

文章编号:1001-9081(2014)03-0710-04

doi:10.11772/j.issn.1001-9081.2014.03.0710

基于邻居路由的 Ad Hoc 网络虫洞检测

曹晓梅^{1,2,3}, 吴雷^{1,2,3*}, 李佳耕^{1,2,3}

(1. 南京邮电大学 计算机学院, 南京 210003; 2. 江苏省无线传感网高技术研究重点实验室(南京邮电大学), 南京 210003;

3. 南京邮电大学 宽带无线通信与传感网技术教育部重点实验室, 南京 210003)

(* 通信作者电子邮箱 imhist1989@163.com)

摘要:针对 Ad Hoc 网络中虫洞检测方法带来的高时延和能耗问题,提出一种低时延和能耗的轻量级虫洞检测方法。即在节点查询路由后,利用路由节点的邻居数目,找出可能受虫洞影响节点的集合,同时依据路由节点的某个邻居节点的路由信息,进一步确定路由节点是否受虫洞影响。仿真结果表明,该方法可有效减少虫洞检测中的路由查询次数,并且与 DeWorm 和 E2SIW 方法相比,可有效减少时间延迟和能量消耗。

关键词:Ad Hoc 网络;虫洞攻击;路由信息;路由节点;虫洞检测

中图分类号: TP393.08 **文献标志码:**A

Wormhole detection based on neighbor routing in Ad Hoc network

CAO Xiaomei^{1,2,3}, WU Lei^{1,2,3*}, LI Jiageng^{1,2,3}

(1. School of Computer Science and Technology, Nanjing University of Posts and Telecommunications, Nanjing Jiangsu 210003, China;

2. Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks (Nanjing University of Posts and Telecommunications), Nanjing Jiangsu 210003, China;

3. Key Laboratory of Broadband Wireless Communication and Sensor Network Technology (Nanjing University of Posts and Telecommunications), Ministry of Education, Nanjing Jiangsu 210003, China)

Abstract: To solve high energy and time delay cost problems caused by wormhole detection in Ad Hoc networks, a light-weighted wormhole detection method, using less time delay and energy, was proposed. The method used the neighbor number of routing nodes to get a set of abnormal nodes and then detect the presence of a wormhole by using the neighbor information of abnormal node when routing process was completed. The simulation results show that the proposed method can detect wormhole with less number of routing query. Compared with the DeWorm (Detect Wormhole) method and the E2SIW (Energy Efficient Scheme Immune to Wormhole attacks) method, it effectively reduces the time delay cost and energy cost.

Key words: Ad Hoc network; wormhole attack; routing information; routing node; wormhole detection

0 引言

Ad Hoc 网络无需固定的网络设施,通过自组织节点即可实现网络的端到端通信功能。由于 Ad Hoc 网络的特性,如开放的网络结构、节点资源有限、动态的网络拓扑结构等^[1],网络很容易遭受到各种各样的攻击。虫洞攻击便是众多攻击中危害较为严重的一个。虫洞攻击^[2]是一种合作式攻击,即攻击者在两虫洞节点间建立一条额外的通道。若其中一个节点收到分组,则转发给另一端的节点,分组在另一端广播。由于虫洞攻击一般是分组在物理上的重放,相比于其他攻击,虫洞攻击可免疫于认证和加密等技术,因而更易于实施。虫洞攻击往往以破坏路由机制为首要目的,攻击者声称自己是最短路径的入口,导致路由指向自己,但不转发或部分转发数据包,继而发动黑洞攻击、拒绝服务攻击等,最终破坏网络的可用性。

现有的虫洞攻击检测方法大体可分为两类:一类是利用时间或外部系统^[3~6];另一类是依靠网络自身的信息^[7~14]。文献[3]中提出了分组约束方法,包括位置约束和时间约束。位置约束方法需要节点位置信息和不严格的时钟同步,分组需要发送节点位置和分组的发送时间字段以限定分组的传输

