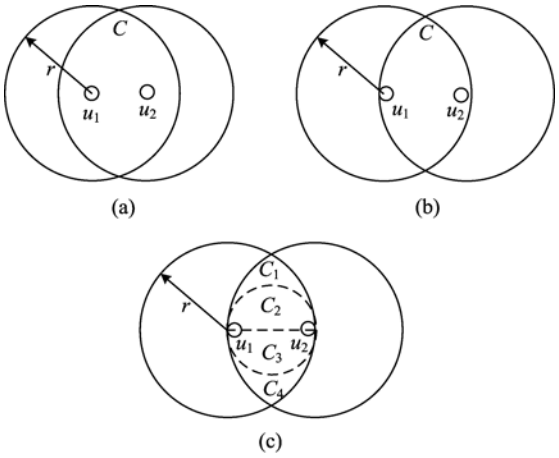

图 3 节点公共邻居区域

Fig. 3 Overlap of node's covering region

$$C = \frac{2}{3}\pi r^2 - \frac{\sqrt{3}}{2}r^2.$$

图 3(b)中 C 区域约占节点通信区域的 40%，假设节点的邻居节点个数为 20，并均匀分布在通信区域内，则两个节点的公共邻居节点约为 7 个节点. 由此可知，即使在最小公共区域面积的情况下也能确保有足够多的公共监听节点.

(Ⅱ) 公共区域 C 中节点收到 alarm 包的个数分析

我们把两节点相隔最大通信距离时通信相交的公共区域分割成如图 3(c)所示的 C_1，C_2，C_3 和 C_4 区域，当节点 u_2 收到上游监听节点发送的 alarm 包时，该数据包必定是 4 个区域中某个节点直接发送或转发. 易知，当 u_2 收到 alarm 包时，C_2 中某节点至少能收到 C_1，C_2 和 C_3 区域中其他节点发送或转发给 u_2 节点的 alarm 包，这部分区域约占 C 区域的 83%，C_1 中某节点至少能收到 C_1 和 C_2 区域中其他节点发送给 u_2 的 alarm 包，这部分区域约占节点通信区域的 50%. 当 u_2 收到上游监听节点发送的 m 个 alarm 包时，C_2 和 C_3 中节点至少能收到 0.83 m 个 alarm 包，C_1 和 C_4 中节点至少能收到 0.5 m 个 alarm 包.

3.2 数据包转发延迟分析

当一个合法数据包的传输路径中没有恶意节点时，由于各节点初始化信任度值高，数据包经过简单验证后被直接转发，延迟较低，当发送数据包节点为恶意节点时，延迟主要集中在恶意节点的 1 跳下游节点，因此对 Sink 节点做出正确决策的反应时间影响较小.

3.3 通信开销

本策略中，每个数据包相对 SEF 策略来说，在没有恶意节点参与的情况下，数据包的长度增加了 $2*(T+1)+4$ 个字节，每个途中节点除转发数据包外，还必须向发送数据包的上游节点回复 ACK 包，通信开销有所增加. 若一个恶意节点伪造成簇头节点并利用其 1 跳邻居节点的 ID 伪造虚假数据包时，通信开销和没有恶意节点参与的情况一致，但该数据包将被下游节点或 Sink 节点识别出来并过滤掉. 若一个恶意节点伪造成簇头节点并任意构建虚假数据包时，节点将被其邻接的下游节点过滤掉. 若伪造成途中节点并发送虚假数据包时，恶意节点的相关邻居节点将识别出该数据包为虚假数据包，并向其下游节点发送 alarm 包，假设节点的邻居节点有 20 个，根据文献[12]，最少将有 7.6 个节点发送 alarm 包，且最多传送 2 跳，则大约增加 16 个 alarm 包，但由于该数据包被恶意节点的邻居下游节点过滤掉且发送节点或其共谋节点被识别出为恶意节点.

当某节点的单向链密钥使用完毕时，该节点将生成新的单向链密钥，向其 1 跳和 2 跳邻居节点广播数据包$\{ID_u, K'^0_u, E(K^m_u, K'^0_u)\}$，节点收到该数据包后，验证通过后用新的密钥替换旧密钥，由于单向链密钥的更新只在节点的 2 跳邻居节点内完成，通信开销较低.

