doi:10.3969/j.issn.1000-436x.2013.08.012

Smart-blacklisting: P2P 文件共享系统假块污染攻击对抗方法

姚汝颢[1]，刘丙双[1]，曲德帅[2]，周渊[2]，韩心慧[1]
（1. 北京大学 计算机科学技术研究所 互联网安全技术北京市重点实验室，北京 100080；
2. 国家计算机网络应急技术处理协调中心，北京 100029）

摘 要：在当前十分流行的 P2P 文件共享网络中，假块污染攻击严重地干扰了正常的文件下载过程。提出了基于概率统计及多轮筛选的对抗假块污染攻击策略——Smart-blacklisting，从理论上证明了该策略的有效性。仿真实验结果表明，该策略可以保证目标文件成功下载并降低假块污染攻击对下载时间及带宽消耗的影响。当攻击强度为 0.2 时，下载时间仅为 eMule 系统黑名单方法的 13%，在带宽消耗方面也仅为其 50%。

关键词：P2P 文件共享系统；eMule；BitTorrent；假块污染攻击
中图分类号：TP393.0 **文献标识码**：A **文章编号**：1000-436X(2013)08-0088-07

Smart-blacklisting: an efficient methodology for mitigating fake block attack in P2P file-sharing systems

YAO Ru-hao[1], LIU Bing-shuang[1], QU De-shuai[2], ZHOU Yuan[2], HAN Xin-hui[1]
(1. Beijing Key Laboratory of Internet Security Technology, Institute of Computer Science and Technology, Peking University, Beijing 100080, China;
2. National Computer Network Emergency Response Technical Team/Coordination Center of China, Beijing 100029, China)

Abstract: Fake block attack intends to prolong the downloading time by providing fake data to make the file block fail in the hash check. P2P file-sharing systems are susceptible to fake block attacks, whereby malicious clients are able to make a big impact on users' downloading experience. An efficient methodology named Smart-blacklisting, which aims to lessen the downloading time and bandwidth wastes interfered by the attack was proposed through using a mathematic model, and the efficiency of this method was analyzed during a simulation experiment. The ovel approach presents 87% downloading time and 50% bandwidth wastes compare less than those of eMule blacklisting method.

Key words: P2P file-sharing system; eMule; BitTorrent; fake block attack

1 引言

P2P 文件共享系统使用户能够更方便地下载到音乐、电影、游戏和软件。自诞生的那一刻起就引起了广泛的争论。普通用户利用 P2P 软件可以更方便、更快捷地下载到所需要的信息，而版权商却因此受到了巨大的损失。虽然面临着多种问题，P2P 文件共享系统也在不断发展进步。第一代集中式 P2P 文件共享软件 Napster[1]在唱片公司的起诉下，最终宣告破产。在此影响下，第二代的 P2P 文件共享软件 Gnutella[2]和 Kazaa[3]开始采用完全去中心化的 P2P 拓扑网络结构。2007 年，Gnutella 成为了互联网上最流行的文件共享软件，市场份额超过 40%。第三代以 eMule[4]和 BitTorrent[5]为代表的 P2P 文件共享软件改善了分布式网络的拓扑结构，结合了 KAD DHT[6]与 Tracker/ed2k 服务器的优势，使节点之间搜索文件的效率得到明显提升，并增强了网络应对恶意攻击的抵抗能力。

随着 P2P 共享软件的不断发展，在其网络上的各种攻击行为也呈现出愈演愈烈的趋势。常见的攻击方式有 Sybil 攻击[7]、索引节点污染攻击(index poisoning)[8]、eclipse 攻击[9]、文件污染攻击[10]和假块污染攻

收稿日期：2013-04-29；修回日期：2013-06-17
基金项目：国家自然科学基金资助项目（61272536）
Foundation Item: The National Natural Science Foundation of China (61272536)