距离;时间约束需要严格的时钟同步,分组传输时需要附加其发送时间,接收节点根据分组收发时间差来限制其传输距离。但是位置约束方法会受到节点间障碍物的影响,时间约束方法对硬件要求比较高。在文献[4]中,作者在路由发现报文中附加额外的信息字段来实现虫洞的检测,该方法需要位置和时间信息,附加的控制报文会增加网络的能量消耗。文献[5]中给出了一个基于时间的虫洞检测方法。对于隐藏的虫洞,文献通过邻居节点监听机制来排除那些不在传输范围的假的邻居,从而排除虫洞的影响;对于暴露的虫洞,文献通过记录发送广播发现报文与接收到广播响应报文的时间差,计算每跳的平均时延,看其是否大于预定阈值来检测该种攻击。文献[6]中提出了一种基于位置的虫洞检测及定位的方法,其关键在于最小跳数的估计,即利用位置信息来估计两节点的最小跳数。该方法可以有效检测虫洞,但是会消耗较多的网络能量。

文献[7]中给出了基于节点邻居信息的虫洞检测方法。其前提是网络在部署中没有受到虫洞的影响,且网络是静态的。网络部署和节点完成邻居查询后,节点验证每个路由控制报文是否来自于其邻居来避免虫洞的影响。文献[8]中利用节点的使用频率和虫洞的参数信息来检测虫洞,同时在路

收稿日期:2013-09-25;修回日期:2013-11-20。

作者简介:曹晓梅(1974-),女,江苏无锡人,副教授,博士,主要研究方向:无线网络安全、传感器网络安全; 吴雷(1989-),男,河南周口人,硕士研究生,主要研究方向:无线传感器网络安全; 李佳耕(1989-),男,山东枣庄人,硕士研究生,主要研究方向:无线传感器网路安全。

由查询中引入惩罚机制。文献[9]假定在网络部署时,每个节点都有其他节点的数字签名,恶意节点没有有效的签名。通过在路由查询报文中加入数字签名来保证路由的可用性。文献[10]中给出了一种基于连通性的虫洞检测方法。但是只对虫洞链路比较远的攻击有效。文献[11]中根据不同类型虫洞对网络拓扑的影响来检测虫洞。文献[12]利用受虫洞影响路径更容易被用于数据传输,受虫洞影响节点使用频率会高于普通节点。通过比较节点的使用频率,来检测虫洞。但是该方法对虫洞攻击的响应比较慢。文献[13]中提出了利用节点邻居路由信息的虫洞检测方法——DeWorm(Detect Wormhole)。文献[14]中给出了E2SIW(Energy Efficient Scheme Immune to Wormhole attack)方法,对DeWorm进行了改进,DeWorm需要节点所有邻居的路由信息,E2SIW仅需要节点最近邻居的路由信息。除上述检测技术外,文献[15]将对称、非对称加密技术与GPS(Global Positioning System)相结合来检测虫洞。

本文提出一种轻量级邻居路由检测(Detect Wormhole by Neighbor Routing,DWNR)方法。类似于DeWorm和E2SIW方法,DWNR也借助节点邻居的路由信息来检测虫洞。相比而言,DeWorm方法检测虫洞时,路由节点的所有邻居节点(下一跳路由节点除外)均要查询到目标节点的路由,然后节点根据返回的路由信息来判断虫洞的存在,该方法逐一检测所有路由节点,至判定虫洞存在或遍历结束为止;E2SIW方法只需距离路由节点最近的邻居的路由信息来判定虫洞是否存在,该方法同DeWorm方法一样要逐一检测所有路由节点;DWNR方法的思想是利用节点的邻居数来筛选可能受虫洞影响的路由节点,然后判定虫洞是否存在,因此,与前两种方法相比,DWNR在一定程度上降低了虫洞检测的次数。

1 本文方法描述

1.1 DWNR方法

DWNR方法的依据是虫洞的存在会影响网络中部分节点的邻居数。方法含有可疑节点检测和判定两个阶段。前者统计路由节点的邻居数量,找到可能受虫洞影响的节点,即可疑节点;后者根据可疑节点及其邻居的路由信息,判定虫洞是否存在,若存在虫洞,则节点选择其他可用路径传输数据。本文假定网络中的虫洞节点成对出现,节点拥有位置信息且邻居表含有邻居节点的位置信息;虫洞节点与普通的网络节点具有同样的通信半径,虫洞链路大于一跳传输距离。方法中涉及的符号定义如表1所示。

