第34卷 第21期 计 算 机 工 程 2008年11月
Vol.34 No.21 Computer Engineering November 2008
·安全技术· 文章编号：1000—3428(2008)21—0136—03 文献标识码：A 中图分类号：TP301

无线传感器网络GEAR协议的安全性改进

周珊珊[1]，林 杉[1]，王翠荣[2]
（1. 东北大学信息学院，沈阳 110004；2. 东北大学秦皇岛软件中心，秦皇岛 066004）

摘 要：GEAR是一种基于位置的能量感知地理路由协议，该文针对GEAR路由协议不能防御虚假路由、选择性转发和女巫攻击等问题，提出SGEAR安全路由协议，引入一种预知部署知识的基于位置的密钥对安全引导模型。对该协议进行了实验仿真和性能分析，实验结果证明SGEAR在抵御上述攻击时，具有较好的连通性和抗俘获性。

关键词：无线传感器网络；安全性；GEAR协议

Security Improvement of GEAR Protocol in Wireless Sensor Network

ZHOU Shan-shan[1], LIN Shan[1], WANG Cui-rong[2]
(1. Information Institute, Northeastern University, Shenyang 110004;
2. Software Center, Northeastern University in Qinhuangdao, Qinhuangdao 066004)

【Abstract】 GEAR is a location-based energy-aware geographically-informed routing protocol. To solve the problem that it is incapable of defending against bogus routing information, sybil and selective forwarding attacks, this paper presents a location pairwise keys bootstrap scheme based on secure geographical and energy aware routing protocol that exploits deployment knowledge. It analyzes the security performance of the SGEAR protocol and proves that it has good capability of connectivity and resilience against node capture.

【Key words】 Wireless Sensor Network(WSN); security; GEAR protocol

1 概述

无线传感器网络(Wireless Sensor Networks, WSN)是由大量低成本且具有感知、数据处理和无线通信能力的传感器节点通过自组织方式形成的网络。对WSN的研究是目前信息领域的一个热点，它多用于军事领域，在大规模部署之前，安全问题必须得到保证[1]。

目前已提出许多针对无线传感器网络的路由协议，但大多数路由协议都没有将安全性作为一个设计目标。GEAR[2]作为一种能量感知的基于位置的地理路由协议，与传统非能量感知的路由协议相比，能极大地延长网络的寿命。GEAR路由的主要思想是：利用位置信息使得“兴趣”的传播仅到达目标区域，而不是传播到整个网络，从而避免洪泛传播方式，减少路由建立的开销。

本文以提高GEAR路由协议的安全性为目标，在保持较低能耗的情况下，在随机密钥对模型的基础上引入基于位置的部署信息，提出了一种用于静态传感器网络的基于部署信息的密钥对安全引导模型。

2 GEAR路由协议及其面临的攻击

在GEAR中，每个节点保存它到其他节点的估计代价(estimated cost)和修正代价(learned cost)。估计代价综合考虑了节点的剩余能量信息和到Sink的距离，修正代价是对估计代价的进一步修正，它考虑在空洞的情况下到目的节点的代价。当所有的邻居节点到目标区域的距离都比节点本身到目标区域的距离远时，就形成了一个空洞。

在没有空洞的情况下，估计代价等于修正代价。在GEAR中兴趣的广播分为2个阶段。第1阶段是将兴趣转发到目标区域。在这个阶段，节点收到消息后，查看是否有邻居节点到目标区域的距离更近，如果有，选择到目标区域最近的邻居节点转发消息。如果没有，就是一个hole。这时，节点可根据修正代价来选择一个邻居节点转发消息。第2阶段是区域内兴趣的广播，就是将兴趣发送给区域内的各个节点。这一阶段可以采用受限flooding方法，或者采用递归的基于位置的轮转来实现[1]。

GEAR具有路由选择和位置信息相关的特性，因此，它能抵抗槽洞攻击、虫洞攻击和HELLO flood攻击，但对虚假路由、选择性转发和女巫攻击则不能防御。

3 安全路由协议SGEAR

3.1 基于部署知识的密钥对安全引导模型

本文采用文献[3]中基于部署知识的随机密钥预分配方案，在随机密钥预分配模型的基础上做了进一步改进，引入基于节点位置的部署信息。概率密度函数$pdfs$表示节点部署知识信息，假设不同区域的节点拥有不同的$pdfs$，并将其引入到Eschenauer随机密钥预分配方案[3](简称E-G方案)中。

为发现哪些节点更有可能相互接近，使节点部署服从二维正态高斯分布。使每个小区域内$G_{i,j}$，任意节点k的分布概率基本相同，当节点部署在(x_i, y_j)，也就是$\mu = (x_i, y_j)$，那

