第37卷 第21期
Vol.37 No.21

计 算 机 工 程
Computer Engineering

2011年11月
November 2011

·博士论文· 文章编号：1000—3428(2011)21—0014—03 文献标识码：A 中图分类号：TN929.5

DDRP中的虫洞攻击分析与预防

王 成，杨宝琨，闫桂荣

(西安交通大学机械结构强度与振动国家重点实验室，西安 710049)

摘 要：定向扩散路由协议极易遭受虫洞攻击。为此，以仅存在2个毒害节点的情况为例，推导毒害节点放置位置与虫洞攻击严重程度间的定量关系。通过OMNeT++上的仿真实验，求解毒害节点最佳放置位置，并说明对应的最大虫洞攻击严重程度。为预防虫洞攻击，提出一种将最佳梯度节点加强转换为梯度节点概率选择加强的策略。仿真实验结果表明，该预防策略是有效的。

关键词：定向扩散路由协议；毒害节点最佳放置位置；最大虫洞攻击严重程度；预防策略；概率选择加强

Analysis and Prevention of Wormhole Attack in DDRP

WANG Cheng, YANG Bao-kun, YAN Gui-rong

(State Key Laboratory of Mechanical Structural Strength and Vibration, Xi'an Jiaotong University, Xi'an 710049, China)

【Abstract】Directed Diffusion Routing Protocol(DDRP) is easy to suffer from wormhole attack. Take only two wormhole nodes in Wireless Sensor Network(WSN) for example, the quantitative relationship between placement of poison nodes and severity of wormhole attack is formulated reduction. The optimal placement of two poison nodes and most severity of wormhole attack are solved by simulation on OMNeT++ platform. In order to prevent wormhole attack, the best gradient node reinforcement is changed into gradient nodes probabilistic selected reinforcement in DDRP. Simulation results prove the effectiveness of the proposed strategy

【Key words】Directed Diffusion Routing Protocol(DDRP); optimal placement of poison nodes; severity of most wormhole attack; prevention strategy; probabilistic selected reinforcement

DOI: 10.3969/j.issn.1000-3428.2011.21.005

1 概述

通信和信息安全是无线传感器网络(Wireless Sensor Network, WSN)在战场应用中的关键，但战场WSN在整个通信过程中，利用空气当媒介，通过无线通信技术来达成信息传递，容易遭受到如同资料篡改、窃听、虫洞攻击与阻绝攻击等方式的攻击。因此，安全的路由协议是非常受到重视的议题。专门为WSN设计的安全路由协议已经可以抵御绝大多数的安全威胁。然而，虫洞是一种透过路由的缺失来加以攻击的新型高级攻击方式，透过2个共谋的恶意节点，透过更快速传输方式，以取得相对于正常路由更好的传输参数，并取得大部分的路由权利，这样可以控制某个区段环境下的路由运作，以便肆意地进行破坏或窃取机密性资料。现存的安全路由机制，依然无法有效地抵御虫洞攻击。

定向扩散路由协议是由Estrin D等人专门为WSN设计的一种路由协议。该协议以数据为中心，引入网络梯度的概念来处理对WSN的查询，广泛应用于战场无线传感器网络中。它采用相邻节点间相互通信的方式来避免维护整个全局的网络拓扑，通过查询数据驱动传输模式以及局部的数据融合来减少网络中的开销，最终形成从源点到目的点的最短路径。因为在一般情况下，虫洞隧道的长度大于一跳距离，但在路由上却表现为一跳距离。因此，定向扩散路由协议的节点在选择路由时倾向于虫洞所在的路径，很容易受到虫洞攻击。

文献[1]将路由协议中“隧道”的建立方式分为报文封装和带外私有链路信道型2种，并将虫洞攻击分为显示攻击和隐式攻击2种。文献[2]提出SAM协议收集MANETs中的路由资料，并依据统计分析后的信息来抵御虫洞攻击。文献[3]通过Algosensim仿真软件对DV-Hop算法中增加检测虫洞攻击及抵抗该攻击的方法前后进行了模拟，并指出虫洞攻击也与攻击者的位置相关。文献[4]对圆形域进行虫洞攻击严重程度分析。以上虫洞攻击的研究集中于模型阶段，没有实际应用，且针对的都不是DDRP协议，没有从理论上进行严密推导，也没有从概率和统计的角度进行定量研究。

