技术交底书-软件通讯类

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 客户名称 |  | | | |
| 发明名称 | 一种基于静态博弈的抗网络拓扑探测的节点防御资源部署策略方法 | | | |
| 技术联系人 |  | 邮箱 |  | |
| 手机 |  | | 专利类型 | 发明  实用新型 |
| 固定电话 |  | |

填写交底书注意事项：

1﹒第一、二、三项为必填项。尤其是**发明内容**的技术方案，一定要写得全面、清楚、完整。

2﹒全文对同一事物的叫法应统一，避免出现一种事物多种名称。

3、请随本交底书一起附带CAD源文件，方便代理人更改，减少申请文件撰写时间。

**一、背景技术/现有技术问题（必填）**

**描述与本发明技术方案最相近的现有技术方案，并指出现有技术方案中存在的缺点。**

**因为本发明不是生来就有的，一般都是针对现有技术的缺陷，做了改动或者彻底改变以前的方案而重新设计，现有的产品什么样的，现有的缺陷写出即可。**

本发明属于网络空间安全技术领域，具体涉及一种对抗网络拓扑探测的选取节点保护的的方法，用以在网络拓扑中选取节点进行保护。

在日益复杂和多样化的网络环境中，对网络空间进行全面、深入的了解变得至关重要。网络空间测绘作为一种系统性、全面性的调查和分析手段，旨在获取有关网络空间地理位置、地貌、资源分布、网络拓扑结构、信息流动规律等方面的数据和信息。然而非法的网络空间测绘活动，尤其是由黑客或恶意组织进行的，可能造成严重的后果，包括安全漏洞的暴露、个人隐私和企业敏感数据的泄露、网络资源的滥用、经济损失，以及对国家安全构成的威胁。其中，网络拓扑是极为重要的网络资源。根据目标网络的拓扑结构，分布式拒绝服务(DDoS)攻击，链接泛洪攻击(LFA)可以通过控制多个端点向网络中注入大量低速率的合法流量，仅破坏少量的关键节点或关键链接，即可对目标网络的连通性产生严重影响。研究表明攻击者需要了解目标网络的拓扑结构和转发行为来执行LFA。如果没有这些信息，攻击者只能“猜测”哪些流共享一个公共链接，这大大降低了攻击的效率。模拟实验表明，在不知道拓扑的情况下堵塞任意链接需要多出5倍的流量，而堵塞特定链接的难度则要大上至少一个数量级。

网络拓扑推断技术主要分为两大类：基于Traceroute的推断和网络断层扫描（Tomography-based）技术。前者通过使用路由跟踪工具，依靠IP头部的TTL字段的递减以及中间路由器发出的ICMP超时报文，来识别源至目标路径上的IP层级节点及其连接。这种方法的优点在于其简便性；在网络管理员未禁用ICMP数据包的情况下，能够轻松映射出目标网络的拓扑结构。相反，网络断层扫描技术基于端到端的测量数据，如丢包率和时延等参数，推测网络的结构。此技术的关键优势在于，数据传输发起点和接收点位于目标网络之外，而数据流则穿过该网络。尽管此方法相较于基于Traceroute的技术更为复杂，但它并不依赖于网络内部节点的协作。

当前对抗拓扑探测的方法中，基于内部节点的网络拓扑探测的一种基础对策是禁止内部节点响应traceroute或ping请求，此举虽能阻断部分探测尝试，但同时也限制了基于这些协议的正常网络功能。另一方面，一些研究通过采用混淆和欺骗技术来阻止网络扫描工具获得准确的网络拓扑信息，如通过生成错误的响应和服务信息来误导攻击者。这些方法通常专注于对抗特定的拓扑探测技术，并未充分考虑防御资源（如蜜罐、防火墙等）的有效配置即应该在拓扑中的哪些节点部署防御资源，忽视了现实中防御者可用防御资源的有限性。此外，在现实网络中，一旦某些节点被探测到，就可能增加其他节点被探测的风险，且不同网络性能下其他节点被探测概率也会有所不同。

**二、发明内容（必填）**

**对本发明技术方案的详细阐述，最好结合附图进行说明，使用状态下的情况。（最核心的部分，务必详细）。**

2﹒对于方法发明，可以是制造方法，测试方法，处理方法，通讯方法及将产品用于特定用途的方法。（对于方法发明，一般需要写明发明的步骤，即第一步要做什么，第二步、第三步要做什么，以及每一步用到的东西和实现的效果）

