(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 116743482 A
(43)申请公布日 2023.09.12

(21)申请号 202310838283.6

(22)申请日 2023.07.10

(71)申请人 哈尔滨工业大学
地址 150001 黑龙江省哈尔滨市南岗区西大直街92号

(72)发明人 张宇 王斌 史建焘 朱国普 张伟哲

(74)专利代理机构 黑龙江立超同创知识产权代理有限责任公司 23217
专利代理师 杨立超 张妍飞

(51)Int.Cl.
H04L 9/40(2022.01)

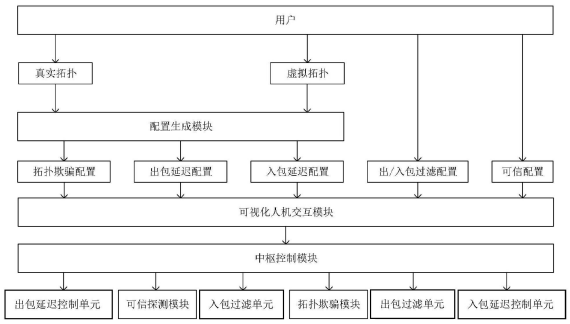
权利要求书2页 说明书13页 附图2页

(54)发明名称

一种抗网络拓扑探测防火墙

(57)摘要

本发明公开了一种抗网络拓扑探测防火墙，涉及抗网络拓扑测量技术领域，用以抵抗攻击者获取目标网络内的拓扑结构。本发明所述防火墙包括包过滤模块、包延迟控制模块、拓扑欺骗模块、可信探测认证模块、配置生成模块、中枢控制模块、可视化人机交互模块；其中包过滤模块使用位图加速技术，快速过滤数据包；包延迟控制模块负责控制数据包的延迟；拓扑欺骗模块负责识别探测包，并生成响应的伪造应答包，欺骗攻击者；可信探测认证模块负责认证可信的探测者；配置生成模块负责根据真实拓扑和虚拟拓扑生成包延迟控制模块和拓扑欺骗模块所需配置。本发明可有效抵抗攻击者获取目标网络内的拓扑结构，并向攻击者展示虚拟拓扑，同时保证延迟一致性。



CN 116743482 A

1.一种抗网络拓扑探测防火墙,其特征在于,包括包过滤模块、包延迟控制模块、拓扑欺骗模块、可信探测认证模块、配置生成模块、中枢控制模块、可视化人机交互模块;其中:

包过滤模块用于快速过滤数据包;

包延迟控制模块用于控制数据包的延迟;

拓扑欺骗模块用于识别探测包,并生成响应的伪造应答包;

可信探测认证模块用于认证可信的探测者,保留系统网络调试功能;

配置生成模块用于根据真实拓扑和虚拟拓扑生成包延迟控制模块和拓扑欺骗模块所需配置;

中枢控制模块用于接收用户命令,并将命令统一下发给各个模块;

可视化人机交互模块用于向用户展示数据,并向中枢控制模块下发用户命令。

2.根据权利要求1所述的一种抗网络拓扑探测防火墙,其特征在于,所述包过滤模块使用基于位图加速的规则匹配算法,快速过滤数据包;所述包过滤模块分包括入包过滤单元和出包过滤单元,入包过滤单元用于过滤进入内网的数据包,出包过滤单元用于过滤发出外网的数据包。

3.根据权利要求2所述的一种抗网络拓扑探测防火墙,其特征在于,所述包过滤模块中所述基于位图加速的规则匹配算法使用键值对的形式存储规则,使用index作为键的一部分以扩展规则数量,拥有Accept、Drop、SrcIP、DstIP、SrcPort、DstPort、TypeWithCode、Protocol8个Map;为了支持子网匹配,在收到数据包后,将源IP和目的IP分别依次使用32、24、16、8、0进行掩码操作,掩码得到的结果作为键的一部分和index一起查询得到5个值,将得到的5个值做或操作,作为源IP项和目的IP项的最终结果;为了支持端口的通配,在查询源端口时,使用源端口和通配源端口分别与index一起查询得到2个值,将结果做或操作得到最终源端口的值;目的端口同理;其余字段只需要配合index查询各自Map即可;将除了Accept和Drop项的查询结果做与操作后,分别与Accept和Drop项进行与操作;如果与Accept项与操作的结果大于与Drop项与操作的结果,则为接收操作;如果小于则丢弃操作;如果等于代表匹配失败,递增index。

4.根据权利要求1所述的一种抗网络拓扑探测防火墙,其特征在于,所述包延迟控制模块通过划分多个数据包队列,其中不同队列对数据包增加的延迟不同,将数据包分发到不同队列中,以获得不同等级的延迟数据包;所述包延迟控制模块包括入包延迟控制单元和出包延迟控制单元,入包延迟控制单元用于给进入的数据包添加延迟,出包延迟控制单元用于给外出的数据包和伪造的ICMP应答报文添加延迟。

5.根据权利要求1所述的一种抗网络拓扑探测防火墙,其特征在于,所述拓扑欺骗模块包括探测包识别单元和应答包生成单元;所述探测包识别单元用于根据数据包的TTL字段和目的IP判断数据包是否为探测包:若目的IP为虚构IP或真实IP,且TTL字段显示数据包不能到达目标,则判定为探测包;应答包生成单元用于判断数据包是否可以触发ICMP差错报文,若不能触发则直接丢弃不应答;否则根据探测包生成ICMP超时报文或ICMP端口不可达报文。

6.根据权利要求1所述的一种抗网络拓扑探测防火墙,其特征在于,所述可信探测模块使用IP的方式认证可信的探测者;根据数据包的不同方向,使用数据包的源IP或目的IP判断数据包是否从可信探测源发出或发往可信探测源。

7.根据权利要求1所述的一种抗网络拓扑探测防火墙,其特征在于,所述配置生成模块使用迪杰斯特拉算法计算防火墙节点到各个主机节点的最短路径,以及路由器节点和主机节点到防火墙的最短路径,生成伪造ICMP应答包所需信息。

8.根据权利要求1所述的一种抗网络拓扑探测防火墙,其特征在于,所述配置生成模块生成的配置包括拓扑欺骗配置、入包延迟控制配置、出包延迟控制配置。

9.根据权利要求1所述的一种抗网络拓扑探测防火墙,其特征在于,所述中枢控制模块与各模块之间通过证书认证身份,并通过数字信封封装消息。

10.根据权利要求1所述的一种抗网络拓扑探测防火墙,其特征在于,所述可视化人机交互模块还用于提供拓扑预览功能。

一种抗网络拓扑探测防火墙

技术领域

[0001] 本发明涉及抗网络拓扑测量技术领域,具体涉及一种抗网络拓扑探测防火墙。

背景技术

[0002] 2022年上半年,中国电信、中国移动和中国联通总计监测发现分布式拒绝服务(英文简称DDoS)攻击316,542起,工业和信息化部网络安全威胁和漏洞信息共享平台总计接报网络安全事件7,415,654件[1],看似平静无波的互联网实则暗潮涌动。Internet是一个开放的、无结构的网络,任何人都可以轻易的接入网络,使得网络空间安全态势错综复杂。

[0003] 大量研究表明,网络攻击前会进行网络侦查。研究统计70%的攻击活动前都进行了网络侦察[2],在一次网络攻击中平均45%的时间花费在了在网络侦查[3]。在侦察阶段,攻击者可以获取目标网络的特征和漏洞,如IP地址空间、网络拓扑和易受攻击的服务器等。

