匿名协议 AMIMR 的抗攻击性分析

郑 明[1,2] 吴建平[1,3]

[1](清华大学计算机科学与技术系 北京 100084)

[2](国防科学技术大学军队政工研究所 湖南 长沙 410074)

[3](清华大学信息网络工程研究中心 北京 100084)

摘 要 匿名通信是一种非常有效的隐私保护方法。但是在匿名通信发展的同时,针对匿名通信的攻击也在增加。分析恶意攻击者对低延迟匿名通信协议进行攻击的过程和方法,并提出防御攻击的方法。根据防御方法,提出利用源地址扩展,基于单向混淆环路进行匿名通信的 AMIMR(Anonymous Communication over Invisible Mix Rings)协议,并描述节点特性、结构特性、拓扑特性和功能特性。对 AMIMR 协议的抗攻击性进行的分析表明协议在阻断攻击过程、抵抗被动攻击和主动攻击方面具有很强的抗攻击性。模拟表明 AMIMR 协议即使在恶意节点率较高的情况下仍然可以获得较高的匿名性。AMIMR 协议的局限性在于部分节点会受到所在网络规则的限制。

关键词 匿名通信 源地址扩展 混淆环路 抗攻击性

中图分类号 TP393 **文献标识码** A

DOI:10.3969/j.issn.1000-386x.2012.10.001

ANALYSING ATTACK TOLERANCE OF ANONYMOUS PROTOCOL AMIMR

Zheng Ming[1,2] Wu Jianping[1,3]

[1](*Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China*)

[2](*Institute of Military Political Work, National University of Defense Technology, Changsha 410074, Hunan, China*)

[3](*Information Network Engineering Research Center, Tsinghua University, Beijing 100084, China*)

Abstract Anonymous communication is a very effective measure for privacy protection. However, the attacks against anonymous communication are also increasing at the time of the development of anonymous communication. In this paper, we first analyse the method and the process of attack against low-latency anonymous communication by malicious attacker and present some defense methods. According to those methods, we then propose a protocol of anonymous communication over invisible mix rings (AMIMR), which utilises the extended source address. We analyse the features of nodes, structure, topology and function in AMIMR. Our analysis on attack tolerance of AMIMR shows that this protocol has strong attack tolerance in blocking attack process and resisting passive attacks and active attacks. Simulation indicates that AMIMR still has high anonymity even in circumstance of quite high malicious node rate. The limitation of AMIMR is that part of its nodes may be restricted by the rule of networks where it is.

Keywords Anonymous communication Source address extension Mix rings Attack tolerance

0 引 言

随着互联网的发展,安全和隐私问题越来越受到用户的重视。匿名通信是目前最有效的隐私保护手段之一。但是随着匿名通信的发展,针对匿名通信的攻击也越来越多。目前提出的低延迟匿名通信协议大部分都具有典型的基于连接特征,即通信路径一般由多个匿名代理串行连接。其通信过程分为两个阶段:一是路径建立阶段,即让路径上的中间节点知道其后继节点和前驱节点,从而建好转发路径;二是数据传输阶段,发送者将数据沿着建好的路径传送给接收者。整个协议通过保证建路的安全性和信息传输的不可追踪性来实现通信的匿名性。而且其一般都基于某个密钥基础设施,即需要信任中心为节点事先分配密钥或密钥参数。在这类匿名通信中,节点一般在建路阶段依靠事先已有的公钥或共享密钥加密传输下一跳路径信息和协商共享会话密钥。在数据传输阶段,节点依靠已协商好的共享会话密钥对收到的信息进行加解密操作,从而做到入出信息的无法关联。

从以往的研究[1]可知所有基于连接的低延迟匿名通信系统都存在被动攻击的威胁。例如流量分析攻击[2]、时间攻击[3]、水印攻击[4]和前驱攻击[5]等被动攻击方式是基于连接的

收稿日期:2012-08-06。2012 中国计算机大会论文。国家自然科学基金项目(60803134);国家重点基础研究发展计划项目(2009CB320505);国家高技术研究发展计划项目(60203044)。**郑明**,讲师,主研领域:网络安全评估,隐私保护。**吴建平**,教授。

低延迟匿名通信系统无法从根本上解决的。虽然低延迟匿名通信系统的设计者们不断地提出改进的方法[6],但是攻击的方法也在不断地进步[7]。目前研究者们提出随机漫游,多链路传输加秘密共享或者数据分片,多路径网络编码等方法来削弱基于路径的持续连接或者数据流特征,但是无法完全消除连接特征,只是增大了攻击者收集信息的难度。