基于节点中心性的抗拓扑探测节点选取方法，包括：

步骤1、建立网络攻击方和防御方的完全信息静态博弈模型，参与者对其他参与者的策略空间和收益函数完全了解。在该博弈模型中博弈的参与者为探测网络拓扑的攻击方和对抗网络拓扑探测的防御方，基于上述现有的拓扑探测方法构建攻击者的策略空间。基于节点的介数中心性构建防御者的策略空间。基于社交网络中的影响力传播模型构建被探测节点的影响力传播模型。最后构建该博弈模型的收益函数，通过收益函数计算纳什均衡得到最优的节点选取方法。

步骤2.攻击者策略空间由两个策略组成，分别是基于内部节点的拓扑探测策略和端到端探测策略。

步骤2.1、给定一个网络拓扑图G，基于内部节点的拓扑探测策略步骤如下：1、计算拓扑图G所有节点的介数中心性，随机选取一个介数中心性为0的节点作为初始探测节点。2、基于图的广度优先算法沿着初始节点继续探测，直到攻击资源消耗完毕。攻击单个节点需要消耗的资源表达式为：

式中表示攻击者探测的单个节点，表示节点的度中心性

步骤2.2、给定一个网络拓扑图G，基于内部节点的拓扑探测策略步骤如下：1、计算拓扑图G所有节点的介数中心性，随机选取两个个介数中心性为0的节点作为初始探测节点。2、探测连通初始节点的路径，若所需资源大于可用攻击资源则重复步骤1直到攻击资源消耗完毕。

步骤3、防御者的策略空间同样由两个策略组成，分别是基于节点中心性的定向保护策略和随机节点保护策略。

步骤3.1、给定一个网络拓扑图G，于节点中心性的定向保护策略步骤如下：1.计算拓扑图G所有节点的介数中心性。2.根据介数中心性从大到小选取节点进行保护（部署防御资源）。保护单个节点需要消耗的资源表达式为：

