# 拟态防御

## 背景

传统的网络安全防御思想是在现有网络基础架构的基础上建立包括防火墙和安全网关、安全路由器 / 交换机、入侵检测、病毒查杀、用户认证、访问控制、数据加密技术、安全评估与控制、可信计算、分级保护等多层次的防御体系，通过不同类型传统安全技术的综应用来提升网络及其应用的安全性。但近年来不断被披露的国内外网络安全事件及由此带来的严重后果也逐渐暴露了传统的网络安全防御技术存在的问题。为此，突破依赖于对网络攻击先验知识的静态、被动式的防御技术的局限，提出网络安全动态防御的创新思路，研究新型网络安全架构的基础理论与关键技术已成为网络安全领域的重要研究方向。

## 国内外相关研究技术成果

### 移动目标防御（MTD）技术

MTD 技术是美国近年来提出的网络空间“改变游戏规则”的革命性技术之一，其构建、评价和部署机制及策略是多样的、不断变化的。这种不断变化的思路可以增加攻击者的攻击难度及代价，有效限制脆弱性暴露及被攻击的机会，提高系统的弹性。在理论研究上，2014 年 Zhuang 等提出一个初步的理论来回答 MTD 的有效性问题，并讨论了 MTD 系统的关键概念和基本性质，提出了MTD 熵假设，即系统配置的熵越大，则该系统就越有效。

移动目标防御技术包括 IP 地址可变、通道数可变、路由和 IP 安全协议（IPSec）信道可变、网络和主机身份的随机性、执行代码的随机性、地址空间的随机性、指令集合的随机性、数据的随机性等。也就是说，移动目标防御能够自动改变一个或多个系统属性，从而使系统攻击表面对攻击者而言是不可预测的。

移动目标防御技术的策略就是致力于构建一种动态的、异构的、不确定的网络来极大增加攻击者的攻击难度，意图通过增加系统的随机性或减少系统的可预见性来对抗同类攻击。在部署、运行网络和系统时，通过有效降低其确定性、相似性和静态性来显著增加攻击成本。该类技术实际上是用通信的方法来解决安全问题。它不再单纯依靠安全系统本身的复杂度进行目标保护，而是还要充分利用目标所处的时间、空间和物理环境复杂性进行保护，从而大大增加攻击难度。变形网络技术。

近几年，移动目标防御技术已取得很多新进展，包括变形网络、自适应计算机网络、自清洗网络，以及移动目标 IPv6 防御、开放流随机主机转换技术等研究。

#### 变形网络技术

2012 年 8 月，美陆军授予雷声公司价值 310 万美 元 的 “ 限 制 敌 方 侦 察 的 变 形 网 络 设 施 ”（MORPHINATOR）项目，为其研制具有“变形”能力的计算机网络原型机，该项目主要研究在敌方无法探测和预知的情况下，网络管理员有目的的对网络、主机和应用程序进行动态调整和配置，从而预防、延迟或制止网络攻击。

#### 自适应计算机网络

2012 年 5 月，美国堪萨斯州大学开始为美空军科学研究办公室研究“自适应计算机网络”，重点研究和量化移动目标防御对计算机网络的影响。将研究计算机网络通过自动改变自身设置和结构来对抗在线攻击的可行性，并开发有效的分析模型，以确定移动目标防御系统的有效性。

#### 自清洗网络

自清洗入侵容忍（SCIT）体系结构可以通过不断清洗服务器以及不断变换个人服务器准则来阻挡或限制网络攻击。这实际就是移动目标防御技术的一种应用。目前已取得多项研究成成果。

#### 移动目标 IPv6 防御

移动目标 IPv6 防御（MT6D）提出了移动目标IPv6 防御的新思路。通过重复转动发送和接收者的地址来实现对用户隐私和目标网络的保护。研究结果表明，MT6D 不但是可行性的，而且还能与新的IPv6 地址无缝绑定。同时 MT6D 能够为平台和应用层提供一种有力的移动目标解决方案