目前的虫洞攻击预防及检测机制[5]，都需仰赖特殊的硬设备，并且需要消耗大量的系统资源，或设立一些不符合WSN的假设。鉴于此，本文设计一种适用于WSN的新安全入侵预防机制，在不需任何的特殊硬件装置或设立一些不符合无线环境的假设，从而躲避虫洞攻击。

2 虫洞攻击严重程度分析

由于4种类型虫洞攻击[1]的分析方法基本一致，以下仅考虑使用Two-phase DDRP，在存在2个恶意节点的随机均匀分布的稠密型WSN中的“显式带外虫洞攻击”。

这里作如下假设：(1)在不存在毒害节点的传感器网络为 Net，传感器网络区域面积为 S_{Net}，传感器节点总个数为 n，传感器节点的密度 $\Phi = n/S$，传感器节点 S 与 D 间的距离为 $d_{S,D}$，最小跳数路由为 $L_{S,D}$，对应的最小跳数为 $N_{S,D}$，普通节点之间的通信半径为 T，正方形边长为 L；(2)存在 M_1 和 M_2 2个毒害节点的WSN为 Net^*，传感器节点数为 $n+2$，S 与 D 间的最小跳数路由为 $L^*_{S,D}$，对应的最小跳数为 $N^*_{S,D}$。

基金项目：国家自然科学基金资助项目(10776026)

作者简介：王 成(1984－)，男，博士研究生，主研方向：无线网络；杨宝琨，博士研究生；闫桂荣，教授

收稿日期：2011-04-15 **E-mail：**wc071@163.com

2.1　虫洞攻击严重程度公式推导

定理 1 面积为 S_C 的区域 C 传感器节点的数目近似服从泊松分布：$P\{x=m\}=(\Phi S_C)^m \mathrm{e}^{-\Phi S_C}/m!\ \ (m=0,1,\cdots,n)$。

定理 2 $N_{S,D}\geqslant d_{S,D}/T$，$N_{S,D}\leqslant 2d_{S,D}/T$，$N^*_{S,D}\leqslant N_{S,D}$。

由定理 2 可得，$N_{S,D}$ 是 $d_{S,D}/T$ 的一个函数 $N_{S,D}=\beta d_{S,D}/T$，$1\leqslant\beta\ \ 2$ 是一个与 *Net* 中节点稠密程度有关的常数，越稠密，β 越小，当 $\Phi\to+\infty$ 时，$\beta\to 1$。

定理 3 在 Net^* 中，当且仅当 $\min(N^*_{S,M_1}+N^*_{D,M_2}+1, N^*_{S,M_2}+N^*_{D,M_1}+1)<N_{S,D}$，$S$ 与 D 间的通信受到虫洞攻击；当且仅当 $\min(N^*_{S,M_1}+N^*_{D,M_2}+1, N^*_{S,M_2}+N^*_{D,M_1}+1)>N_{S,D}$，$S$ 与 D 间的通信不受到虫洞攻击。

定理 4 在 Net^* 中，当且仅当 $\min(d_{S,M_1}+d_{D,M_2}, d_{S,M_2}+d_{D,M_1})\leqslant d_{D,M_1})\leqslant d_{S,D}$，$S$ 与 D 之间的通信受到虫洞攻击。

