基于 POF 的网络窃听攻击移动目标防御方法

马多贺[1]，李琼[2]，林东岱[1]

（1. 中国科学院信息工程研究所信息安全国家重点实验室，北京 100093；
2. 哈尔滨工业大学计算机学院信息对抗技术研究所，黑龙江 哈尔滨 150001）

摘 要：网络窃听攻击是网络通信安全的重大威胁，它具有隐蔽性和无干扰性的特点，很难通过传统的流量特征识别的被动防御方法检测到。而现有的路径加密和动态地址等方法只能混淆网络协议的部分字段，不能形成全面的防护。提出一种基于协议无感知转发（POF, protocol-oblivious forwarding）技术的移动目标防御（MTD, moving target defense）方法，通过私有协议分组随机化策略和动态路径欺骗分组随机丢弃策略，大大提高攻击者实施网络窃听的难度，保障网络通信过程的隐私性。通过实验验证和理论分析证明了该方法的有效性。

关键词：移动目标防御；窃听攻击；协议栈随机化；网络空间欺骗；协议无感知转发

中图分类号：TP393

文献标识码：A

doi: 10.11959/j.issn.1000-436x.2018025

Moving target defense against network eavesdropping attack using POF

MA Duohe[1], LI Qiong[2], LIN Dongdai[1]

1. State Key Laboratory of Information Security, Institute of Information Engineering, CAS, Beijing 100093, China
2. Institute of Information Countermeasure Techniques, School of Computer Science and Technology, Harbin Institute of Technology, Harbin 150001, China

Abstract: Eavesdropping attack hereby was the major attack for traditional network communication. As this kind of attacks was stealthy and untraceable, it was barely detectable for those feature detection or static configuration based passive defense approaches. Since existing encryption or dynamic address methods could only confuse part of fields of network protocols, they couldn't form a comprehensive protection. Therefore a moving target defense method by utilizing the protocol customization ability of protocol-oblivious forwarding (POF) was proposed, through private protocol packet randomization strategy and randomly drop deception-packets on dynamic paths strategy. It could greatly increase the difficulty of implementing network eavesdropping attack and protect the privacy of the network communication process. Experiments and compare studies show its efficiency.

Key words: moving target defense, eavesdropping attack, protocol randomization, cyber space deception, protocol-oblivious forwarding

1 引言

网络窃听[1,2]已经成为黑客实施网络攻击的重要步骤和手段。网络窃听的攻击者通过镜像流量、数据复制等方式截获网络数据，再利用网络分析软件对数据进行解析，从而获取通信双方的位置信息

收稿日期：2017-07-01；**修回日期**：2017-12-10

通信作者：李琼，qiongli@hit.edu.cn

基金项目：国家重点研发计划课题基金资助项目（No.2017YFB1010000）；国家高技术研究发展计划（“863”计划）基金资助项目（No.2015AA016106）；中国科学院信息工程研究所“青年之星”计划基金资助项目（No.Y7Z0201105）；国家自然科学基金资助项目（No.61471141）；深圳市技术攻关基金资助项目（No.JSGG20160427185010977）

Foundation Items: The National Key Research and Development Program of China (No.2017YFB1010000), The National High Technology Research and Development Program of China (863 Program) (No.2015AA016106), “Young Scientist Program” of Institute of Information Engineering CAS (No.Y7Z0201105), The National Natural Science Foundation of China (No.61471141), The Key Technology Program of Shenzhen (No.JSGG20160427185010977)

以及通信的内容。当前，wireshark等多种软件已经能够对各种标准协议进行全分组分解，甚至加密数据分组仍然能够通过流量统计分析手段进行猜测和逆向得到部分位置信息。由于该类攻击手段具有隐蔽性和无干扰性的特点，传统网络安全设备无法通过流特征检测攻击。

通常情况下，网络传输采用标准协议，在通信过程中传输路径也相对固定，攻击者很容易截获数据分组并重组和恢复数据分组的内容，达到窃取隐私数据[3,4]或篡改数据分组以便构造中间人（man-in-the-middle）攻击[5,6]、DDoS等其他攻击的目的。在无线网络中，由于无线信号不受物理限制，攻击者部署装置以接收信号进行网络窃听相对容易，因此，无线网络安全性受到极大威胁。网络窃听攻击利用现有网络通信过程中网络协议和传输路径不变的弱点，在网络传输路径上实施数据分组抓取的窃听攻击或入侵网络传输节点，从传输设备内部进行内存读取、数据分组捕获[5]。因此，静态的网络配置是造成网络攻击者能够成功实施窃听攻击的根本原因，为黑客实施网络窃听攻击带来了便利。

目前，针对网络窃听攻击的防御研究主要分为被动防御和主动防御。被动防御方法包括网络隔离和数据加密。VLAN等网络隔离技术[7,8]限制网络广播分组的传播范围，能够在一定程度上抵御网络窃听攻击，然而该方法对于同一个子网内的窃听攻击者是无效的。VPN等隧道加密技术、SSL等端到端的加密技术对传输数据的负载部分进行了加密，但无法抵御内部攻击[1]，同时无法抵御基于统计的流量追踪攻击[3]。在无线网络防窃听攻击方面，由于无线中继设备本身就具有协议协商和路径调度的机制，因此，研究者能够在无线传输协商过程中间提出新的安全调度策略和新的安全增强的加密协议。这些方法易于实施和验证，被学术界广泛研究，其中，随机网络线性编码（RLNC）方法以及加密的随机网络线性编码是最为常用的方法。但是网络编码只保护网络传输的数据字段，对数据分组头部没有保护。这些被动防御方法也没有改变网络传输过程中的配置静态性问题，攻击者能够获取到加密隧道的数据分组，并且能够对加密数据分组进行基于统计特征和协议分析等逆向攻击，以获取“源—目的”通信流对[9]，得到通信双方的位置信息。为了解决被动防御手段的不足，主动防御方法被研究者相继提出，其中，移动目标防御[10]不依赖于攻击检测，成为网络安全研究的新方向。

MTD是一种主动防御技术，它通过多样的、动态改变的构建部署机制及策略来增加攻击者的攻击难度和代价，有效限制漏洞暴露和被攻击者利用的机会[11,12]。网络MTD的核心思想和改变保护目标网络属性来转移攻击面，以提高攻击的难度和增加攻击成本的方式使攻击者放弃攻击。但是现有网络MTD技术仍然受标准协议[13~15]和静态路径的制约[16~18]，攻击面转换空间有限。

软件定义网络（SDN, software defined networking）[19]的发展以及协议无感知转发[20]技术的出现，打破了以往传统网络中静态标准协议的固有模式，给解决针对传统网络协议分析的安全防御问题带来新的思路。

本文提出一种基于POF的移动目标防御方法，实现不可信网络环境中明文数据分组的安全传输。该方法利用POF的协议定制能力实现网络通信会话的传输协议和传输路径随时间不断变换，同时在传输过程中混入网络欺骗分组，从而增加窃听者捕获、重组通信会话真实信息的难度，达到网络通信过程中隐私保护的目的。

本文的主要贡献包括如下 3 个方面。

1) 提出一种基于POF的抗网络窃听攻击移动目标防御机制（POFMTD），在POFMTD机制中提出从窃听攻击的网络协议、传输路径、网络分组和消息内容 4 个属性进行移动攻击面动态转换，提高窃听攻击实施的代价，实现对网络数据传输过程的保护。

2) 将窃听防御的攻击面转换维度从载体协议、环境路径扩展到内容本身，引入了虚假网络分组传输的欺骗防御策略。通过不同的私有协议将消息分组和欺骗分组随机化封装，提高攻击者辨别截获数据真实性的难度，降低重组会话消息的概率。

3) 提出路径随机化和欺骗分组随机丢弃方法，对不同私有协议的传输路径进行动态随机化，减小局部攻击中攻击者截获全部会话消息数据分组的概率；在动态路径中进行欺骗分组的随机丢弃，保障混淆消息内容的同时，接收端对欺骗无感知。

2 网络窃听威胁模型和相关背景

2.1 威胁模型

网络通信过程中的窃听攻击按照不同的标准

可以划分为不同的类型[1]，同时也可以按照攻击的位置来划分，如针对路由路径的攻击或针对网络设备节点的攻击。按照攻击的范围，网络窃听攻击可以分为局部攻击和全局攻击。而节点都在一条或多条传输路径上，因此，可以用入侵路径的多少来计算窃听攻击的范围。如果攻击者能够窃听通信之间的所有路径，则为全局攻击；如果攻击者只窃听通信中的部分路径，则为局部攻击。按照攻击的危害性，网络窃听攻击可以分为会话消息攻击和数据分组攻击。本文主要按照攻击危害性的威胁模型来进行安全性分析。

2.1.1　网络窃听攻击杀伤链

攻击杀伤链是对攻击过程和关键步骤的抽象。在网络窃听攻击中，主要包含 4 个层次：1) 通过搭线、流量镜像等方式入侵网络路径；2) 复制网络数据分组，而非阻断数据分组，这与其他主动攻击不同；3) 由获取的数据分组进行网络协议解析，提取分组头或负载；4) 重组负载数据，还原会话消息内容。在进行网络窃听攻击防御时，主要目标是切断这 4 个杀伤链中的一个或多个。