我们在混淆环路 Mix Ring 协议[8]的基础上提出了一种基于不可见混淆环路的低延迟匿名通信协议 AMIMR[9],通过进行源地址扩展和建立有向不可逆环路,实现混淆环路的不可见化,能够消除数据流特征、连接特征,并对关键节点和关键信息进行了保护。本文通过分析恶意攻击者对低延迟匿名通信协议进行攻击的过程和方法,总结匿名通信协议进行防御的方法,并依据分析结果对 AMIMR 协议进行抗攻击性分析。

1 匿名通信的威胁模型

匿名通信系统一般通过提出威胁模型来表明该系统能够防御攻击者。攻击者的能力分为三个方面:可达能力、攻击能力和适应能力。

攻击者的可达能力分为全局和本地两种。具有全局能力的攻击者可以访问所在网络中所有的节点和链路,而具有本地能力的对手只能访问所在网络中部分的节点和链路。

攻击能力分为被动和主动两种。攻击的目的是为了识别消息的发送者或接收者。被动攻击一般由匿名通信网络的外部观测者发起,其主要行为为观测网络中传输的消息、网络中数据的流量,并通过对消息和流量的分析达到攻击的目的。主动攻击一般由匿名通信网络的内部节点发起,其主要行为为通过其控制的部分通信节点修改通信消息、追溯通信行为、修改通信行为,来达到攻击的目的。

适应能力分为动态和静态两种。在匿名通信系统中,攻击者的适应能力一般是动态的,动态地跟踪网络的变化,实时地收集路径选择算法信息,实时地监控网络传输的消息和流量的变化。

2 匿名通信中的攻击和防御

2.1 匿名通信的攻击过程

在匿名通信系统中,攻击者进行一次完整的攻击一般经过:① 信息收集阶段,也就是攻击的准备阶段;② 攻击实施阶段,即攻击者使用什么方法进行攻击。这两个阶段并不是完全独立的,信息收集阶段所做的工作是攻击实施的前提,没有充分地收集到详细的资料,有经验的攻击者是不会贸然采取攻击行动的。而攻击的实施是依据所收集到的信息进行分析,然后进行相应的行动。而且,这两个阶段从时间上完全分开是不可能的,攻击者在攻击实施的过程中,经常会多次收集信息,帮助其进行下一步的动作。在一次攻击的动作结束后,通过信息的收集,验证攻击的有效性。

在经过攻击准备阶段以后,攻击者根据收集到的信息,开始进行攻击。在攻击实施中,将攻击分为主动攻击和被动攻击两种。被动攻击的特点是偷听或监视传送,其目的是获得正在传送的信息。主动攻击涉及修改数据流或创建错误的数据流,它包括假冒、重放、修改信息等。

2.2 低延迟匿名通信的攻击方法

2.2.1 被动攻击方法

流量分析攻击[2] 基于低延迟匿名通信系统一个转发节点接收到的数据会在短时间内连续转发的特点,因此当一个节点连续向另一节点转发多个数据包后,攻击者能记录下转发的数据包数,然后观察下一节点是否会将同样数量的数据包快速转发给另一个节点,并利用这个方法一直追踪到数据的最终目的地。

时间攻击[3] 假设攻击者控制了匿名通信链路的入口和出口节点,攻击者观测到入口节点获得一个转发数据包后,记录下发生时间,当链路的出口节点获得一个数据包后,同样记录下发生时间。当对大量数据包进行这种统计后,攻击者可以通过概率统计来确定哪些数据包处于同一个匿名通信流中。

水印攻击[4] 攻击者通过在匿名通信链路的入口处主动扰乱转发时间或者使数据包形成特定流量特征的方法来形成水印,然后在出口处检测水印,以此确定是否属于同一个匿名通信流。

前驱攻击[5] 是一种和时间攻击配合使用的攻击手段。攻击的主要原理是基于用户偏好对真实用户进行推测。一个用户可能会长时间访问相同的某些资源,而攻击者则会以一定的概率出现在访问者的信道当中,如果有多个节点进行合谋,根据推算可以在较短时间内实现对真实发送者的追踪。

2.2.2 主动攻击方法

路径选择攻击[10] 是恶意节点攻击通信发起者周围的邻居节点。例如恶意节点可以使用洪泛的方法使目标节点周围的正常邻居节点服务能力降低,只留下恶意节点。在这种情况下,通信发起者选择的所有合作节点将很大几率是恶意节点。

拥塞攻击[11] 是攻击者刻意制造大流量任务,然后测量匿名通信系统中各个节点的转发延迟,以判定哪些节点在为这个大流量任务服务,从而进一步追踪通信的真实双方。因为一般情况下 P2P 匿名通信系统中的转发节点大多是普通的个人主机,可利用资源有限,而且低延迟匿名通信系统为了保证系统效率,大多采用先来先服务策略,所以大流量的转发任务会损害同时进行的其他任务的转发效率。McLachlan 等将拥塞攻击实施在了 Morph Mix 系统中,Evans 等又对该攻击方式做了扩展,有效降低了攻击者需要的资源,而且攻击效果更明显。