定义 1 虫洞攻击严重程度 η

$\eta=(Net^*$中受虫洞攻击的通信节点对数$/C_n^2\cdot 100\%$

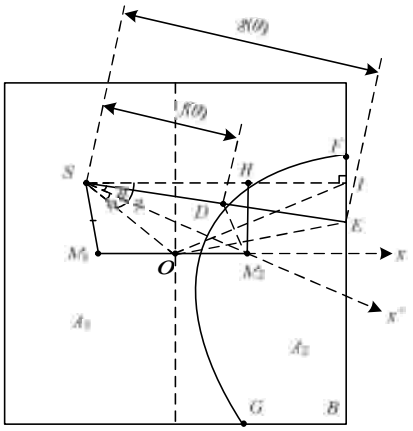
定义 2 最大虫洞攻击严重程度 $\eta_{\max}$

$\eta_{\max}=\max\{\eta\,|\,$恶意节点$M_1$、$M_2$各种放置下$\}$

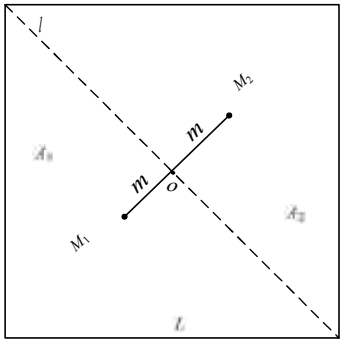
其中，$\eta_{\max}$ 的求解包括以下 2 个问题：(1) M_1 和 M_2 应该如何放置，才能达到 $\eta_{\max}$；(2) $\eta_{\max}$ 是多少。这都与 WSN 的形状有关，以下就以正方形区域为例，求取这 2 个问题的解析解和数值仿真解。

2.2　正方形区域最大虫洞攻击严重程度

因为正方形的几何对称特点，M_1 和 M_2 应该对称放置才能达到 $\eta_{\max}$。以下考虑图 1(a)中垂线 $l\in[T/2, L/2]$ 和图 1(b)对角线 $l\in[T/2,\sqrt{2}L/2]$ 2 种布置方案。



(a)中垂线配置方案



(b)对角线配置方案

图 1　恶意节点放置示意图

定义 3 不可到达区域 U_S

在 Net^* 中，对 S，有一个区域 U_S，其内部的任一节点 D，都有 $\min(d_{S,M_1}+d_{D,M_2}, d_{S,M_2}+d_{D,M_1})\leqslant d_{S,D}$，则称该区域 U_S 是 S 不可到达区域。S 和 U_S 内任何节点之间的通信都受到虫洞攻击，而与 U_S 以外任何节点间的通信都不会受到虫洞攻击。

定理 5 对于图 1，至少 50%的节点间的通信不会受到虫洞攻击。

定理 6 对于图 1(a)，$\Delta U_S=\frac{1}{2}\int_{\theta_-}^{\theta_+}\{[g(\theta)]^2-[f(\theta)]^2\}\mathrm{d}\theta$，其中，$g(\theta)$ 为正方形边界到 S 的距离；$f(\theta)$ 为以 S 和 M_2 为焦点的双曲线的右半支到 S 的距离；θ_- 和 θ_+ 是以 S 和 M_2 为焦点的双曲线的右半支与正方形区域边界的交点，即分别为 $g(-\theta)=f(-\theta)$ 和 $g(\theta)=f(\theta)$ 的解。

定理 7 $\eta=E[\Delta U_S]/L^2$，而：

$$E[\Delta U_S]=2\{\int_{\frac{\pi}{2}}^{\frac{3}{4}}[\int_0^{\frac{L}{2\sin\alpha}}\Delta U_S r\,\mathrm{d}r]\,\mathrm{d}\theta+\int_{\frac{1}{4}}^{\frac{-}{}}[\int_0^{\frac{-L}{2\cos\alpha}}\Delta U_S r\,\mathrm{d}r]\,\mathrm{d}\theta\}$$

2.3　仿真验证与求解

找到定理 7 的解析解是很困难的，本文采用 OMNeT++ 平台进行多次数值模拟，对随机生成的 100 个不同的 WSN，不同的 T，通过变步长法后统计平均得到的结果，如图 2 所示。

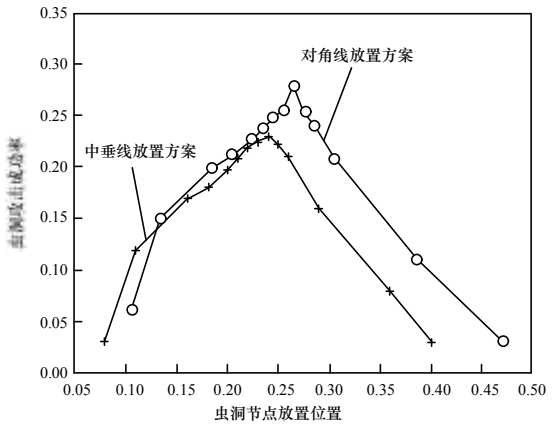


图 2　恶意节点放置位置与虫洞攻击严重程度间的关系

由图 2 可知，对于图 1(a)中垂线配置方案，达到最大虫洞攻击严重程度时 m 的数值解为：$l\approx 0.23L\sim 0.24L$，最大虫洞攻击严重程度 $\eta_{\max}$ 为：$\eta_{\max}\approx 22\%\sim 23\%$。同理，对于图 1(b)，达到最大虫洞攻击严重程度时 m 的数值解为：