2.1.2　网络窃听攻击类型

1) 会话消息攻击。攻击者窃听某个通信过程中的所有数据分组，通过数据分组逆向分析，将所获得的所有数据分组按照网络协议进行重组、解析，从而获得完整的会话信息[21]。该类攻击的前提是攻击者能够窃听通信双方的所有传输路径，且能够逆向分析通信双方所使用的所有网络协议。这是一种全局窃听攻击。

2) 数据分组攻击。攻击者不需要窃取完整的会话数据分组，针对单数据分组或少量数据分组即可完成攻击。该类攻击包含多种形式，例如，对数据分组的分组头进行分析，以追踪通信双方的源—目的地址；或对数据分组进行计数、时间统计或*TTL*分析等，以得出数据流，进而获取源—目的地址对。该类攻击不需要路由固定，也不要求一定能解密数据负载，只需要知道标准网络协议，并可解析数据分组头部。由该分析的结果，为进一步的DDoS攻击、重放攻击、MITM[22]攻击做好准备。该类窃听攻击属于局部窃听攻击，只需要窃听部分节点或链路。

从图 1 的网络窃听威胁模型和杀伤链可知，会话消息攻击相比数据分组攻击理论杀伤链更完整，在窃听路径、捕获数据分组数量、协议解析的深度等方面参数向量维度更多。图 1 中以*N*、*M*、*W*表示多次攻击，1 表示单次攻击，0 表示攻击无关。在现有的网络通信环境下，路径数和协议数基本上都是单一固定的，这大大降低了窃取所有数据分组并还原出完整会话消息的难度。因此，如何将网络通信过程中的单维参数提升为多维参数，是降低窃听攻击风险的关键。

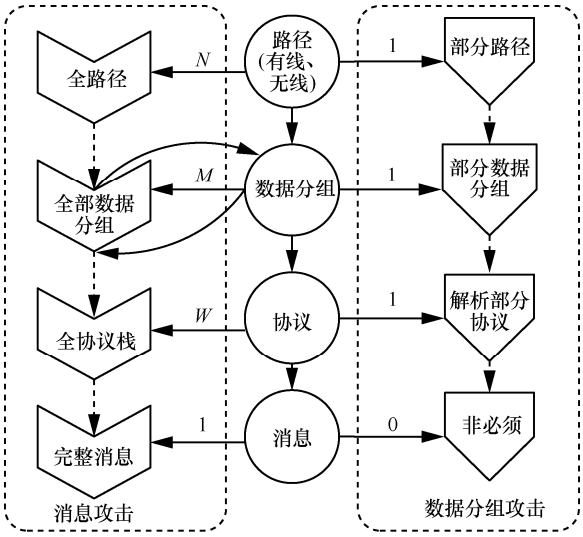


图 1　网络窃听威胁模型和杀伤链

2.2　POF 网络架构

软件定义网络是一种全新的网络架构，其特点是将网络的转发平面和控制平面分离，其物理实现上由一个控制器和多个路由交换设备（如SDN交换机）组成。OpenFlow是ONF最先提出的一种SDN实现协议，不足之处在于每种网络协议都在OpenFlow中完整定义，并且需要OpenFlow控制器和交换机不断升级才能支持这些网络协议。

为了改进OpenFlow的不足，人们积极探索更为通用的网络数据转发方法。其中，斯坦福大学学者联合Intel、Google、Microsoft等产业界数位专家提出了P4（programming protocol-independent packet processors）的概念[23]。P4 为SDN开发者提供了高级编程接口，从控制器层进行网络协议抽象，不同的协议经过P4 转换成各个SDN交换机中可以识别的OpenFlow流标规则，但是P4 没有从本质上改变SDN交换机适配不同网络协议的问题。华为提出了协议无感知转发的概念并以此提出了POF技术[20]。POF的优点是交换机不再解析协议，而是统一采用偏移量和特征值来进行网络协议转发，使交换机不需随新协议的出现而升级软硬件。目前，学术界研究热点包括POF架构[24]、POF控制器[25]、

POF数据交换[20]以及基于POF的网络内容分发应用[26]等。POF已经成立开源社区，致力于推动POF应用和标准化。

POF技术将控制器和转发设备接口的抽象层次降低至更细粒度的数据分组转发操作指令，转发设备对任何协议字段的理解，都统一抽象为该字段在数据分组中的偏移和字段的长度。转发设备不需要感知分组的协议类型以及转发流程，这就彻底摆脱了交换设备对特定标准协议的预先支持。

图 2 给出了POF数据交换的原理示意。POF控制器为交换机的每个流表下发不同的{*offse, length*}定位数据分组比特流中的{*key*}，并为匹配上该条规则的数据分组设置转发动作{*action*}。

传统网络设备和OpenFlow交换机只支持标准网络协议[27]，而不能改变其类型或结构化字段。POF除具备SDN基本的控制与转发相分离的特性外，还具有高度的协议自制能力。因此，POF技术的出现，极大降低了网络数据传输对承载协议类型的要求限制，使私有协议传输与协议变换成为可能。

2.3 相关研究

目前，已经有基于MTD技术的网络安全防御方法研究[9,13,14,18]，包括端口随机化和网络地址随机化等。文献[14]对网络的端口号进行随机实现基于端口跳变的MTD。“网络地址空间随机化”[9]是通过目标主机的IP地址进行随机混淆，来抵御扫描攻击和DDoS攻击，是最常用的网络移动目标防御方法。但是IPv4 的IP地址范围和端口数量比较小，即使IP地址和端口同时进行随机化[18]，其转换空间也比较有限。文献[13]提出一种基于IPv6 地址随机化的MTD方法，其地址空间为 2^{128}，使攻击面转换空间足够大，暴力破解攻击很难实现。但是现有的网络MTD方法只是随机化IP地址、端口等部分协议字段，数据分组头及数据负载等字段未进行随机化，主要用以抵御扫描攻击和DDoS攻击，因此，在传统网络架构下缺少有效的网络窃听攻击防御方法。

Corbett等[27]将MTD思想和OpenFlow技术结合应用于无线网络的安全防御中，提出了MAC和QAM的随机化弹性协议栈方法来抵御攻击者干扰网络传输。受限于OpenFlow的扩展能力，该方法只能实现无线网络协议的部分字段随机化。POF是基于软件定义网络架构的一种新的实现技术，它具备控制层面与转发层面分离的特性。同时POF作为SDN的扩展，控制层与转发层分离更加彻底，使转发设备彻底摆脱了对特定协议的依赖，不再感知分组的协议类型，而是统一采用偏移量（*offset*）和长度（*length*）来定位匹配特征值（*key*）进行网络数据分组的转发[25]。以上特性决定了POF具备高度的协议自制能力，允许用户自定义协议作为传输载体进行网络通信。

SDN在网络安全中的应用已经为国内外学术界所重视[28]。SDN改变了传统以IP转换[29]和端跳变的方式实现主动防御[30]，推动了移动目标防御技术的发展。在华为[20,25]和中国科学院[31,32]的共同研究推动下，POF技术的特性为构建新的网络移动目标防御系统提供更广阔的技术途径。已有的研究表明，基于POF协议随机化方法构建的安全防御方法能够

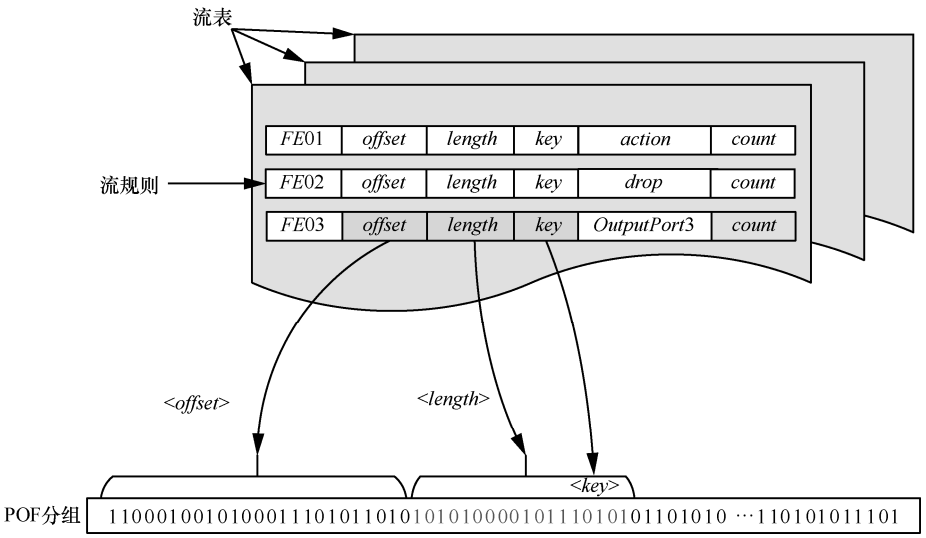


图 2 POF 数据交换的原理示意

有效保护SDN控制器免受“盲DDoS”攻击[31]，并且在抵御窃听攻击方面具有一定的优势[33]。

但是，现有方法都只从网络协议、路由路径等数据载体和网络环境来进行MTD攻击面转换，无法全面覆盖窃听攻击的 4 个主要杀伤链。特别是在全路径窃听环境下，会话消息的内容仍然面临单一性的威胁。

近年来，网络空间欺骗（cyber space deception）[34,35]研究逐渐系统化，已经远远突破蜜罐的范畴。特别是云计算、虚拟化等技术成熟，带动了网络空间欺骗方法在MTD中的应用研究[36,37]。本文将采用网络欺骗思想来构建会话消息的内容属性多样性。