式中表示防御者部署防御资源的单个节点，表示节点的度中心性，表示节点的介数中心性。

步骤3.2、给定一个网络拓扑图G，随机节点保护策略随机选取图中的进行保护，直到防御资源消耗完毕。

步骤4.1、基于模拟得到了双方的策略之后，首先被探测到的节点向未被探测到的节点传播影响力，影响力传播计算公式为：

；



式中表示被探测到的节点向未被探测到的节点传播的影响力大小，表示邻居对自身产生的影响。

此时未被探测到的节点更新其被探测到的概率，更新规则为：

；

；

式中表示节点的被探测邻居节点影响力的总和，表示未被探测到的节点探测到的概率，表示节点的度中心性，是预设参数。

步骤4.2、未被探测到的节点之间进行影响力传播，影响力传播计算公式为：

；

；

式中表示未被探测的节点向其未被探测的邻居节点传播的影响力大小，表示节点的未被探测邻居节点影响力的总和，表示节点的度中心性，是预设参数。

此时未被探测到的节点更新其被探测到的概率，更新规则为：

；

式中表示节点的邻居节点（包括被探测的和未被探测的）影响力的总和，表示节点的度中心性，是预设参数。

步骤4.3、迭代步骤4.1和步骤4.2后可得到未被探测的节点被探测的稳定概率大小（理论：马尔科夫决策的收敛性）

步骤5、构建该博弈模型的收益计算方法，首先统计被探测成功的节点的损失值，之后计算节点潜在被探测的概率。

步骤5.1、攻击者的收益计算表达式为：

；

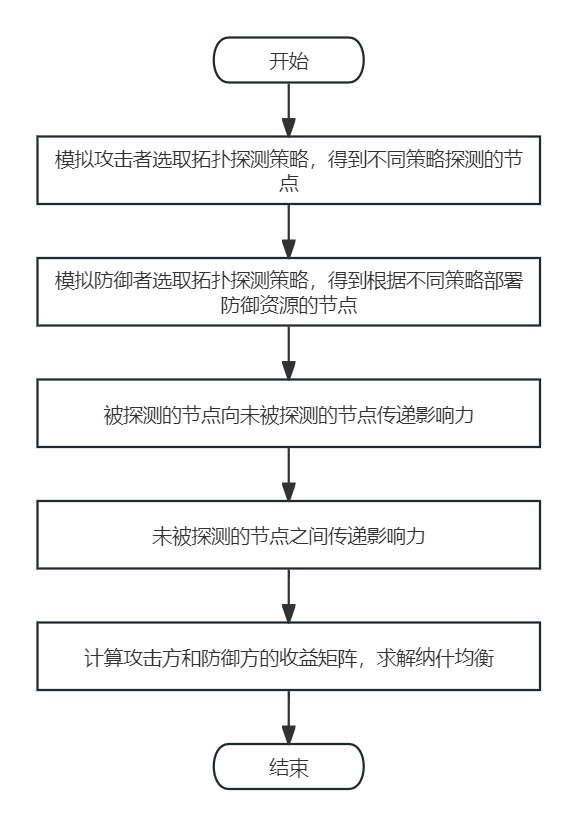
式中表示攻击者的收益，分别表示攻击者和防御者的策略，表示网络拓扑的性能（性能越好被探测节点影响力传播能力越小），攻击者的收益是双方策略的函数，表示攻击者探测成功的节点集合，表示未被攻击者探测成功且防御者没有部署防御资源的节点集合。

步骤5.2、防御者的收益计算表达式为：

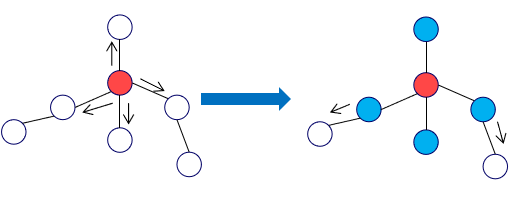
；

式中表示防御者的收益，分别表示攻击者和防御者的策略，表示网络拓扑的性能（性能越好被探测节点影响力传播能力越小），防御者的收益是双方策略的函数，表示攻击者探测成功的节点集合，表示未被攻击者探测成功且防御者没有部署防御资源的节点集合。

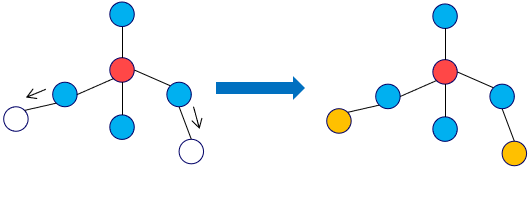
步骤6、根据步骤5.1和步骤5.2计算双方收益矩阵，之后根据收益矩阵求解纳什均衡后得到最优的节点防御资源部署方法。



图一 摘要流程



图二 步骤4.1影响力传播第一过程



图三 步骤4.2影响力传播第二过程

**三、本发明的优点（必填）**

**与第一部分的现有技术方案相比，本发明技术方案有何优点或有益效果，所述优点或有益效果是由本发明技术方案带来的。**

本方法注重考虑了现实中防御者可用防御资源的有限性，且考虑了在不同的网络拓扑性能下某些被探测到的节点对其他未被探测的节点影响后，防御者使用本方法可以使其损失降到最低。

**四、替代方案（选填）**

**对第二部分中的本发明技术方案，是否还有其他的替代方案同样能完成本发明的目的。**

本发明所解决的问题，采用了一个手段，针对这个手段，是否还有其他的方法能够等同于这个手段？

若有，则提出并写出来。

若无，则不用填写此栏。

**五、本发明的关键点和保护点（选填）**

**请列出对本发明创造最想保护的技术点。**

1. **在对抗网络探测情境下构建的攻防博弈模型**
2. **被探测节点影响力传播模型**

**六、附图（选填）**

1﹒**实用新型专利申请必须有至少一个附图**。**在机械、电学、物理领域中涉及产品结构的发明专利申请，也必须有附图。**

**附图的基本要求**

1﹒必须是黑色的线条图，最好是CAD图纸（或者CAD软件能够）打开的图档或Visio格式的图，图中的线条不能有锯齿，图上要有标记，并写明各标记所代表的部件；CAD软件为AutoCAD、Solidworks软件。

2﹒附图中必须详细体现本发明的发明点所涉及的各部件的组成及连接关系、以及其与现有技术中所涉及部件的连接关系。