击[11]。对于普通用户，这些攻击行为严重影响了搜索和下载资源的效率。本文研究的假块污染攻击发生在数据下载阶段，攻击节点通过在 P2P 文件共享网络中伪造大量虚假客户端，接受其他节点的下载请求后上传虚假数据，从而导致下载节点因为校验失败而丢弃大量数据，延长下载时间并增加带宽浪费，严重的情况下会使用户无法成功下载到目标文件。

2　相关研究工作及背景知识

2.1　相关研究工作

近些年来，P2P 文件共享系统被越来越广泛地应用，根据文献[12]可知，在欧洲地区，P2P 文件共享网络带宽消耗占整个网络中的 70%，据 Cisco 专家估算，P2P 流量将持续增长，预计 2014 年的 P2P 流量将会较 2009 年翻倍。P2P 文件共享系统的安全性已经受到国内外学者及工程人员的重视。在各种各样的安全威胁下，文件污染攻击与假块污染攻击被认为占据着重要的部分。

文献[13]对 4 种流行的 P2P 文件共享系统中的文件污染状况进行了测量，证实了文件污染攻击普遍存在。文献[14]通过对 KAD 网络中伪造文件名称及文件元信息的状况进行测量从而揭示了文件污染攻击对用户的影响。与文件污染攻击相比，假块污染攻击也普遍存在于 P2P 文件共享网络中。因其攻击方式更加隐蔽，用户只有在下载文件的过程中才会受到攻击，这给探测与对抗假块污染攻击提出了更高的要求。文献[15]中的研究结果表明，一种综合节点索引攻击和假块污染攻击的方式将会给 P2P 文件共享网络带来更大的影响，表明了抵御假块污染攻击的重要性。文献[16]对 BitTorrent 网络中假块污染攻击的状况进行了测量，并提出简单的对抗策略。但由于仅在一个 tracker 服务器上进行测量实验，并且只选取了票房最高的 20 部影片，从而使测量结果具有局限性。而其提出的基于节点上传数据正确性状况的比率进行判定的黑名单方式，由于受到攻击节点规模、文件块下载并行度和攻击节点攻击策略等多方面的影响，并不具备实际可用性，在本文实验部分对其和 Smart-blacklisting 的有效性进行了评估，表明了其方法的局限性和不足。文献[11]提出了对 BitTorrent 验证协议的完善，虽然可以解决假块污染攻击的问题，但其对协议层的修改会造成原有版本不兼容的问题，这会在很大程度上影响 P2P 共享网络的可用性。文献[17]提出了一种集中式的爬虫机制，主动探测文件污染和假块污染攻击节点，但由于 P2P 网络庞大的节点和文件规模，使其可用性大大降低。

本文提出的应对假块污染攻击的 Smart-blacklisting 策略，并没有对 P2P 协议层进行修改，保证了 P2P 文件共享系统的兼容性。与已有方法相比，Smart-blacklisting 更重视保证普通用户的下载过程，最大程度上降低假块污染攻击对下载时间的影响。由于 Smart-blacklisting 应用在普通用户的客户端上，并不需要集中式的处理，从而完整地维护了 P2P 分布式网络的灵活性及完整性。

2.2　背景知识

2.2.1　P2P 文件下载及验证机制

P2P 文件共享网络客户端下载文件的步骤如下：客户端首先寻找目标文件的下载来源，然后对文件分块下载。文件下载来源的获取可以通过中心服务器[18]（eMule/aMule）/tracker 服务器[19]（BitTorrent）或者基于 Kademlia 协议的分布式散列表（DHT）。

为了加快文件的下载，P2P 文件共享网络软件采用如图 1 所示的分块下载方式。在 eMule/aMule 中，每个文件会被首先划分为 9.28 MB 的块（part），然后每个块会被细分为 180 KB 大小的块（block）。在 BitTorrent 中，每个文件会被首先划分为 256 KB 的片（piece），之后每个片会被进一步划分为 16 KB 的块（block）。

