(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112073411 B
(45)授权公告日 2022.10.04

(21)申请号 202010930058.1

(22)申请日 2020.09.07

(65)同一申请的已公布的文献号
申请公布号 CN 112073411 A

(43)申请公布日 2020.12.11

(73)专利权人 软通智慧信息技术有限公司
地址 300308 天津市滨海新区天津自贸试验区(空港经济区)东七道2号中兴产业基地7号楼402

(72)发明人 张艳玲 柏翔 雒冬梅 宋朝宁

(74)专利代理机构 北京品源专利代理有限公司 11332
专利代理师 孟金喆

(51)Int.Cl.
H04L 9/40(2022.01)
H04L 41/12(2022.01)
H04L 41/14(2022.01)

(56)对比文件
CN 108809979 A,2018.11.13
CN 109558729 A,2019.04.02

审查员 丁彬

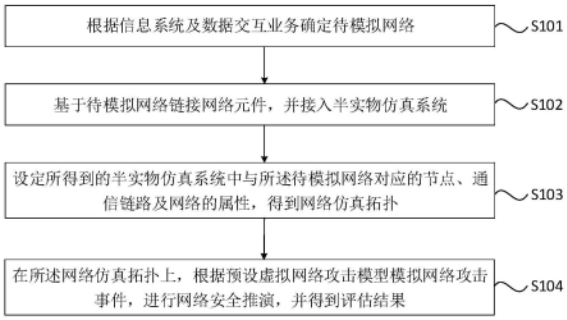
权利要求书2页 说明书10页 附图3页

(54)发明名称

一种网络安全推演方法、装置、设备及存储介质

(57)摘要

本发明实施例公开了一种网络安全推演方法、装置、设备及存储介质。其中,该方法包括:根据信息系统及数据交互业务确定待模拟网络;基于待模拟网络链接网络元件,并接入半实物仿真系统;设定所得到的半实物仿真系统中与所述待模拟网络对应的节点、通信链路及网络的属性,得到网络仿真拓扑;在所述网络仿真拓扑上,根据预设虚拟网络攻击模型模拟网络攻击事件,进行网络安全推演,并得到评估结果。本发明实施例提供的技术方案,通过接入半实物仿真系统,实现在网络仿真拓扑中引入了实物设备,能够对真实业务系统网络环境进行更准确的模拟,提高了网络安全推演过程的准确性。



CN 112073411 B

1.一种网络安全推演方法,其特征在于,包括:

根据信息系统及数据交互业务确定待模拟网络;

基于待模拟网络链接网络元件,并接入半实物仿真系统;

设定所得到的半实物仿真系统中与所述待模拟网络对应的节点、通信链路及网络的属性,得到网络仿真拓扑;

在所述网络仿真拓扑上,根据预设虚拟网络攻击模型模拟网络攻击事件,进行网络安全推演,并得到评估结果,包括:

根据预设虚拟网络攻击模型模拟网络攻击事件,针对所述网络攻击事件根据防御量化体系得到待模拟网络的评估结果,所述评估结果包括待模拟网络的防御能力;

若所述防御能力不满足预设第一防御标准,则重新进行网络安全推演;

所述防御量化体系包括防御系统、评估标准、评估要求及评估方法,其中,所述防御系统由分布于攻击端、中间网络和被攻击端的防火墙、入侵检测、入侵追踪和速率限制组成。

2.根据权利要求1所述的方法,其特征在于,所述接入半实物仿真系统包括:

通过接入虚拟机对至少一个网络元件的物理属性进行模拟;

接入至少一个实体设备,所述至少一个实体设备用于针对网络攻击事件进行防护。

3.根据权利要求1所述的方法,其特征在于,在所述接入半实物仿真系统之后,还包括:

定义预设虚拟网络攻击模型对应的攻击主机的数量、攻击位置及被攻击主机。

4.根据权利要求3所述的方法,其特征在于,所述预设虚拟网络攻击模型对应的攻击方式包括以下至少一种:

串行网络攻击、并行网络攻击及选择网络攻击。

5.根据权利要求1所述的方法,其特征在于,所述根据预设虚拟网络攻击模型模拟网络攻击事件,针对所述网络攻击事件根据防御量化体系得到待模拟网络的评估结果,包括:

根据预设虚拟网络攻击模型调用攻击策略库中对应的攻击策略模拟网络通过攻击主机对被攻击主机的攻击位置发起模拟攻击,调用防护策略库中对应的防护策略进行相应的防护,根据防御量化体系对防护结果进行量化,得到待模拟网络的第一防御能力。

6.根据权利要求5所述的方法,其特征在于,还包括:

若所述第一防御能力不满足预设第二防御标准,则重新根据预设虚拟网络攻击模型调用攻击策略库中对应的攻击策略模拟网络通过攻击主机对被攻击主机的攻击位置发起模拟攻击,并利用防御模块中的防御策略和工具进行防护。

7.一种网络安全推演装置,其特征在于,包括:

待模拟网络确定模块,用于根据信息系统及数据交互业务确定待模拟网络;

仿真系统接入模块,用于基于待模拟网络链接网络元件,并接入半实物仿真系统;

网络拓扑确定模块,用于设定所得到的半实物仿真系统中与所述待模拟网络对应的节点、通信链路及网络的属性,得到网络仿真拓扑;

网络安全推演模块,用于在所述网络仿真拓扑上,根据预设虚拟网络攻击模型模拟网络攻击事件,进行网络安全推演,并得到评估结果;

所述网络安全推演模块,具体包括:

评估结果确定单元,用于根据预设虚拟网络攻击模型模拟网络攻击事件,针对所述网络攻击事件根据防御量化体系得到待模拟网络的评估结果,所述评估结果包括待模拟网络

的防御能力；

重新推演单元，用于若所述防御能力不满足预设第一防御标准，则重新进行网络安全推演；

所述防御量化体系包括防御系统、评估标准、评估要求及评估方法，其中，所述防御系统由分布于攻击端、中间网络和被攻击端的防火墙、入侵检测、入侵追踪和速率限制组成。

8.一种计算机设备，其特征在于，所述计算机设备包括：

一个或多个处理器；

存储装置，用于存储一个或多个程序；

当所述一个或多个程序被所述一个或多个处理器执行，使得所述一个或多个处理器实现如权利要求1-6中任一所述的网络安全推演方法。

9.一种计算机可读存储介质，其上存储有计算机程序，其特征在于，该程序被处理器执行时实现如权利要求1-6中任一所述的网络安全推演方法。

一种网络安全推演方法、装置、设备及存储介质

技术领域

[0001] 本发明实施例涉及网络信息安全技术，尤其涉及一种网络安全推演方法、装置、设备及存储介质。

背景技术

[0002] 随着计算机和网络技术的发展，网络空间已逐渐演变为一个类似于陆、海、空、天等真实存在的客观领域，其通过对数据的产生、存储、修改和交换，实现对物理系统的操控并影响人的认知和社会活动。在网络空间越来越被重视的同时，其面临的安全威胁与挑战也与日俱增，各种攻击手段和方法如网络攻击、程序漏洞、计算机病毒、逻辑炸弹、预置后门、恶意软件等在网络空间中层出不穷。因此，网络安全尤其重要。