$l\approx 0.26L\sim 0.28L$

达到最大虫洞攻击严重程度 $\eta_{\max}$ 为：

$\eta_{\max}\approx 24\%\sim 27\%$。

3　降低虫洞攻击严重程度的预防策略

3.1　梯度节点概率动态选择加强策略

文献[6]提出一个新颖的观点：从使用者的角度出发，用分析跳数的方式，对路由表中的相关信息设立门坎值，尽量避免明显可能存在危害的路由，用来躲避虫洞攻击。

该机制具备躲避虫洞攻击的效果，但在 Two-phase DDRP 中，每一传感器节点仅能感知并选择梯度方向的一个邻居节点作为下一跳路由节点，这与知道全局路由，分析跳跃次数并能对路由表中的相关信息设立门坎值的情形完全不同。故根据 Two-phase DDRP 的特点，将最佳梯度节点加强改为梯度节点概率选择加强，来减少最少跳数路由被选中的概率，从而降低虫洞攻击的严重程度。

3.2 P 概率和 Sin 概率策略

在 P 概率策略中，最佳梯度邻居节点被选为下一跳路由结点的概率为 p，次最佳梯度邻居节点被选为下一跳路由结点的概率为 1-p。如果每一节点的梯度邻居节点个数≥2，则 $L^*_{S,D}$ 被选中的概率仅为：$p^{N^*_{S,D}}$。当 $N^*_{S,D}$ 较大时，显然 $p^{N^*_{S,D}}$ 较小，选择其他路径的概率为 $1-p^{N^*_{S,D}}$，$p\in[0,1]$。$p=1$ 即最佳梯度节点加强；$p=0$ 即次最佳梯度节点加强。

为了在降低虫洞攻击严重程度的同时，WSN 的平均路由跳数不要增加太多，故在确保跳数少的路由尽量不被选中的同时，跳数多的路由也尽量不被选中，而应尽量选择跳数居中的路由。Sin 概率策略如下：

$$p(S,S_{nexti})=\begin{cases}1 & k=1\\ \dfrac{1}{2} & k=2\\ \sin\dfrac{(i-1)}{k-1}/\sum\limits_{i=1}^{k}\sin\dfrac{i-}{k-1} & k>2\end{cases}$$

即使用利用类似 Sin 函数的归一化概率轮盘，最佳梯度和最坏梯度邻居节点被选为下一跳路由节点的概率都较小，而中间梯度节点被选为下一跳路由节点的概率较大。

4 仿真结果比较

本文仅考虑 2 个恶意节点放置在正方形 WSN 中最佳位置，即对于图 1(b)中垂线配置方案，达到最大虫洞攻击严重程度时，在 OMNeT++平台进行多次数值模拟仿真后 P 概率策略和 Sin 概率策略的统计平均结果如图 3、图 4 所示。可以看出，在 P 概率策略中，p 值越小，虫洞攻击严重程度越小，但 WSN 中的平均路由跳数也越大。同时，Sin 概率策略是一种虫洞预防效果和 WSN 的平均路由跳数增加都较平衡的一种加强策略。