基金项目：河北省科技厅博士基金资助项目(55470130-3)；东北大学“985”信息化平台基金资助项目

作者简介：周珊珊(1982－)，女，硕士，主研方向：无线传感器网络安全；林 杉，硕士；王翠荣，教授、博士

收稿日期：2007-12-11 **E-mail：**zhoussneu@hotmail.com

么 k 的分布概率就是：

$$f_k^{i,j}(x,y\,|\,k\in G_{i,j})=\frac{1}{2\pi\sigma^2}\mathrm{e}^{-[(x-x_i)^2+(y-y_j)^2]/2\sigma^2}=f(x-x_i,y-y_j) \tag{1}$$

3.2 SGEAR 安全路由设计

3.2.1 密钥预分布

将密钥池(密钥数为 $|S|$)被划分成若干个子密钥池(密钥数为 $|Sc|$)，每个子密钥池对应于一个部署组，若两个子密钥池是水平或垂直相邻，则至少共享 $a|Sc|$ 个密钥；若两个子密钥池是对角相邻，则至少共享 $b|Sc|$ 个密钥(a, b 满足以下关系： $0<a,b<0.25$ 且 $4a+4b=1$)。

由于节点以栅格形式分布，节点周围的密钥池被分为 8 个部分。选择密钥的算法如下：

(1)对组 $S_{1,1}$，从 S 中选择 $|Sc|$ 个密钥，并将这些密钥从 S 中去除。

(2)对每个组 $S_{1,j}$，从密钥池 $S_{1,j-1}$ 中选择 $a|Sc|$ 个密钥；然后从 S 中选择 $w=(1-a)\times|Sc|$ 个密钥，并将 w 个密钥从 S 中去除。

(3)对组 $S_{i,j}$ ($i=2,3,\cdots,t$, $j=1,2,\cdots,n$)，从密钥池 $S_{i-1,j}$ 和 $S_{i,j-1}$ 中选择 $a|Sc|$ 个密钥；从组 $S_{i-1,j-1}$ 和 $S_{i-1,j+1}$ 中选择 $b|Sc|$ 个密钥；最后从 S 中去除这 w 个密钥。容易看出每个组选择的密钥都是不同的。其中，

$$w=\begin{cases}(1-(a+b))\cdot|Sc|, & j=1\\ (1-2(a+b))\cdot|Sc|, & 2\le j\le n-1\\ (1-(2a+b))\cdot|Sc|, & j=n\end{cases}$$

本文根据共享密钥池 S 的大小 $|S|$ 来计算每个组的密钥池大小 $|Sc|$。根据密钥池建立过程，每个组首先从它的左、上、左上和右上邻居组中选择 $a|Sc|$ 或者 $b|Sc|$ 个密钥，然后从 S 中选择剩下的密钥。因为每个组从中选择的密钥数量是不同的，且其总和应该是 $|S|$，所以有如下等式：

$$|Sc|=\frac{|S|}{tn-(2tn-t-n)a-2(tn-t-n+1)b} \tag{2}$$

3.2.2 相邻节点交换位置和能量信息

在GEAR路由中，每个节点知道自己的位置和剩余能量信息以及目标区域的位置信息。为安全获取邻居节点的位置和能量信息，每个节点广播一条包含所携带密钥索引的消息，邻居节点用这条消息来查找自己是否与该节点共享密钥[4]。

在上述步骤完成后，节点间存在共享密钥，整个传感器网络相当于密钥共享图 G，定义如下：

定义 1 V 表示传感器网络中的所有节点。密钥共享图 $G(V,E)$ 按如下方式建立：对任何 2 个节点 i 和 j，需同时满足：(1)节点 i 和 j 至少有一个共享密钥；(2)节点 i 和 j 距离在一次无线传输距离范围内，单跳就能到达。

相邻节点间的密钥建立起来以后就可以通过一个简单的交换机制获取邻居节点的位置和能量信息。假定节点 u 位置坐标是 (i_u,j_u)，剩余能量信息为 e_u，节点 u 发送一个加密的消息给它的邻居节点 v，加密公式如下：

$$I=\{u,(i_u,j_u),e_u\}\,|_k \tag{3}$$

其中，I 表示加密后的位置和能量信息；u 是节点 ID；k 是加密密钥。若节点 u 和 v 之间有直接密钥，k 就可以是 $f_k(x,y\,|\,k\in G_{i,j})$。邻居节点 v 利用共同的密钥解密该消息，并回复一个消息给节点 u，这样节点 u 就获得其邻居节点的位置和剩余能量信息。

3.2.3 查询消息传到目标区域

Sink 节点用单播方式将一条包括源位置、目标区域和消息认证码的查询消息发给距目标区域最近的邻居节点，该消息用共享的密钥加密，只有与 *Sink* 节点有共享密钥对的邻居能够解密该消息。*Sink* 节点的邻居解密该消息，添加自己的位置信息后再加密该消息，并发给自己的靠近目的节点的邻居，依次按贪婪算法进行下去。