[0004] 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。Meier等人的研究表明[4]: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。

[0005] 为了应对网络侦察,有学者提出了多种不同的主动防御解决方案,包括移动目标防御[5]、拟态防御[6]、欺骗防御[7]等。其中欺骗防御利用攻击者依赖收集到信息制定攻击计划的特点,通过给攻击者提供错误信息,降低目标受到攻击的影响。从博弈论的角度也可证明在侦察阶段对攻击者实施欺骗比发现侦察后阻断侦察的收益更高[8]。

[0006] 链路泛洪攻击中比较成熟的攻击理论主要有Coremelt[9]攻击和Crossfire[10]攻击。Coremelt通过控制大量机器人节点相互发送流量,淹没关键链路,从而降低目标网络与外部网络的连通性,证明了攻击的可行性;进一步,Crossfire通过控制大量机器人节点,向目标网络附近的公共服务器发送大量低速率合法流量,攻击行为更加隐蔽,攻击流与典型的“流量风暴”(Flash crowds)的流量模式难以区分。Crossfire攻击的详细攻击流程如下:(1)构建链路图,分析持久链路。攻击者控制机器人运行traceroute获取通往目标区域附近的公共服务器和诱饵服务器的路由器级拓扑。探测结果为路由器接口IP地址的序列,链路由两个相邻的接口IP标识。网络中可能存在负载均衡设施,对这些负载均衡链路实施泛洪攻击会增加攻击的复杂性。通过多次traceroute探测,就可以在很大概率上排除这些“暂时性”的链路(在6次探测中都存在的链路,其为暂时性链路的概率仅为(1/2)^6,得到持久链路,用作攻击链路候选集。(2)计算流量密度,选择目标链路。一个持久链路的流量密度被定义为机器人与公共服务器或诱饵服务器之间可以通过该链路创建的流的数量。流量密度在链路图遵循幂律分布,这使得攻击者能够轻易地发现一组高流密度的链路。通过贪婪算法,选择对目标区域影响最大的多组不相交目标链路集。(3)分配攻击流量,淹没目标链路。在

保证攻击流量不可辨别性的同时将目标链路所需的总攻击流量相对平均地分配给多个机器人,使得目标链路的总流量略高于链路带宽。攻击者指挥机器人生成攻击流,慢慢增加攻击流的发送速率,直到指定速率。除此之外,机器人可以根据目标链路的状态动态地调整其流量强度。如果目标链路的实际带宽小于分配的攻击带宽,一旦目标链路被淹没,机器人会停止增加攻击流量的发送速率。(4)滚动式攻击。对同一组目标链路进行连续的淹没可能会激活路由器的故障检测机制,导致网络路由的改变。攻击者通过动态改变目标链路集,进一步延长攻击时间,并提高攻击不可检测性。

[0007] 现有的防御措施很难抵御链路泛洪攻击攻击。在链路泛洪攻击中,僵尸网络中的机器人都拥有合法的IP地址,很难将其与合法用户区分;攻击流没有直接发往目标网络,目标网络的入侵检测系统也鞭长莫及;敌手的攻击成本很低,其产生攻击流量的带宽成本比骨干链路带宽成本低几个数量级[11]。

[0008] 一般来说,网络拓扑推断主要有两种方式:基于traceroute的网络拓扑推断技术和网络断层扫描技术(tomography-based topology inference)。基于traceroute的网络拓扑推断技术利用路由跟踪工具探测目标网络,该工具利用IP头部的TTL字段,通过递减TTL并触发中间路由器的ICMP超时报文,来发现从源到目标的路径上的IP级节点和链路。这种方法比较简单,在有内部节点的配合的情况下(网络管理员没有禁用ICMP数据包),很容易获取目标网络拓扑。网络断层扫描技术主要利用端到端的测量信息,如丢包率[12]、时延[13]等指标,来推断目标网络的拓扑结构。这种技术的特点在于,发送端和接受端位于目标网络的外部,而流量穿过目标网络。相较于基于Traceroute的网络拓扑推断,这种方法虽然比较复杂,但不需要内部节点的配合。

[0009] 实现抗网络拓扑探测,需要解决两个关键问题,分别是在如何设计虚拟拓扑,以及如何欺骗敌手,使其探测并相信虚拟拓扑。在设计虚拟拓扑方面,主要有两种观点:一种是生成随机拓扑,另一种是根据真实拓扑生成虚拟拓扑。第一种观点比较容易实现,由于其与真实拓扑完全独立,敌手根据随机拓扑发起的攻击很难对真实拓扑同样有效。第二种观点认为:完全随机的虚拟拓扑会被攻击者识别,攻击者进而采取其他的网络侦察手段或直接发动攻击。因此,需要在生成虚拟拓扑的同时,保证虚拟拓扑与真实拓扑相似,同时保护真实拓扑中的关键节点或链路。为了实现这一目标可分为两步。第一步是判定瓶颈节点或链接,判定的指标可以分为静态指标和动态指标[14]。静态指标有:介数中心性(Betweenness Centrality)、亲密度中心性(Closeness Centrality)、最小切中心性(Mincut Centrality)、度中心性(Degree Centrality)等。动态指标有:链路负载、链路可用带宽、链路延迟等。根据上面的指标可以制定出一套计算瓶颈链接或节点的方法。第二步是如何设计能够保护真实拓扑的虚拟拓扑。这一步往往使用第一步的指标,将问题转换成优化问题进行求解。

[0010] 在欺骗方面,可以按照防御位置分成两大类,一种是网络边界防御,一种是网络内部防御。网络边界防御比较有代表性的有Trassare等人提出的智能路由器[15]、ProTO[16]、AntiTomo[17]。Trassare等人在边界基于Linux构建了一个智能路由器。其关键思想是利用介数中心性确定网络中的关键节点,并通过增加虚拟链接使关键节点的中心性最小化,然后智能路由器根据虚拟拓扑在边界响应traceroute,以欺骗恶意的检测,影响攻击者推断网络拓扑结构。文章没有考虑数据包延迟方面的信息,这种不一致性容易被攻击者察觉。

ProTO首先针对基于延迟进行网络断层扫描的攻击者进行建模，利用机器学习算法构建一个高可靠率、低误报率的分类模型，用来判定探测包，在边界处操纵探测包的延迟，使攻击者探测到独立于真实拓扑的随机虚拟拓扑。随后AntiTomo在生成虚拟拓扑方面对ProTO做出改进，使得生成的随机拓扑满足欺骗性、安全性、成本低、效率高的约束，以提升系统性能。网络边界防御优点是容易部署，对于内部节点透明；缺点也很明显，只能防御外部的敌人，对于内部敌人的探测束手无策，并且边界处可能成为系统瓶颈。网络内部防御主要是利用SDN技术来控制数据包的路由策略、修改数据包或生成响应包，还可以配合虚拟化技术将探测包重路由到蜜网，最终达到隐藏瓶颈节点，转移攻击者攻击目标的目的。NetObfu[18]利用SDN技术，在网络中部署SDN节点，通过控制器控制节点以其在虚拟拓扑中的身份响应攻击者。虚拟拓扑的呈现主要通过SDN节点的分裂、伪装和隐藏来实现。BottleNet[14]综合静态和动态度量信息，识别网络瓶颈，通过在部署节点部署基于幂律分布生成的随机蜜网来降低瓶颈节点的度量。网络内部防御优点是存在防御内部敌人的可能性，缺点是需要改变原有的拓扑结构，部署难度和代价较高，且随着网络规模的增大，控制节点可能会成为网络瓶颈。