[0003] 现有的网络安全推演方法，主要靠专业工具搭建虚拟网络拓扑环境，设置主机、服务器、路由等元件的通信协议规则，制定网络威胁扫描、感染、传递规则去模拟推演网络数据包传输情况。

[0004] 但是虚拟网络拓扑环境无法与实网系统做到一一映射，定制化及模块化的组件无法模拟新型网络空间设备性能，没有链接真实信息系统主机设备属性，通信协议规则影响过大。因此，现有的网络安全推演方法准确性有限，无法预演真实网络受到威胁后的应急处置。

发明内容

[0005] 本发明实施例提供了一种网络安全推演方法、装置、设备及存储介质，提高了网络安全推演过程的准确性。

[0006] 第一方面，本发明实施例提供了一种网络安全推演方法，该方法包括：

[0007] 根据信息系统及数据交互业务确定待模拟网络；

[0008] 基于待模拟网络链接网络元件，并接入半实物仿真系统；

[0009] 设定所得到的半实物仿真系统中与所述待模拟网络对应的节点、通信链路及网络的属性，得到网络仿真拓扑；

[0010] 在所述网络仿真拓扑上，根据预设虚拟网络攻击模型模拟网络攻击事件，进行网络安全推演，并得到评估结果。

[0011] 第二方面，本发明实施例提供了一种网络安全推演装置，该装置包括：

[0012] 待模拟网络确定模块，用于根据信息系统及数据交互业务确定待模拟网络；

[0013] 仿真系统接入模块，用于基于待模拟网络链接网络元件，并接入半实物仿真系统；

[0014] 网络拓扑确定模块，用于设定所得到的半实物仿真系统中与所述待模拟网络对应的节点、通信链路及网络的属性，得到网络仿真拓扑；

[0015] 网络安全推演模块，用于在所述网络仿真拓扑上，根据预设虚拟网络攻击模型模拟网络攻击事件，进行网络安全推演，并得到评估结果。

[0016] 第三方面，本发明实施例提供了一种计算机设备，该计算机设备包括：

[0017] 一个或多个处理器；

[0018] 存储装置，用于存储一个或多个程序；

[0019] 当所述一个或多个程序被所述一个或多个处理器执行，使得所述一个或多个处理器实现本发明任意实施例所述的网络安全推演方法。

[0020] 第四方面，本发明实施例提供了一种计算机可读存储介质，其上存储有计算机程序，该程序被处理器执行时实现本发明任意实施例所述的网络安全推演方法。

[0021] 本发明实施例提供了一种网络安全推演方法、装置、设备及存储介质，首先根据信息系统及数据交互业务确定待模拟网络，接着基于待模拟网络链接网络元件，并接入半实物仿真系统，然后设定所得到的半实物仿真系统中与待模拟网络对应的节点、通信链路及网络的属性，得到网络仿真拓扑，最后在网络仿真拓扑上，根据预设虚拟网络攻击模型模拟网络攻击事件，进行网络安全推演，并得到评估结果，通过接入半实物仿真系统，实现在网络仿真拓扑中引入了实物设备，能够对真实业务系统网络环境进行更准确的模拟，提高了网络安全推演过程的准确性。

附图说明

[0022] 图1为本发明实施例一提供的一种网络安全推演方法的流程图；

[0023] 图2为本发明实施例二提供的一种网络安全推演方法的流程图；

[0024] 图3A为本发明实施例三提供的一种网络安全推演方法的流程图；

[0025] 图3B为本发明实施例三提供的方法中网络安全推演方法的框架图；

[0026] 图3C为本发明实施例三提供的方法中网络安全推演过程的结构图；

[0027] 图4为本发明实施例四提供的一种网络安全推演装置的结构示意图；

[0028] 图5为本发明实施例五提供的一种计算机设备的结构示意图。

具体实施方式

[0029] 下面结合附图和实施例对本发明作进一步的详细说明。可以理解的是，此处所描述的具体实施例仅仅用于解释本发明，而非对本发明的限定。另外还需要说明的是，为了便于描述，附图中仅示出了与本发明相关的部分而非全部结构。

[0030] 实施例一

[0031] 图1为本发明实施例一提供的一种网络安全推演方法的流程图，本实施例可适用于对网络空间的安全进行推演的情况。本实施例提供的网络安全推演方法可以由本发明实施例提供的网络安全推演装置来执行，该装置可以通过软件和/或硬件的方式实现，并集成在执行本方法的计算机设备中。

[0032] 参见图1，本实施例的方法包括但不限于如下步骤：

[0033] S101，根据信息系统及数据交互业务确定待模拟网络。

[0034] 其中，待模拟网络可以为与需要模拟的真实业务系统网络环境相匹配的网络。

[0035] 在互联网时代，尤其是智慧城市信息系统中接入的信息数据较多，应用场景复杂多样，数据跨领域交换频繁，从而面临的网络安全威胁防不胜防，网络攻击手段层出不穷，网络安全态势变得越来越严峻。为了带动智慧城市数据受控共享、网络安全综合防控及网络安全监测设备等相关的技术突破和产品升级改造，推动物联网与新型智慧城市等领域的

建设，对网络安全进行推演是非常有必要的。而在对网络安全进行推演时首先需要确定待模拟网络，也就是与需要模拟的真实业务系统网络环境相匹配的网络，此时可以根据信息系统及数据交互业务确定构成真实业务系统网络环境相匹配网络的主要元素以及主要元素之间的数据交互情况，由此可以确定出待模拟的网络。

[0036] 具体的，构成网络环境的主要元素包括主机元素、路由器元素和网络元素等，通过将这三个核心的元素有机的组合能够实现复杂的网络环境。

[0037] S102，基于待模拟网络链接网络元件，并接入半实物仿真系统。

[0038] 其中，半实物仿真系统为将数学模型、物理模型或实体结合起来组成的仿真系统，组成部分包括：核心主机、仿真计算机、环境模拟设备、物理模型或实体以及进行数据交互及同步的接口。