#### 开放流随机主机转换（OFRHM）技术

开放流随机主机转换（OFRHM）技术就是利用开放流研究移动目标防御体系结构，实现 IP 地址的不可预知性及高速变换，同时保持配置的完整性，并最小化操作管理。研究结果表明 OFRHM 能够有效防御秘密扫描、蠕虫传播以及其他基于扫描的攻击。

移动目标防御不是直接被动对抗网络攻击行为本身[5-6]，而是预先对抗构成攻击行为的各种准备活动。它并不单纯依靠额外固定附加的安全机制，而主要通过随机调动信息系统本身原有资源的冗余性、异构性和空间分布性来构成安全机制，从而大大提高了系统的弹性。因此，移动目标防御技术的优势非常明显，它不再单纯依靠安全系统本身的复杂度进行目标保护，而是还要充分利用目标所处的时间、空间和物理环境复杂性进行保护，大大增加了攻击难度。应该说，移动目标防御要比传统安全系统更上一层楼。

### 端信息跳变技术

端信息跳变技术是指在端到端的数据传输中通信双方或一方按协定伪随机地改变端口、地址、时隙、加密算法甚至协议等端信息，从而破坏敌方的攻击与干扰，实现主动网络防护。

基于端信息跳变的主动网络防护模型包括预警分析、协同控制、端信息管理和任务切换 4 个模块以及众多任务机群。预警分析模块负责对当前网络遭受的攻击进行信息收集分析；协同控制模块是整个系统的核心，协调各模块实现网络防御；端信息管理模块用于伪随机地产生端信息跳变图案；任务切换模块则按照协同控制模块的指令进行干扰、通信、蜜罐等任务转换，实现协同防御。研究结果表明，相比于传统的网络防护技术，端信息跳变具有抗攻击性强、主动性、抗截获性、性能增量性等优势。

定义端信息（为由地址、端口、跳变时隙、加密算法、协议（功能角信息组成的多元组，。其中，地址和端口是网络传输所必须的两大信息，决定着数据包在网络上的传输方式和传输路径（在环境下，地址指的是地址，端口指的是网络端口号；跳变时隙是端信息跳变自适应模块的重要信息，决定着服务性能和安全性能；协议指的是传输层的协议类型（、等；功能角色是指任务机群的角色类型（服务主机或蜜耀主机。

定义端信息跳变为由端信息状态空间、生成函数、跳变条件和伪随机序列组成的多元组，可以表示为。其中，端信息状态空间是指端信息可能处于的所有状态集合，一般情况下，在地址和端口确定的情况下，端信息状态空间是一个有限集合，有；生成函数定着端信息的生成方式以及可能的取值；跳变条件定着端信息的起始时间和生命周期；伪随机序列为生成函数提供了伪随机的生成因子。在任意时刻，可以通过计算出该时刻的通信端信。

#### 端信息跳变攻击技术

在已知的网络攻击手段中所采用的端信息跳变技术几乎涵盖了端信息跳变的所有实现形式，包括变端口木马、反弹端口木马、跳代理、协议转换攻击、跳加密方法攻击、时隙跳变、混合跳变等。

变端口木马。是传统木马程序的变种，由于防火墙对常见的木马端口进行了封杀，导致使用固定端口的木马程序无法连通黑客主机，于是它通过简单地改变木马程序所使用的通信端口，从而达到突破防火墙的封锁的目的。

反弹端口木马。与普通的木马程序不同，反弹端口木马的端口是随机的，由受感染的主机主动向黑客主机发起网络连接，并且伪装为数据流量，而不是向传统木马那样由黑客主机主动发起，因为防火墙一般对内部外连的数据流量不做过多的检测分析。显然，这种端口随机的反弹端口木马对于穿透防火墙十分有效。