表1 符号定义

符号	描述
M_1, M_2	虫洞节点对
P_{ij}	源节点 <i>i</i> 到目的节点 <i>j</i> 的路径
B_{M_1}	虫洞节点 <i>M₁</i> 的一跳邻居集合
B_{M_2}	虫洞节点 <i>M₂</i> 的一跳邻居集合
$S(P_{ij})$	路径 <i>P_{ij}</i> 上可疑节点的集合
$N(m)$	节点 <i>m</i> 的一跳邻居列表
$Z(N(m))$	距离节点 <i>m</i> 最近的邻居节点
$C(m)$	节点 <i>m</i> 的一跳邻居数目
$P_{ij}(m)$	路径 <i>P_{ij}</i> 上距节点 <i>i</i> 第 <i>m</i> 跳的节点

1.2 可疑节点的检测

假定Ad Hoc网络含有的节点数为*N*,节点的部署区域为*L × L*,节点的通信半径为*R*,定义*Ψ*为网络的平均节点密度。则有:

$$\Psi = \frac{N}{L \times L} \quad (1)$$

根据式(1),可知每个节点的邻居数*C*为:

$$C = \pi R^2 \times \Psi \quad (2)$$

由于虫洞的特性,受虫洞影响的节点会将虫洞另一端所覆盖的节点作为其邻居。在虫洞节点和网络节点通信距离一致的情况下,根据式(2),受虫洞节点影响的节点其邻居数大约为*2C*,普通节点大约为*C*。利用这个特性,源节点根据每个路由节点的邻居数量信息,可以找到受虫洞影响的节点。

路由查询中,路由节点在发送路由响应分组时添加其邻居节点数信息。从而,源节点接收到的路径信息中包含了所需的信息。假定源节点为*S*,目的节点为*D*,*S*经查询得到路径*P_{SD}*,路径*P_{SD}*跳数为*n*。首先*S*计算总邻居数*Sum*:

$$Sum = C(P_{SD}(0)) + C(P_{SD}(1)) + \dots + C(P_{SD}(n)) \quad (3)$$

根据式(3)求平均值*Avg*:

$$Avg = sum / (n + 1) \quad (4)$$

源节点*S*对邻居数大于*Avg*的路由节点,除单独节点(上下跳节点邻居数均小于*Avg*)外,均成对放入集合*S(P_{SD})*,完成可疑节点的检测。

网络中含有虫洞影响节点的路径有3种情况:

- 1) 仅含有一个受影响的节点,如图1路径*P₁₄*;
- 2) 含有一对虫洞影响节点,但两节点在虫洞同一端,如图1路径*P_{af}*;
- 3) 含有一对虫洞影响节点,节点分布在虫洞不同端,如图1路径*P_{AE}*。

