

# 基于 $k$ 匿名假包注入的汇聚节点位置隐私保护

宋 杰, 张 昆

(安徽大学 计算机科学与技术学院, 安徽 合肥 230601)

**摘 要:**无线传感器网络已经被广泛应用于日常生活中,隐私问题成为其应用的一大阻碍。汇聚节点是无线传感器网络中的关键节点,一旦汇聚节点遭到攻击被恶意破坏后,那么整个无线传感器网络将有可能面临瘫痪的危险。针对汇聚节点的位置隐私保护问题,提出了基于  $k$  匿名假包注入策略的汇聚节点位置隐私保护方案,并分析了方案的安全时间和能量消耗两个方面的性能,最后通过 GA 算法给出了匿名节点的部署方案。方案对于全局流量攻击者和逐跳追踪攻击者具有一定的抵御能力。

**关键词:**无线传感器网络;汇聚节点位置隐私保护; $k$  匿名;假包注入

中图分类号:TP393

文献标识码:A

文章编号:1673-629X(2015)02-0156-04

doi:10.3969/j.issn.1673-629X.2015.02.036

## Research on Sink-location Privacy Protection Based on $k$ -Anonymity and Fake Packet Injection

SONG Jie, ZHANG Kun

(School of Computer Science and Technology, Anhui University,  
Hefei 230601, China)

**Abstract:** Wireless sensor networks have been widely used in daily life, the privacy has become a major obstacle for their application. Sink node is key node in wireless sensor network, once the sink node attackers attacks the sink node, the entire sensor networks will be paralyzed. For the location privacy of sink node, propose a scheme of  $k$ -anonymity and fake packet injection for location privacy and analyze the performance of security of time and energy consumption. Finally give a scheme of deployment for the anonymous nodes through the GA algorithm. The scheme has a certain resilience of the global view attacker and the hop-track attacker.

**Key words:** wireless sensor networks; sink node location privacy protection;  $k$ -anonymity; fake packet injection

## 0 引 言

无线传感器网络 (Wireless Sensor Networks, WSN) 被认为是 21 世纪最具有应用前景的技术<sup>[1-7]</sup>, 被广泛应用于国防军事、工农业生产、智慧城市和环境监测等领域。无线传感器网络的关键节点位置隐私保护问题分为源节点位置隐私保护和汇聚节点位置隐私保护问题。其中, 汇聚节点是连接传感器网络和外部互联网的网关, 不仅负责接收源节点发送过来的监测数据并发送给观测者, 同时还承担着向网络发布任务的工作, 在网络中十分重要。一旦汇聚节点遭受攻击, 整个网络将有可能瘫痪<sup>[8-9]</sup>。如何保护汇聚节点的位置隐私是一个值得研究的问题。

## 1 系统模型

### 1.1 网络模型

假定无线传感器网络由一个汇聚节点和大量的普通节点构成。网络模型具有下列特性:

(1) 周期数据报告。无线传感器网络中, 在一个周期网络中, 每个节点都会采集监控区域中的信息, 并周期性地向汇聚节点传输数据。文献[10-11]均采用此类网络。

(2) 均匀分布的网络。网络是由汇聚节点和大量传感器节点组成, 且这些传感器节点被均匀密集地部署在网络中。网络中只有一个汇聚节点来收集网络中采集的数据。

收稿日期: 2014-03-12

修回日期: 2014-06-18

网络出版时间: 2014-12-27

基金项目: 国家自然科学基金资助项目(61271352); 安徽省自然科学基金项目(KJ2010B123)

作者简介: 宋 杰(1966-), 男, 副教授, 研究方向为嵌入式系统、计算机原理与接口、生物信息学; 张 昆(1989-), 男, 硕士研究生, 研究方向为嵌入式系统、无线传感器网络。