发明内容

[0011] 为此，本发明提出一种抗网络拓扑探测防火墙，用以解决攻击者可以通过类traceroute工具轻易获取目标网络拓扑的问题。

[0012] 一种抗网络拓扑探测防火墙，包括包过滤模块、包延迟控制模块、拓扑欺骗模块、可信探测认证模块、配置生成模块、中枢控制模块、可视化人机交互模块；其中：

[0013] 包过滤模块用于快速过滤数据包；

[0014] 包延迟控制模块用于控制数据包的延迟；

[0015] 拓扑欺骗模块用于识别探测包，并生成响应的伪造应答包；

[0016] 可信探测认证模块用于认证可信的探测者，保留系统网络调试功能；

[0017] 配置生成模块用于根据真实拓扑和虚拟拓扑生成包延迟控制模块和拓扑欺骗模块所需配置；

[0018] 中枢控制模块用于接收用户命令，并将命令统一下发给各个模块；

[0019] 可视化人机交互模块用于向用户展示数据，并向中枢控制模块下发用户命令。

[0020] 进一步地，所述拓扑欺骗模块包括探测包识别单元和应答包生成单元；所述探测包识别单元用于根据数据包的TTL字段和目的IP判断数据包是否为探测包：若目的IP为虚构IP或真实IP，且TTL字段显示数据包不能到达目标，则判定为探测包；应答包生成单元用于判断数据包是否可以触发ICMP差错报文，若不能触发则直接丢弃不应答；否则根据探测包生成ICMP超时报文或ICMP端口不可达报文。

[0021] 进一步地，所述包延迟控制模块通过划分多个数据包队列，其中不同队列对数据包增加的延迟不同，将数据包分发到不同队列中，以获得不同等级的延迟数据包；所述包延迟控制模块包括入包延迟控制单元和出包延迟控制单元，入包延迟控制单元用于给进入的数据包添加延迟，出包延迟控制单元用于给外出的数据包和伪造的ICMP应答报文添加延迟。

[0022] 进一步地，所述包过滤模块使用基于位图加速的规则匹配算法，快速过滤数据包；

所述包过滤模块分包括入包过滤单元和出包过滤单元，入包过滤单元用于过滤进入内网的数据包，出包过滤单元用于过滤发出外网的数据包。

[0023] 进一步地，所述可信探测模块使用IP的方式认证可信的探测者；根据数据包的不同方向，使用数据包的源IP或目的IP判断数据包是否从可信探测源发出或发往可信探测源。

[0024] 进一步地，所述包过滤模块中所述基于位图加速的规则匹配算法使用键值对的形式存储规则，使用index作为键的一部分以扩展规则数量，拥有Accept、Drop、SrcIP、DstIP、SrcPort、DstPort、TypeWithCode、Protocol 8个Map；为了支持子网匹配，在收到数据包后，将源IP和目的IP分别依次使用32、24、16、8、0进行掩码操作，掩码得到的结果作为键的一部分和index一起查询得到5个值，将得到的5个值做或操作，作为源IP项和目的IP项的最终结果；为了支持端口的通配，在查询源端口时，使用源端口和通配源端口分别与index一起查询得到2个值，将结果做或操作得到最终源端口的值；目的端口同理；其余字段只需要配合index查询各自Map即可；将除了Accept和Drop项的查询结果做与操作后，分别与Accept和Drop项进行与操作；如果与Accept项与操作的结果大于与Drop项与操作的结果，则为接收操作；如果小于则丢弃操作；如果等于代表匹配失败，递增index。

[0025] 进一步地，所述配置生成模块使用迪杰斯特拉算法计算防火墙节点到各个主机节点的最短路径，以及路由器节点和主机节点到防火墙的最短路径，生成伪造ICMP应答包所需信息。

[0026] 进一步地，所述中枢控制模块与各模块之间通过证书认证身份，并通过数字信封封装消息。

[0027] 进一步地，所述可视化人机交互模块还用于提供拓扑预览功能。

[0028] 进一步地，所述配置生成模块生成的配置包括拓扑欺骗配置、入包延迟控制配置、出包延迟控制配置。

[0029] 本发明的有益技术效果是：

[0030] 本发明提出一种抗网络拓扑探测防火墙，该防火墙系统能够抵抗攻击者获取目标网络内的拓扑结构，并可实现自定义虚拟拓扑欺骗攻击者，并在延迟方面使数据包的行为与虚拟拓扑一致。除此之外，还保留了可信探测源的网络调试功能，并实现了简单的数据包过滤功能。

附图说明

[0031] 本发明可以通过参考下文中结合附图所给出的描述而得到更好的理解，所述附图连同下面的详细说明一起包含在本说明书中并且形成本说明书的一部分，而且用来进一步举例说明本发明的优选实施例和解释本发明的原理和优点。

[0032] 图1是本发明所述的一种抗网络拓扑探测防火墙的结构示意图；

[0033] 图2是本发明实施例中数据包处理流程图；

[0034] 图3是本发明实施例中出包延迟控制流程图；

[0035] 图4是本发明实施例中简单网络拓扑示例图。

具体实施方式

[0036] 为了使本技术领域的人员更好地理解本发明方案,在下文中将结合附图对本发明的示范性实施方式或实施例进行描述。显然,所描述的实施方式或实施例仅仅是本发明一部分的实施方式或实施例,而不是全部的。基于本发明中的实施方式或实施例,本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施方式或实施例,都应当属于本发明保护的范围。

[0037] 本发明提出一种抗网络拓扑探测防火墙,针对使用类traceroute探测工具的攻击者,旨在隐藏目标网络的真实拓扑,向攻击者展示虚拟拓扑,并在延迟方面,使数据包的表现尽可能与虚拟拓扑一致。

[0038] 本发明实施例提出一种抗网络拓扑探测防火墙,包括包过滤模块、包延迟控制模块、拓扑欺骗模块、可信探测认证模块、配置生成模块、中枢控制模块、可视化人机交互模块;其中:包过滤模块用于快速过滤数据包;包延迟控制模块用于控制数据包的延迟,尽可能让数据包在延迟方面表现的与虚拟拓扑一致;拓扑欺骗模块用于识别探测包,并生成响应的伪造应答包,欺骗攻击者;可信探测认证模块用于认证可信的探测者,保留系统的网络调试功能;配置生成模块用于根据真实拓扑和虚拟拓扑生成包延迟控制模块和拓扑欺骗模块所需的配置,生成的配置包括拓扑欺骗配置、入包延迟控制配置、出包延迟控制配置;中枢控制模块用于接收用户命令,并将命令统一下发给各个模块,统一向包过滤模块、包延迟控制模块、可信探测认证模块、拓扑欺骗模块下发规则;可视化人机交互模块负责向用户展示数据,并向中枢控制模块下发命令。

[0039] 本实施例中,优选地,所述拓扑欺骗模块包括探测包识别单元和应答包生成单元;所述探测包识别单元用于根据数据包的TTL字段和目的IP判断数据包是否为探测包:若目的IP为虚构IP或真实IP,且TTL字段显示数据包不能到达目标,则判定为探测包;应答包生成单元用于判断数据包是否可以触发ICMP差错报文,若不能触发则直接丢弃不应答;否则根据探测包生成ICMP超时报文或ICMP端口不可达报文。