3.4 存储开销

NWFFS 中每个传感器节点需要存储$\lceil m/d_1 \rceil + d_2$ 个单向链密钥、一个密钥分区中的 L 个密钥、1 跳邻居节点的 ID 和对应的单向链密钥和信任度值、2 跳邻居节点的 ID 和对应的单向链密钥. 假设每个节点的邻居节点平均为 c 个且均匀布置，节点的通信半径为 r，则每个节点其 2 跳邻居节点的个数为 $3c$ 个，每个节点的 2 跳邻居节点的 ID 和对应的单向链密钥用一个一维数组来保存. 假设对称密钥和单向链密钥的长度分别为 8 个字节和 4 个字节，节点 ID 的长度为 2 个字节，节点信任度占 1 个字节，则每个节点需要保存的 1 跳邻居节点的 ID 和对应的 2 跳邻居节点的 ID 的字节数为$2*(c+c^2)$，需保存的单向链密钥为 $4c*(2+4)$ 个，合计为 $8*L+(\lceil m/d_1 \rceil + d_2)*4+2*(c+c^2)+4c*(2+4)+c$ 字节的存储空间. 如 $m=2\,000$，$d_1=100$，$d_2=10$，$L=5$，$c=20$，则需要耗费大约1 500字节的存储空间. 随着科技的不断发展，传感器节点的性能不断提高，如 MICAz 节点配置了 128 kB 的内

部存储器和 512 kB 的外部存储器，能满足用户需求.

3.5　仿真实验

为了进一步验证所提算法的性能，我们利用 OMNET++建立了模拟仿真平台，通过仿真实验来比较 SEF 和 NWFFS 的性能. 本文仿真实验的环境如下：假设仿真场景是一个 500 m×500 m 的区域，Sink 节点部署在坐标(0,0)上，2 000个节点随机部署在仿真区域内，平均节点的度数是 20，详细的配置参数如表 1 所示. 仿真实验中，我们采用的是随机选取攻击节点的方式(假如攻击者能随意俘获任意位置和任意数量的节点，攻击节点即可轻易地发起合谋攻击，任何协议都将失去效力)，将 1 000次实验数据的平均值作为最终的实验结果. 我们主要从过滤能力和抗俘获性等方面来分析算法的性能.

表 1　参数配置表

Tab. 1　Parameter configuration list

参数	参数值
仿真区域	500 * 500 m^2
节点数目	2 000
通信半径	29.8 m
感知半径	29.8 m
全局密钥池大小	400
密钥分区数目	20
节点存储密钥数目	10
节点信任度上限阈值 ub	0.8
节点信任度下限阈值 lb	0.1
alarm 包阈值 w	5
数据包的不同分区密钥数 T	5

(Ⅰ) 过滤性能分析

网络中虚假数据包越早被过滤掉，就越能节省网络的通信、存储等开销，降低虚假数据攻击的效果. 图 4 比较了在两种协议下虚假数据包被过滤前平均在网络中被传输的跳数，由图 4 可以看出，SEF 协议中虚假数据包平均的传输跳数明显高于 NWFFS 协议，并且 SEF 协议中虚假数据包平均的传输跳数随着恶意节点数量增加而增加；对于 NWFFS 协议，虚假数据包平均的传输跳数几乎是一个常数值，该策略可以有效地过滤网络中的虚假数据包，从而减轻了虚假数据攻击的危害.

图 5 表示随着被俘获节点数目的增多，协议过滤虚假数量包的能力. 由图 5 可以看出，到当被俘获节点数量较小时(<3)，SEF 有较好的性能，然而当

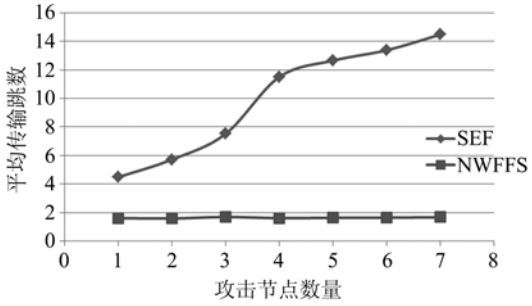

图 4　虚假数据被过滤前平均传输跳数

Fig. 4　Average fowarding hops before a forged packet is filtered

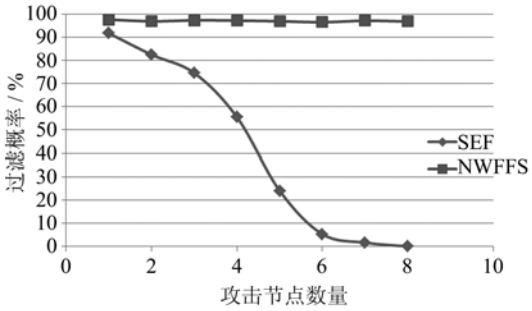

图 5　虚数数据包过滤概率

Fig. 5　The probability of a forged packet filtered

俘获节点数量增加，SEF 过滤能急速下降，当网络中被俘获的节点数量达到 8 时，SEF 基本没有过滤能力；然而，本文的协议在网络中有较多恶意节点的情况仍然具有非常好的过滤能力. 分析可知，在策略 SEF 中，任意俘获节点的密钥都可以被利用起来，用于发起合谋攻击，而在 NWFFS 协议中，只有任意俘获的节点都是邻居节点，才能发起合谋攻击，生成不可能被过滤掉的虚假数据包.