跳代理。是十分有效的攻击隐藏技术，黑客通过一系列的代理主机转发攻击流量，每一个代理都有独立的地址，每一次转发都经过隐藏处理，使受害者难以追踪真正的攻击者。从代理主机的拓扑结构看，可以将跳代理划分为广度跳代理技术和深度跳代理技术两种基本类型。在前者情况下，攻击者在不同的时间或跳变时隙使用不同的代理服务器进行流量转发，如图所示；而后者则通过多次级联使用代理服务器向受害者发起网络攻击，如图所示。

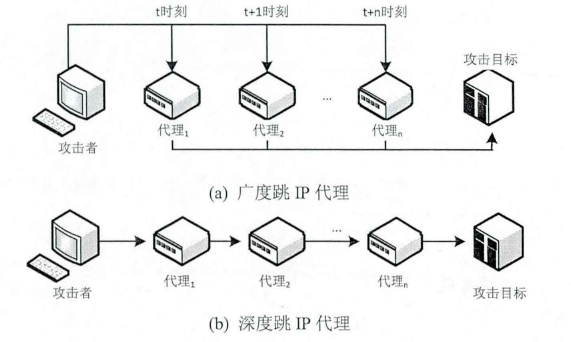


Figure 1跳IP攻击示意图

协议转换攻击。它是一种网络攻击的隐藏手段，通常攻击者可以利用协议中的某些特性进行攻击流量的协议转换，如异常流量处理机制等，当路由器收到一个未知地址的数据包，它会返回一个网络层的数据包给数据包的源地址，告知目的网络不可达。攻击者就可以利用这种特性向受害者发起网络攻击，如图所示。

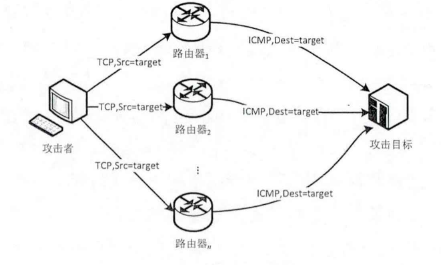


Figure 2协议转换攻击

跳加密方法。是攻击者为了防止网络监管人员破译其对网络肉鸡的控制指令，而进行的动态加密过程，能够有效地躲避监听和追踪。这种跳加密的方法一般包括加密种子跳变和加密算法跳变等两种方式。

混合跳变攻击。以上所讲述的跳变攻击类型都是端信息跳变攻击的拔本实现形式，而基于多种跳变形式的泡合跳变己经出现并取得了显著的攻击效果，值得网络防护人的髙度重视，如种傻端、地址、协议、加密方法身利用代理跳板（混合跳变攻击技术。它将攻击的数据包转化为数据包成功突破的端口封锁，并可以多个中间代理跳板，每一级代理加密的方式进行数掘传输和指令传达。

#### 端信息跳变防御技术

虚实交枝的跳变攻击提高了黑客们的攻效而作为一种对抗策略，如见被合理利用，也能够有效提升御方的防护能力。近年來出现了用于端跳变的主动防护技术、以及基于端口跳变和地地跳变的隐蔽通信技术。

有研究对基于端跳变的攻防 dos行了研究，将网络通信时划分为等问隔的离散时隙，网络服务的端口由时隙、密钥和成生函数决定。可信用户利用合法授权的方式获得密钥，而攻攻击者无法获得，以致无法锁定攻击的目标端口。

由研究同样利用端口跳变进行网络通信，在通过随机变换的通信端抵御攻击和截获攻。为了实现服务器与客户端之间的端口同步，文献利用通信过程已经成功确认的ACK报文微微端口生成函数的一个个因子结合共享的密钥，生成通信端口。

在美国军方的APOD了基于端口和地址的混合跳变研究，提出了基于虚假端口地址的抗端口扫描和抗攻击的网络防护方法。该方法中服务器的端口和地址并不跳变，而是在通信过程中使用虚假的端口和地址，从而迷惑攻击者。该方法提出了两个重要的概念，分别包括跳变代理和网关。跳变代理部署在客户端的前端，用于解析客户端的网络请求并进行虚假地址替换；而网关部署在服务器的前端，对客户端的网络请求进行逆向替换，转化为点到点的请求。