网络出版地址: <http://www.cnki.net/kcms/detail/61.1450.TP.20141227.1343.029.html>

## 1.2 攻击者模型

为了定位到汇聚节点的位置,攻击者通常具有先进的装备和技术,攻击者具有两种攻击能力:全局流量分析攻击和逐跳追踪汇聚节点。

(1)全局流量分析来攻击汇聚节点。

攻击者具有足够的能力,可以监听整个网络的通信情况。根据文献[12],攻击者不能解析出数据包,只能进行外部攻击。攻击者定位汇聚节点的过程分为两个阶段:节点位置收集阶段和视觉搜索阶段。攻击者监听全网的通信状况,依据离汇聚节点越近,通信流量越大的特点,攻击者首先收集出所有靠近汇聚节点的节点集合,再通过视觉搜索的方式找到确切的汇聚节点的物理位置。

(2)逐跳追踪攻击汇聚节点。

攻击者在逐跳追踪汇聚节点的位置时,通过数据包先后发送顺序判断节点的传输方向,逐跳跟踪到汇聚节点。攻击逐跳追踪汇聚节点位置的过程:攻击者首先在A节点位置附近监听无线信号,如果首先监听到A节点发送了一个数据包,过了一段时间后节点B也发送了一个数据包,由此,攻击者判断节点A将数据包传送给节点B,攻击者移动到节点B位置继续监听网络信号,如此往复,最终渐渐靠近汇聚节点,判断出汇聚节点的位置。

## 2 k匿名假包注入方案

针对现有工作的不足之处,提出基于k匿名假包注入策略的汇聚节点位置隐私保护方案(KAFP)。KAFP方案的基本思想是选取k个节点来模仿汇聚节点周围节点的通信状况,同时,为了抵御逐跳追踪的攻击者,在这k个节点处,以一定的概率生成假包并向远离汇聚节点的方向进行定向转发。

### 2.1 k匿名策略

k匿名策略指在网络中部署k个匿名节点来模仿汇聚节点周围节点的网络通信流量。匿名节点通过泰森多边形将网络划分成k个子区域。匿名节点负责收集这个子区域中所有产生的数据包。使用基于欧几里得最小生成树(Euclidean Minimum-Spanning Tree-based, EMST-based)的路由算法来连接k个匿名节点,并且这k个节点非常接近高通信流量。

每个消息包向汇聚节点传输的过程中分为两个阶段:区域内传播和区域间传播。在区域内传播的过程中,区域首先将产生的数据包发送到匿名节点,匿名节点收到该数据包时,转发数据进行区域间传输;沿着EMST路由树将这个数据包传输到其他的匿名节点,最终达到汇聚节点。定义K为k个匿名节点的位置矢量。

## 2.2 假包注入策略

为了抵御逐跳追踪的攻击者,向网络中引入了类似于LPR<sup>[13]</sup>协议中的假包注入策略<sup>[14]</sup>。在匿名节点收到其区域内发过来的数据包时,产生一个假包,同时通过定向路由将假包传播到远离汇聚节点的位置。具体设计为:首先,网络在初始化的过程中,节点将邻居节点分为近邻居集合和远邻居集合。在网络区域中,节点先将数据包沿着最短路径传输到匿名节点,然后匿名节点转发数据包的同时产生一个假包,在远邻居集合中随机选择一个远邻居节点向其发送假数据包,这个远邻居节点收到假数据包后,也随机选择一个远邻居节点向其转发假数据包,依次向下传播。同时,设定匿名节点在只有收到自己所属区域内节点发送过来的数据包才有可能产生假包,而对于EMST路径传输过来的数据包,并不产生假包。这样,减少了通信流量,减小了流量的不对称性。为了降低能量消耗,在匿名节点收到数据包时,设置以pfake概率产生假数据包,同时,为每一个假包设置一个生存时间TTL,即假包在网络中转播的最大跳数。通过调节TTL跳数和假包发送概率pfake大小来平衡网络中的能量消耗和汇聚节点的位置隐私性。