[0040] 本实施例中,优选地,所述包延迟控制模块通过划分多个数据包队列,其中不同队列对数据包增加的延迟不同,将数据包分发到不同队列中,以获得不同等级的延迟数据包;所述包延迟控制模块包括入包延迟控制单元和出包延迟控制单元,入包延迟控制单元用于给进入的数据包添加延迟,出包延迟控制单元用于给外出的数据包和伪造的ICMP应答报文添加延迟。

[0041] 本实施例中,优选地,所述包过滤模块分包括入包过滤单元和出包过滤单元,入包过滤单元用于过滤进入内网的数据包,出包过滤单元用于过滤发出外网的数据包;并根据传输层协议分为四个规则列表,分别为TCP、UDP、ICMP和其他,使用基于位图加速的规则匹配算法,快速过滤数据包。

[0042] 本实施例中,优选地,所述包过滤模块中所述基于位图加速的规则匹配算法使用键值对的形式存储规则,使用index作为键的一部分以扩展规则数量,拥有Accept、Drop、SrcIP、DstIP、SrcPort、DstPort、TypeWithCode、Protocol 8个Map;为了支持子网匹配,在收到数据包后,将源IP和目的IP分别依次使用32、24、16、8、0进行掩码操作,掩码得到的结果作为键的一部分和index一起查询得到5个值,将得到的5个值做或操作,作为源IP项和目的IP项的最终结果;为了支持端口的通配,在查询源端口时,使用源端口和通配源端口分别

与index一起查询得到2个值,将结果做或操作得到最终源端口的值;目的端口同理;其余字段只需要配合index查询各自Map即可;将除了Accept和Drop项的查询结果做与操作后,分别与Accept和Drop项进行与操作;如果与Accept项与操作的结果大于与Drop项与操作的结果,则为接收操作;如果小于则丢弃操作;如果等于代表匹配失败,递增index。

[0043] 本实施例中,优选地,所述可信探测模块使用IP的方式认证可信的探测者;根据数据包的不同方向,使用数据包的源IP或目的IP判断数据包是否从可信探测源发出或发往可信探测源。

[0044] 本实施例中,优选地,所述配置生成模块使用迪杰斯特拉算法计算防火墙节点到各个主机节点的最短路径,以及路由器节点和主机节点到防火墙的最短路径,生成伪造ICMP应答包所需信息。

[0045] 本实施例中,优选地,所述配置生成模块生成的配置包括拓扑欺骗配置、入包延迟控制配置、出包延迟控制配置。

[0046] 本实施例中,优选地,所述中枢控制模块与各模块之间通过证书认证身份,并通过数字信封封装消息。

[0047] 本实施例中,优选地,所述可视化人机交互模块还用于提供拓扑预览功能。

[0048] 不同模块之间的关系如图1。用户将真实拓扑和虚拟拓扑输入到配置生成模块后,配置生成模块会生成拓扑欺骗配置、出包延迟配置和入包延迟配置。可视化人机交互模块用于接收上面的三个配置,除此之外,还支持用户配置出/入包过滤配置和可信配置。可视化人机交互模块向中枢控制模块下发命令,中枢控制模块接收命令后,做出相应的处理(缓存规则等),向出包延迟控制单元、可信探测认证模块、入包过滤单元、拓扑欺骗模块、出包过滤单元、入包延迟控制单元下发命令。

[0049] 整个数据包的处理流程如图2所示。进入的数据包由in开头标识,伪造的应答包由spoof开头标识,外出数据包由out开头标识。进入的数据包首先经过外网交换机,外网交换机将数据包发送到1号设备。到达1号设备后,数据包会首先经过可信探测模块,如果判定数据包为可信探测,会跳过后面的检查,直接通过in-3转发,到达2号设备;否则继续向下。接下来经过入包过滤模块,会按照数据包匹配的规则处理数据包,如果匹配的规则动作为Accept,则继续向下,否则直接丢弃数据包。接下来经过拓扑欺骗模块,首先根据数据包的目的IP和TTL字段判定数据包是否为探测包,如果不是探测包,会通过in-3转发,到达2号设备;否则,继续判断当前探测包是否可以触发ICMP差错报文;如果不可以触发ICMP差错报文,则直接丢弃数据包,否则伪造ICMP应答报文,将伪造的报文通过spoof-1转发。到达2号设备后,数据包会首先经过可信探测模块,如果判定数据包为可信探测,会跳过入包延迟控制单元,直接通过内网交换机到达内网。否则,数据包会进入入包延迟控制单元,根据数据包的目的IP,为数据包补足真实拓扑与虚拟拓扑跳数的差值,再通过in-6转发给内网交换机,到达内网。

[0050] 外出的数据包首先经过内网交换机,内网交换机会将数据包发送到1号设备。到达1号设备后,首先会经过可信探测模块。如果判定数据包为可信探测,会跳过出包过滤单元,直接通过out-3转发给2号设备;否则,经过出包过滤单元,按照数据包匹配的规则处理数据包。如果匹配的规则动作为Accept,则通过out-3转发给2号设备,否则直接丢弃数据包。到达3号设备后,数据包会首先经过可信探测模块,如果判定数据包为可信探测,会跳过出包

延迟控制单元，直接通过外网交换机发送到外网。否则，数据包会进入出包延迟控制单元，根据内网数据包的源IP和TTL，为内网数据包补足与虚拟拓扑中外出跳数的差值，或为伪造的ICMP报文伪造进入内网并发出的延迟，再通过外网交换机，到达外网。

[0051] 进一步对于各个模块所实现的功能进行详细说明。

[0052] 1、包过滤模块中使用基于位图加速的规则匹配算法，以TCP规则为例，假设存在以下规则：

[0053] 表1TCP过滤规则

[0054]

规则号	协议	源 IP	目的 IP	源端口	目的端口	动作
1	TCP	192.168.52.10/32	192.168.17.10/32	*	80	accept
2	TCP	192.168.52.10/32	192.168.17.10/32	*	443	accept
3	TCP	192.168.52.11/32	192.168.17.10/32	*	80	drop

[0055] 上面的规则，在程序中会按照如下存储(其中1000为TCP规则的起始位置，记作index，以支持更多条规则)：

[0056] 表2TCP过滤规则的具体存储

[0057]

Map	Key	Value
Accept	1000	110
Drop	1000	001
源 IP	(192.168.52.10/32,1000)	110
	(192.168.52.11/32,1000)	001
目的 IP	(192.168.17.10/32,1000)	111
源端口	(*,1000)	111
目的端口	(80,1000)	101
	(443,1000)	010

[0058] 在上述表格中，每个项都用一个二进制数字来表示其在规则中的使用情况。其中，数字的每一位代表了对应的规则中是否使用了该项，1表示使用，0表示未使用。

[0059] 例如：当收到一个192.168.52.10:8888发往192.168.17.10:443的TCP数据包时，计算方法如下：

[0060] 1)将使用源IP、源端口、目的IP、目的端口查询Map，将结果进行与操作：

[0061] 110&111&111&010＝010

[0062] 2)将结果分别与Accept和Drop对应项进行与操作：

[0063] 010&110＝010

[0064] 010&001＝000

[0065] 3)010>000，代表规则匹配成功，且Accept的规则先于Drop的规则，采取Accept操作。

[0066] 为了支持IP掩码，将IP地址依次使用32、24、16、8、0掩码后，配合index进行查询，将5次查询结果做或操作，作为这一项的值。端口号的通配也是分别查询index与通配端口和具体端口组成的key对应的value值，将值做或操作，作为这一项的值。