### 拟态式蜜罐动态博弈模型

拟态式蜜罐是指在传统蜜罐网络基础上通过综合运用模拟服务环境的保护色机制和模拟蜜罐特征的警戒色机制进行拟态演化和对抗博弈，以有效迷惑和诱骗攻击者，实现网络对抗。保护色指蜜罐在硬件、软件、数据、服务信息等方面模仿周边服务器和网络环境的特征，使得攻击者难以识别蜜罐的存在；而警戒色指服务器在硬件、软件或数据等方面模仿蜜罐特征，使得攻击者将该系统认作蜜罐而躲避攻击。蜜罐防护是防御者和攻击者参与的理性、非合作的诱骗过程，攻防双方策略相互依存，都期望保护自身信息并获得对方信息以获得收益最大化，因而构成了非合作不完全信息动态博弈。从不同局中人视角来看，博弈对手具有不同的类型。在攻击者视角中，博弈对手不再是只有“真实服务”这一单一服务类型，而是增加了“蜜罐和“伪蜜罐”这两种欺骗服务类型；从防御者视角来看，博弈对手有合法用户和攻击者两种不同类型的来访者。给定攻防双方收益矩阵，根据攻击者是否知晓伪蜜罐的存在，可分析确定出双方策略到达贝叶斯纳什均衡的条件。

文献［８］将遗传算法应用到入侵检测系统中，用于获得入侵检测的分类规则集，并使用主成分分析的方法识别网络连接的最重要特征．文献［９］则利用遗传算法优化并生成入侵检测系统的规则集，分析网络信息的编码和遗传算法的参数设置问题．文献［１０］将蜜罐与入侵检测系统相结合，利用遗传算法分析 Ｈｏｎｅｙｄ收集的网络流量，优化攻击者的特征规则，为入侵检测提供了辅助决策．文献［１１］针对恶意软件开展研究，防御者利用遗传算法演化恶意软件的特征，预测僵尸网络存活机制，从而对未知的恶意软件具有更好的预防效果．文献［１２］人则提出了一种基于遗传算法的最优决策树策略用于恶意软件检测，将遗传算法和决策树相结合，构建了反恶意软件分类器．文献［１３］提出了一种基于遗传算法的混合蜜罐系统，采用签名的方法来进行攻击特征规则优化，并且引入高、低交互蜜罐，提高了整个蜜罐系统对攻击者的迷惑性．文献［１４］也提出了基于遗传算法的蜜罐系统，对蜜罐收集到的攻击者相关信息建立信任度，并基于信任度指导遗传算法进行优化，生成新的入侵检测规则，辅助检测平台分流．文献［１５］中通过遗传算法改进蜜网的动态负载均衡，构建了最小通信开销的动态负载均衡模型，利用遗传算法获得了更小通信开销的负载分配方案，相对贪心算法能进一步减少蜜网动态负载均衡中负载迁移次数，降低额外通信开销．

#### 拟态蜜罐演化策略

在拟态蜜罐系统中，蜜罐演化的目标是提高蜜罐的诱骗度，吸引更多攻击者；而伪蜜罐演化的目标则是为了模拟蜜罐吓退攻击者．拟态蜜罐系统演化框架包括拟态感知、服务特征库、拟态服务和拟态演化四个功能单元，其演化策略流程如图所示．