3.2.4 查询消息在目标区域内传播

GEAR 路由中，消息到达目标区域的第一个节点时，若该节点的邻居数量大于一个预设的阈值，则使用迭代地理转发机制，否则使用洪泛机制。

若采用迭代地理转发机制，在地理迭代过程中，将查询消息以单播方式分别传到子区域中心节点，此时安全通信仍然采用和上面类似的方式。若节点收到不能认证的消息，则丢弃。

若采用洪泛机制，使用广播方式，在安全方面需要解决的问题是广播包的认证问题。一个方法是采用 $\mu TESLA$ 协议[5]。该协议开销不大，适合传感器网络。若两相邻节点有直接的共享密钥，则可用此进行广播包的认证。若两相邻节点使通过密钥路径建立共享密钥，可用事先协商好会话密钥进行广播认证。

4 实验环境和性能分析

本文采用 NS2 仿真平台对所设计的路由协议进行仿真。NS2 作为比较成熟的仿真平台，可以对无线局域网、多跳 Ad hoc 等网络进行仿真。其中，本文所改进的 GEAR 协议作为 Directed Diffusion 协议的一个 filter 应用集成在 NS2 中，因此，本文在 NS2 平台下对其加以安全性改进。

4.1 局部连通性概率

在基于部署知识的密钥安全方案中，对于节点 n_i,n_j 事件 $A(n_i,n_j)$, $B(n_i,n_j)$ 定义如下[3]： $A(n_i,n_j)$ ：节点 n_i 和 n_j 是邻居节点； $B(n_i,n_j)$ ：表示节点 n_i 和 n_j 至少有一个共享密钥； p_{local} 是局部联通性概率，即任意 2 个节点间至少存在共享一个密钥的概率。

$$p_{\mathrm{local}}=\Pr(B(n_i,n_j)\,|\,A(n_i,n_j)) \tag{4}$$

根据条件概率的性质有：

$$p_{\mathrm{local}}=\Pr(B(n_i,n_j)\,|\,A(n_i,n_j))=\frac{\Pr(B(n_i,n_j)\text{and}A(n_i,n_j))}{\Pr(A(n_i,n_j))} \tag{5}$$

其中，

$$\Pr(B(n_i,n_j)\text{ and }A(n_i,n_j))=\frac{1}{2\pi\sigma^2}\mathrm{e}^{-\frac{(x-x_j)^2+(y-y_j)^2}{2\sigma^2}}\cdot\mathrm{d}x\mathrm{d}y \tag{6}$$

$$\Pr(A(n_i,n_j))=\int_{x=0}^{X}\int_{y=0}^{Y}\sum_{j\in\Psi}\sum_{i\in\psi}\Pr(n_j\in groupj)\Pr(n_i\in groupi)\cdot f_R(d_{jZ}\,|\,n_j\in groupj)\cdot g(d_{jZ}\,|\,n_j\in groupj)\mathrm{d}x\mathrm{d}y \tag{7}$$

局部连通性和节点所携带密钥数目的关系如图 1 所示。实验表明，在同等条件下，该方案提高了节点的连通概率。例如，当节点预分配的密钥数为 50 时，E-G方案[3]的节点连通概率仅为 0.029，而该方案能够达到 0.383。

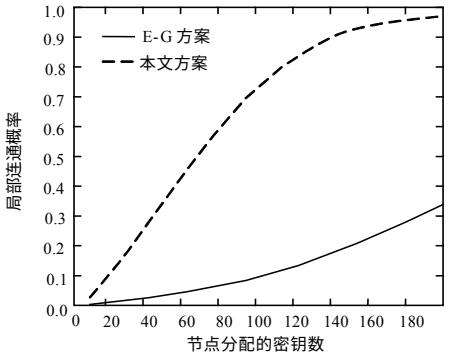

图 1　局部连通性

4.2　节点抗俘获性

为了评价这个策略的抗俘获性，需要得知入侵者在俘获 x 个节点时的正常节点通信被俘概率。因为密钥在整个区域里不是均匀的分布，这 x 个被俘获的节点位置影响分析的结果。假设这 x 个节点是随机分布在部署区域的。虽然在现实中被俘获节点更有可能集中在某一区域，这是因为入侵者更可能俘获其周围的节点。这种情况下，部分网络的抗俘获性会低于整个网络。由于篇幅所限，本文不考虑本地抗俘获性。

假设 k 是 2 个未被俘获节点的通信密钥。除了这 2 个节点以外的节点被俘获时，k 不被俘获的可能性是 $1-\frac{m}{|S|}$，m 是每个节点上的密钥数。当 x 个节点被俘获，k 不被俘获的可能性是 $(1-\frac{m}{|S|})^x$。因此，正常节点通信被俘概率为 $(1-\frac{m}{|S|})^x$。