## 3 方案分析

在基于k匿名假包注入策略的汇聚节点位置隐私保护方案(KAFP)中,针对全局流量分析攻击者和逐跳攻击者,都设计了相应抵御策略:k匿名策略和假包注入策略。

接下来针对这两种攻击者对KAFP方案从节点安全性和网络能量消耗两个方面进行了分析。

在分析之前,根据区域内的路由算法,定义网络中EMST的欧氏距离为:

$$EMST(K) = \sum_{(i,j) \in EMST} \|p_i - p_j\| \quad (1)$$

其中,  $\|p_i - p_j\|$  表示匿名节点之间的欧氏距离。

### 3.1 安全性分析

使用安全时间来衡量网络中汇聚节点的安全性,所谓安全时间指的是攻击者从攻击位置追踪定位到汇聚节点的时间。接下来分别分析两种攻击者追踪汇聚节点的安全时间。

(1)全局流量分析攻击者。

周期采集数据传播的网络中,每个节点都会传播一个数据包,那么在一个数据包传输周期内,EMST内节点传播的数据包的数量等于整个网络的节点数。为了定位出汇聚节点的物理位置,攻击者需要沿着EMST进行视觉搜索。

用v表示攻击者的搜索速度,r表示节点的通信半

径,那么攻击者的搜索时间近为:

$$\Phi(K) = \frac{\text{EMST}(K) \times r}{v} \quad (2)$$

(2) 逐跳攻击者。

数据包从源节点传输到汇聚节点有两个阶段:首先从源节点传输到所属区域的匿名节点,匿名节点再转发该数据包,并沿着 EMST 传输到汇聚节点。当逐跳攻击者追踪数据包到匿名节点时,它有一半的概率去追踪假包,那么就是有  $\text{pfake}/2$  的概率被引入到离汇聚节点较远的位置,增大了网路节点的安全时间。数据包沿着 EMST 向汇聚节点传输时,经过每一个匿名节点时都有可能被假包误导。假设数据包在传输到汇聚节点之前经过  $n$  个匿名节点,那么追踪者就会有  $n * \text{pfake}/2$  的概率被引到一个离汇聚节点较远的位置。这样,对逐跳追踪攻击者就有较强的抵御能力。同时注意到,网络中匿名节点数越多,攻击者被误导的概率就越大,网络的安全性也越强。

### 3.2 能量消耗分析

定义网络的能量消耗使用数据包传播的跳数来表示。假定网络中的每跳的平均传播距离为  $\lambda_h$ 。这样,在节点分布均匀的网络中,从节点传播一个数据包到选定的节点的平均能量消耗近似为<sup>[15-16]</sup>:

$$e_i \approx \frac{\|n_i - p_j\|}{\lambda_h} \quad (3)$$

平均总能量消耗值等于每个节点在区域内的通信消耗能量、在区域之间传播的能量消耗以及匿名节点产生假包定向传播产生的能量消耗。每个周期内,所有节点都会产生一个消息并传播,因此,每个节点在区域内传播消息的平均能量消耗是

$$E_a(K, W) \approx \frac{1}{\lambda_h |N|} \quad (4)$$

而每个周期内每个节点在区域间传输消耗的平均

能量是

$$E_c(K) \approx \frac{\text{EMST}(K)}{\lambda_n} \quad (5)$$

区域内匿名节点在收到一个数据包后,就会以一定的概率( $\text{pfake}$ )产生一个假包,并向远邻居定向传播 TTL 跳(假包的生存周期),而一个周期内,匿名节点为每个数据包以一定概率产生一个假包,因此每个节点因假包注入消耗的能量为式(6)。

$$E_f = \frac{\text{pfake} \bullet \text{TTL}}{|N|} \sum_{j=1}^k \sum_{n_i \in W_j} |n_j| \quad (6)$$

因此

$$E_f = \text{pfake} \bullet \text{TTL} \quad (7)$$

综合上述三式,一个周期内,每个节点的平均总能量消耗为:

$$E = E_a(K, W) + E_c(K) + E_f \quad (8)$$

## 4 实验与分析

在 1 000 m×1 000 m 的范围内,均匀部署 2 500 个节点,并使用 GA 遗传算法在网络中寻找  $k$  个最优的节点。节点通信半径为 40 m,因此,在网络中的平均每跳长度值为 2/340 m。把  $K$  作为算法中的“染色体”, $K$  就是被选择的  $k$  个节点位置,随着  $k$  的变化,执行多次实验。

对于每个  $k$ ,做 10 次实验。并且把种群设置为  $k = 100$ ,交叉概率为 0.8,最大的迭代次数为 100。设定匿名节点产生假包的概率  $\text{pfake} = 0.5$ ,假包在网络中的传播次数  $\text{TTL} = 10$ ,那么每个节点因假包注入消耗的能量为  $E_f = 5$ 。