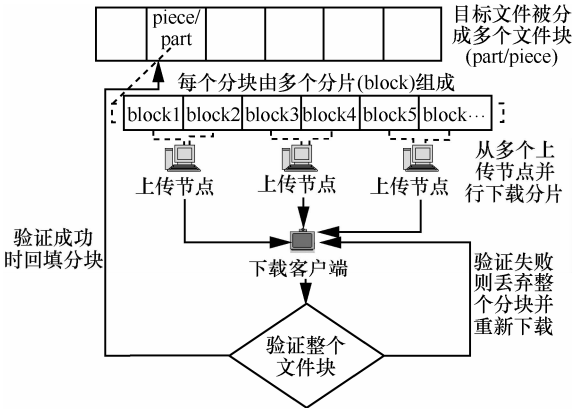


图 1　P2P 文件共享系统下载及验证机制

当 P2P 文件共享软件客户端下载到目标文件的一个文件块（piece/part）时，通常是从多个节点下载到同一文件块的部分来加快下载速度。当文件块下载完成时，客户端通过计算整块的散列值来验证数据的完整性和正确性。如果散列验证失败，客户端则丢弃整个文件块（piece/part）并重新下载。

2.2.2 假块污染攻击原理

假块污染攻击(fake block attack)[11]是在文件交换过程中针对分块机制的一种攻击方式，攻击者通过上传虚假分片（block），造成文件块验证失败，从而浪费大量的带宽。例如在 BitTorrent 协议中，客户端每下载完一个分块（256 KB），都会验证对应块的散列值，如果验证失败则丢弃整个分块。而假块污染攻击客户端只需要在一个大分块内上传一个错误的小分块，就可以造成整个分块校验失败，由于不能定位具体错误小分块，下载客户端就会丢弃整个分块。

在当前 P2P 共享软件黑名单策略中，当整个分块验证失败时，下载客户端会将所有参与上传该分块数据的节点加入屏蔽黑名单，从而导致一部分上传了正确数据的节点被屏蔽。因此，假块污染攻击客户端会拖累一部分好的客户端，使得下载客户端很难选择到好的客户端，最终导致下载时间大量延长甚至下载失败。

文献[11]中的分析表明，影响假块污染攻击效果的主要因素有文件的热度、块内并行度、攻击者的带宽、攻击节点数和污染带宽扩散系数。因此，对抗假块污染攻击的基本方法有：降低块内并行度，让节点尽量从一个下载源下载一个完整的分块，并消除污染带宽扩散系数，减少因为校验失败而丢弃的数据量。

2.2.3 eMule 对抗假块污染攻击的黑名单策略

当前主流的 P2P 文件共享软件均采用基于信誉值的黑名单机制来抵御假块污染攻击。在 eMule 0.50a 版本的实现如下。

$$\frac{nDataCorrupt}{nDatacorrupt + nDataVerified} > BanThreshold$$

其中，*nDataCorrupt* 为验证失败的块（part）中所丢弃的该节点上传总量，*nDataVerified* 为验证成功块（part）中该节点的上传总量，*BanThreshold* 为 0.32。当节点该值大于 *BanThreshold* 时，会被系统封禁 2 h。

本文提出的 Smart-blacklisting 对抗策略通过在校验失败时降低块内并行度，并根据校验失败时下载并行度给节点的攻击行为进行罚分，通过多轮的筛选方式，最终帮助客户端成功下载到目标文件，并有效地降低了假块污染攻击对下载时间和带宽消耗的影响。

3 Smart-blacklisting 算法

3.1 算法介绍

基于已有对抗假块污染攻击方法的局限性，本文提出了 Smart-blacklisting 算法；在文件传输过程中对上传节点攻击行为进行评估，当文件块散列验证失败时，依据文件块的下载并行度给每个节点进行罚分，以降低这些节点被再次选入下载队列的优先级，并适当降低下载并行度。重新下载文件块时，优先选择罚分最小的节点，通过多次尝试及筛选，最终完成文件下载。

图 2 所示为单个 FileBlock 下载时的对抗策略，每一轮从罚分最小的节点中选取，当多个 FileBlock 并行下载时，共同更新全局上传节点列表的罚分，使得 P2P 文件共享客户端可以更快地筛选出正常节点并完成下载。