3　基于 POF 的移动目标防御方法

本文主要研究通信过程中网络窃听防御，因此，本文假设网络通信的双方（发送方和接收方）以及用以网络管理的POF控制器是可信的，不会成为网络窃听攻击者的同谋。具体到本系统中，控制器、私有协议产生模块和通信客户端默认是相互可信的，不会泄露私有协议安全信息。

移动目标防御的核心思想旨在转换受保护目标的属性以不断改变其暴露的攻击面[7,21]，使攻击者迫于成本和难度增加的考虑而放弃攻击。根据以上对攻击模型的分析，网络通信过程的攻击面主要由网络协议（network protocol）、传输路径（routing path）、网络分组（packet）和消息内容（message）共同构成。因此，本文提出的MTD方法的核心内容是构造这 4 个属性的多样性以得到较大的转换空间，从而大大提高MTD攻击面的转换不可预测性。

首先，定义攻击面 4 个属性的转换空间（shifting space）和转换频率（shifting frequency）。然后，用二维向量 $\boldsymbol{N}(SS_n, SF_n)$、$\boldsymbol{R}(SS_r, SF_r)$、$\boldsymbol{P}(SS_p, SF_p)$、$\boldsymbol{M}(SS_m, SF_m)$ 分别表示MTD模型中的网络协议、传输路径、网络分组和消息内容的转换空间和转换频率。

因此，这里可以采用数学抽象方法，将MTD系统用函数 $\mathbb{Z}_{\mathrm{MTD}}(\cdot)$ 表示，其定义为

$$<\boldsymbol{N}^s, \boldsymbol{R}^s, \boldsymbol{P}^s, \boldsymbol{M}^s> \xrightarrow{\mathbb{Z}_{\mathrm{MTD}}(\cdot)} <\boldsymbol{N}^\alpha, \boldsymbol{R}^\alpha, \boldsymbol{P}^\alpha, \boldsymbol{M}^\alpha> \quad (1)$$

其中，$<\boldsymbol{N}^s, \boldsymbol{R}^s, \boldsymbol{P}^s, \boldsymbol{M}^s>$ 为原始系统的 4 个属性向量；$<\boldsymbol{N}^\alpha, \boldsymbol{R}^\alpha, \boldsymbol{P}^\alpha, \boldsymbol{M}^\alpha>$ 为经过MTD转换后的 4 个属性向量。

对于静态系统，属性的转换频率均为 0；而MTD系统的属性转换频率各不相同，但一般至少有一个大于 0。为了简化，将SF_n、SF_r、SF_p、SF_m都略去暂不考虑，则MTD的效果只与转换空间SS_n、SS_r、SS_p、SS_m有关，它们为可等价替换的子属性值组成的集合为

$$SS_k = [k_1, k_2, k_3, \cdots, k_X], k \in \{n, r, p, m\} \quad (2)$$

其中，空间大小 $\mathcal{S}ize(SS_k) = X$。为了度量MTD的安全性，采用函数 $\Theta_{SS}()$ 来比较转换空间，在归一化各属性的差异性的假设下，定义安全性比较的计算式为

$$\Theta_{SS}(\mathbb{Z}^{\beta}{}_{\mathrm{MTD}}(\cdot)) \succ \Theta_{SS}(\mathbb{Z}_{\mathrm{MTD}}(\cdot)) = \{\sum \mathcal{S}ize(SS_k) > \sum \mathcal{S}ize(SS_k) \mid k \in \{n, r, p, m\}\} \quad (3)$$

通过上述分析可以看出，抵御网络窃听攻击的MTD系统的核心，是提高SS_n、SS_r、SS_p、SS_m的空间大小。本文提出的MTD方法，采用私有协议族封包随机化策略和动态路径欺骗分组随机丢弃策略。系统架构如图 3 所示，构建端到端的透明欺骗网络，从协议、路径、数据分组、消息内容 4 个维度提升了MTD攻击面转换的不可预测性。

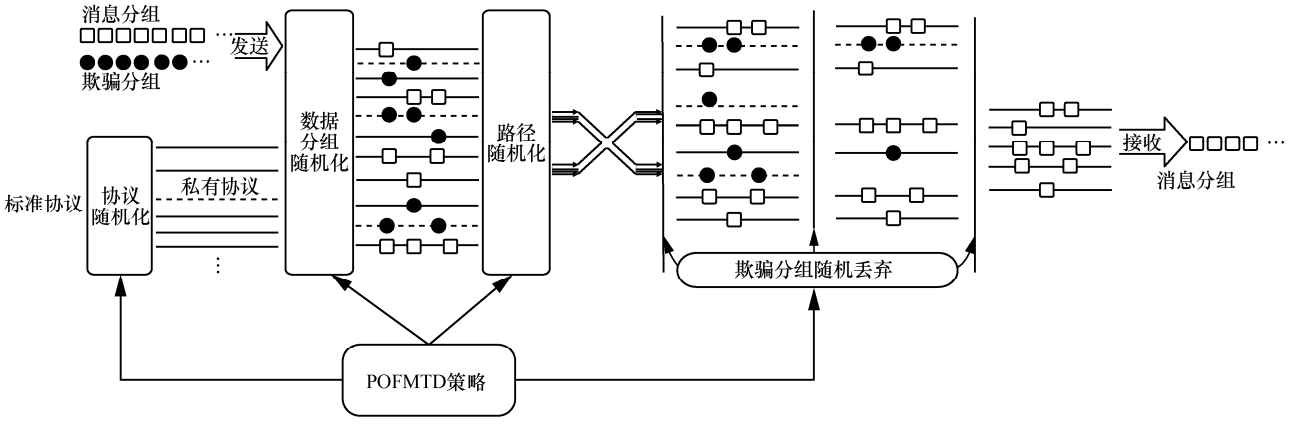


图 3　接收端欺骗无感知的 MTD 系统架构

3.1 私有协议族封包随机化

该策略主要采用POF产生的私有网络协议族进行通信消息分组和欺骗分组的随机封包，从而在网络协议层、数据分组层实现攻击面的多样化。

1) 私有协议产生

传统的网络传输设备按照固定的结构化字段来识别协议，字段结构的细微改动，都可能造成数据分组无法传输。因此，传统网络协议是标准的、单一的、固定的和静态的。

为了提高网络传输协议的冗余性和多样性，本文采用POF的无感知特性来构建私有协议族。POF协议能够摆脱固定协议的束缚，可以根据{*key*, *offset*, *length*}的抽象结构识别和创建任意非通用协议。在MTD研究领域，经典的方法是随机插入冗余比特来构造攻击面属性的多样性，同样通过在标准协议中插入随机的无效字段构造私有协议[31]。以TCP/IP协议为例，将原始标准协议定义为OSP，其中，包括MAC、IP等N个结构化字段，进行校准后，利用随机化算法在此标准协议字段中随机插入二进制字符串，以达到混淆协议的目的。这里给出一个协议随机化产生私有协议的算法。

算法 1 网络协议栈随机化

输入 随机向量 $\boldsymbol{R}(\gamma,M)=[r_1,r_2,r_3,\cdots,r_M]$

原始标准协议 $OSP=[f_1,f_2,\cdots,f_N]$

输出 私有协议 $PP=[p_1,p_2,p_3,\cdots,p_{(M+N+1)}]$

① $list[N+M+1]$

② for each $i\in[1,N+M+1]$ do

③ $p_i\leftarrow$ NULL

④ $list[i]\leftarrow i$

⑤ end for

⑥ $id\leftarrow random(1,N+M)$

⑦ $p_{(id)}\leftarrow$ PPID

⑧ $list.remove\{list[id]\}$

⑨ $list.lenth\leftarrow list.lenth-1$

⑩ for each $j\in[1,M]$ do

⑪ $l\leftarrow random(2,list.lenth)$

⑫ $k\leftarrow list[l]$

⑬ $p_k\leftarrow r_k$

⑭ $list.remove\{list[k]\}$

⑮ $list.lenth\leftarrow list.lenth-1$

⑯ end for

⑰ $q\leftarrow 1$

⑱ for each $t\in[1,M+N+1]$ do

⑲ if $p_t\neq$ NULL

⑳ $p_t\leftarrow f_q$

㉑ $q\leftarrow q+1$

㉒ end if

㉓ end for

㉔ return PP

为了正确识别这些私有协议，通信双方需要知道协议的ID和随机向量的偏移量和长度，符号定义 $Secpp=\{(\text{PPID},offset(\text{PPID})),\cup_{i:1\to M}(offset(r_i),length(r_i))\}$。$Secpp$由通信双方和POF控制器离线秘密分享[17]，通信实体便可以使用私有协议传输数据。