网络抗俘获性结果与基本的 E-G 密钥预分配策略的对比如图 2 所示。

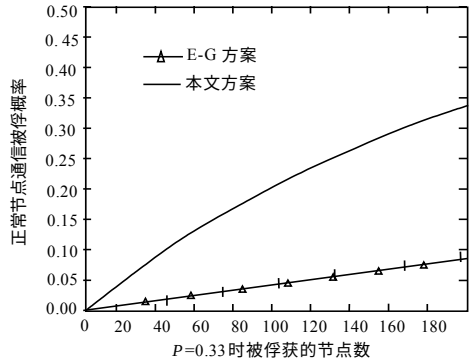

图 2　网络的抗俘获性

本文的策略在 x 个节点被俘获时，极大地减少了正常节点通信被俘概率。这种改进的优点是，当具有相同的密钥池大小 $|Sc|$ 时，为了达到相同的本地连通性，本文策略需要更小的 m。如当 $|S|=100\,000$ 时，为了达到 $p=0.33$，基本策略需要 $m=200$，本文策略只需要 $m=46$。m 的值越小，抗俘获性越好。性能提高来自部署知识，减少了节点中不必要的密钥数。

5　结束语

传感器节点有限的资源给传感器网络安全路由的设计与实现带来了挑战。本文以提高网络安全性为首要设计目标，对GEAR路由协议进行了改进，通过引入基于部署信息的密钥对引导方案，提高了对网络攻击的抵御能力，使设计的SGEAR安全路由协议具有更好的安全性能。实验结果表明，与原有协议相比，SGEAR协议在局部连通性和抗俘获性方面有很大提高。但是单个节点的泄密仍可能阻碍全网的通信，未来的研究方向是采用冗余的技术[6]，将数据报文沿多条路径发送，设计一个具有入侵容忍能力的安全路由。

参考文献

[1] Akkaya K, Younis M. A Survey on Routing Protocols for Wireless Sensor Networks[J]. Ad Hoc Networks, 2005, 3(3): 325-349.

[2] Yu Yan, Estrin D, Govindan R. Geographical and Energy-aware Routing: A Recursive Data Dissemination Protocol for Wireless Sensor Networks[R]. Los Angeles, USA: Computer Science Dept., UCLA, Technical Report: UCLA-CSD TR-01-0023, 2001-05.

[3] Eschenauer L, Gligor V. A Key Management Scheme for Distributed Sensor Networks[C]//Proc. of the 9th ACM Conf. on Computer and Communications Security. New York, USA: [s. n.], 2002.

[4] Du Wenliang, Deng Jing. A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge[C]//Proc. of the IEEE INFOCOM'04. Piscataway, USA: [s. n.], 2004.

[5] Perrig A, Szewczyk R, Wen V, et al. Spins: Security Protocols for Sensor Networks[J]. ACM Wireless Network, 2002, 8(5): 521-534.

[6] Nasser N, Chen Yunfeng. Secure Multipath Routing Protocol for Wireless Sensor Networks[C]//Proceedings of International Conference on Distributed Computing Systems Workshops. Toronto, Ontario, Canada: [s. n.], 2007.

（上接第 119 页）

参考文献

[1] Chaum D. Blind Signatures for Untraceable Payments[EB/OL]. (2000-06-25). http://citeseer.ist.psu.edu/cotext/2064/0.html.

[2] Shamir A. Identity-based Cryptosystems and Signature Schemes[C]// Proceedings of CRYPTO84 on Advances in Cryptology. New York, USA: Springer Verlag, 1985.

[3] Boneh D, Franklin M K. Identity Based Encryption from the Weil Pairing[J]. SIAM Journal on Computing, 2003, 32(3): 586-615.

[4] Mihir B, Chanathip N, Neven G. Security Proofs for Identity-based Identification and Signature Schemes[C]//Proc. of the Eurocrypt 2004. Berlin, Germany: Springer Verlag, 2004.

[5] Vo D L, Zhang Fangguo, Kim K. A New Threshold Blind Signature Scheme form Pairings[C]//Proc. of the 2003 Symposium on Cryptography and Information Security. Tokyo, Japan: [s. n.], 2003.

[6] Liang Xiaohui, Cao Zhenfu, Chai Zhenchuan, et al. ID-based Threshold Blind Signature Scheme from Bilinear Pair[Z]. 2006.

[7] Cheng Xiaoguo, Xu Weidong, Wang Xinmei. A Threshold Blind Signature from Weil Pairing on Elliptic Curves[J]. Journal of Electronics, 2006, 23(1): 76-80.