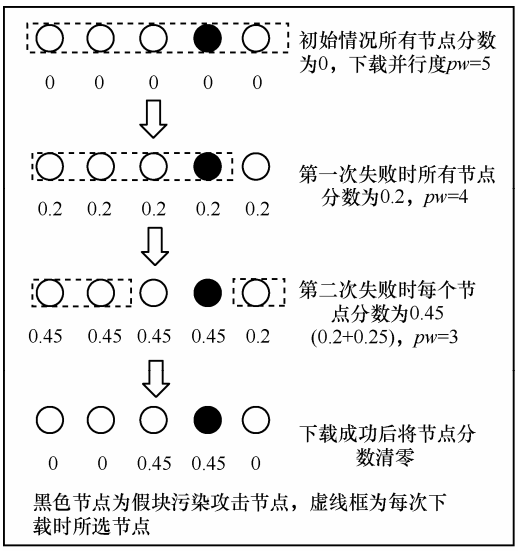


图 2 Smart-blacklisting 策略示意

算法描述如下。

算法 1 Smart-blacklisting 文件块下载

输入：文件块的散列，攻击节点判定阈值 *T*

输出：文件分块 *partFile* //如果失败 *partFile* = null

1) 上传节点列表 *uploadPeerList*:($peer_1$, $peer_2$, …, $peer_n$)。

2) 攻击节点列表 malPeerList //初始为空。

3) 块下载并行度 *pw*。

4) *partFile* = null。

5) Repeat

6) 从 *uploadPeerList* 中选择 *pw* 个最小 point 的 *peer* 加入到 *downloadQueue* 中。

```
7)    if downloadQueue.isEmpty() then
8)      return null
9)    end if
10)   从 downloadQueue 中下载 fileBlock。
11)   if hash Check(fileBlock) == false then
12)     for all peer in downloadQueue do
13)       peer.point = peer.point + 1/pw
14)       if pw == 1 or peer.point > T then
15)         uploadPeerList.remove(peer)
16)         malPeerList.add(peer)
17)       end if
18)     end for
19)     c = min(c−1, 1)
20)     partFile = null
21)   else
22)     for all peer in downloadQueue do
23)       peer.point = 0
24)     end for
25)   end if
26)   downloadQueue.clear()
27) until partFile ≠ null
28) return partFile
```

Smart-blacklisting 算法在没有假块污染攻击时不会有额外的处理，在保证文件下载成功的情况下，尽量减小下载延时受假块污染攻击的影响。Smart-blacklisting 算法并不需要像文献[11]一样修改协议层的实现，因此可以在保证 P2P 文件共享系统兼容性的情况下来缓解假块污染攻击造成的影响。下面通过模型分析和仿真实验验证 Smart-blacklisting 算法的有效性。并根据成功下载完成时节点罚分的分布情况提出 T 的取值范围。

3.2　模型分析

模型分析中各符号的含义如表 1 所示。

表 1　　模型分析符号

符号	含义
N	正常上传节点数
M	假块污染攻击节点数
pw	下载并行度
P_{succeed}	P(单次下载成功)
P_{fail}	P(单次下载失败)
$P_{x\text{-attacknode}}$	P(x 个攻击节点 | 单次下载失败)
$E_{\text{ar-df}}$	E(攻击节点率 | 单次下载失败)
E_{ar}	E(单次下载包含攻击节点率)
$E_{\text{rt-sb}}$	E(Smart-blacklisting 重试下载次数)
$E_{\text{rt-eMule}}$	E(eMule 重试下载次数)