由此，通信双方可以从如图 4 所示的私有协

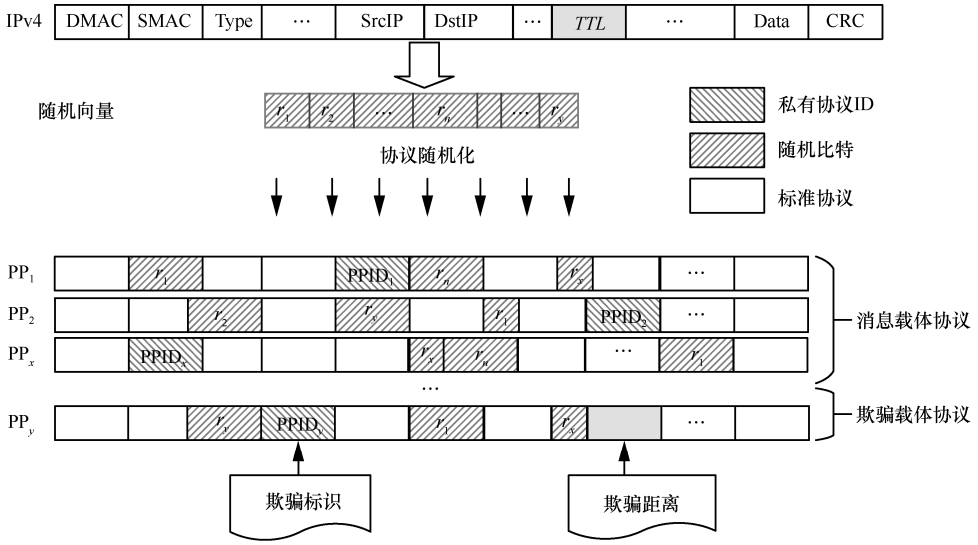


图 4 私有协议池

议池中选择若干私有协议组成一个私有协议族分别封装消息分组（message packet）和欺骗分组（deception packet）。其中，用于封装欺骗分组的协议需要控制器中标记其私有协议ID（对应deception flag），并用*TTL*标记欺骗分组传输的最远跳数（对应deception distance）。

2) 网络封包欺骗

为了提高窃听攻击者重组数据分组的难度，本文提出一种消息分组随机化方法，如图 5 所示，将消息拆分成多个数据字段，每个数据字段封装在不同的私有协议的负载中。同时，为了增加欺骗性，可以在数据分组中随机混入少量的欺骗分组，通过设置较短的传输距离，在这些数据分组到达可信接收客户端之前，POF交换机将其丢弃，这样既不增加接收端的负担，又给中间节点的窃听攻击者带来迷惑性。封装欺骗分组的私有协议ID都由控制器标记为deception flag，以给交换机的流标设置相应的随机分组丢失动作（drop action）；欺骗分组传输的最远跳数为不大于传输路径的最大节点数的一个整数，并赋值给*TTL*字段。

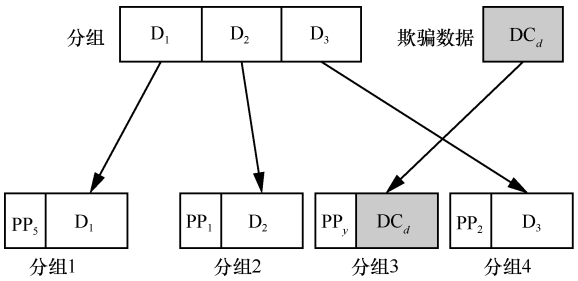


图 5　消息封包随机化

通信时，消息内容通过不同的私有协议发送给接收端，避免了单一协议被攻击造成隐私泄露的风险；同时网络路径中混杂了欺骗分组，敌手难以分辨真假。

假设消息为M_{sg}，将其平均拆分为q个添加了顺序号的数据块 $M_{sg}=\{D_1,D_2,D_3,\cdots,D_q\}$。诱骗消息为$M_{dc}$，拆分后的数据序列为 $M_{dc}=\{DC_1,DC_2,\cdots,DC_\varepsilon\}$。通信双方选择 $PPC^M=\{PP^m{}_1,PP_2^m,PP_3^m,\cdots,PP_\mu^m\}$来封装消息分组；$PPC^D=\{PP^d{}_1,PP^d{}_2,PP^d{}_3,\cdots,PP_\delta^d\}$是用来封装欺骗分组的私有协议族。

3.2　动态路径欺骗分组随机丢弃

该部分的MTD策略主要实现网络通信过程中的消息分组和欺骗分组的动态路径管理，以及在传输过程中对欺骗数据分组进行随机丢弃，实现对接收端的欺骗无感知。

1) 路由路径随机化

传统路由策略基于目的IP、*TTL*或其他协议标签，传输路径一般为最短路径算法。一旦传输会话建立，路由路径将保持不变。固定的传输链路为攻击者实施窃听攻击带来了便利，传输链路作为攻击面暴露了网络传输链路的脆弱性。

本文的MTD策略中，提出一种基于路由信息和私有协议相结合的动态路由策略，该策略通过保持路径的动态转换保证网络路由的不可知性和系统攻击面的不可预测性。

假设在通信双方之间存在Ψ条传输可达路径，所有传输可达路径组成的集合 $L=\{l_1,l_2,\cdots,l_\Psi\}$。路径上的交换机由 $S_\xi(in_port, out_port)$表示，（*in_port*, *out_port*）为交换机与邻近交换机之间的进出连接端口。每条路径l_i包含一个途经交换机集合的向量，表示为 $l_i=[\boldsymbol{S}_\xi,\boldsymbol{S}_{\xi+1},\cdots,\boldsymbol{S}_{\xi+x}]$。

当选择一个包含$\mu+\sigma$个协议的私有协议族 $PPC=\{PP_1,PP_2,PP_3,\cdots,PP_{\mu+\sigma}\}$来传输消息分组和欺骗分组时，控制器根据随机算法周期性地将这些私有协议分配到Ψ条传输路径。该随机调度算法不区分消息分组协议和欺骗分组协议。

每个交换机的第一级流表通过私有协议PPID实现网络数据分组的快速转发。控制器利用随机化算法更新每个交换机的一级流表，用以部署动态随机路由信息策略。控制器实施的动态路由策略对通信客户端透明，通信双方不需要知道路由信息。

2) 欺骗分组随机丢弃

承载欺骗分组的私有协议在交换网络中用以扩大传输数据的多样性。欺骗数据分组混淆在传输路径中，以迷惑窃听攻击者，阻碍其进行会话消息分组的重组。为了对接收端透明，也为了减少传输带宽损耗，本文MTD方案提出欺骗分组随机丢弃策略，在链路中的某一交换节点上下发drop指令，将欺骗分组丢弃。各个欺骗分组均在中途节点被丢弃，因而接收端不需关注接收到的数据分组的真伪类型，欺骗分组对接收端是无感知的。控制器生成欺骗分组丢弃策略的随机化算法如下。

算法 2　欺骗分组随机丢弃

输入　欺骗私有协议族 $PPC^D=\{PP^d{}_1, PP^d{}_2, PP^d{}_3, \cdots, PP_\delta^d\}$

动态欺骗路径集合 $L=\{l_1,l_2,\cdots,l_\kappa\}$

输出 欺骗路径节点流表规则集 $FL^D=[fl_1^d,fl_2^d,\cdots,fl_\chi^d]$

① $distance \leftarrow$ NULL
② $SetList(FL^D)$
③ for each $i\in[1,\delta]$ do
④ $rp^i \leftarrow random(1,k)$//任意选取一条路径；
⑤ $nodes\_Np_i \leftarrow countAllNodes(l_{rpi})$
⑥ $distance \leftarrow PP^d_i.TTL \leftarrow nodes\_Np_i$
⑦ for each $j \in [1, nodes\_Np_i]$ do
⑧ $fl^d(rp^i).S_j.key \leftarrow PP^d_i.PPID;$
⑨ if ($random(1,distance)>coin(0,1)$
⑩ $fl^d(rp^i).S_j.action \leftarrow output$
⑪ else
⑫ $fl^d(rp^i).S_j.action \leftarrow drop$ //丢弃欺骗分组
⑬ end if
⑭ $distance= distance-1$
⑮ if ($distance<1$)
⑯ $fl^d(rp^i).S_j.action \leftarrow drop$
⑰ end if
⑱ end for
⑲ return FL^D
⑳ end for

3.3 POFMTD 原型系统实现

基于以上随机化方法，构建基于POF的移动目标防御原型系统，如图 6 所示。其中，私有协议产生模块通过动态协议算法，生成通信所需要的私有协议族，并将协议的安全信息SecPP以XML文件形式离线秘密分享给控制器和通信客户端。

控制器根据私有协议信息和通信双方的路径信息，周期地生成相应的流表信息，下发到交换网络中。路径随机化和变更由MTD动态策略模块完成。通信客户端根据私有协议信息，封装载荷，发送通信数据，并对接收到的私有协议数据分组进行去随机化和解析。控制器、私有协议产生模块和通信客户端默认是相互可信的，不会泄露私有协议安全信息。