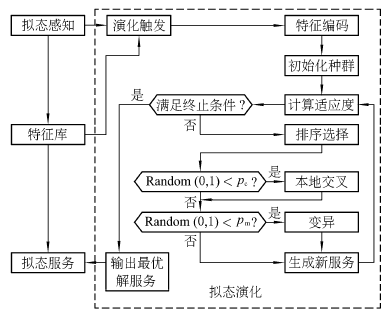


Figure 3拟态演化策略

拟态感知模块通过主动交互和被动扫描的方式获取当前网络环境信息和服务信息；特征库模块是服务或蜜罐形式化构建的特征集合；拟态服务模块则依据特 征库中服务和蜜罐特征进行罐／伪蜜罐服务的 模 拟．拟态 演化 模 块 是 核 心 模块，完成蜜罐／伪蜜罐服务的演化，主要包括了演化触发和演化算法模块．前者用于检测蜜罐或服务器网络流量，判定是否进行蜜罐或服务的演化；后者则主要依据蜜罐／伪蜜罐针对攻击者收益设计的目标函数，指导遗传算子对编码后的服务特征向量进行交叉、变异等操作，产生具有较高适应度的新一代蜜罐服务特征，从而提高拟态蜜罐的自适应度．演化算法中，当产生的（０，１）之间的随机数 Ｒａｎｄｏｍ（０，１）小于交叉概率 ｐｃ时，进行本地交叉运算；而当随机数小于变异概率ｐｍ时，启动变异运算．经过交叉、变异等运算后，系统演化产生新的服务

#### 特征编码

服务特征编码．一般而言，服务是包含若干服务操作的集合．简化起见，本文中的服务仅表示服务的一个操作，服务的输入输出参数对应确定的对象．为定义适合编码的特征向量，将服务用一个四元组描述：

Ｓ ＝ ｛Ｉｎｐｕｔ，Ｏｕｔｐｕｔ，Ｄｅｓｃｒｉｐｔｉｏｎ，ＱｏＳ｝，式中：Ｉｎｐｕｔ为输入参数集合，主要分为｛Ｉｃ，Ｉｔ｝，即请求输入内容和输入类型；Ｏｕｔｐｕｔ为输出参数集合，主要分为｛Ｏｃ，Ｏｔ｝，即响应输出内容和输出类型；Ｄｅｓｃｒｉｐｔｉｏｎ＝｛Ｄｉ｜ｉ＝１，２，…，ｎ服务所拥有变量集合｝，即服务功能和基本描述．这里，服务功能表示服务功能命令参数集合，服务基本描述则主要包括服务ＩＰ地址、端口号、服务类型、采用协议类型、服 务 版本等；ＱｏＳ 代表 服务的一组服务质量，常规服务的 ＱｏＳ一般包括服务响应时间、服务费用、服务可靠性等．蜜罐特征编码．拟态蜜罐中，服务者可以伪装为蜜罐特征从而迷惑攻击者．这些蜜罐特征主要有模拟 Ｈｏｎｅｙｄ 畸 形ＩＰ 包 响 应、修 改 ＮｅｔＢＩＯＳ的应答、模拟 Ｓｅｂｅｋ特征等．此外，由于当前大部分攻击者只针对流行热点应用开展攻击，因此伪蜜罐主机也可以伪装成某些垃圾或过时的服务，达到诱骗和躲避攻击者的目的．

## 待解决的问题和后续研究

1、网络脆弱节点拟态防御

路由器在网络中的位置和路由转发功能决定了它将是攻击者实施攻击的一个极佳切入点。路由器一旦被攻击者控制, 将会对整个网络产生难以估量的危害。针对主机的攻击, 主要危害的是主机自身, 而针对路由器的安全攻击, 危害的则是与路由器相连接的整个网络, 其危害远远超过针对主机的攻击。通过路由器可以方便地获取用户隐私数据、监控用户上网行为、获取账户密码信息、篡改关键用户数据、推送传播虚假信息、扰乱网络数据流向、瘫痪网络信息交互、直接发起网络攻击等等。 路由器的安全威胁, 国产品牌主要来自两个方面: 一是系统设计与实现中的漏洞无法避免, 二是使用开源代码无意识带入的陷门。对国外品牌而言, 漏洞同样无法避免, 更重要的是, 外国政府为实现战略意图植入的后门。因此, 漏洞和后门等带来的不确定威胁是路由器安全的头号大敌。