式(1)为单个文件块单次下载成功的概率，选取的上传节点全部为正常节点。

$$P_{\text{succeed}}=\frac{C_N^{pw}}{C_{N+M}^{pw}} \tag{1}$$

式(2)中当选取的上传节点包含假块污染攻击节点时，会导致下载失败。

$$P_{\text{fail}}=1-\frac{C_N^{pw}}{C_{N+M}^{pw}} \tag{2}$$

式(3)表示当单次下载失败时，所选节点中包含 x 个假块污染攻击节点的概率。

$$P_{x\text{-attacknods}}=\frac{C_M^x C_N^{pw-x}}{C_{N+M}^{pw}-C_N^{NW}} \tag{3}$$

$$E_{\text{ar-df}}=\sum_{x=1}^{pw}\frac{C_M^x C_N^{pw-x}}{C_{N+M}^{pw}-C_N^{pw}}\cdot\frac{x}{pw}>E_{\text{ar}}=\frac{M}{N+M} \tag{4}$$

由式(4)可得，每次下载失败后 Smart-blacklisting 筛选策略在平均情况下会减小剩余节点中假块污染攻击节点所占比率的数学期望。

对于不同的 $pw_1>pw_2$

$$\begin{aligned}E_{\text{ar-df}(pw_1)}&=\sum_{x=1}^{pw_1}\frac{C_M^x C_N^{pw_1-x}}{C_{N+M}^{pw_1}-C_N^{pw_1}}\cdot\frac{x}{pw_1}<E_{\text{ar-df}(pw_2)}\\&=\sum_{x=1}^{pw_2}\frac{C_M^x C_N^{pw_2-x}}{C_{N+M}^{pw_2}-C_N^{pw_2}}\cdot\frac{x}{pw_2}\end{aligned} \tag{5}$$

由式(5)可得，Smart-blacklisting 算法针对节点下载并行度的特定罚分($\frac{1}{pw}$)，有助于区分正常节点和假块污染攻击节点的上传行为，从而提高下载成功率。上传节点被罚分越多，该节点为攻击节点的概率就越大。

由于 Smart-blacklisting 算法依据下载并行度对节点的惩罚力度加以区分，下载失败后的重试时优先使用包含攻击节点率低的节点，并且经过每次失败下载，在平均情况下，剩余节点中攻击节点比率的数学期望减小。因此，Smart-blacklisting 算法存在重试下载次数有限的上限。

$$P_{\text{rt-sb}}<\frac{C_{N+M}^{pw}}{C_N^{pw}} \tag{6}$$

由于 eMule 在高强度攻击的状况下可能下载不成功，即使其成功时由于式(1)中每次的成功率较低，所以重试次数的数学期望更多；而式(4)中 Smart-blacklisting 策略会减少剩余节点中假块污染攻击节点所占比率的数学期望，式(5)中依据并行度罚分可以区分节点的上传行为，即

$$E_{\text{rt-sb}} < E_{\text{rt-6Mule}} \tag{7}$$

4 仿真实验

4.1 实验环境及参数设定

实验基于 ubuntu 12.04 上的 OMNeT++4.2.2[20]版本进行仿真。实验中实现了 Smart-blacklisting 策略，由于当前假块污染攻击对抗策略的相关研究较少，考虑到文献[11]中对抗策略的协议兼容性等问题，本文选取了 eMule 黑名单策略[4,16]中的 H_3 策略进行对比试验，为了仿真 eMule 系统中的下载环境，具体参数选择如表 2 所示。

表 2　　仿真实验参数

参数名	参数值
正常上传节点数	N = 100
假块污染攻击节点数	M
攻击节点判定阈值	T
攻击强度	M/N
节点并行度	pw = 20
下载文件块数	*partFileNum* = 100
单个 *partFile* 包含的 block 数	53（与 eMule 系统一致）
单个 block 大小	*blockSize* = 180 KB
文件大小	954 MB

实验仿真了一个客户端下载文件的过程，实验中假设所有上传节点都拥有完整文件，单个上传节点带宽有限。通过增大假块污染攻击的强度，比较 Smart-blacklisting 算法同 eMule 当前黑名单算法以及文献[15]中 H_3 算法的下载时间延时和带宽消耗情况。4.4 节分析了当文件成功下载后每个节点的罚分分布，给出了选取攻击节点判定阈值 T 的范围。