4 攻击实验仿真

4.1 实验环境设置

本文测试环境包括POF控制器和POF交换机以及用以通信的客户端和用来模拟窃听攻击的攻击

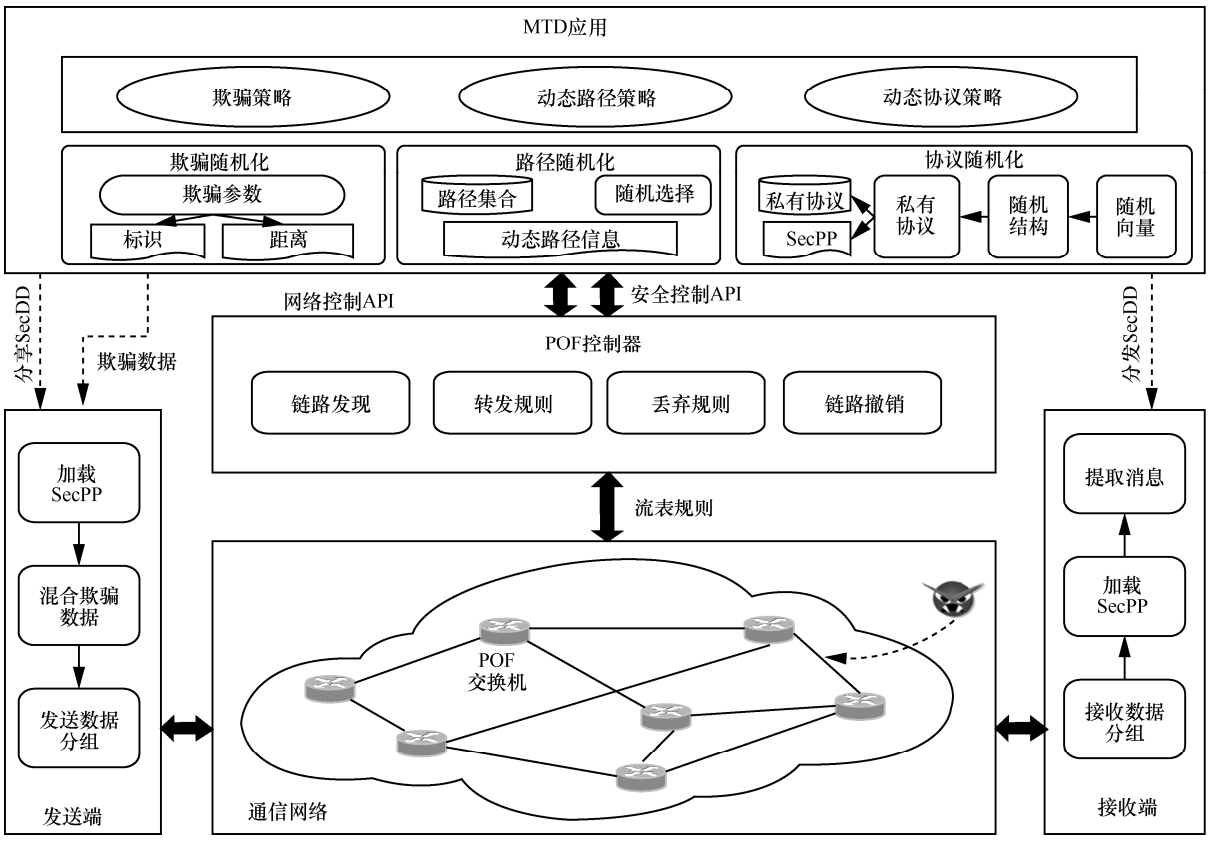


图 6 POFMTD 原型系统

主机。POF交换机和一台POF控制器来搭建实验网络环境，POF交换机和控制器来源于POF开源项目。

客户端和攻击服务器运行于Windows 7 操作系统，浏览器采用Chrome 39.0 和Firefox 47.0。分组分发软件基于Python类库Scapy编写的网络分组分发程序。

实验网络的交换机拓扑结构如图 7 和图 8 所示，这些交换机由控制器进行策略控制（为简化拓扑，略去控制器的位置）。客户端host A与host B所在POF交换网络之间形成多条通路：$L=\{l_1, l_2, l_3, \cdots\}$。本次实验基于UDP进行字段随机化来产生私有协议。

4.2　攻击测试

防窃听攻击通过在不可信链路上发送数据分组、接收数据分组来测试攻击者截获数据分组的数量和重组数据分组的成功率，如表 1 所示。Scapy根据定义的私有协议格式进行通信数据分组的发送。

攻击者在[S_0, S_1, S_2]路径上进行抓取分组窃听，并采用wireshark协议分析软件进行协议解析和通信消息恢复。由于攻击者不知私有协议的结构信

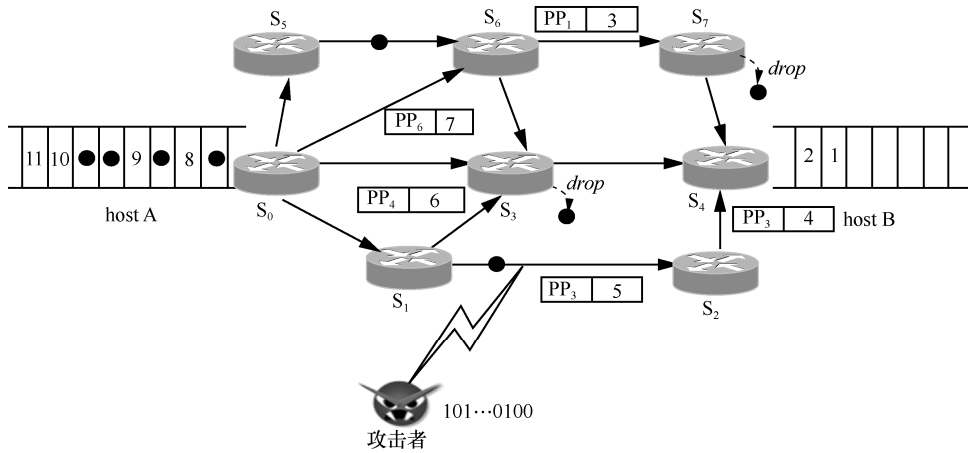


图 7　时隙 1 内不同协议的动态传输路径

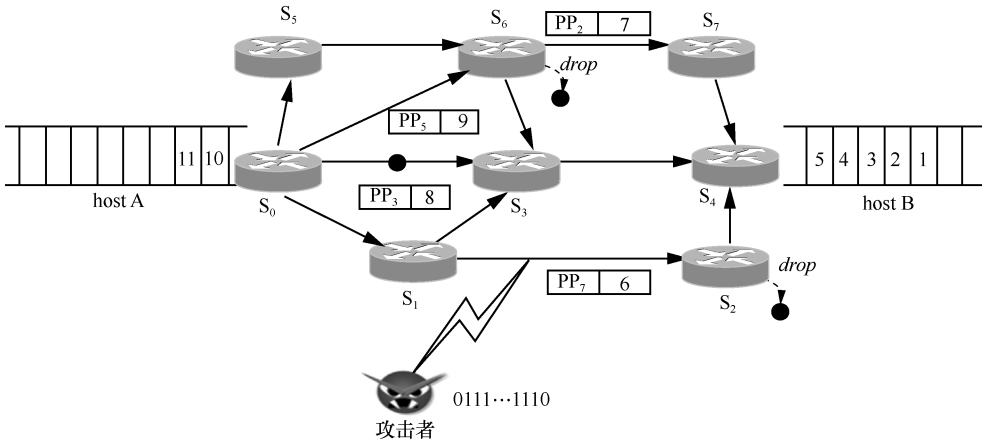


图 8　时隙 2 内不同协议的动态传输路径

表 1　　**网络窃听攻击测试**

消息分组数量	欺骗分组数量	协议数量	传输路径数（含 $S_1 \rightarrow S_2$）	窃听数据分组比例	重组会话成功率	通信端接收数据分组比例
10	0	1（标准 UDP）	1	100%	100%	100%
9	1	1(私有协议)	1	100%(含欺骗数据)	0(fail)	100%（不含欺骗数据）
100	0	2(私有协议)	2	35%	0(fail)	100%
1 000	0	5(私有协议)	2	30%	0(fail)	100%
10 000	0	5(私有协议)	4	5%~11%	0(fail)	95%~100%

息（也即SecPP），因此，无法利用捕获数据分组进行逆向分析。

对于host B等合法用户，使用Lua语言对已知私有协议结构信息（如SecPP）编写插件模型并嵌入至wireshark。客户端host B接收到来自客户端host A的信息，并且使用客户端双方与控制器共享的私有协议的SecPP对该数据分组的内容进行解析。

除了私有协议随机化之外，通信方host A将会话消息分成多份，封装在不同的协议中并发送给接收端host B。控制器每隔一段时间，通过更新交换机流表以改变不同协议的传输路径。因此，窃听攻击在单路径上无法窃听到会话消息的全部分组。

欺骗分组是一种用来干扰攻击者重组会话消息的假数据，在测试中该类数据的最远传输距离不会超过最短路径的跳数，随机分组丢失算法可以保证在数据分组到达合法接收端之前被POF交换机设置*drop*动作而丢弃，不影响合法通信接收方，却可以迷惑在链路中进行窃听的攻击者。欺骗分组与有效数据分组共享带宽，过多的欺骗分组起不到应有的欺骗效果，反而影响传输效率，因此，测试中欺骗分组设置了相对较小的比例。

实验表明本文的MTD方法可以有效抵御窃听攻击对网络通信过程的威胁。

4.3 性能测试

在POFMTD实验环境进行性能测试时，本文主要对标准网络协议（UDP）与私有协议的网络性能进行对比。分组分发工具用Scapy分别发送UDP数据分组以及基于UDP随机化产生的私有协议数据分组，随机化向量为 4 B。性能测试工具用Iperf在服务器上进行统计。

在网络吞吐量性能方面，实验中采用的POF交换机为软件交换机，未采用硬件加速和内核优化，利用Iperf测试POF交换机之间的转发标准协议和私有协议的转发吞吐量。当最大分组长度设置为1 460 B时，转发标准网络协议的转发吞吐量平均为 943.49 Mbit/s，转发私有协议的网络性能为942.05 Mbit/s。当最大分组长度设置为 68 B时，转发标准网络协议的转发吞吐量平均为213.61 Mbit/s，转发私有协议的网络性能为 215.18 Mbit/s。发送端均以10 Mbit/s发送测试流量，对于标准网络协议UDP，利用Iperf测试得到的平均带宽为 9.89 Mbit/s，而私有协议的平均带宽为 9.81 Mbit/s，与标准带宽之间差距都较小。