[0039] 在确定了待模拟网络之后，基于待模拟网络可以通过网络模型设计、节点设计及进程设计链接网络元件，网络元件例如可包括主机、服务器、路由器、交换机、防火墙、网关、客户机、异步传输模式(Asynchronous Transfer Mode，简称ATM)、数字用户线路(Digital Subscriber Line，简称DSL)、综合业务数字网(Integrated Services Digital Network，简称ISDN)等设备，通过网络元件的链接，能够全面反映网络的相关特性，保障数据在待模拟网络中的顺利传输。同时为了与真实网络环境进行映射，可以接入半实物仿真系统，将实际的网络系统映射到半实物仿真环境。

[0040] S103，设定所得到的半实物仿真系统中与所述待模拟网络对应的节点、通信链路及网络的属性，得到网络仿真拓扑。

[0041] 在网络元件已经链接好之后，由于网络元件中各元件的属性不同，此时还需要对网络元件的属性进行设置，而网络元件是通过网络模型设计、节点设计及进程设计链接的，由此可以设定在半实物仿真系统中与待模拟网络对应的节点、通信链路及网络的属性，例如将某主机内存设为2核，将某条通信链路上数据吞吐量设置为20M/s，这样就得到了网络仿真拓扑，并且在该网络仿真中对业务信息系统、主机、服务器、路由及网关等设备都进行了数字化映射。

[0042] 可选的，网络模型设计、节点设计及进程设计主要是通过网络设备、链路和协议模型，分为network、node和process三个层次，模拟网络流量的传输，从而获取网络设计或优化所需要的网络性能数据。最底层为Process进程模型，以有限状态机来描述协议；其次为Node节点模型，由相应的协议模型构成，反映设备特性；最上层为Network网络模型。三层模型和真实业务系统的网络、设备、协议层次对应，从而全面反映了真实业务系统网络的相关特性。

[0043] S104，在所述网络仿真拓扑上，根据预设虚拟网络攻击模型模拟网络攻击事件，进行网络安全推演，并得到评估结果。

[0044] 其中，预设虚拟网络攻击模型模拟网络攻击事件的过程可以相当于人为制造一些木马文件或者病毒，发动攻击以后，病毒在网络仿真拓扑中按照一定的扫描机制，不断的感染主机，感染后的主机又会按照扫描机制去感染其他机器。

[0045] 得到网络仿真拓扑之后，在该网络仿真拓扑中，通过预设虚拟网络攻击模型对网络攻击事件进行模拟，从而进行网络安全推演，最终能够得到评估结果。其中，网络安全推演可以为模拟预设虚拟网络攻击模型在网络仿真拓扑下，网络攻击病毒扩散的原理、机制、

路径，分析在不同扫描、传染策略下病毒复制速度和机理，从而加强防御手段，在综合防御工具、技术手段的协同控制下，保障信息系统安全。例如，可以实时捕获通信链路上每一帧数据包信息，然后动态加载防护工具，结合网络态势分析技术以及预警处置技术，预演通信链路上威胁传播路径及速度，并将仿真推演结果存储在相应的位置中。

[0046] 本实施例提供的技术方案，首先根据信息系统及数据交互业务确定待模拟网络，接着基于待模拟网络链接网络元件，并接入半实物仿真系统，然后设定所得到的半实物仿真系统中与待模拟网络对应的节点、通信链路及网络的属性，得到网络仿真拓扑，最后在网络仿真拓扑上，根据预设虚拟网络攻击模型模拟网络攻击事件，进行网络安全推演，并得到评估结果，通过接入半实物仿真系统，实现在网络仿真拓扑中引入了实物设备，能够对真实业务系统网络环境进行更准确的模拟，提高了网络安全推演过程的准确性。

[0047] 实施例二

[0048] 图2为本发明实施例二提供的一种网络安全推演方法的流程图。本发明实施例是在上述实施例的基础上进行优化。可选的，本实施例对接入半实物仿真系统之后的过程进行详细的解释说明。

[0049] 参见图2，本实施例的方法包括但不限于如下步骤：

[0050] S201，根据信息系统及数据交互业务确定待模拟网络。

[0051] S202，基于待模拟网络链接网络元件，并接入半实物仿真系统。

[0052] 可选的，所述接入半实物仿真系统可以具体包括：通过接入虚拟机对至少一个网络元件的物理属性进行模拟；接入至少一个实体设备，所述至少一个实体设备用于针对网络攻击事件进行防护。

[0053] 具体的，为了更好地对待模拟网络中网络元件的运行过程进行模拟，可以通过接入虚拟机对至少一个网络元件，例如主机服务器进行虚拟映射，在这个映射过程中需要设定一些属性参数去模拟该网络元件的实际运行过程，例如，可以设置虚拟机配置参数，指定CPU核数、内存以及操作系统，支持虚拟机的重启、删除、进入虚拟机、关闭、查看详情、批量关闭等功能，运行状态为已关机的虚拟机不能被重启，运行状态为运行中的虚拟机不可被删除等。另一方面，可以通过接入至少一个实体设备，针对网络攻击事件作出相应的防护，实体设备可以为新研制的智能网关、病毒检测设备等。

[0054] 需要说明的是，本实施例中在实际的网络安全推演过程中允许虚拟机进行监控管理，查询虚拟机关联的业务。

[0055] S203，定义预设虚拟网络攻击模型对应的攻击主机的数量、攻击位置及被攻击主机。

[0056] 在预设虚拟网络攻击模型中可以根据仿真需求和实际条件定义攻击主机的数量、攻击位置及被攻击主机，例如攻击主机的作用是为网络安全提供真实、实时的仿真流量，可以灵活制造出与实际情况相同的攻击环境，为攻防演练和对抗提供仿真条件。具体的，针对分布式攻击工具(主要是DDos攻击)，可以尝试在不同的位置进行攻击，用以区别和分析不同的位置所产生攻击的不同。如攻击主机可以按照一定的规则进行分布，有组织的产生较小、看似正常的数据流量，由半实物仿真系统的接口进入模拟网络中进行攻击，穿透目标防火墙防御措施后进入被攻击主机，将被攻击主机系统资源耗尽，使其陷入瘫痪。

[0057] 可选的，所述预设虚拟网络攻击模型对应的攻击方式可以包括以下至少一种：串

行网络攻击、并行网络攻击及选择网络攻击。

[0058] 具体的，由于网络攻击过程的多样性和复杂性，不同网络攻击方式对应的虚拟网络攻击模型也不相同。通过对网络攻击组织方式进行描述，能够表示网络攻击中存在并行、同步、冲突及因果依赖等关系，进而模拟网络攻击的过程，分析网络攻击的特点，为网络安全推演过程提供支撑。由于复杂的网络攻击方式可以通过简单网络攻击方式的有机组合进行表述，那么预设虚拟网络攻击模型对应的攻击方式可以为：串行网络攻击、并行网络攻击、选择网络攻击中的至少一种，或者这三种的有机组合。根据实际需求，可以人为选择不同的攻击方式进行模拟。