4.2 下载时间分析

在下载时间实验中，随着攻击强度的加大，Smart-blacklisting 方法基本保证了文件能够成功下载，并且尽可能地减少下载过程受到假块污染攻击的影响。由图 3 可以看出，文献[16]中的 H_3 方法的效果在不同 T 时差别很大。而影响到 T 的因素有下载并行度、攻击节点上传比率、攻击节点规模等多种因素，在实践环境下很难找到最优值。即使在文献[16]中推荐阈值 T=0.5 的情况下，当攻击强度大于 0.2 时，H_3 也无法成功下载整个文件。而 eMule 中采用的传统黑名单方法由于误判率较高，导致大部分正常节点都被假块污染攻击节点拖累进黑名单，严重地影响了下载过程。当攻击强度大于 0.2 时，所有正常节点都被误判成攻击节点，最终导致下载失败。对于 Smart-blacklisting 算法，即使在攻击强度为 1 的情况下，也可以成功下载文件。通过实验对比表明了 Smart-blacklisting 算法对于抵御假块污染攻击的有效性以及相较已有方法的优势。

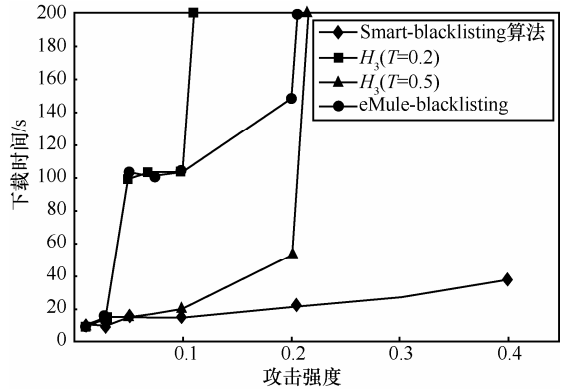


图 3　下载时间测试结果

4.3 带宽消耗分析

在带宽消耗的仿真实验中，Smart-blacklisting 算法也明显优于已有方法。值得注意的是，虽然在攻击强度处于[0.01, 0.2]时，eMule-blacklisting 和 $H_3(T$=0.2) 的下载延时是 $H_3(T$=0.5)和 Smart-blacklisting 下载延时的 5 倍左右，但带宽的消耗却没有这样大的差别。这是因为在 eMule-blacklisting 和 $H_3(T$=0.2)中大量节点被黑名单所屏蔽，所以可供客户端连接的节点数量相较 $H_3(T$=0.5)和 Smart-blacklisting 的差距明显。因此在上传节点带宽有限的情况下，下载延时相比后两者更加明显。

在 P2P 文件共享系统中，大部分的开销集中在带宽消耗上。根据图 4 可知，Smart-blacklisting 算法可以明显减小带宽消耗受到假块污染攻击的影响，因此该方法的运营开销和效率也优于当前已有方法。

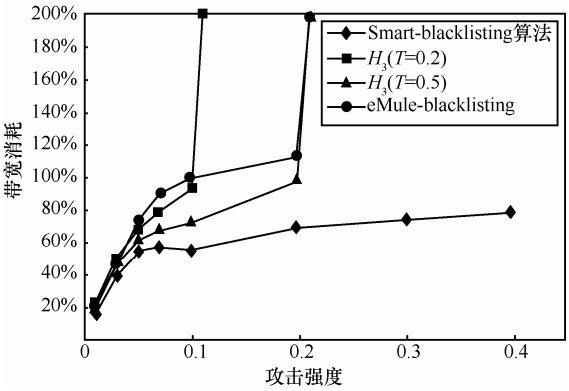


图 4　带宽消耗测试结果

4.4　节点罚分分析

图 5 统计了当攻击强度为 0.4 时，文件成功下载后上传节点的罚分分布情况。当节点罚分小于 3 时，Smart-blacklisting 算法的误判率为 0。在实际应用中，在保证下载成功率及下载速度的前提下，可以将 T 尽可能设小，这样可以避免假块污染攻击节点对带宽消耗和下载时间的影响；当可选节点数较小时，可适当提高 T 以使文件成功下载。Smart-blacklisting 算法可以帮助 P2P 客户端尽快地筛选出正常的上传节点，如图 5 中罚分在[0,3)的节点，从而帮助客户端更快下载完目标文件。