研究提出了一种基于动态异构冗余机制(Dynamic Heterogeneous Redundancy, DHR)的网络脆弱节点拟态防御体系结构

## 技术方向

### 基于DHR的网络脆弱节点拟态防御架构

研究动态异构冗余结构，内含移动目标防御机制, 是一种主动防御模型, 可以有效的应对已知和未知的安全威胁。

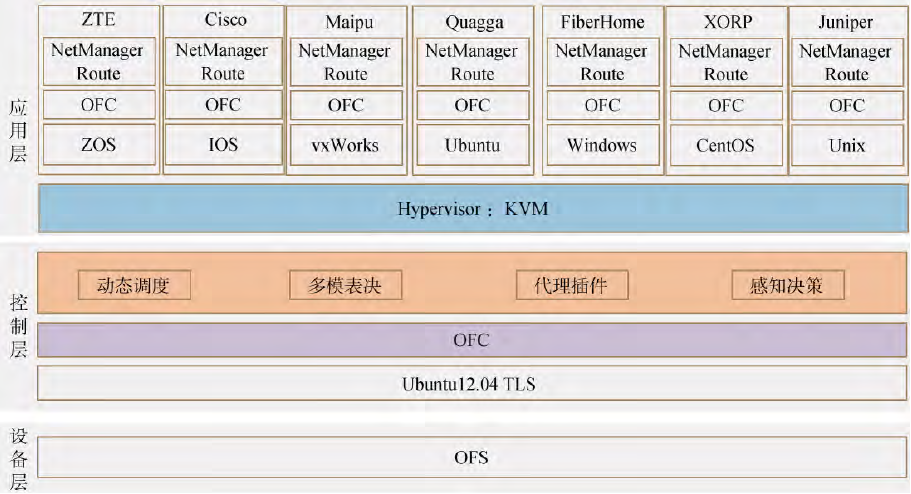
异构性: 异构性即功能等价的两个执行体结构组成不相同, 描述的是两个执行体之间的差异性, 这种差异性可以保证同样的攻击不会同时使两个执行体同时失效, 当然不包含针对功能原理的攻击。功能执行体的漏洞和后门具有独特性一种攻击方法只会对一种功能执行体发生作用。DHR模型通过引入多个异构功能执行体, 并行对输入的攻击消息进行处理,进而对威胁进行感知, 并针对威胁做更一步处理。

冗余性: 冗余性是指工作集的异构并行执行体的多样化。直观上认为, 冗余性可以支持表决结果的正确性。通过增加异构执行体工作集中的执行体的数量, 可以明显提升威胁感知的准确率, 同时也为动态性提供支撑。

动态性: 动态性是指在不同时刻下轮换对外呈现的工作执行体, 是一种主动防御手段。

### 技术路线

#### 应用层异构体搭建



应用层采用虚拟化技术和实体设备搭建异构执行体。该分层结构实际上就是在传统的路由器结构基础上, 在 OFS 和 OFC 之间引入了实现 DHR 功能所需的相关模块, 并在 Controller 层面引入多个异构执行体。设备层与控制层采用标准 Openflow 接口, 建立一个 Openflow 通道; 控制层与应用也采用标准的 Openflow 接口, 每一个功能执行体分别与控制层建立独立的 Openflow 通道。对于 OFS 而言, 它连接控制层的控制器, 由控制层对 OFS 进行配置管理。对于应用层而言, 每一个功能执行体分别视控制层为一台 OFS, 并对其进行配置与管理。

异构执行体要求提供标准的 Openflow 接口, 在控制器上运行各种路由协议和管理协议。

#### 拟态插件集开发

拟态插件集中代理插件单元作为功能执行体和外部路由器之间通信的关口, 需要对进出执行体的消息进行操作。这些消息包括各个层面的消息, 例如IP 层的 OSPF、ISIS, 传输层 TCP、UDP 以及应用的BGP、RIP、FTP、SNMP 等。每一种协议都有自己的状态机, 简单的复制分发可能导致各个执行体的相应协议无法正确运行。同时, 还要考虑执行体的切换以及上下线过程中的状态恢复、数据同步等对各个协议状态机的影响。

可以依托工业协议的分析能力，提供更多的协议状态机分开能力