网络时延与传输路径有关，实验中采用同样的动态路径策略进行MTD路径随机化，测试比较最短路径与最长路径中的网络时延性能。在标准网络协议传输下，测试得到的在最短路径和最长路径下平均网络时延分别为 10.772 ms、20.779 ms；而进行私有协议通信测试中，在最短路径和最长路径下平均网络时延分别为 11.547 ms、21.589 ms（偏差分别为 7.72%、3.90%）。使用 10 Mbit/s带宽进行Iperf测试最短路径下的网络分组丢失率，得到的分组丢失率分别为 0.55%、0.61%。

除此之外，在性能上启用POFMTD策略前后，单个交换机上的CPU使用率几乎相同，即采用MTD策略对CPU性能的影响几乎可以忽略不计，这也是协议无感知转发的一大优势。

5 安全分析

下面给出POFMTD模型的安全性理论分析，按照网络窃听攻击威胁模型中所述，这里主要针对数据分组分析的部分窃听攻击以及针对消息内容分析的完全窃听攻击 2 种情况进行分析。本文将窃听攻击的影响因素进行抽象，用P_{pEv}表示数据分组攻击成功的概率，用P_{sEv}表示会话消息攻击成功的概率。网络协议空间大小为Γ，通传输路径的空间大小为Φ。通信过程中使用δ个私有协议和$\hbar$条传输路径进行动态传输，共传输M个数据分组，其中，m个有效数据分组和ε个欺骗分组。另外，定义窃取网络协议事件为A_{np}，获取协议种类数目为ρ；窃听网络路径事件为A_{nr}，入侵传输路径共有κ条；逆向解析私有协议事件为A_{rp}，协议被成功解析的数目为ξ；窃取会话消息事件为A_{ms}，成功解析的消息数据分组个数为ϖ。因此，网络窃听攻击的概率可以定义为$\Pr(EavAtt)=\Pr(A_{np}(\rho),A_{sr}(\kappa),A_{rp}(\xi),A_{ms}(\varpi))$。

5.1 抗数据分组攻击的安全性

相对于信息论安全（也即香农安全），通信过程中的数据分组攻击是一种弱安全窃听攻击。 敌手从截获的少量数据分组中无法获取完整、有意义的会话信息，但是攻击者可以得到一些间接的情报，这对于威胁网络通信是有价值的。为了实施数据分组攻击，攻击者需要入侵通信双方的传输路径，截获通信过程中至少一个协议并逆向分析其结构。数据分组攻击不需要解析全部消息内容，因此，即使协议中数据负载部分是密文，或窃听攻击者只

捕获部分数据分组，也可以成功实施数据分组攻击。数据分组攻击成功后，攻击者通过篡改协议内容以构造中间人攻击或DDoS攻击等。

例如，威胁模型分析，数据分组窃听攻击是一种局部攻击，攻击者最直接的目的是逆向解析出真实的信源和信宿，即假设敌手恰好在通信会话周期内在任意路由路径上捕获到任意一个会话数据分组并解析该协议的结构，攻击即成功。

M个数据分组落到敌手所在的任意路径上的联合概率可表示为

$$\begin{aligned}&\Pr(A_{nr}(\kappa),A_{ms}(\varpi)\,|\,\forall\varpi\in[1,M])\\&=1-\left(1-\frac{1}{\kappa}\right)^{\max(\varpi)}=1-\left(1-\frac{1}{\kappa}\right)^{M}\end{aligned}\tag{4}$$

在$M>>\hbar$ 的情况下，敌手捕获到一个数据分组的可能性是一个关于参数M的增函数。因此，数据分组窃听攻击的概率可以定义为

$$\begin{aligned}&P_{pEv}=\Pr(EavAtt\,|\,\forall\rho\in[1,\delta],\forall\kappa\in[1,\hbar],\forall\varpi\in[1,M])\\&=\Pr(A_{np}(\rho),A_{nr}(\kappa),A_{rp}(\xi),A_{ms}(\varpi)\,|\\&\forall\rho\in[1,\delta],\forall\kappa\in[1,\hbar],\forall\varpi\in[1,M])\end{aligned}\tag{5}$$

本文进行评估的目标是找到敌手攻击成功率函数的上限。根据以上分析，敌手无意理解数据分组的内容，因而截获任意数据分组和截获任意网络协议在当前环境下是等价的。另外可知，成功实施数据分组攻击的条件为$\xi\geqslant1$，本文取其最基本条件为 1，即敌手只需要从截获的数据分组中逆向解析出一个私有协议结构，就能成功知道信源和信宿。

$$\begin{aligned}&P_{pEv}=\Pr(A_{np}(\rho),A_{nr}(\kappa),A_{rp}(\xi),A_{ms}(\varpi)\,|\\&\forall\rho\in[1,\delta],\forall\kappa\in[1,\hbar],\forall\varpi\in[1,M],\xi=1)\\&=\Pr(A_{nr}(\kappa),A_{rp}(\xi),A_{ms}(\varpi)\,|\,\forall\kappa\in[1,\hbar],\\&\forall\varpi\in[1,M])\leqslant\Pr(A_{rp}(\xi)\,|\,\xi=1)\Pr(A_{nr}(\kappa),\\&A_{ms}(\varpi)\,|\,\forall\kappa\in[1,\hbar],\forall\varpi\in[1,M])\\&=\Pr(A_{rp}(\xi)\,|\,\xi=1)(1-(1-\frac{1}{\kappa})^{M})\\&=\lim_{M\to\infty}\Pr(A_{rp}(\xi)\,|\,\xi=1)\end{aligned}\tag{6}$$

根据以上分析，已知私有协议的随机化空间为Γ，假设产生这些私有协议的概率分布属于均匀分布，本文可以得出逆向破解一个私有协议的概率$\Pr(A_{rp}(\xi)|\xi=1)=\dfrac{1}{\Gamma}$。这意味着逆向破解一个私有协议的概率与网络协议的随机化空间直接相关。在传统网络传输中，都采用标准协议，也就是协议空间为 1，协议的一成不变性使敌手进行数据分组窃听攻击易如反掌。部分网络MTD研究通过随机化方法来达到传输协议的动态性，如端口跳变[14]、IP跳变[11]、端跳变[18]等。然而，这些MTD方法只能随机化部分协议字段，因此，协议的随机化空间非常有限。在IPv4 中双向IP跳变的最大随机化空间也只有 232，而大部分情况下，IP跳变只能使用C类IP地址。即使是基于IPv6 的MTD跳变[12]，其协议空间也只有 2 个 128 bit。由图 9(a)和图 9(b)可以看出，POFMTD在网络协议随机化程度和MTD机制的随机化向量等方面，相对于单一的协议字段随机化MTD方法，有较大的转换空间，可以获得更大的防御熵。

基于POF技术对全部标准协议随机化来产生私有协议，突破了主机地址甚至IP地址空间的限制。暴力破解IPv6 随机地址需要的时间量级为 10^{10} h，而暴力破解POFMTD的时间量级为 $2^{1\,000}$h，呈现指数级的倍增[31]。如图 9(c)所示，路由路径的动态变化，也能大大降低数据分组落在不安全链路上的概率，提高窃听者截获数据分组的代价。

采用式(1)的度量方法，表 2 给出不同网络MTD模型的随机化程度比较，这里空间大小以熵来计算。

5.2　抗会话消息攻击的安全性

会话消息攻击比数据分组攻击的要求更为苛刻。攻击者需要捕获到通信会话过程中的全部数据分组，并且能够解析协议和负载，以重组消息内容。

在本文提出的消息封包随机化方法中，消息被平均拆分为M个数据块（m个有效数据分组和ε个欺骗分组），每个数据块包含顺序号。消息数据分组通过δ个私有协议来封装并通过$\hbar$条路由路径发送到接收端。从敌手的路径窃听能力方面，本文分别给出攻击成功概率的下限和上限，也即会话消息窃听攻击的概率定义为

$$\begin{aligned}P_{sEv}&=\Pr(EavAtt)=\Pr(A_{np}(\rho),A_{sr}(\kappa),A_{rp}(\xi),A_{ms}(\varpi))\\&=\begin{cases}\min(P_{sEv})=\Pr(A_{sr}(\kappa))\Pr(A_{np}(\rho),A_{rp}(\xi),\\A_{ms}(\varpi)\,|\,A_{sr}(\kappa)),\kappa=1\\\max(P_{sEv})=\Pr(A_{sr}(\kappa))\Pr(A_{np}(\rho),A_{rp}(\xi),\\A_{ms}(\varpi)\,|\,A_{sr}(\kappa)),\kappa=\hbar\end{cases}\end{aligned}\tag{7}$$

表 2 **MTD 模型的随机化程度对比**

模型	协议空间	路径空间	封包空间	消息内容空间	抗数据分组窃听	抗会话消息窃听
IP MTD	32	0	0	0	P	×
Port MTD	16	0	0	0	×	×
End MTD	48	0	0	0	P	×
MT6D	128	0	0	0	P	×
POFMTD	12 000	$\ln(\mathbb{S}ize(SS_r))$	$\ln(\mathbb{S}ize(SS_p))$	$\ln(\mathbb{S}ize(SS_m))$	√	√