根据文献[12],使用泰森多边形划法对  $k$  个匿名节点进行区域划分,并使用遗传算法 GA 计算出  $K$  在图中的位置。图 1 中,当  $k = \{3, 4, 5, 6, 10, 16\}$  时,使用最小生成树来连接这些匿名节点,划分出了它们各自

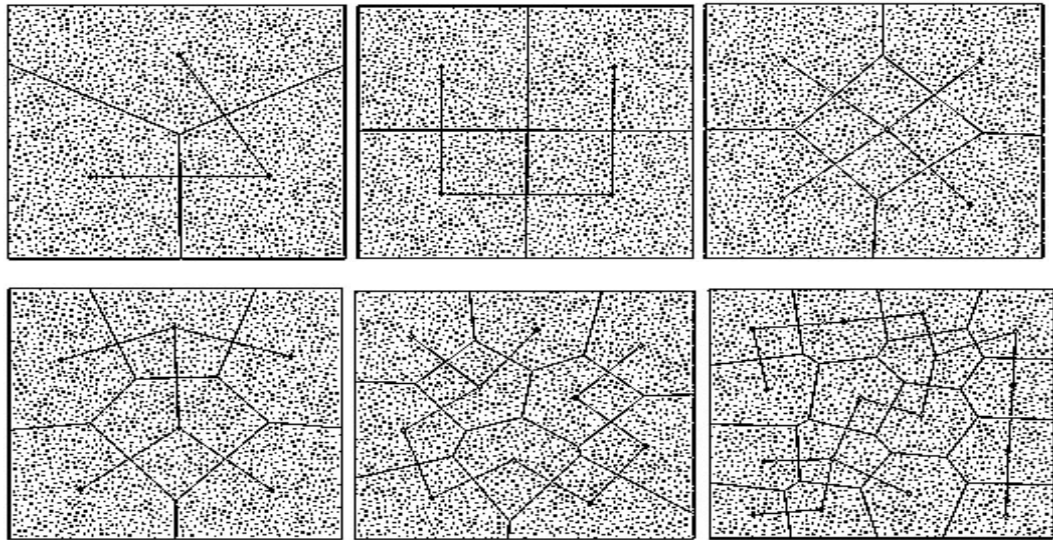


图 1 使用遗传算法计算出的  $K$



的区域。

图2中,随着 $k$ 值的增加,不断增加,而区域内能量消耗却不断减小。可以看到的是,当划分的区域增多时,区域内的节点与该区域的匿名节点之间的距离不断减小,因此区域内的能量消耗是不断减小的。而 $k$ 值的增加,致使网络中匿名节点更多,这也导致了 $EMST(K)$ 的增大。可以观察到,随着 $k$ 值的变化, $EMST(K)$ 有较小的变化,引起的区域间能量消耗变化远大于区域内能量消耗变化,因此, $k$ 值变大时,区域间能量消耗变化较快,并且很快达到接近整体消耗的水平。同时,图1中,匿名节点将区域划分为 $k$ 个大小近似的区域,可以使用圆来近似表示这些区域。回归分析表明,当 $k = 0.64$ 时,圆与区域的近似度最高。在满足安全时间的情况下,当 $EMST(K)$ 值最接近安全时间时,整个网络的能耗接近最小。因此,由公式(8)先计算出最佳的匿名节点数 $k$ ,然后再使用遗传算法计算出匿名节点的位置 $K$ 。

$$EMST(K) = 2(k-1)\sqrt{\frac{BA_0}{k\pi}}$$

(9)