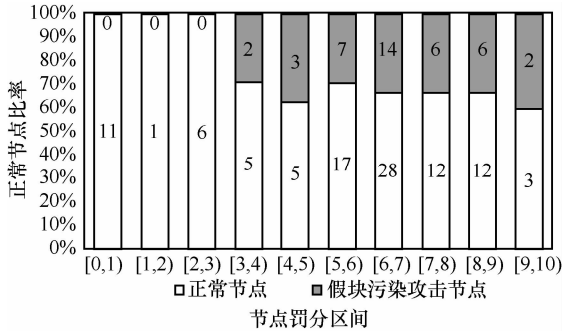


图 5　下载成功后节点罚分分布（攻击强度为 0.4）

根据 4.2 节和 4.3 节的实验结果，当攻击强度大于 0.4 时，eMule-blacklisting 和 H_3 方法已经无法完成下载，而根据图 5 中的实验结果，在罚分[0,3)区间内全部为正常节点。这个结果与 3.2 节中的模型分析一致。

当多个文件块并行下载时，由于块内下载并行度较大，会导致部分正常上传节点被并行罚分。这种情况主要发生在罚分较多的正常上传节点上，因此增加了假块污染攻击节点的误判率。下一步工作中将通过调整 Smart-blacklisting 中的并行罚分策略来降低误判率。

5　结束语

由于 P2P 文件共享软件在传输过程中的散列校验存在缺陷，使得假块污染攻击有了可乘之机。对于 eMule 和 BT 等 P2P 文件共享系统，假块污染攻击在文件传输阶段导致用户下载速度严重下降，带宽浪费加大，影响了系统的可用性，并且威胁到了系统的安全。本文提出了基于概率统计及多轮筛选方式的 Smart-blacklisting 防御策略，通过模型分析和仿真实验，与已有方法相比，Smart-blacklisting 方法对于假块污染攻击有更强的对抗能力。在保证用户下载成功的前提下，在下载延时和带宽消耗方面也优于当前已有方法。由于不需要对已有 P2P 文件系统验证的协议层进行修改，使得 Smart-blacklisting 具有良好的兼容性，很容易在当前系统中实现。

下一步的工作将会测量整个 P2P 共享网络系统中的假块污染攻击状况，并依据实际测量结果调整 Smart-blacklisting 的部分参数，使其在真实的网络环境中更加有效，并降低假块污染攻击节点的误判率。与此同时，还将在主流 P2P 文件共享系统中实现 Smart-blacklisting 策略，提升 P2P 软件对于假块污染攻击的对抗能力。

参考文献：

[1] Napster [EB/OL]. http://en.wikipedia.org/wiki/Napster.

[2] Gnutella [EB/OL]. http://en.wikipedia.org/wiki/Gnutella.

[3] Kazza [EB/OL]. http://en.wikipedia.org/wiki/Kazaa.

[4] eMule [EB/OL]. http://www.emule-project.net/.

[5] BitTorrent [EB/OL] http://www.bittorrent.com/.

[6] MAYMOUNKOV P, MAZIERES D. Kademlia: A Peer-to-Peer Information System Based on the XOR Metric[M]. Springer Berlin Heidelberg, 2002. 53-65.

[7] DOUCEUR J R. The Sybil Attack[M]. Springer Berlin Heidelberg, 2002. 251-260.

[8] LIANG J, NAOUMOV N, ROSS K W. The index poisoning attack in P2P file sharing systems[A].IEEE INFOCOM[C]. Barcelona, Spain, 2006. 1-12.