注：P 表示部分支持。

首先分析 $\max(P_{sEv})$ 的情况。此时，有 $\Pr(A_{sr}(\kappa))=1$，$\rho=\delta$ 以及 $\varpi=M$。这里认为敌手在破解协议的情况下，从 M 个数据分组中能够完全获取 m 个有效消息内容，仅考虑破解协议的概率为

$$\begin{aligned}&\max(P_{sEv})\\&=\Pr(A_{sr}(\kappa))\Pr(A_{np}(\rho),A_{rp}(\xi),A_{ms}(\varpi)\mid A_{sr}(\kappa))\\&=\Pr(A_{ms}(\varpi))\Pr(A_{np}(\rho),A_{rp}(\xi)\mid A_{ms}(\varpi))\\&=\Pr(A_{np}(\rho),A_{rp}(\xi))=\prod_{\lambda=0}^{\delta-1}\left(\frac{1}{\Gamma-\lambda}\right)\end{aligned}\tag{8}$$

接下来分析敌手窃听攻击的最坏情况。当 $\kappa=1$ 时，意味着攻击者可以等概率窃听任意一条路由路径且只能在会话过程中窃听该条路径。假设动态路径的平均转换周期为 π，则会话周期 Ω 时间内共发生 $n=\dfrac{\Omega}{\pi}$ 次协议转换。本文依然得出最坏情况下敌手攻击能得到的最好概率大小为

$$\begin{aligned}&\min(P_{sEv})\\&=\Pr(A_{sr}(\kappa))\Pr(A_{np}(\rho),A_{rp}(\xi),A_{ms}(\varpi)\mid A_{sr}(\kappa))\\&=\Pr(A_{sr}(\kappa))\Pr(A_{ms}(\varpi)\mid A_{sr}(\kappa))\cdot\\&\Pr(A_{np}(\rho),A_{rp}(\xi)\mid A_{sr}(\kappa),A_{ms}(\varpi))\\&=\frac{1}{\hbar}\left(\sum_{i=0}^{\varepsilon}\mathrm{C}_M^{m+i}\left(\frac{1}{\hbar}\right)^{m+i}\left(1-\frac{1}{\hbar}\right)^{\varepsilon-i}\right)\cdot\\&\left(\frac{m}{M}\right)^m\prod_{j=0}^{\left(\min\left\{n\frac{\delta}{\hbar},\delta\right\}\right)-1}\left(\frac{1}{\Gamma-j}\right)\end{aligned}\tag{9}$$

由以上分析可知，$\max(P_{sEv})\leqslant\left(\dfrac{1}{\Gamma}\right)^{\delta}$，$\min(P_{sEv})\leqslant\dfrac{(\hbar-1)^{\varepsilon}}{\hbar^{M+1}}\left(\dfrac{1}{\Gamma}\right)^{\delta}$。即使攻击者可以窃听所有传输路径，在私有协议空间较大的情况下，实施会话消息窃听攻击成功的概率仍然很小。

5.3 欺骗分组效能

MTD的欺骗策略，将原本静态、单一为真的网络数据分组引入了多样化的欺骗分组，从而扩大了窃听攻击防御的消息内容属性的转换空间。敌手无法确认截获数据分组的真伪，进而提高了会话消息窃听攻击的难度。

本文提出的欺骗分组随机丢弃算法，一方面能够将欺骗分组均匀混淆在传输链路中，另一方面，能够降低传输的带宽消耗，达到安全和消耗的折中。

以欺骗私有协议族 $PPC^D=\{PP^d{}_1,PP^d{}_2,PP^d{}_3,\cdots,PP_\delta^{\ d}\}$ 为例，共计传输M个欺骗分组，每个分组大小为W。动态欺骗路径集合为 $L=\{l_1,l_2,\cdots,l_\kappa\}$，不妨假设$k$个路径均有$N$个节点。下面从欺骗覆盖度和带宽消耗 2 个维度进行分析。

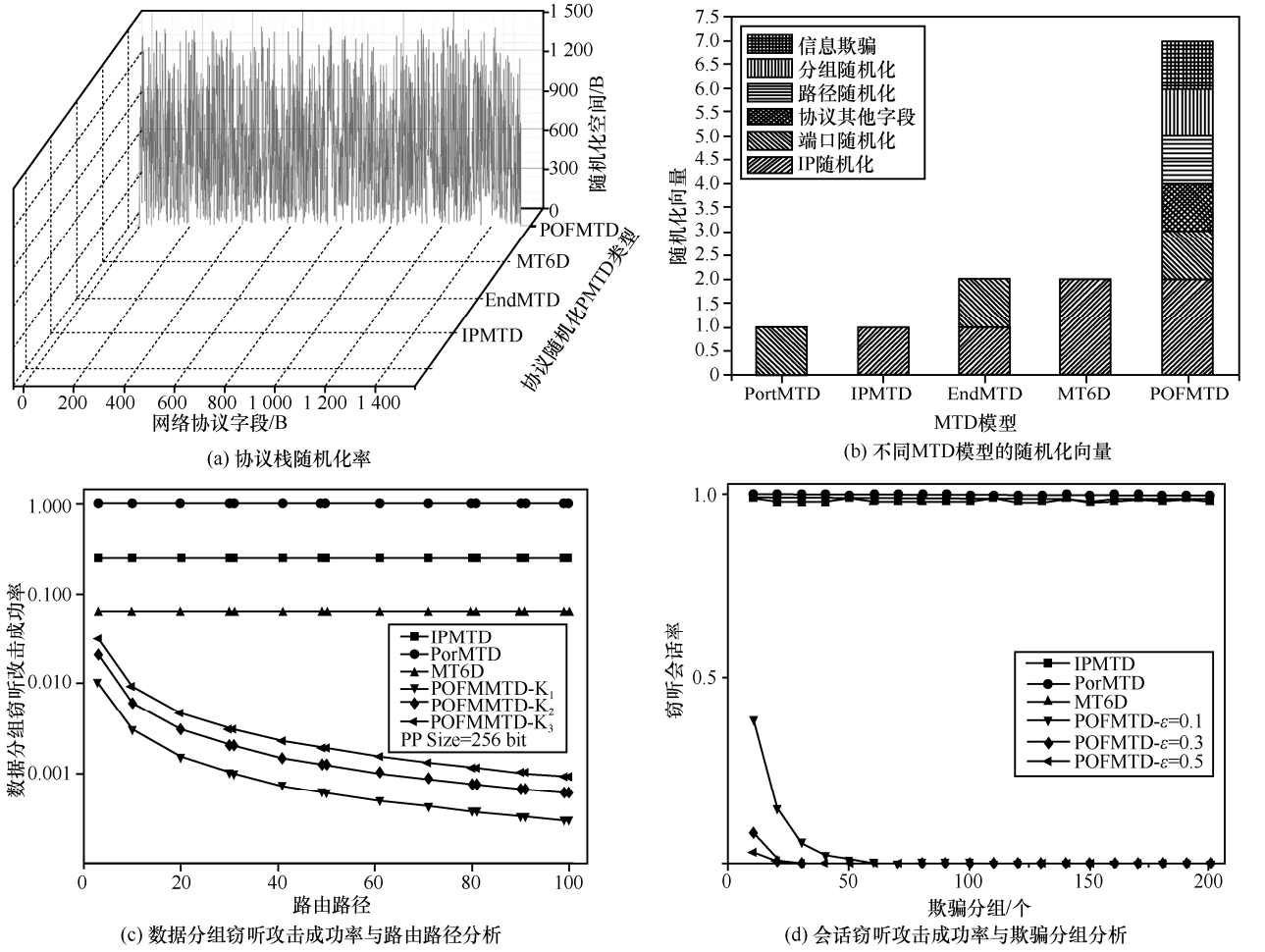
1) 欺骗数据分组按照概率在传输链路中各个节点间出现的情况统计，计算出覆盖度。全路径的节点为$k\times N$的二维矩阵，只要有欺骗数据曾经在二维矩阵的点上传输过，就表示覆盖了该节点。M个欺骗分组被分配到δ个私有协议中，平均每个协议传输的欺骗分组个数为 $\dfrac{M}{\delta}$；私有协议每次在一条路径上传输，根据欺骗分组随机丢弃算法，协议在路径中传播到终点服从概率为ρ的分布，其平均距离数学期望为 $\mathrm{E}=\rho N$。因此，欺骗覆盖度可表示为

$$C_v=\frac{\dfrac{M}{\delta}\mathrm{E}\delta}{kN}=\frac{M\rho N}{kN}=\frac{M\rho}{k}\tag{10}$$

当ρ=0.5，k=10，则在防护周期内，M>20 即可覆盖所有节点。在满足覆盖度的情况下，欺骗分组的个数M与概率ρ成反比。

2) 按照数据分组大小，计算实际随机丢弃前的实际有效传输总带宽与传输会话消息的总带宽比，计算欺骗分组的传输损耗为

$$P_b=\frac{\left(\dfrac{M}{\delta}W\right)\delta\mathrm{E}}{B_wN}=\frac{(MW)\rho N}{B_wN}=\frac{(MW)\rho}{B_w}\tag{11}$$



(a) 协议栈随机化率　(b) 不同MTD模型的随机化向量

(c) 数据分组窃听攻击成功率与路由路径分析　(d) 会话窃听攻击成功率与欺骗分组分析

图 9　MTD 安全性分析

其中，B_w为总带宽，不妨取 10 MB；而ρ=0.5，M=1 000，W=1 024 B。则P_b=4.7×10^{-9}。正常网络传输环境下，欺骗分组的带宽消耗可以通过欺骗分组个数控制以及随机丢弃算法的概率分布控制，来降低对带宽的影响。