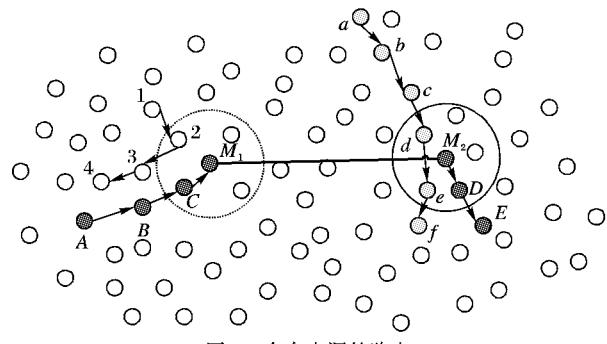


图1 含有虫洞的路由

图1中*B_{M1}*含有4节点,*B_{M2}*含有5个节点。路径*P_{AE}*为*A-B-C-D-E*,节点*C,D*受到虫洞节点*M₁,M₂*的影响,在邻居节点数上会高于节点*A,B,E*。路径*P₁₄*为*1-2-3-4*,节点*2*由于受到虫洞的影响,邻居数会高于其他路由节点。路径*P_{af}*为*a-b-c-d-e-f*,相比其他路由节点,*d,e*会有较多的邻居。采用平均值策略,可得到可疑节点集合*S(P_{AE})*为(*C,D*),*S(P₁₄)*为(2),*S(P_{af})*为(*d,e*)。观察图1可知,只有节点*C,D*间存在虫洞,节点*2,d,e*并没有包含虫洞。即除路径*P_{AE}*外,其他两个路径是可用的。因此,仅用路由节点邻居数量的多少来检测虫洞,存在很大的误差。不过可以利用这个特性,得到路径中受虫洞影响节点的集合,然后利用接下来的方法判定虫洞是否

存在。

1.3 可疑节点的判定

经过路由查询过程,得到路径 P_{SD} 。源节点通过可疑节点检测过程,得到可疑节点集合 $S(P_{SD})$ 。根据已有的 P_{SD} 和 $S(P_{SD})$,可疑节点判定过程如下:

1) 从 $S(P_{SD})$ 中,取出节点对假定为 $P_{SD}(i)$ 、 $P_{SD}(i+1)$ ($0 \leq i \leq n-2$)。

2) 源节点 S 向节点 $P_{SD}(i)$ 发出路由查询命令。

3) $P_{SD}(i)$ 根据邻居表计算距离得到节点 $Z(N(P_{SD}(i)))$,并向该节点发送 $N(P_{SD}(i))$ 、 $P_{SD}(i+2)$ 信息。节点 $Z(N(P_{SD}(i)))$ 查询到 $P_{SD}(i+2)$ 的路径,路径不包含节点 $N(P_{SD}(i))$ 和 $P_{SD}(i+1)$,并将路径跳数值 H 返回给 $P_{SD}(i)$ 。

4) $P_{SD}(i)$ 根据收到的跳数值 H ,将其与预定阈值相比较,若 H 大于等于预定值,则认为节点 $P_{SD}(i)$ 、 $P_{SD}(i+1)$ 间存在虫洞,执行步骤 6);反之,认为虫洞不存在,继续执行后续步骤。

5) 若 $S(P_{SD})$ 不为空,返回步骤 1);反之,结束判定过程。

6) 节点 $P_{SD}(i)$ 将查询所得路径来替代虫洞路径用于数据传输。

具体示例如图 2 所示。

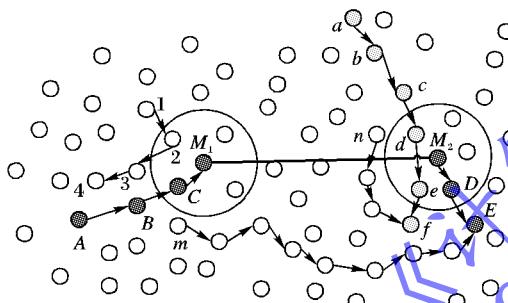


图 2 可疑节点判定示例

图 1 中得出结论,路径 P_{AE} 的可疑节点集合 $S(P_{AE})$ 为 (C, D) ,路径 P_{14} 的可疑节点集合 $S(P_{14})$ 为 (2) ,路径 P_{af} 的可疑节点集合 $S(P_{af})$ 为 (d, e) 。由于虫洞节点成对出现,排除路径 P_{14} 存在虫洞的可能性。文中取预定阈值为 3。以路径 P_{AE} 为例,判定过程如下:

1) 从 $S(P_{AE})$ 中取出节点 C, D ;
2) 节点 C 计算得到最近邻居节点 m ;
3) 节点 m 查询到节点 E 的路径 P_{mE} ,得到路径跳数为 8;
4) 节点 C 接收到跳数值 8,判定 $8 > 3$,节点 C, D 间存在虫洞;

5) 节点 C 将路径 P_{mE} 作为新的数据传输路径;
6) 集合 $S(P_{AE})$ 为空,判定结束。

若跳数为 n 的路径 P_{SD} ,其可疑节点对为 $P_{SD}(n-1)$ 、 $P_{SD}(n)$;那么,由节点 $P_{SD}(n)$ 查找 $Z(P_{SD}(n))$,查询到 $P_{SD}(n-2)$ 的路径。