[0059] S204，设定所得到的半实物仿真系统中与所述待模拟网络对应的节点、通信链路及网络的属性，得到网络仿真拓扑。

[0060] S205，在所述网络仿真拓扑上，根据预设虚拟网络攻击模型模拟网络攻击事件，进行网络安全推演，并得到评估结果。

[0061] 本实施例提供的技术方案，首先根据信息系统及数据交互业务确定待模拟网络，接着基于待模拟网络链接网络元件，并接入半实物仿真系统，然后定义预设虚拟网络攻击模型对应的攻击主机的数量、攻击位置及被攻击主机，设定所得到的半实物仿真系统中与待模拟网络对应的节点、通信链路及网络的属性，得到网络仿真拓扑，最后在网络仿真拓扑上，根据预设虚拟网络攻击模型模拟网络攻击事件，进行网络安全推演，并得到评估结果，通过接入半实物仿真系统，实现在网络仿真拓扑中引入了虚拟机和实体设备，能够对真实业务系统网络环境进行更准确的模拟，同时通过定义预设虚拟网络攻击模型中攻击主机的数量、攻击位置及被攻击主机可以对网络攻击进行模拟，为网络安全推演过程提供支撑，进而提高网络安全推演过程的准确性以及推演结果的准确性。

[0062] 实施例三

[0063] 图3A为本发明实施例三提供的一种网络安全推演方法的流程图。本发明实施例是在上述实施例的基础上进行优化。可选的，本实施例对根据预设虚拟网络攻击模型模拟网络攻击事件，进行网络安全推演，并得到评估结果的过程进行详细的解释说明。

[0064] 参考图3A，本实施例的方法包括但不限于如下步骤：

[0065] S301，根据信息系统及数据交互业务确定待模拟网络。

[0066] S302，基于待模拟网络链接网络元件，并接入半实物仿真系统。

[0067] S303，定义预设虚拟网络攻击模型对应的攻击主机的数量、攻击位置及被攻击主机。

[0068] S304，设定所得到的半实物仿真系统中与所述待模拟网络对应的节点、通信链路及网络的属性，得到网络仿真拓扑。

[0069] S305，根据预设虚拟网络攻击模型模拟网络攻击事件，针对所述网络攻击事件根据防御量化体系得到待模拟网络的评估结果，所述评估结果包括待模拟网络的防御能力。

[0070] 其中，防御量化体系可以包括防御系统、评估标准、评估要求及评估方法等，防御系统由分布于攻击端、中间网络和被攻击端的防火墙、入侵检测、入侵追踪和速率限制等防御设备组成。防火墙主要是通过核心资源库中的黑、白名单及过滤数据包，过滤掉有问题的数据包流量，只允许正常网络流量通过，并将流经的网络流量包发送给入侵检测设备，供其异常检测；入侵检测主要是检测攻击，利用检测知识库和检测算法对数据包流量进行异常

匹配，若在一段时间出现了大量的异常数据包，就认为受到了攻击；入侵追踪主要是追踪攻击源，可以部署在路由器上，采用伪造IP地址等手段发动攻击后，入侵追踪设备可以根据追踪算法，追踪到真正的攻击源，将攻击源信息发送给防火墙，达到防御目的。评估标准、评估要求及评估方法可以为根据待模拟网络中本次网络推演所针对的主要目标设备设定的。

[0071] 具体的，根据预设虚拟网络攻击模型模拟网络攻击事件，针对网络攻击事件先通过防御量化体系中的防御系统中各防御设备相互通信、功能互补、协同完成防御网络攻击的任务。主要是采用入侵追踪、速率限制等防御设备，分析影响防御能力的防御设备指标，如防御设备自我学习时间、入侵追踪阈值和入侵追踪部署策略，综合考虑攻击源端防御、被攻击端防御效果、防御速率、防御准确性及防御成本等方面建立防御能力量化模型，从而达到根除攻击流量的目的，进而结合评估标准、评估要求及评估方法得到最终的评估结果，评估结果中包括了待模拟网络的防御能力。

[0072] 进一步的，所述根据预设虚拟网络攻击模型模拟网络攻击事件，针对所述网络攻击事件根据防御量化体系得到待模拟网络的评估结果，可以具体包括：根据预设虚拟网络攻击模型调用攻击策略库中对应的攻击策略模拟网络通过攻击主机对被攻击主机的攻击位置发起模拟攻击，调用防护策略库中对应的防护策略进行相应的防护，根据防御量化体系对防护结果进行量化，得到待模拟网络的第一防御能力。

[0073] 具体的，可以针对预设虚拟网络攻击模型先调用核心资源库中的攻击策略库中对应的攻击策略模拟网络通过攻击主机对被攻击主机的攻击位置发起模拟攻击，然后调用核心资源库中的防护策略库中所对应的防护策略进行相应的防护，最后根据防御量化体系对防护结果进行量化，例如攻击5秒以后网络堵塞分数比攻击10s以后的网络堵塞分数低，说明该防御能力薄弱，堵塞程度越来越严重，从而就得到了待模拟网络的第一防御能力。

[0074] 更进一步的，若所述第一防御能力不满足预设第二防御标准，则重新根据预设虚拟网络攻击模型调用攻击策略库中对应的攻击策略模拟网络通过攻击主机对被攻击主机的攻击位置发起模拟攻击，并利用防御模块中的防御策略和工具进行防护。

[0075] 具体的，可以预先设置一个第二防御标准对第一防御能力进行评估，如果第一防御能力不能满足预设第二防御标准，则说明防护策略库中对应的防护策略不能很好的对模拟攻击进行防护，此时需要使用更高的防御手段来应对网络攻击。因此需要重新根据预设虚拟网络攻击模型调用攻击策略库中对应的攻击策略模拟网络通过攻击主机对被攻击主机的攻击位置发起模拟攻击，然后通过防御模块中的防御策略和工具进行防护。

[0076] 图3B为本发明实施例三提供的方法中网络安全推演方法的框架图，参见图3B，该框架图包括：核心资源库、防御模块以及模拟仿真推演。

[0077] 核心资源库，主要用于知识沉淀以及核心成果保存，并为后续的网络安全推演提供支撑。核心资源库中可存储攻击策略、防护策略、常用功防工具、威胁情报信息以及靶标和场景资源等。通过对攻击策略库中的工具进行管理，添加及更新，可以增强攻击策略库的灵活性及扩展性。