经分析可知，该随机丢弃算法，在保障接收端对欺骗无感知的情况下，在安全覆盖度和带宽消耗比指标上都有较好的性能。

欺骗的本质，是增加消息内容攻击面的不确定性。如图 9(d)所示，欺骗数据的引入，能够加速降低会话消息重组的成功率。

综上分析，本文提出的POFMTD模型可用于IPv4 和IPv6 协议的有线或无线网络中。鉴于IP跳变端口跳变以及二者结合等只是全协议栈随机化的一些特例，无法实现接收端无感知的欺骗分组策略，本文提出的方法具有更好的安全性。

6　结束语

本文提出一种基于协议无感知转发（POF）的抗网络窃听攻击移动目标防御机制。在该MTD安全机制中，本文将网络窃听攻击防御的攻击面转换维度扩展到协议、路径、网络分组和消息内容 4 个层面，提出基于POF实现的私有协议族封包随机化策略和动态路径欺骗分组随机丢弃策略，提供了网络通信过程攻击面转换的熵空间。理论分析和实验结果表明，本文提出的MTD方法可显著增加攻击者实施数据分组攻击和内容消息攻击的难度，有效防止网络通信过程中的信息泄露。

网络空间欺骗是一种主动防御方法，而欺骗分组的混入，为基于协议无感知转发的抗网络窃听攻击带来了新思路。在未来，如何解决和优化欺骗信息量与网络传输效率之间的矛盾，是基于POF的移动目标防御的关键问题之一和重要研究方向。

参考文献：

[1] ZHANG P, JIANG Y, LIN C, et al. P-coding: secure network coding against eavesdropping attacks[C]//INFOCOM. 2010: 1-9.

[2] XIA H D, JOSÉ C B. Hardening web browsers against man-in-the-middle and eavesdropping attacks[C]//The 14th International Conference on World Wide Web.2005.

[3] KEWLEY D, FINK R, LOWRY J, et al. Dynamic approaches to thwart adversary intelligence gathering[C]//DARPA Information Survivability Conference & Exposition II. 2001: 176-185.

[4] CHOI H, PATRICK M D, THOMAS F, et al. Privacy preserving communication in MANETs[C]//The 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks. 2007: 233-242.

[5] HWANG H, JUNG G, SOHN K, et al. A study on MITM (man in the middle) vulnerability in wireless network using 802.1 X and EAP[C]//International Conference on Information Science and Security. 2008: 164-170.

[6] WAGNER R. Address resolution protocol spoofing and man-in-the-middle attacks[J].The SANS Institute, 2001.

[7] SYVERSON P F, GOLDSCHLAG D M, REED M G. Anonymous connections and onion routing[C]//IEEE Symposium on Security and Privacy. 1997: 44-54.

[8] ZHANG P, JIANG Y, LIN C, et al. Padding for orthogonality: Efficient subspace authentication for network coding[C]//INFOCOM. 2011: 1026-1034.

[9] SIFALAKIS M, SCHMID S, HUTCHISON D. Network address hopping: a mechanism to enhance data protection for packet communications[C]//2005 IEEE International Conference on Communications. 2005: 1518-1523.

[10] JAJODIA S, GHOSH A K, SWARUP V, et al. Moving target defense: creating asymmetric uncertainty for cyber threats[J]. Springer Ebooks, 2011: 54.

[11] ANTONATOS S, AKRITIDIS P, MARKATOS E P, et al. Defending against hitlist worms using network address space randomization[J]. Computer Networks, 2007, 51(12): 3471-3490.

[12] JAFARIAN J H, AL-SHAER E, DUAN Q. OpenFlow random host mutation: Transparent moving target defense using software defined networking[C]//The First Workshop on Hot Topics in Software Defined Networks.2012: 127-132.

[13] DUNLOP M, GROAT S, URBANSKI W, et al. MT6D: a moving target IPv6 defense[C]//Military Communications Conference. 2011: 1321-1326.

[14] LEE H C J, THING V L L. Port hopping for resilient networks[C]//Vehicular Technology Conference. 2004: 3291-3295.

[15] ERIKSSON J, FALOUTSOS M, SRIKANTH V, et al. Routing amid colluding attackers[C]//IEEE International Conference on Network Protocols, 2007.

[16] REED M, GOLDSCHLAG D. Onion routing[J]. Communications of the ACM, 1999(42): 39-41.

[17] GOLDSCHLAG D M, MICHAEL G R, PAUL F. Syverson hiding routing information.[J] Information Hiding, Springer Berlin Heidelberg, 1996, 1174: 137-150.

[18] SHI L, JIA C, LÜ S, et al. Port and address hopping for active cyber-defense[M]// Intelligence and Security Informatics. Springer Berlin Heidelberg, 2007:295-300.

[19] CHOWDHARY A, SANDEEP P, DIJIANG H. SDN based scalable MTD solution in cloud network[J]//2016 ACM Workshop on Moving Target Defense. 2016: 27-36.

[20] SONG H, GONG J, CHEN H, et al. Unified POF programming for Diversified SDN Data Plane[J]. Eprint Arxiv, 2014: 92-97.

[21] AL-SHAER E. Toward network configuration randomization for moving target defense[J]. Moving Target Defense, Springer New York, 2011: 153-159.

[22] ASOKAN N, VALTTERI N, KAISA N. Man-in-the-middle in tunnelled authentication protocols[C]//International Conference on Security Protocols. 2003: 42-48.

[23] BOSSHART P, DAN D, IZZARD M, et al. Programming protocol-independent packet processors[J]. ACM Sigcomm Computer Communication Review, 2013, 44(3): 87-95.

[24] WANG Z, WANG L, GAO X, et al. An architecture of content-centric networking over protocol-oblivious forwarding[C]//IEEE Globecom Workshops. 2015: 1-5.

[25] TAN X, ZOU S, GUO H, et al. POFOX: towards controlling the protocol oblivious forwarding network[M]//Advances in Parallel and Distributed Computing and Ubiquitous Services. Springer Singapore, 2016.

[26] HU D, LI S, XUE N, et al. Design and demonstration of SDN-based flexible flow converging with protocol-oblivious forwarding (POF)[C]//IEEE Global Communications Conference. 2015: 1-6.

[27] CORBETT C, UHER J, COOK J, et al. Countering intelligent jamming with full protocol stack agility[J]. IEEE Security & Privacy Magazine, 2014, 12(2): 44-50.

[28] 张朝昆, 崔勇, 唐翯祎, 等. 软件定义网络 (SDN) 研究进展[J]. 软件学报, 2015, 26(1): 62-81.
ZHANG C K, CUI Y, TANG H Y, et al. State-of-the-art survey on software-defined networking (SDN)[J]. Journal of Software, 2015, 26(1): 62-81.

[29] CARROLL T E, CROUSE M, FUIP E W, et al. Analysis of network address shuffling as a moving target defense[C]//2014 IEEE International Conference on Communications (ICC). 2014: 701-706.

[30] 石乐义, 贾春福, 吕述望. 基于端信息跳变的主动网络防护研究[J]. 通信学报, 2008, 29(2): 106-110.
SHI L Y, JIA C F, LYU S W. Research on end hopping for active network confrontation[J]. Journal on Communications, 2008, 29(2): 106-110.

[31] MA D, XU Z, LIN D. A moving target defense approach based on POF to thwart blind DDoS attack[C]//International Conference on Computer Communications & Networks. 2015.

[32] 李佟, 葛敬国, 鄂跃鹏, 等. 基于标签的 POF 网络虚拟化技术研究[J]. 计算机应用研究, 2017, 34(3).
LI T, GE J G, E Y P, et al. Label-based POF network virtualization[J]. Application Research of Computers, 2017, 34(3).

[33] MA D H, WANG L, LEI C, et al. Thwart eavesdropping attacks on network communication based on moving target defense[C]// Performance Computing and Communications Conference (IPCCC). 2017: 1-2.

[34] JAJODIA S, WANG C, SUBRAHMANIAN V, et al. Cyber deception[M]. Springer International Publishing, 2016.

[35] JAJODIA S, PARK N, PIERAZZI F, et al. A probabilistic logic of cyber deception[J]. IEEE Transactions on Information Forensics & Security, 2017(99): 1-1.

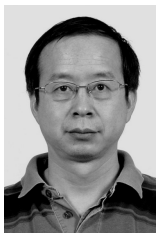
[36] ALBANESE M, BATTISTA E, JAJODIA S. Deceiving attackers by creating a virtual attack surface[M]//Cyber Deception. Springer International Publishing, 2016.

[37] AL-SHAER E, GILLANI S F. Agile virtual infrastructure for cyber deception against stealthy DDoS attacks[M]//Cyber Deception. Springer International Publishing, 2016.

[作者简介]

马多贺（1982-），男，安徽霍邱人，博士，中国科学院信息工程研究所助理研究员，主要研究方向为移动目标防御、应用安全、云安全、网络与系统安全等。

李琼（1976-），女，湖南吉首人，博士，哈尔滨工业大学教授、博士生导师，主要研究方向为量子密码、多媒体安全、生物识别等。



林东岱（1964-），男，山东聊城人，中国科学院信息工程研究所研究员、博士生导师，主要研究方向为密码理论、安全协议、网络空间安全等。