2 仿真结果及分析

2.1 仿真环境与参数选取

本文使用 Java 语言和 Matlab 工具进行算法的模拟,整个网络模拟场景大小为 $1200 \text{ m} \times 1200 \text{ m}$,节点规模分为 144,

190,240,288 个,节点的通信半径为 180 m。节点随机分布在部署区域,移动速度为 8 m/s,运动方向随机。网络中存在一对虫洞节点,虫洞链路为 400 m,虫洞节点通信半径与普通节点一致。路径的源节点、目的节点随机选取。

本文提出的虫洞检测方法涉及到可疑节点选取策略。可疑节点选取应保证如果路径存在虫洞,则受虫洞影响的节点对一定包含在可疑节点集合中。可疑节点的检测有两种:一种是与路径平均邻居数相比;一种是与路径最小的邻居数相比。仿真环境下,根据得到的含有虫洞的路径,这两种策略的表现如表 2 所示,其中命中率表示仿真所得可疑节点集合中包含虫洞节点的集合所占的比例。

表 2 不同可疑节点选取策略的表现

策略	命中率/%	可疑节点集合平均大小
平均邻居数	99.86	2.26
最小邻居数	100.00	4.11

从表 2 可知:平均邻居数策略可以降低能量消耗;最小邻居数策略可以有效得到可疑节点集合。可以根据不同的侧重点,选择相应的策略。本文仿真使用的是平均邻居数策略。

较高的路由跳数预定阈值会降低虫洞的检测率;较低的阈值会带来较高的错判率。阈值的选取需要根据需求的不同来选取。仿真环境下,不同阈值下的检测率和错判率如表 3 所示。

表 3 不同阈值下的虫洞检测率和错判率

阈值	虫洞检测率/%	错判率/%
2	100.00	4.54
3	99.79	1.14
4	98.99	0.51

2.2 仿真结果

将本文所提出的虫洞检测方法 DWNR 与 DeWorm、E2SIW 方法在不同规模的网络下得到的仿真结果如图 3~6 所示。

图 3 中给出了不同网络规模下,一次虫洞检测花费的代价。从图 3 中可以看出,DeWorm 方法随着网络规模的增大需要路由查询的次数也就越多,即消耗的网络能量也就更多。E2SIW 和 DWNR 方法路由查询次数一直处于较低的状态,即消耗的能量较小。

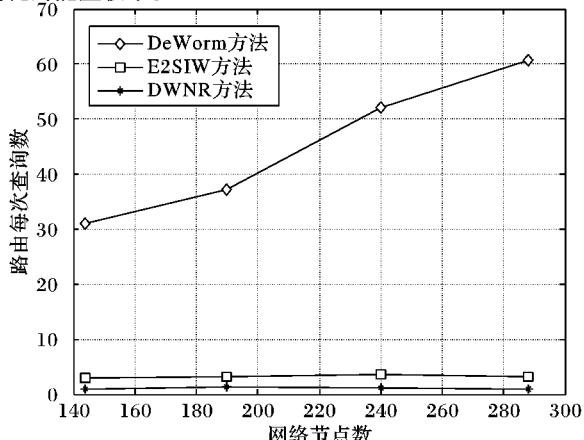


图 3 一次虫洞检测中平均路由查询数

图4中随着网络节点数的增加,DeWorm方法虫洞检测时延逐渐增大,E2SIW方法带来的检测时延增加相对比较平缓,DWNR方法的检测时延略有增加。从图4中可以看出,DWNR方法在虫洞检测时延上优于DeWorm、E2SIW方法。