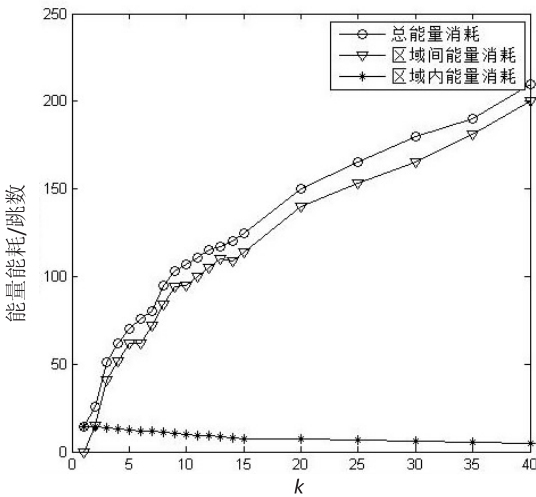


图2 区域内部能耗和区域间能耗与 $k$ 值的关系图

5 结束语

针对无线传感器网络中的汇聚节点位置隐私保护问题,提出基于 $k$ 匿名假包注入策略的保护方案,对全局流量分析攻击者以及逐跳追踪攻击者具有有效的抵御能力。最后对方案从理论和实践进行了分析,并给出了网络中匿名节点的部署方案。

参考文献:

[1] 李建中, 李金宝, 石胜飞. 传感器网络及其数据管理的概

念、问题与进展[J]. 软件学报,2003,14(10):1717-1727.

[2] 李福龙. 无线传感器网络基站位置隐私保护协议研究[D]. 哈尔滨:哈尔滨工业大学,2012.

[3] 于海斌,曾鹏,王忠锋,等. 分布式无线传感器网络通信协议研究[J]. 通信学报,2004,25(10):102-110.

[4] 孙利民,李建中. 无线传感器网络[M]. 北京:清华大学出版社,2005.

[5] 李晓维. 无线传感器网络技术[M]. 北京:北京理工大学出版社,2007.

[6] 高红亮,汪秉文,高超,等. 无线传感器网络 QoS 仿真与研究[J]. 计算机工程与科学,2012,34(11):7-13.

[7] 唐加山,王燕. 无线传感器网络中改进的 EEUC 路由协议[J]. 重庆邮电大学学报:自然科学版,2013,25(2):172-177.

[8] 康林. 无线传感器网络位置隐私保护方案研究[D]. 大连:大连理工大学,2013.

[9] Callaway E H. 无线传感器网络:体系结构与协议[M]. 王永斌,曲晓旭,译. 北京:电子工业出版社,2007:33-36.

[10] Li Y, Ren J. Providing source-location privacy in wireless sensor networks[J]. Lecture Notes in Computer Science, 2009, 5682:338-347.

[11] Selavo L, Wood A, Cao Q, et al. Luster: wireless sensor network for environmental research[C]//Proceedings of the 5th international conference on embedded networked sensor systems. New York, NY, USA: ACM, 2007:103-116.

[12] Akkaya K, Younis M. A survey on routing protocols for wireless sensor networks[J]. Ad Hoc Networks, 2005, 3: 325-349.

[13] Shao Min, Yang Yi, Zhu Sencun, et al. Towards statistically strong source anonymity for sensor networks[C]//Proc of 27th IEEE international conference on computer communications. Phoenix: IEEE, 2008.

[14] Kamat P, Zhang Y, Trappe W, et al. Enhancing source-location privacy in sensor network routing[C]//Proceedings of the 25th international conference on distributed computing systems. Ohio, USA: [s. n.], 2005.

[15] Liu Zhenhua, Xu Wenyan. Zeroing-in on network metric minima for sink location determination[C]//Proceedings of the 3rd ACM conference on wireless network security. Hoboken: ACM, 2010:99-104.

[16] Chai Guofei, Xu Miao, Xu Wenyan, et al. Enhancing sink-location privacy in wireless sensor networks through k-anonymity[J]. International Journal of Distributed Sensor Networks, 2012, 2012:648058.

# 基于k匿名假包注入的汇聚节点位置隐私保护

作者：[宋杰](#)，[张昆](#)，[SONG Jie](#)，[ZHANG Kun](#)  
作者单位：[安徽大学 计算机科学与技术学院, 安徽 合肥, 230601](#)  
刊名：[计算机技术与发展](#)[ISTIC](#)  
英文刊名：[Computer Technology and Development](#)  
年，卷(期)：2015 (2)

引用本文格式：[宋杰](#), [张昆](#), [SONG Jie](#), [ZHANG Kun](#) [基于k匿名假包注入的汇聚节点位置隐私保护](#) [期刊论文]-[计算机技术与发展](#) 2015 (2)