[0078] 防御模块主要以镜像伴生系统为核心的主动防护体系，提供强大的防御能力，包括镜像伴生、智能感知、入侵判别、态势分析、追踪溯源及处置策略等功能，可以将针对于待模拟网络系统的疑似恶意行为自动重定向至镜像伴生，并深入分析，从而采取有效防护措施，使网络信息系统免于伤害。

[0079] 模拟仿真推演主要通过预设虚拟网络攻击模型，实时捕获通信链路上每一帧数据包信息，动态加载防护工具手段，结合网络态势分析技术以及预警处置技术，预演网络链路上威胁传播路径及速度，并对推演过程及结果进行存储。同时，针对预设虚拟网络模拟攻击模型，根据防御量化体系得到待模拟网络的评估结果。

[0080] 示例性的，图3C为本发明实施例三提供的方法中网络安全推演过程的结构图，参见图3C，该过程主要包括确定需求、准备阶段、执行阶段、分析阶段以及得到评估结果。

[0081] 确定需求，主要是确定本次网络安全推演过程的测试目标和测试内容，例如待模拟网络中某一网络元件的防御能力。

[0082] 准备阶段可以包括：仿真环境构建、仿真参数设置及仿真实验设置。

[0083] 执行阶段可以包括：仿真控制、实时运行及参数统计。

[0084] 准备阶段和执行阶段都是基于半实物仿真系统的。

[0085] 分析阶段包括：评估标准、评估要求及评估方法。

[0086] 可选的，在分析阶段，还可以通过服务器负载研究服务器是否有能力处理扩展网络的额外业务。在待模拟网络与扩展网络连接后，整个网络的延时性能是否满足要求，可以通过统计以太网延时，进行前后的延时比较得到。对于网络性能中稳定性来讲，服务器负载起着主要作用，可以从服务器节点中选取；以太网延时可以查看整个网络的延迟性能，它可以在网络仿真拓扑中选取。对于一个网络仿真拓扑在进行网络安全推演后，还可以扩展该网络并且推演验证在增加额外负载下，网络是否仍然能够很好地工作，此时需要复制当前推演场景，并构建扩展网络部分，选定相关统计量运行仿真，对得到的评估结果进行比较。

[0087] 最终的得到的评估结果可以通过评估报告进行展示，分析阶段和得到评估结果可以在评估系统中完成。

[0088] S306，若所述防御能力不满足预设第一防御标准，则重新进行网络安全推演。

[0089] 具体的，在实际的网络安全推演过程中，可以设置一个第一防御标准作为衡量防御能力是否达标的指标，如果防御能力不满足预设第一防御标准，则重新进行网络安全推演，直到防御能力达到预设第一防御标准寻求，说明这时的防护方案能够很好的抵抗网络攻击事件。

[0090] 本实施例提供的技术方案，首先根据信息系统及数据交互业务确定待模拟网络，其次基于待模拟网络链接网络元件，并接入半实物仿真系统，定义预设虚拟网络攻击模型对应的攻击主机的数量、攻击位置及被攻击主机，接着设定所得到的半实物仿真系统中与待模拟网络对应的节点、通信链路及网络的属性，得到网络仿真拓扑，然后根据预设虚拟网络攻击模型模拟网络攻击事件，针对网络攻击事件根据防御量化体系得到待模拟网络的评估结果，评估结果包括待模拟网络的防御能力，最后若所述防御能力不满足预设第一防御标准，则重新进行网络安全推演，通过接入半实物仿真系统，实现在网络仿真拓扑中引入了实物设备，能够对真实业务系统网络环境进行更准确的模拟，同时通过预设第一防御标准对防御能力进行评估，在防御能力不满足预设第一防御标准时重新进行网络安全推演，最终能够不断的提高防御能力以及找寻最佳的防护方案，为以后的网络安全推演提供参考。

[0091] 实施例四

[0092] 图4为本发明实施例四提供的一种网络安全推演装置的结构示意图，如图4所示，该装置可以包括：

[0093] 待模拟网络确定模块401，用于根据信息系统及数据交互业务确定待模拟网络；

[0094] 仿真系统接入模块402，用于基于待模拟网络链接网络元件，并接入半实物仿真系统；

[0095] 网络拓扑确定模块403，用于设定所得到的半实物仿真系统中与所述待模拟网络对应的节点、通信链路及网络的属性，得到网络仿真拓扑；

[0096] 网络安全推演模块404，用于在所述网络仿真拓扑上，根据预设虚拟网络攻击模型模拟网络攻击事件，进行网络安全推演，并得到评估结果。

[0097] 本实施例提供的技术方案，首先根据信息系统及数据交互业务确定待模拟网络，接着基于待模拟网络链接网络元件，并接入半实物仿真系统，然后设定所得到的半实物仿真系统中与待模拟网络对应的节点、通信链路及网络的属性，得到网络仿真拓扑，最后在网络仿真拓扑上，根据预设虚拟网络攻击模型模拟网络攻击事件，进行网络安全推演，并得到评估结果，通过接入半实物仿真系统，实现在网络仿真拓扑中引入了实物设备，能够对真实业务系统网络环境进行更准确的模拟，提高了网络安全推演过程的准确性。

[0098] 进一步的，上述仿真系统接入模块402，可以具体用于：

[0099] 通过接入虚拟机对至少一个网络元件的物理属性进行模拟；接入至少一个实体设备，所述至少一个实体设备用于针对网络攻击事件进行防护。

[0100] 进一步的，上述网络安全推演装置，还可以包括：

[0101] 攻击模型定义模块，用于定义预设虚拟网络攻击模型对应的攻击主机的数量、攻击位置及被攻击主机。

[0102] 进一步的，所述预设虚拟网络攻击模型对应的攻击方式包括以下至少一种：串行网络攻击、并行网络攻击及选择网络攻击。

[0103] 进一步的，上述网络安全推演模块404，可以具体包括：

[0104] 评估结果确定单元，用于根据预设虚拟网络攻击模型模拟网络攻击事件，针对所述网络攻击事件根据防御量化体系得到待模拟网络的评估结果，所述评估结果包括待模拟网络的防御能力；

[0105] 重新推演单元，用于若所述防御能力不满足预设第一防御标准，则重新进行网络安全推演。

[0106] 进一步的，上述评估结果确定单元，可以具体用于：

[0107] 根据预设虚拟网络攻击模型调用攻击策略库中对应的攻击策略模拟网络通过攻击主机对被攻击主机的攻击位置发起模拟攻击，调用防护策略库中对应的防护策略进行相应的防护，根据防御量化体系对防护结果进行量化，得到待模拟网络的第一防御能力。