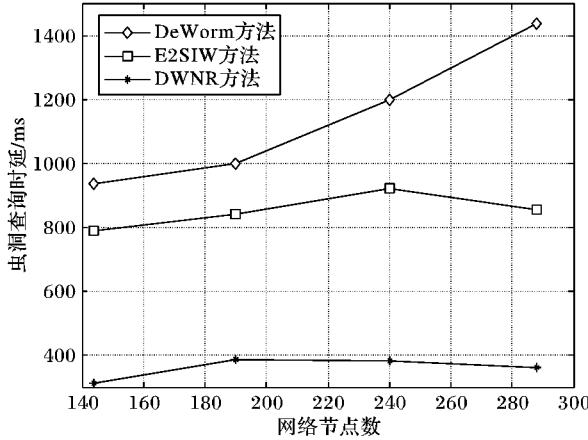


图4 3种方法的虫洞检测平均时延对比

从图5~6中可以看出,随着节点的增多,3种方法的虫洞检测成功率也随着提升,错判率随之下降。与DeWorm、E2SIW方法相比,DWNR有着较低的错判率,在检测率上有所降低,但并没有较大的差别。

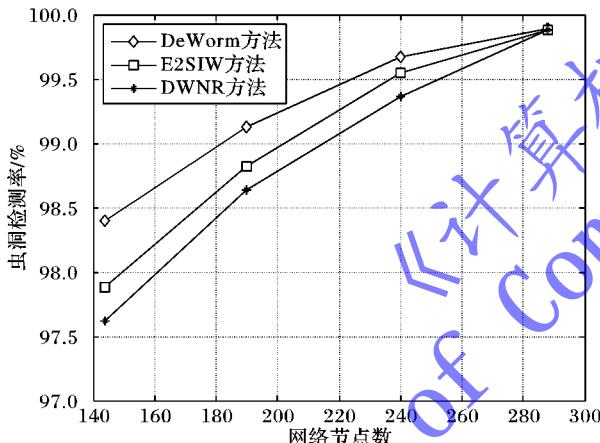


图5 3种方法的虫洞检测成功率对比

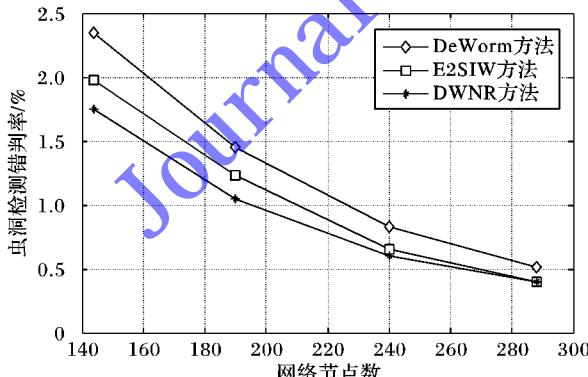


图6 3种方法的虫洞检测错判率对比

2.3 性能分析

假设源节点S到目的节点D的路径为 P_{SD} ,跳数为H。虫洞影响节点为 $P_{SD}(n)$ 和 $P_{SD}(n-1)$ ($1 \leq n \leq H$)。DeWorm方法在检测中需要路由节点所有邻居的路由,查询次数Num为:

$$Num = C(P_{SD}(0)) + C(P_{SD}(1)) + \dots + C(P_{SD}(n-1))$$

E2SIW方法仅需距离路由节点最近的邻居节点的查询路由,因此要n次的路由查询,DWNR方法根据式(4)得到Avg,且满足以下条件:

$$\min \{C(P_{SD}(0)), C(P_{SD}(1)), \dots, C(P_{SD}(n))\} \leq Avg \leq \max \{C(P_{SD}(0)), C(P_{SD}(1)), \dots, C(P_{SD}(n))\}$$

当 $C(P_{SD}(0)) = C(P_{SD}(1)) = \dots = C(P_{SD}(n))$ 时,等号成立。通过可疑节点判定策略得到的集合 $S(P_{SD})$ 最多包含n-1个节点,最少为0个节点。DWNR方法最多需要n-1次路由查询。对于节点均匀的网络,DWNR方法需要的路由查询次数接近于1,在节点随机分布的情况下,路由查询次数约为n/3。相比DeWorm和E2SIW方法,DWNR路由查询次数更少,能量和时间消耗更低。