[0067] 2、拓扑欺骗模块记录到达所有IP地址所需TTL值的，以此判定数据包是否为探测包，TTL小于目的IP对应值的数据包为探测包。之后判定当前数据包是否需要生成ICMP应答报文。在互联网中，以下几种情况不需要生成ICMP应答报文：

[0068] (1)数据包不是IP分片的第一片

[0069] (2)数据包为ICMP差错报文

[0070] (3)数据包的目的地址是广播地址或多播地址

[0071] (4)数据包的源地址是特殊地址(零地址、广播地址、多播地址、环回地址)

[0072] 最后，需要为探测包生成相应的ICMP应答报文。模块支持生成两种ICMP应答报文，分别为端口不可达报文和超时报文。对于不能到达目标的探测包，生成ICMP超时报文；能够到达目标，但是目标为虚构IP，则生成ICMP端口不可达报文。

[0073] 3、入包延迟控制单元负责为进入内网的数据包添加延迟。在收到数据包后，根据数据包的目的IP，查询数据包的进入差异延迟，记作in_diff。将数据包的TTL设置为TTL-in_diff，延迟通道设置为in_diff。

[0074] 出包延迟控制单元负责为外出的数据包添加延迟。外出的数据包中包含欺骗模块生成的ICMP应答报文和内网生成的数据包。在收到数据包后：1)检查数据包的源IP是否为虚构IP：a)如果为虚构IP，则数据包由欺骗模块生成，需要补足进入和出去的两个延迟。在数据包中，欺骗模块已经指定了数据包外出的跳数(Default_TTL-TTL)。查询探测包进入源IP需要的跳数(in_hop)，将延迟等级设置为((Default_TTL-TTL)+in_hop)；b)如果数据包不是虚构IP，则向下进行检查。2)检查数据包的类型：a)如果数据包不为ICMP类型，则认为该数据包由内网产生，需要补足外出的跳数。通过源IP查询到外出跳数(out_hop)，由于数据包已经经历过(Default_TTL-TTL)跳，只需再补充(out_hop-(Default_TTL-TTL))跳的延迟。将延迟等级设置为(out_hop-(Default_TTL-TTL))，并修正TTL为(Default_TTL-out_hop)；b)如果数据包为ICMP类型，则继续检查；3)检查ICMP的Type和Code：ICMP为超时报文，与1)a)处理一致；ICMP为其他类型，与2)a)处理一致；4)最后计算ICMP：流程图如图3所示。

[0075] 4、可信探测模块负责检查探测行为是否为经过授权的可信探测。本发明中采用源IP的方式判断探测是否可信。模块并不独立使用，需要配合欺骗模块、出/入包过滤单元、出/入包延迟控制单元一起使用。

[0076] 在本发明中，拓扑结构的表示参考RFC 2328设计。在拓扑结构中，有三类对象：路由器(Router)、网络(Net)和主机(Host)。路由器：可以有多个连接目标，连接目标可以是路由器、网络和主机，数据包从路由器发往目标有非负代价；网络：可以有多个连接目标，连接目标可以是路由器和主机，数据包从网络发往目标代价为零；主机：只能有一个连接目标，连接目标可以是路由器或主机，数据包从主机发往目标代价为零。

[0077] 图4是一个简单的网络拓扑图。圆形代表路由器节点，中间的文字表明路由器的ID，连接线处带有箭头的文字表明接口和代价信息。云朵代表网络节点，中间的文字表明网络的网络号和子网掩码。矩形代表主机节点，中间的文字表明主机的IP地址。将图中对象使用JSON的形式序列化存储，得到的文本文件即为拓扑文件。

[0078] 5、配置生成模块负责解析真实拓扑和虚拟拓扑，通过分析虚拟拓扑，生成欺骗配置和出包延迟配置，在比对真实拓扑后生成入包延迟配置。虚拟拓扑中Host增加了Fake字段，用于标识虚拟拓扑中Host的状态。通过支持虚构Host，可以在敌手扫描网络时，扩大网

络空间,构造诱饵节点,增强欺骗效果。在生成欺骗配置时,支持多种模式生成ICMP超时报文:源模式(ICMP超时报文的源IP为收到触发数据包的接口IP)、路由模式(ICMP超时报文的源IP为当前路由的ID)、最近出口模式(ICMP超时报文的源IP为从当前路由到防火墙最短路径所经过的接口IP)。

[0079] A.欺骗配置生成算法的目标是根据输入的虚拟拓扑生成相应的欺骗配置。下面是对该算法的详细描述:

[0080] 首先,该算法声明了一个全局变量ICMP_MODE,用于控制生成ICMP配置的方式。

[0081] 接下来,算法解析输入的虚拟拓扑结构,并将节点和边添加到图g1中。

[0082] 然后,以防火墙节点为源点,使用迪杰斯特拉算法计算从防火墙到图g1中所有节点的最短路径。

[0083] 对于虚拟拓扑中的每一个主机,算法执行以下步骤:

[0084] 1.获取从防火墙到该主机的所有最短路径集合paths。

[0085] 2.初始化一个空列表icmp_list,用于存储生成的ICMP配置。

[0086] 3.对于路径集合paths中的每一条路径path,进行以下操作:

[0087] -如果ICMP_MODE设置为SOURCE_MODE,则将path传递给子函数以源模式生成ICMP配置,将子函数返回的ICMP配置项添加到icmp_list中。

[0088] -从路径path中提取路由器序列router_path。

[0089] -如果ICMP_MODE设置为ROUTER_MODE,则将router_path传递给子函数以路由模式生成ICMP配置,将子函数返回的ICMP配置项添加到icmp_list中。

[0090] -如果ICMP_MODE设置为NEAREST_MODE,则将router_path传递给子函数以最近出口模式生成ICMP配置,将子函数返回的ICMP配置项添加到icmp_list中。

[0091] 4.输出主机对应的icmp_list。

[0092] 5.如果该主机是虚构主机,则计算并输出从该主机到防火墙的外出跳数。

[0093] 该算法中包含的三个子函数如下:

[0094] 子函数以源模式生成ICMP配置,接受参数path,功能是以SOURCE_MODE模式生成所需ICMP配置。具体步骤如下:

[0095] 1.获取路径中的第一个路由器router。

[0096] 2.如果路由器为空,则返回一个空列表[[]]。

[0097] 3.如果路由器不为空且索引位置为i:

[0098] -获取router与前一项相连的接口IP。

[0099] -将path[i+1:]作为参数传递给以源模式生成ICMP配置函数,得到结果result。

[0100] -获取路由器到防火墙最短路径的跳数hops。

[0101] -计算hops与interface的笛卡尔积,得到icmps。

[0102] -初始化空列表final_result。

[0103] -对于icmps中的每一个icmp,以及result中的每一个icmp_list:

[0104] -复制icmp_list,并在最前面插入icmp,得到final_icmp_list。

[0105] -将final_icmp_list添加到final_result中。

[0106] 4.返回final_result。

[0107] 子函数以路由模式生成ICMP配置,接受参数router_path,功能是以ROUTER_MODE

模式生成所需ICMP配置。具体步骤如下：

[0108] 1.如果路由器路径router_path的长度为0,则返回一个空列表[[]]。

[0109] 2.获取路由器路径中的第一个路由器router。

[0110] 3.将router_path[1:]作为参数传递给以路由模式生成ICMP配置函数,得到结果result。

[0111] 4.获取路由器到防火墙最短路径的跳数hops。

[0112] 5.计算hops与router的ID的笛卡尔积,得到icmps。

[0113] 6.初始化空列表final_result。

[0114] 7.对于icmps中的每一个icmp,以及result中的每一个icmp_list：

[0115] -复制icmp_list,并在最前面插入icmp,得到final_icmp_list。

[0116] -将final_icmp_list添加到final_result中。

[0117] 8.返回final_result。

[0118] 子函数以最近出口模式生成ICMP配置,接受参数router_path,功能是以NEAREST_MODE模式生成所需ICMP配置。具体步骤如下：

[0119] 1.如果路由器路径router_path的长度为0,则返回一个空列表[[]]。

[0120] 2.获取路由器路径中的第一个路由器router。

[0121] 3.将router_path[1:]作为参数传递给以最近出口模式生成ICMP配置函数,得到结果result。

[0122] 4.获取从路由器到防火墙最短路径的接口与跳数的二元组列表icmps。

[0123] 5.初始化空列表final_result。

[0124] 6.对于icmps中的每一个icmp,以及result中的每一个icmp_list：

[0125] -复制icmp_list,并在最前面插入icmp,得到final_icmp_list。

[0126] -将final_icmp_list添加到final_result中。

[0127] 7.返回final_result。

[0128] 通过以上步骤,该算法能够根据虚拟拓扑结构生成相应的欺骗配置,用于对攻击者进行欺骗。生成的ICMP配置项可以根据全局变量ICMP_MODE的不同设置而有所区别,以满足场景的需求。

[0129] B.出包延迟配置生成算法是根据输入的虚拟拓扑,生成相应的出包延迟配置。下面是对该算法的详细描述：

[0130] 首先,算法解析输入的虚拟拓扑结构,并将节点和边添加到图g1中。

[0131] 接下来,以防火墙节点为源点,使用迪杰斯特拉算法计算从防火墙到图g1中所有节点的最短路径。

[0132] 对于虚拟拓扑中的每一个路由器,算法执行以下步骤：

[0133] 1.输出路由器的ID和从防火墙到该路由器的最短路径的跳数列表。

[0134] 2.对于路由器的每一个接口,执行以下操作：

[0135] -输出接口的IP和从防火墙到该路由器的最短路径的跳数列表。

[0136] 接下来,对于虚拟拓扑中的每一个主机,算法执行以下步骤：

[0137] 1.如果主机是虚构主机,则执行以下操作：

[0138] -输出主机的IP,并标注该主机为虚构。

[0139] -输出从防火墙到该虚构主机的最短路径的跳数列表。

[0140] 2.否则,如果主机是真实主机,则执行以下操作:

[0141] -计算从该主机到防火墙的最短路径。

[0142] -输出主机的IP,并标注该主机为真实。

[0143] -输出从该主机到防火墙的最短路径的跳数列表。

[0144] 通过以上步骤,该算法能够根据虚拟拓扑结构生成出包延迟配置。算法输出的信息可用于实现出包延迟的准确控制。

[0145] C.入包延迟配置生成算法是根据输入的虚拟拓扑和真实拓扑,生成相应的入包延迟配置。下面是对该算法的详细描述:

[0146] 首先,算法解析输入的虚拟拓扑结构,并将节点和边添加到图g1中。同时,解析输入的真实拓扑结构,并将节点和边添加到图g2中。

[0147] 接下来,以防火墙节点为源点,分别使用迪杰斯特拉算法计算图g1和图g2中防火墙到所有节点的最短路径。

[0148] 对于真实拓扑中的每一个主机,算法执行以下步骤:

[0149] 1.获取从防火墙到该主机的进入跳数列表real_in_hops。

[0150] 2.对real_in_hops进行去重操作,得到去重后的列表。

[0151] 3.如果去重后的real_in_hops列表长度不为1,则抛出异常,表示真实拓扑中该主机的进入跳数不唯一。

[0152] 4.获取在虚拟拓扑中从防火墙到该主机的进入跳数列表virtual_in_hops。

[0153] 5.初始化一个空列表in_diff,用于存储虚拟拓扑与真实拓扑进入跳数的差异。

[0154] 6.对于virtual_in_hops中的每一个in_hop,执行以下操作:

[0155] -将in_hop减去real_in_hops[0]的结果加入in_diff。

[0156] 7.输出主机的IP和in_diff。

[0157] 通过以上步骤,该算法能够根据虚拟拓扑结构和真实拓扑结构生成入包延迟配置。算法输出了主机的IP地址以及虚拟拓扑与真实拓扑进入跳数的差异。这些差异信息可实现入包延迟的准确控制。

[0158] 6、中枢控制模块负责接收可视化人机交互模块的命令,缓存规则,并向出入包过滤单元、出入包延迟控制单元、欺骗模块、可信探测认证模块下发命令。

[0159] 7、可视化人机交互模块提供了可视化操作出入包过滤单元、欺骗模块、出入包延迟控制单元、可信探测认证模块的界面。

[0160] 尽管根据有限数量的实施例描述了本发明,但是受益于上面的描述,本技术领域内的技术人员明白,在由此描述的本发明的范围内,可以设想其它实施例。对于本发明的范围,对本发明所做的公开是说明性的,而非限制性的,本发明的范围由所附权利要求书限定。

[0161] 本发明援引的文献如下:

[0162] [1]中国互联网络中心.第50次中国互联网络发展状况统计报告.2022,50:76-77

[0163] [2]PANJWANI S,TAN S,JARRIN K M,et al.An experimental evaluation to determine if port scans are precursors to an at-tack[C]//2005International Conference on Dependable Systems and Networks(DSN'05).2005:602-611.

[0164] [3]KEWLEY D,FINK R,LOWRY J,et al.Dynamic approaches to thwart adversary intelligence gathering[C]//Proceedings DARPA Information Survivability Conference and Exposition II DIS-CEX'01.2001,1:176-185.

[0165] [4]Meier R,Tsankov P,Lenders V,et al.NetHide:Secure andPractical Network Topology Obfuscation[C]//27th USENIX Security Symposium(USENIX Security 18).2018:693-709.

[0166] [5]Moving target defense:creating asymmetric uncertainty for cyber threats[M].Springer Science&Business Media,2011.

[0167] [6]邬江兴.网络空间拟态防御研究[J].信息安全学报,2016,1(4):1-10.

[0168] [7]Han X,Kheir N,Balzarotti D.Deception techniques in computer security:A research perspective[J].ACM Computing Surveys(CSUR),2018,51(4):1-36.

[0169] [8]Horák K,Zhu Q,Bošanský B.Manipulating adversary's belief:A dynamic game approach to deception by design for proactive network security[C]//International Conference on Decision and Game Theory for Security.Springer,Cham,2017:273-294.

[0170] [9]Studer A,Perrig A.The coremelt attack[C]//Computer Security-ESORICS 2009:14th European Symposium on Research in Computer Security,Saint-Malo,France,September 21-23,2009.Proceedings 14.Springer Berlin Heidelberg,2009:37-52.

[0171] [10]Kang M S,Lee S B,Gligor V D.The crossfire attack[C]//2013IEEE symposium on security and privacy.IEEE,2013:127-141.