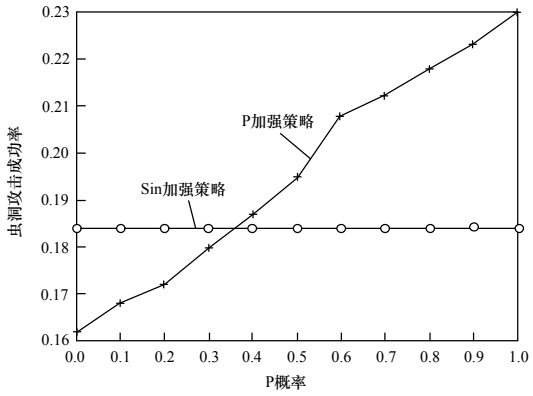


图 3 加权概率与虫洞攻击严重程度

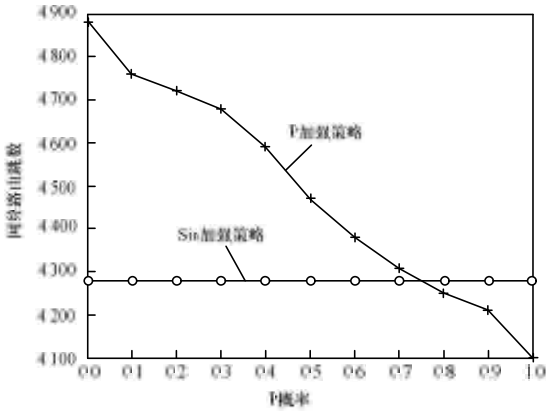


图 4 加权概率与路由跳数

5 结束语

本文所有的公式推导、定义、定理、结论及仿真结果都是在仅存在 2 个恶意节点和正方形战场区域中随机均匀分布的，且都是使用 Two-phase DDRP 的 WSN 中“显式”带外信道型下进行的。但其基本原理和分析方法可以推广应用于其他战场区域形状、路由协议、传感器节点分布类型、“隧道”模型、虫洞攻击类型和 WSN 中存在多个恶意节点的情况。除了 P 概率和 Sin 概率策略外，也可提出其他梯度节点概率选择加强策略。值得注意的是，任何梯度节点概率动态选择加强策略在降低虫洞攻击的严重程度的同时，都会增加通信代价。

参考文献

[1] 谭长庚, 李婧榕. Ad Hoc 网络中合谋攻击研究综述[J]. 计算机工程, 2010, 36(3): 177-179.

[2] 周启明, 何 勇. DV-Hop 中虫洞攻击的仿真及其抵抗方法[J]. 计算机工程与应用, 2010, 46(14): 88-90.

[3] Qian Lijun. Detection of Wormhole Attacks in Multi-path Routed Wireless Ad Hoc Networks: A Statistical Analysis Approach[J]. Journal of Network and Computer Applications, 2007, 30(1): 308-330.

[4] Majid K, Hugues M, Vijay K B. Severity Analysis and Countermeasure for the Wormhole Attack in Wireless Ad Hoc Networks[J]. IEEE Trans. on Wireless Communications, 2009, 8(2): 736-745.

[5] 张 毅, 王小非, 夏学知. Ad Hoc 网络环境中避免虫洞攻击的路由算法[J]. 计算机工程, 2007, 33(3): 138-140.

[6] 任上鸣, 赖溪松. 无线随意网路之虫洞攻击研究与预防[C]// 第六届离岛信息技术与应用研讨会会议论文集. 武汉: [出版者不详], 2007.

编辑 陈 文

(上接第 13 页)

基于语义与基于消息内容的服务路由算法，以提高消息交换路由成功率，增强消息路由的鲁棒性与可靠性。

参考文献

[1] Bell M. Service-oriented Modeling: Service Analysis, Design, and Architecture[M]. New York, USA: [s. n.], 2008.

[2] Liu Zhuangye, Yao Zhen. Study on Key Issues About Service-oriented Architecture[J]. Computer Engineering and Design, 2009, 30(3): 600-604.

[3] 谢继晖, 白晓颖, 陈 斌, 等. 企业服务总线研究综述[J]. 计算机科学, 2007, 34(11): 13-18.

[4] 温 睿, 李国义, 王 飞, 等. 基于 SOA 总线的资源协同组织机制[J]. 计算机工程, 2010, 36(8): 261-263.

[5] Ron T, Peter W. JSR-208 Java Business Integration Specification 1.0[S]. 2005.

[6] Zelenka A. Open Source ESB for SOA & Integration[EB/OL]. (2007-02-16). http://redmonk.com/public/OpenSourceESBs.pdf.

[7] Sui Xin, Zhu Yunlong, Nan Lin. An Architecture Design of a JBI-based Enterprise Service Bus[C]//Proc. of 2009 Int'l Conf. on Interoperability for Enterprise Software and Applications. Beijing, China: [s. n.], 2009.

编辑 陈 文