[0108] 进一步的，上述网络安全推演模块404，还可以具体包括：

[0109] 防护单元，用于若所述第一防御能力不满足预设第二防御标准，则重新根据预设虚拟网络攻击模型调用攻击策略库中对应的攻击策略模拟网络通过攻击主机对被攻击主机的攻击位置发起模拟攻击，并利用防御模块中的防御策略和工具进行防护。

[0110] 本实施例提供的网络安全推演装置可适用于上述任意实施例提供的网络安全推演方法，具备相应的功能和有益效果。

[0111] 实施例五

[0112] 图5为本发明实施例五提供的一种计算机设备的结构示意图，如图5所示，该计算

机设备包括处理器501、存储装置502和通信装置503；计算机设备中处理器501的数量可以是一个或多个，图5中以一个处理器501为例；计算机设备中的处理器501、存储装置502和通信装置503可以通过总线或其他方式连接，图5中以通过总线连接为例。

[0113] 存储装置502作为一种计算机可读存储介质，可用于存储软件程序、计算机可执行程序以及模块，如本发明实施例中的网络安全推演方法对应的模块(例如，用于网络安全推演装置中的待模拟网络确定模块401、仿真系统接入模块402、网络拓扑确定模块403和网络安全推演模块404)。处理器501通过运行存储在存储装置502中的软件程序、指令以及模块，从而执行计算机设备的各种功能应用以及数据处理，即实现上述的网络安全推演方法。

[0114] 存储装置502可主要包括存储程序区和存储数据区，其中，存储程序区可存储操作系统、至少一个功能所需的应用程序；存储数据区可存储根据终端的使用所创建的数据等。此外，存储装置502可以包括高速随机存取存储器，还可以包括非易失性存储器，例如至少一个磁盘存储器件、闪存器件、或其他非易失性固态存储器件。在一些实例中，存储装置502可进一步包括相对于处理器501远程设置的存储器，这些远程存储器可以通过网络连接至计算机设备。上述网络的实例包括但不限于互联网、企业内部网、局域网、移动通信网及其组合。

[0115] 通信装置503，用于实现服务器之间的网络连接或者移动数据连接。

[0116] 本实施例提供的一种计算机设备可用于执行上述任意实施例提供的网络安全推演方法，具备相应的功能和有益效果。

[0117] 实施例六

[0118] 本发明实施例六还提供了一种计算机可读存储介质，其上存储有计算机程序，该程序被处理器执行时实现本发明任意实施例中的网络安全推演方法，该方法具体包括：

[0119] 根据信息系统及数据交互业务确定待模拟网络；

[0120] 基于待模拟网络链接网络元件，并接入半实物仿真系统；

[0121] 设定所得到的半实物仿真系统中与所述待模拟网络对应的节点、通信链路及网络的属性，得到网络仿真拓扑；

[0122] 在所述网络仿真拓扑上，根据预设虚拟网络攻击模型模拟网络攻击事件，进行网络安全推演，并得到评估结果。

[0123] 当然，本发明实施例所提供的一种包含计算机可执行指令的存储介质，其计算机可执行指令不限于如上所述的方法操作，还可以执行本发明任意实施例所提供的网络安全推演方法中的相关操作。

[0124] 通过以上关于实施方式的描述，所属领域的技术人员可以清楚地了解到，本发明可借助软件及必需的通用硬件来实现，当然也可以通过硬件实现，但很多情况下前者是更佳的实施方式。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品可以存储在计算机可读存储介质中，如计算机的软盘、只读存储器(Read-Only Memory，ROM)、随机存取存储器(Random Access Memory，RAM)、闪存(FLASH)、硬盘或光盘等，包括若干指令用以使得一台计算机设备(可以是个人计算机，服务器，或者网络设备等)执行本发明各个实施例所述的方法。

[0125] 值得注意的是，上述网络安全推演装置的实施例中，所包括的各个单元和模块只是按照功能逻辑进行划分的，但并不局限于上述的划分，只要能够实现相应的功能即可；另

外，各功能单元的具体名称也只是为了便于相互区分，并不用于限制本发明的保护范围。

[0126] 以上所述仅为本发明的优选实施例，并不用于限制本发明，对于本领域技术人员而言，本发明可以有各种改动和变化。凡在本发明的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

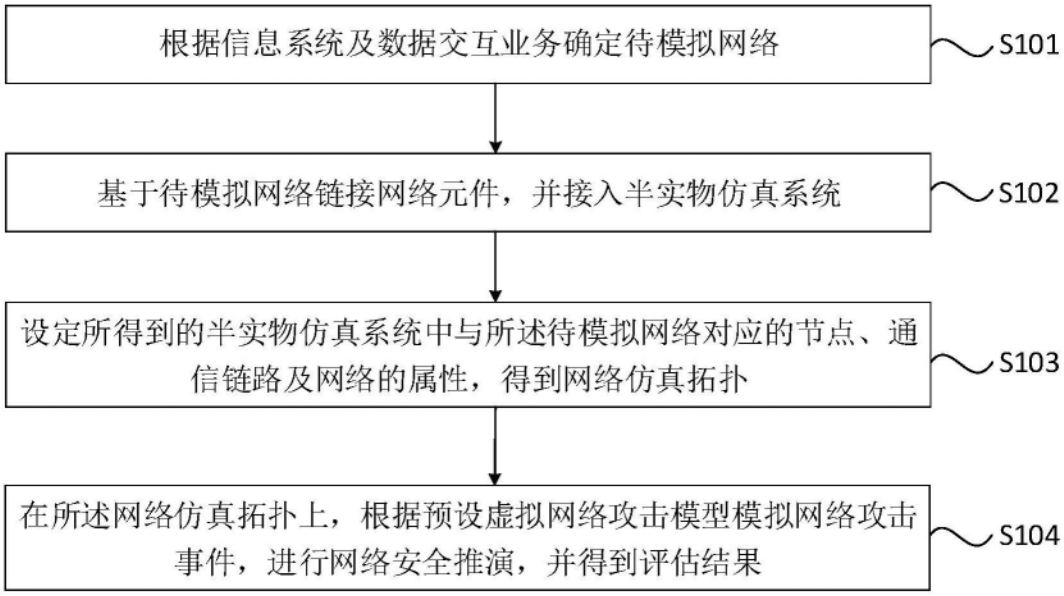

根据信息系统及数据交互业务确定待模拟网络
S101
基于待模拟网络链接网络元件，并接入半实物仿真系统
S102
设定所得到的半实物仿真系统中与所述待模拟网络对应的节点、通信链路及网络的属性，得到网络仿真拓扑
S103
在所述网络仿真拓扑上，根据预设虚拟网络攻击模型模拟网络攻击事件，进行网络安全推演，并得到评估结果
S104