[9] SINGH A. Eclipse attacks on overlay networks: threats and defenses[A]. IEEE INFOCOM[C]. Barcelona, Spain, 2006. 22-30.

[10] LIANG J, KUMAR R, XI Y, *et al*. Pollution in P2P file sharing systems[A]. INFOCOM 2005 24th Annual Joint Conference of the IEEE Computer and Communications Societies[C]. Miami, USA, 2005. 1174-1185.

[11] 史建焘, 张宏莉, 方滨兴. BitTorrent 假块污染攻击的对抗方法研究[J]. 计算机学报, 2011, 34(1):15-24.
SHI J T, ZHANG H L, FANG B X, Study on the countermeasures of Bit Torrent fake block attack[J]. Chinese Journal of Computers, 2011, 34(1):15-24.

[12] SCHULZE H, MOCHALSKI K. Internet study 2008/2009[J]. IPOQUE Report, 2009, 37:351-362.

[13] CHRISTIN N, WEIGEND A S, CHUANG J. Content availability, pollution and poisoning in file sharing peer-to-peer networks[A]. Proceedings of the 6th ACM Conference on Electronic Commerce ACM[C]. Vancouver, Canada, 2005. 68-77.

[14] MONTASSIER G, CHOLEZ T, DOYEN G, *et al.* Content pollution quantification in large P2P networks: a measurement study on KAD[A]. Peer-to-Peer Computing(P2P), 2011 IEEE International Conference on IEEE[C]. Tokyo, Japan, 2011. 30-33.

[15] KONG J, CAI W, WANG L, *et al*. A study of pollution on BitTorrent[A]. Computer and Automation Engineering (ICCAE), 2010 The 2nd International Conference on IEEE[C]. 2010. 118-122.

[16] `DHUNGEL P, WU D, ROSS K W. Measurement and mitigation of BitTorrent leecher attacks[J]. Computer Communications, 2009, 32(17):1852-1861.

[17] LIANG J, NAOUMOV N, ROSS K W. Efficient blacklisting and

pollution-level estimation in P2P file-sharing systems[A]. Technologies for Advanced Heterogeneous Networks[C]. Springer Berlin Heidelberg, 2005. 1-21.
[18] Ed2k URI scheme [EB/OL]. https://en.wikipedia.org/wiki/Ed2k_URI_scheme.
[19] BitTorrent tracker [EB/OL]. https://en.wikipedia.org/wiki/ BitTorrent_tracker.
[20] OMNeT++ [EB/OL]. http://omnetpp.org/.

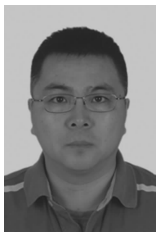
作者简介：

姚汝颢（1989-），男，宁夏银川人，北京大学硕士生，主要研究方向为 P2P 网络安全。

刘丙双（1985-），男，河北唐山人，北京大学博士生，主要研究方向为 P2P 网络安全。

曲德帅（1975-），男，辽宁大连人，国家计算机网络应急技术处理协调中心工程师，主要研究方向为信息安全与网络攻防。

周渊（1972-），男，江苏无锡人，国家计算机网络应急技术处理协调中心高级工程师，主要研究方向为互联网安全。



韩心慧[通信作者]（1969-），男，河南开封人，博士，北京大学高级工程师，主要研究方向为网络与信息安全。

（上接第 87 页）

[11] XIAO G Z, MASSEY J L. Aspectral charact erizat ion of correlation-immune comb ining functions[J]. IEEE Trans IT , 1988, 34(3):569-571.
[12] 冯登国, 肖国镇. 有限域上的函数的相关免疫性和线性结构的谱特征[J]. 通信学报,1997, 18(1):40-45.
FENG D G, XIAO G Z. Spectral characterization of correlation-immune and linear structures of functions over finite field[J]. Journal on Communications, 1997, 18(1):40-45.

作者简介：

李卫卫（1980-），女，上海人，硕士，上海政法学院讲师，主要研究方向为计算机取证与现代密码学。