(Ⅱ) 抗俘获性分析

随着网络中被俘获的节点数目增多，节点可以伪造的事件区域必将增长. 我们将恶意节点可以在该区域内伪造出虚假数据包而不被过滤的区域面积占总的部署区域面积的比例来衡量协议的抗节点俘获性. 从图 6 可以看出，当网络被俘获的节点数量为 5(即协议中构造数据包需要密钥分区的个数)，在 SEF 协议中，攻击节点平均可以伪造 61.3%区域的事件，而 NWFFS 几乎不能处理任何区域的事件. 当网络中恶意节点数量增加到 49 个，在 SEF 协议中，恶意节点可以伪造任何区域的事件，此时在 NWFFS 协议中，恶意节点仅能伪造 3.4%区域的事件，这是因为SEF协议无法防范不同区域恶意节点

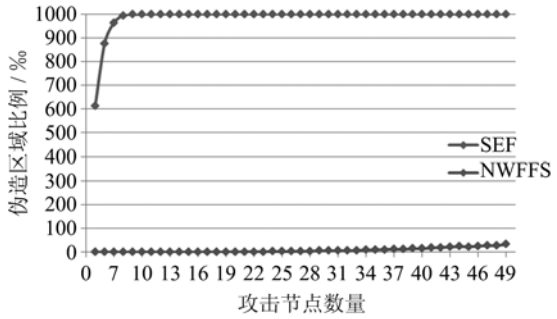

图 6 伪造事情区域占总部署区域的比例

Fig. 6 The percentage of forged events' region

的合谋攻击.可见我们的协议极大地提高了抗俘获性,降低了恶意节点的合谋攻击能力.

4 结论

本文提出了一个基于邻居节点监听的虚假数据过滤策略.该策略中,每个节点保存 2 跳邻居信息,接收数据包节点通过监听上游节点是否发送 ACK 包来判断上游节点是生成数据包的节点还是中间转发节点,确保恶意节点不能成功伪造其他区域发生的事件而不被识别出来,在绝大多数情况下,虚假数据包将在 1 跳之内被过滤掉.理论分析与实验结果表明,该策略具有良好的过滤效果和抗俘获性.

参考文献(References)

[1] 崔莉, 鞠海玲, 苗勇, 等. 无线传感器网络研究进展[J].计算机研究与发展, 2005, 42(1): 163-174.

[2] Perrig A, Stankovic J, Wagner D. Security in wireless sensor networks[J]. Communications of the ACM, 2004, 47(6): 53-57.

[3] Ye F, Luo H, Lu S, Zhang L. 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] 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]// Proceedings of the 25th IEEE Symposium on Security and Privacy. Washington, USA: IEEE Press, 2004: 259-271.

[5] Ma M. Resilience of sink filtering scheme in wireless sensor networks [J]. Computer Communications, 2006, 30(1): 55-65.

[6] Yuan T, Zhang S Y, Zhong Y P, et al. KAEF: An en-route scheme of filtering false data in wireless sensor networks [C]// IEEE International Performance Computing and Communications Conference. Austin, USA: IEEE Press, 2008: 193-200.

[7] Yu Z, Guan Y. A dynamic en-route scheme for filtering false data[C]// Proceedings of the 3rd ACM International conference on Embedded Networked Sensor Systems. Barcelona, Spain: ACM Press, 2005: 294-295.

[8] Yang H, Ye F, Yuan Y, et al. Toward resilient security in wireless sensor networks[C]// Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing. Urbana-Champaign, USA: ACM Press, 2005: 34-45.

[9] Yu L, Li J Z. Grouping-based resilient statistical en-route filtering for sensor networks[C]// Proceedings of 28th International Conference on Computer and Communications, Joint Conference of the IEEE Computer and Communications Societies. Rio de Janeiro, Brazil: IEEE Press, 2009: 1 782-1 790.

[10] Marti S, Giuli T, Lai K, et al. Mitigating Routing Misbehavior in Mobile Ad Hoc Networks [C]// Proceedings of the 6th Annual International Conference on Mobile Computing and Networking. Boston, USA: ACM Press, 2000: 255-265.

[11] Zhu S, Setia S, Jajodia S. LEAP: Efficient security mechanisms for large-scale distributed sensor networks [C]// Proceedings of the 10th ACM Conference on Computer and Communications Security. Washington, USA: ACM Press, 2003: 62-72.

[12] Lee S B, Choi Y H. A resilient packet-forwarding scheme against maliciously packet-dropping nodes in sensor networks[C]// Proceedings of the 4th ACM Workshop on Security of Ad Hoc and Sensor Networks. Alexandria, USA: ACM Press, 2006: 59-70.