图1

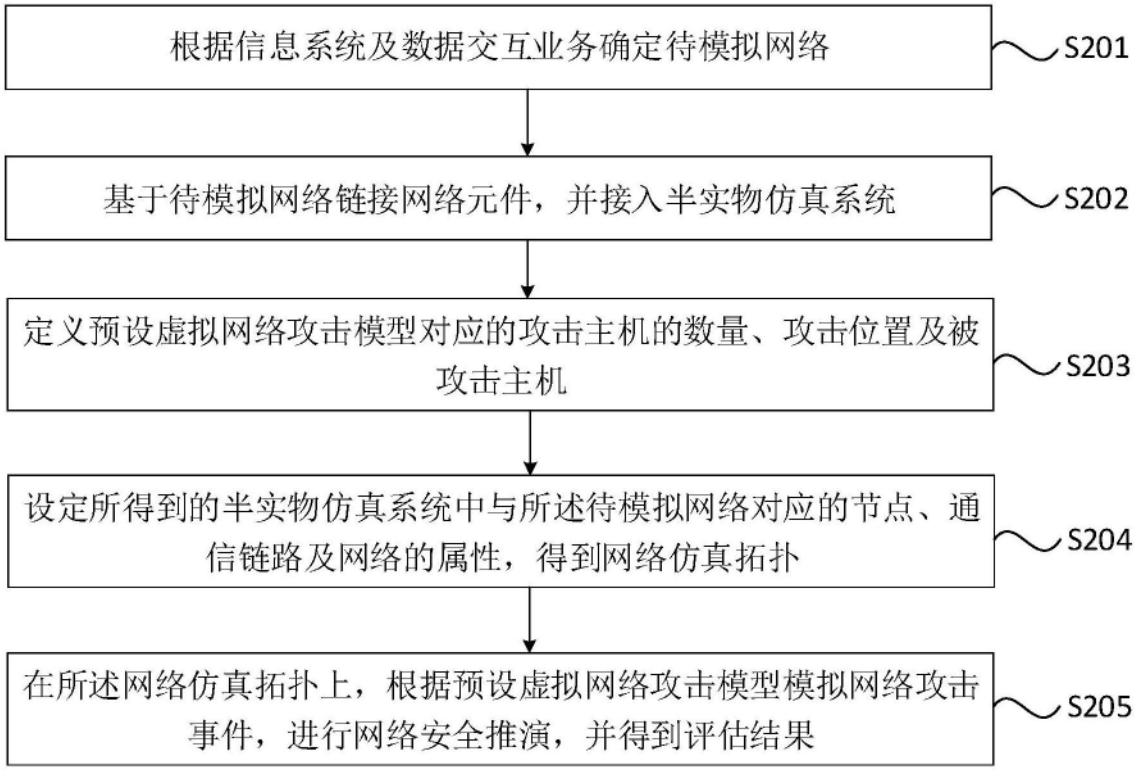

根据信息系统及数据交互业务确定待模拟网络
S201
基于待模拟网络链接网络元件，并接入半实物仿真系统
S202
定义预设虚拟网络攻击模型对应的攻击主机的数量、攻击位置及被攻击主机
S203
设定所得到的半实物仿真系统中与所述待模拟网络对应的节点、通信链路及网络的属性，得到网络仿真拓扑
S204
在所述网络仿真拓扑上，根据预设虚拟网络攻击模型模拟网络攻击事件，进行网络安全推演，并得到评估结果
S205