[0172] [11]Kang M S,Gligor V D,Sekar V.SPIFFY:Inducing Cost-Detectability Tradeoffs for Persistent Link-FloodingAttacks[C]//NDSS.2016,1:53-55.

[0173] [12]Coates M,Castro R,Nowak R,et al.Maximum likelihood network topology identification from edge-based unicast measurements[J].ACM SIGMETRICS Performance Evaluation Review,2002,30(1):11-20.

[0174] [13]Nguyen H,Zheng R.A binary independent component analysis approach to tree topology inference[J].IEEE Transactions on Signal Processing,2013,61(12):3071-3080.

[0175] [14]Kim J,Nam J,Lee S,et al.BottleNet:Hiding network bottlenecks using SDN-based topology deception[J].IEEE Transactions on Information Forensics and Security,2021,16:3138-3153.

[0176] [15]Trassare S T,Beverly R,Alderson D.A technique for network topology deception[C]//MILCOM 2013-2013 IEEE Military Communications Conference.IEEE,2013:1795-1800.

[0177] [16]Hou T,Qu Z,Wang T,et al.ProTO:Proactive topology obfuscation against adversarial network topology inference[C]//IEEE INFOCOM 2020-IEEE Conference on Computer Communications.IEEE,2020:1598-1607.

[0178] [17]Liu Y,Xing C,Zhang G,et al.AntiTomo:Network topology obfuscation against adversarial tomography-based topology inference[J].Computers& Security,2022,113:102570.

[0179] [18]Liu Y,Zhao J,Zhang G,et al.NetObfu:A lightweight and efficient network topology obfuscation defense scheme[J].Computers&Security,2021,110: 102447。

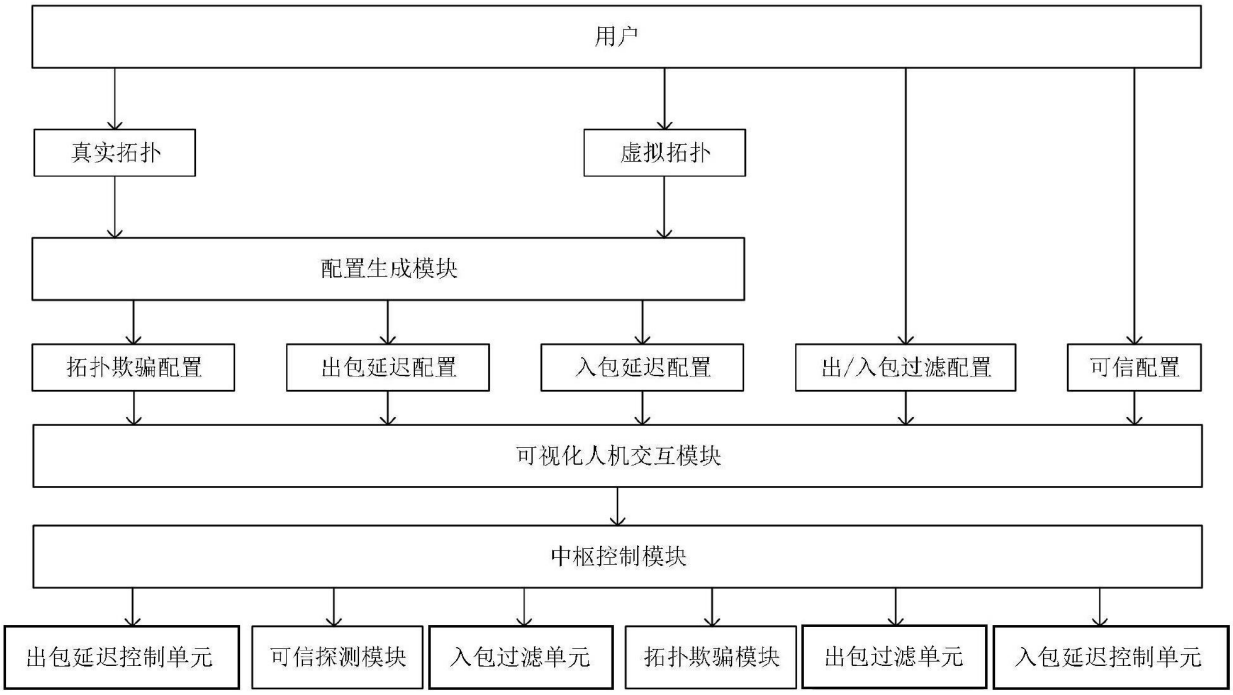

用户
真实拓扑
虚拟拓扑
配置生成模块
拓扑欺骗配置
出包延迟配置
入包延迟配置
出/入包过滤配置
可信配置
可视化人机交互模块
中枢控制模块
出包延迟控制单元
可信探测模块
入包过滤单元
拓扑欺骗模块
出包过滤单元
入包延迟控制单元

图1

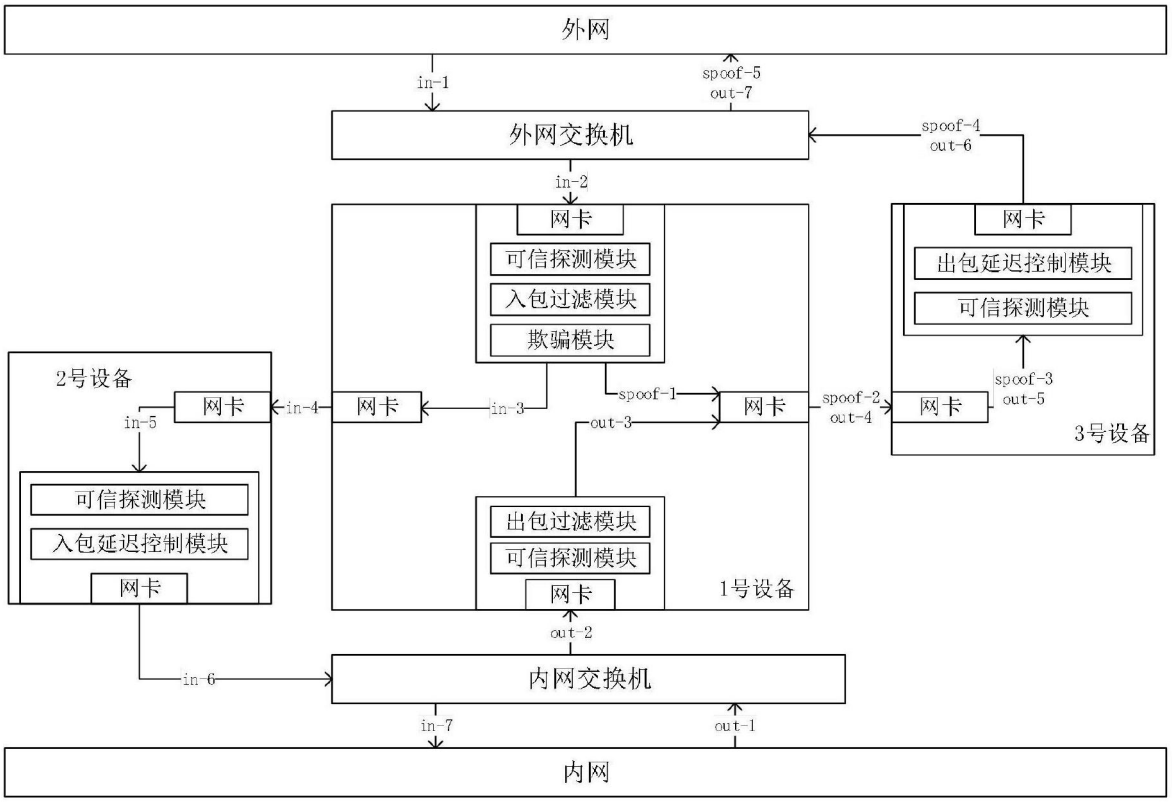

外网
in-1
spoof-5
out-7
外网交换机
spoof-4
out-6
in-2
网卡
可信探测模块
入包过滤模块
欺骗模块
网卡
出包延迟控制模块
可信探测模块
spoof-3
out-5
3号设备
2号设备
网卡
in-4
网卡
in-3
spoof-1
网卡
spoof-2
out-4
网卡
in-5
out-3
可信探测模块
入包延迟控制模块
网卡
出包过滤模块
可信探测模块
网卡
1号设备
out-2
in-6
内网交换机
in-7
out-1
内网