3 结语

虫洞的存在会改变网络部分节点的邻居节点数,本文根据此特性提出了一种能耗和时延较低的虫洞检测方法——DWNR方法。该方法依靠邻居节点的路由查询来检测虫洞的存在,方法除了GPS以外不依赖特殊硬件。相比DeWorm、E2SIW方法,该方法的优点在于统计路由节点的邻居数,筛选出待检测路由节点,进而减少虫洞检测次数;与其他方法^[8-12]对比,该方法不需占用额外的节点内存,实时性强,且有较小的能量开销和较低的时间延迟。最后仿真和理论分析证明,在不同网络规模的情况下,该方法可以有效降低网络能量消耗和虫洞检测带来的时间延迟,同时具有较高的虫洞检测率。

参考文献:

- [1] YANG H, LUO H, YE F, et al. Security in mobile Ad Hoc networks: challenges and solutions [J]. IEEE Wireless Communications, 2004, 11(1): 38–47.
- [2] CHUN H Y, PERRIG A, JOHNSON D B. Wormhole attacks in wireless networks [J]. IEEE Journal on Selected Areas in Communications, 2006, 24(2): 370–380.
- [3] HU Y-C, PERRIG A, JOHNSON D B. Packet leashes: a defense against wormhole attacks in wireless Ad Hoc network [C]// Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. Washington, DC: IEEE Computer Society, 2003: 1976–1986.
- [4] FU Y, ZHANG X, ZHANG T, et al. Research on wormhole attack detection in wireless mesh networks [J]. Journal on Communications, 2011, 32(1): 59–65. (付颖芳, 张兴, 张婷, 等. 无线Mesh网络中的虫洞攻击检测研究[J]. 通信学报, 2011, 32(1): 59–65.)
- [5] CHOI S, KIM D Y, LEE D H, et al. WAP: wormhole attack prevention algorithm in mobile Ad Hoc networks [C]// Proceedings of the 2008 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing. Washington, DC: IEEE Computer Society, 2008: 343–348.
- [6] WANG X, WONG J. An end-to-end detection of wormhole attack in wireless Ad Hoc networks [C]// Proceedings of the 31st Annual International Computer Software and Applications Conference. Washington, DC: IEEE Computer Society, 2007: 39–48.

(下转第723页)

5 结语

本文将隐写通信系统中的隐写方和主动攻击方作为博弈双方,在对博弈双方进行失真约束基础上,以信息嵌入率和错误率两个目标作为收益函数,建立了主动攻击下的隐写系统博弈模型。借助二人有限零和博弈基本理论,本文分析了博弈均衡的存在性,并给出了均衡局势下隐写方和攻击方的最优混合策略求解方法。最后给出一个简单实例对文中的博弈模型进行了说明和验证。本文提出的模型不仅可为隐写方选择最优隐写算法和容错方法提供决策依据,也可指导隐写算法设计者选择最优容错方法。需要注意的是,给定策略集时,安全性限制和隐秘载体失真限制的取值直接决定了信息嵌入率和错误率。为了获得满意的信息嵌入率和错误率,如何设定安全性限制和隐秘载体失真限制将是下一步研究的重点。

参考文献:

- [1] LIU C, LI Z, WANG Z. A game-theoretic model to covert communication systems [J]. Journal on Communications, 2004, 25(5): 160–165. (刘春庆, 李忠新, 王执铨. 隐秘通信系统的对策论模型 [J]. 通信学报, 2004, 25(5): 160–165.)
- [2] LIU G, DAI Y, ZHAO Y, et al. Modeling steganographic counter-work by game theory [J]. Journal of Nanjing University of Science and Technology: Natural Science, 2008, 32(2): 199–204. (刘光杰, 戴跃伟, 赵玉鑫, 等. 隐写对抗的博弈论建模 [J]. 南京理工大学学报: 自然科学版, 2008, 32(2): 199–204.)
- [3] JIANG C, PANG Y, LIN J. The steganography capacity game analysis based on the digital images [J]. Microelectronics and Computer, 2010, 27(1): 22–24. (蒋翠玲, 庞毅林, 林家骏. 数字图像隐写容
- 量的博弈分析 [J]. 微电子学与计算机, 2010, 27(1): 22–24.)
- [4] SCHÖTTLER P, BÖHME R. A game-theoretic approach to content-adaptive steganography [C]// Proceedings of the 14th International Conference on Information Hiding. Berlin: Springer, 2012: 125–141.
- [5] JOHNSON B, SCHÖTTLER P, BÖHME R. Where to hide the bits? [C]// Proceedings of the Third International Conference Decision and Game Theory for Security. Berlin: Springer, 2012: 1–17.
- [6] ETTINGER J. Steganalysis and game equilibria [C]// Proceedings of the Second International Workshop on Information Hiding, LNCS 1525. Berlin: Springer, 1998: 319–328.
- [7] LIU D, HUANG Z. Game theory and its application [M]. Changsha: National University of Defence Technology Press, 1996: 23–60. (刘德铭, 黄振高. 对策论及其应用 [M]. 长沙: 国防科技大学出版社, 1996: 23–60.)
- [8] COX I J, MILLER M L, BLOOM J A, et al. Digital watermarking and steganography [M]. Waltham, MA: Morgan Kaufmann Publishers, 2008: 117–123.
- [9] MELIKAINEN J. LSB matching revisited [J]. IEEE Signal Processing Letters, 2006, 13(5): 285–287.
- [10] CRANDALL R. Some notes on steganography [EB/OL]. [2013-07-12]. <http://os.inf.tu-dresden.de/~westfeld/-Crandall.pdf>.
- [11] CACHIN C. An information-theoretic model for steganography [C]// Proceedings of the Second International Workshop on Information Hiding, LNCS 1525. Berlin: Springer, 1998: 306–318.
- [12] TANG G Y. Suboptimal control for nonlinear systems: a successive approximation approach [J]. System and Control Letters, 2005, 54(5): 429–434.

(上接第 713 页)

- [7] GUO J, LEI Z Y. A kind of wormhole attack defense strategy of WSN based on neighbor nodes verification [C]// Proceedings of the IEEE 3rd International Conference on Communication Software and Networks. Washington, DC: IEEE Computer Society, 2011: 564–568.
- [8] AZER M A, KASSAS M E, SOUDANI S E. An innovative approach for the wormhole attack detection and prevention in wireless Ad Hoc networks [C]// Proceedings of the 2010 International Conference on Networking, Networking, Sensing and Control. Washington, DC: IEEE Computer Society, 2010: 366–371.
- [9] SHARMA P, TRIVEDI A. An approach to defend against wormhole attack in Ad Hoc network using digital signature [C]// Proceedings of the IEEE 3rd International Conference on Communication Software and Networks. Washington, DC: IEEE Computer Society, 2011: 307–311.
- [10] BAN X, SARKAR R, CAO J. Local connectivity tests to identify wormholes in wireless networks [C]// Proceedings of the Twelfth ACM International Symposium on Mobile Ad Hoc Networking and Computing. New York: ACM Press, 2011: 1–11.
- [11] DONG D, LI M, LIU Y, et al. Topological detection on wormholes in wireless Ad Hoc and sensor networks [J]. IEEE/ACM Transactions on Networking, 2011, 19(6): 1787–1796.
- [12] AZER M A. Wormhole attacks mitigation in Ad Hoc networks [C]// Proceedings of the Sixth International Conference on Availability, Reliability and Security. Washington, DC: IEEE Computer Society, 2011: 561–568.
- [13] HAYAJNEH T, KRISHNAMURTHY P, TIPPER D. Deworm: a simple protocol to detect wormhole attacks in wireless Ad Hoc networks [C]// Proceedings of the Third International Conference on Network and System Security. Washington, DC: IEEE Computer Society, 2009: 73–80.
- [14] DHURANDHER S K, WOUNGANG I, GUPTA A, et al. E2SIW: an energy efficient scheme immune to wormhole attacks in wireless Ad Hoc networks [C]// Proceedings of the 26th International Conference on Advanced Information Networking and Applications Workshops. Washington, DC: IEEE Computer Society, 2012: 472–477.
- [15] KEER S, SURYAVANSHI A. To prevent wormhole attacks using wireless protocol in MANET [C]// Proceedings of the 2010 International Conference on Computer and Communication Technology. Washington, DC: IEEE Computer Society, 2010: 159–163.