图2

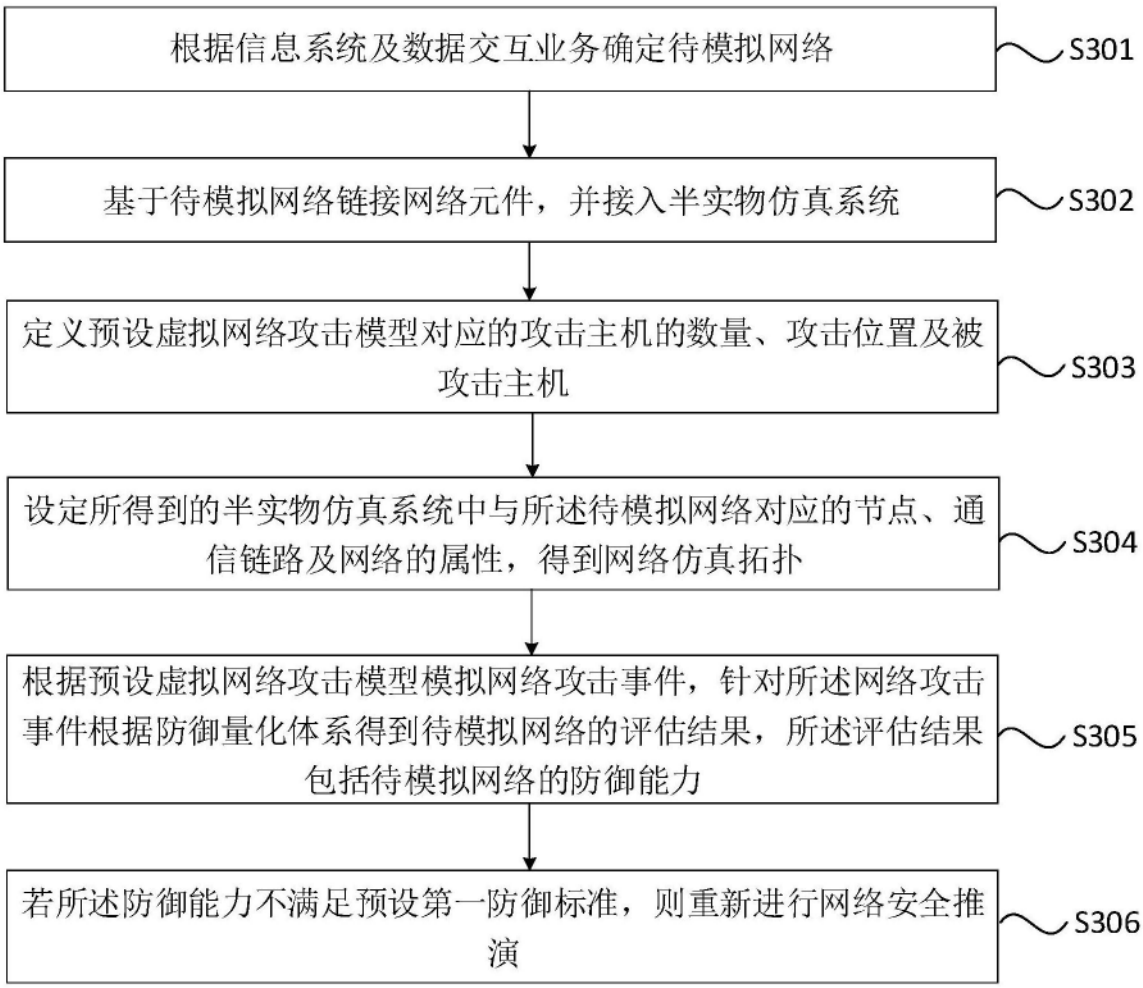

根据信息系统及数据交互业务确定待模拟网络
S301
基于待模拟网络链接网络元件，并接入半实物仿真系统
S302
定义预设虚拟网络攻击模型对应的攻击主机的数量、攻击位置及被攻击主机
S303
设定所得到的半实物仿真系统中与所述待模拟网络对应的节点、通信链路及网络的属性，得到网络仿真拓扑
S304
根据预设虚拟网络攻击模型模拟网络攻击事件，针对所述网络攻击事件根据防御量化体系得到待模拟网络的评估结果，所述评估结果包括待模拟网络的防御能力
S305
若所述防御能力不满足预设第一防御标准，则重新进行网络安全推演
S306

图3A

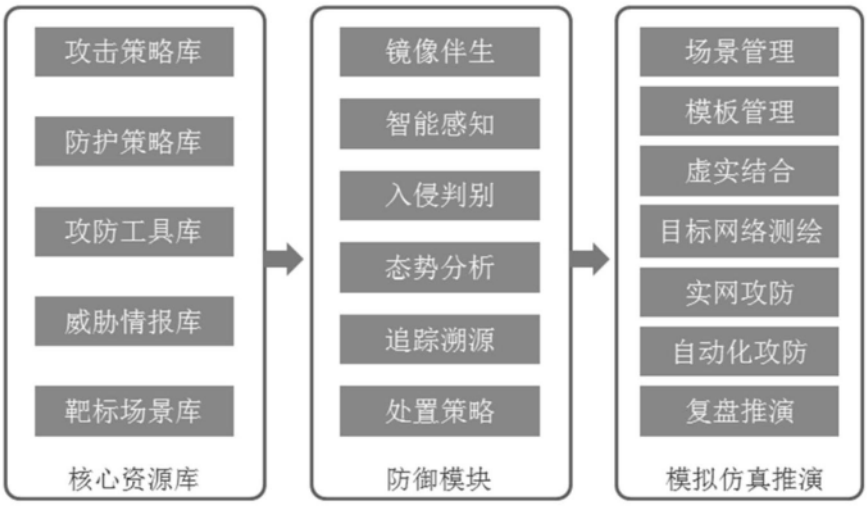

攻击策略库
防护策略库
攻防工具库
威胁情报库
靶标场景库
核心资源库
镜像伴生
智能感知
入侵判别
态势分析
追踪溯源
处置策略
防御模块
场景管理
模板管理
虚实结合
目标网络测绘
实网攻防
自动化攻防
复盘推演
模拟仿真推演

图3B

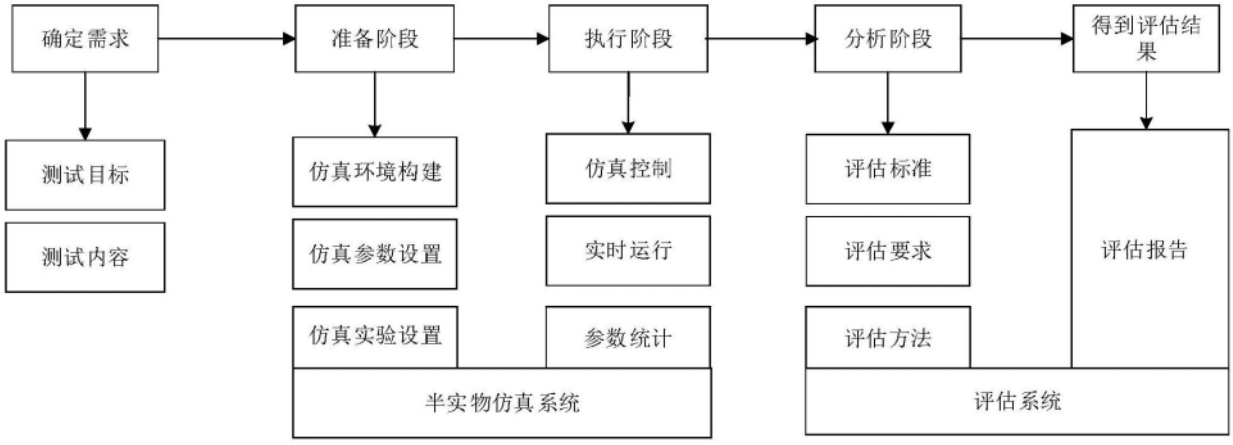

确定需求
准备阶段
执行阶段
分析阶段
得到评估结果
测试目标
测试内容
仿真环境构建
仿真参数设置
仿真实验设置
仿真控制
实时运行
参数统计
评估标准
评估要求
评估方法
评估报告
半实物仿真系统
评估系统

图3C

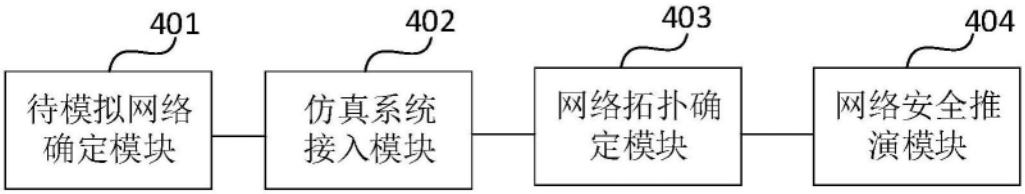

401
待模拟网络确定模块
402
仿真系统接入模块
403
网络拓扑确定模块
404
网络安全推演模块

图4

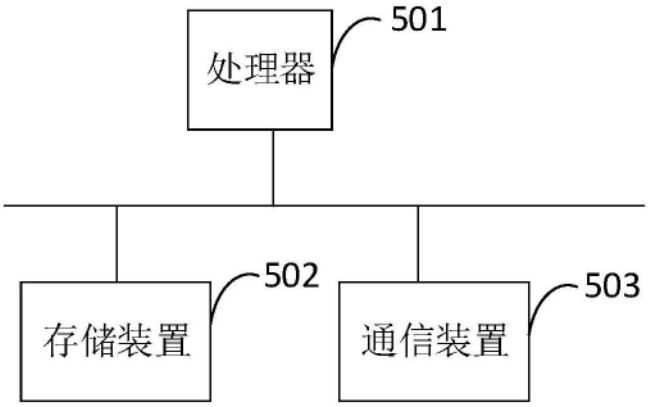

501
处理器
502
存储装置
503
通信装置

图5