图2

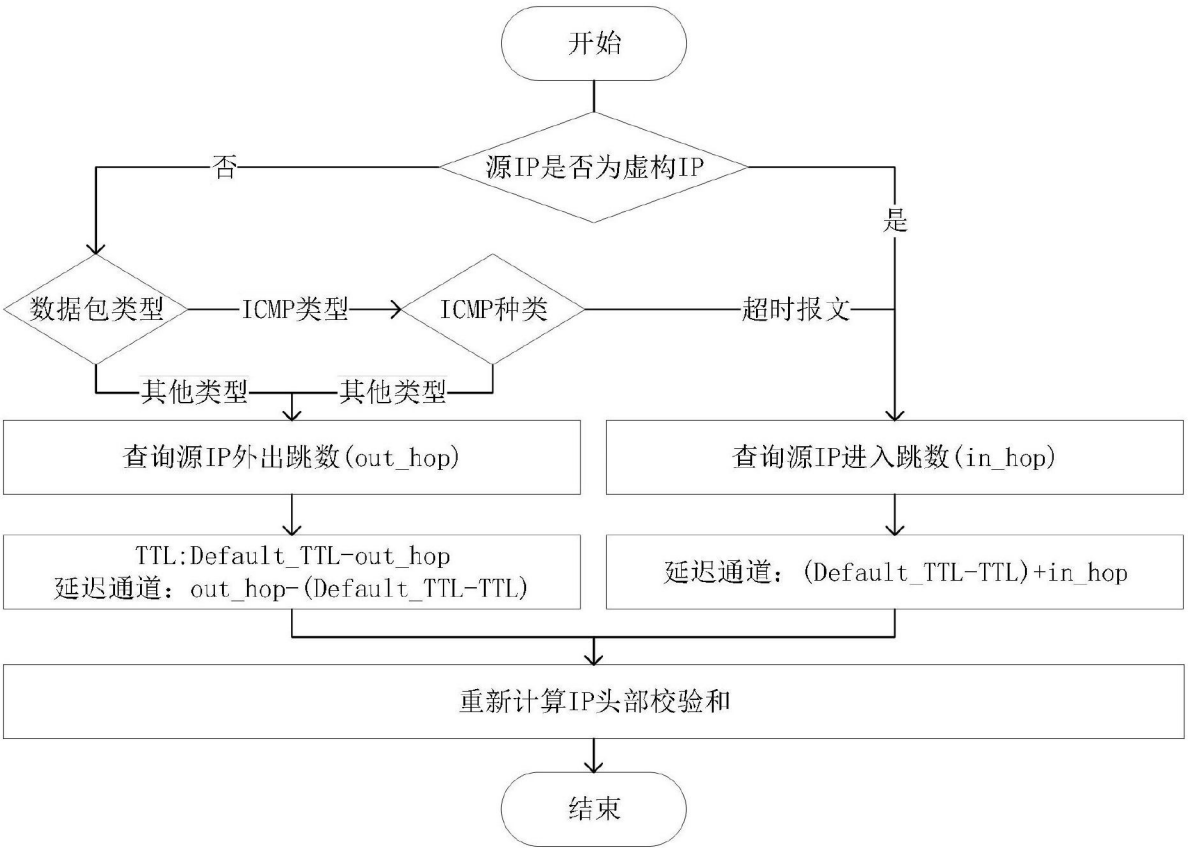

开始
源IP是否为虚构IP
否
是
数据包类型
ICMP类型
ICMP种类
超时报文
其他类型
其他类型
查询源IP外出跳数(out_hop)
查询源IP进入跳数(in_hop)
TTL:Default_TTL-out_hop
延迟通道：out_hop-(Default_TTL-TTL)
延迟通道：(Default_TTL-TTL)+in_hop
重新计算IP头部校验和
结束

图3

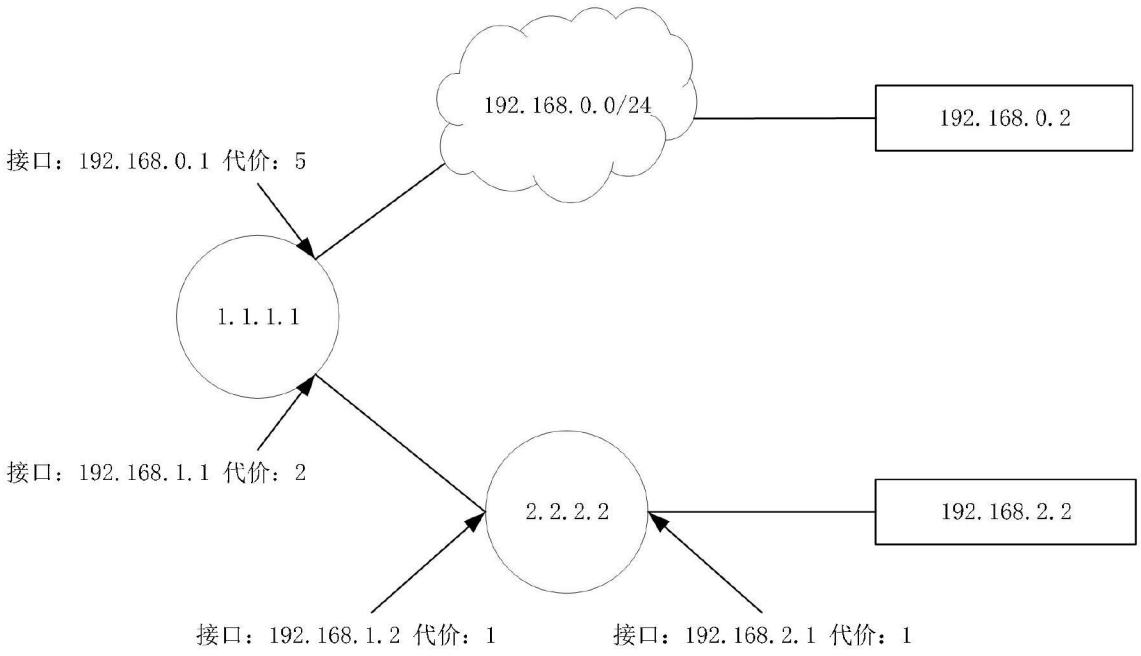

192.168.0.0/24
192.168.0.2
接口：192.168.0.1 代价：5
1.1.1.1
接口：192.168.1.1 代价：2
2.2.2.2
192.168.2.2
接口：192.168.1.2 代价：1
接口：192.168.2.1 代价：1

图4