封锁攻击[12,13] 是攻击者作为恶意节点获取大量匿名通信节点的地址,通过控制网络路由、设置过滤、攻击入口节点或者目录服务器等方法破坏匿名用户与匿名通信系统间的可达性,以达到降低匿名通信系统可用性的目的。

2.3 匿名通信的防御方法

1) 限制信息泄露

信息泄漏是低延迟匿名通信中最难解决的问题。网络延迟将泄漏信息并破坏匿名性。源地址和目标地址也将泄漏信息并破坏匿名型。张甲等提出了 IPv6 的匿名通信中一个轻量级扩展。他利用 DHCPv6 扩展匿名节点在 IPv6 网络中使用的源地址。这种源地址扩展能限制信息的泄漏。

2) 保护关键节点

目前最广泛使用的 Tor 通过谷歌的电子邮件系统来保护他们的入口-桥节点地址。Tor 每次只公布三个桥节点地址。并且 Tor 定期更换桥地址,以防止它们被封锁。这是一种利用带外数据对关键节点进行保护的方法。

3) 消除数据流特征

为了消除数据流的特点,它通常可以建立多个连接或覆盖信道来实现这一效果。但建立多个连接的成立将引入新的问题,如建立多个链接将导致在合作节点的数量大幅增加,节点故障会降低效率,或不能在出口节点组装出一个完整的数据流。覆盖信道也可以隐藏数据流的特点,但它会导致沟通效率下降。他们限制了低延迟匿名通信的能力范围。

4) 消除连接特征

为了消除连接的特点,随机漫游通过不同的转发路径转发的关键和消息[8]。多路径网络编码把信息拆分成多个部分并独立编码[11]。我们知道,多路径将会使覆盖拓扑变复杂,更加容易增加了威胁。文献[8]引入环路的方式来取代连接模式。而环路模式不会把拓扑结构变复杂,并且有效地消除了连接特征。

3 AMIMR 的特性

3.1 AMIMR 的节点特性

AMIMR 的中转节点需要拥有使用扩展源地址的能力。在 IPv4 环境中是可以使用伪造源地址,在 IPv6 环境中时可以通过 DHCPv6 获得多个 IPv6 地址[14]。拥有使用扩展源地址的能力会帮助节点抵抗流量分析的威胁。

3.2 AMIMR 的结构特性

单向混淆环路是 AMIMR 的匿名信道结构。环路上的节点将自己要发送的信息转发到环路上。目录服务器指定的出口节点向环路外的目的节点转发并接收响应。出口节点将响应数据包打包后转发到环路上。环路上的每个节点在接收到数据包后都检查是否属于自己的。如果是则解包,如果不是则向下一跳转发。

3.3 AMIMR 的拓扑特性

AMIMR 中的节点可以同时属于多个单向混淆环路。只有建环者掌握环路上所有的节点地址。其他的节点只知道自身的下一跳地址。而通过数据包中的环路标识号来判断数据包属于哪一个环路,并重新打包后按照转发表进行转发。

AMIMR 为了获得更好的效率,采用了混合 P2P 结构,在不同的自治域之间是网状结构,在自治域内是混合结构。节点可以分为目录服务器,骨干节点和普通节点。

3.4 AMIMR 的匿名功能特性

AMIMR 中的正常节点是要求有使用扩展源地址能力的。在发送或者接收匿名数据包的时候不会被网络安全规则过滤。但是受限节点处于部署了源地址验证或者进行了过滤设置的网络。所以 AMIMR 采用 pass 数据包来支持受限节点的匿名化。受限节点自身不建立环路,而是将匿名数据包向目录服务器提供的环路节点进行发送。环路节点接收到 pass 包后按照正常的匿名数据包向下一跳转发。同时目录服务器会指定环路上的两个节点分别作为该任务的入口节点和出口节点。这种 pass 功能可以为不具备使用扩展源地址能力的节点提供匿名服务,同时保证匿名性不下降。

3.5 AMIMR 的系统功能特性

AMIMR 中的正常节点在进行转发的时候会对转发的数据包进行 repackage,即常见包格式的重构。每次转发都对数据包的进行重编码,套用常见通信协议的包格式。

AMIMR 还会随机的进行环路微调。如果一个环路长期运行,泄露的信息会随着时间增长而增加。AMIMR 会定期对环路进行微调。改变环路上的节点数量和参与节点。

4 AMIMR 的抗攻击性分析

要研究一个匿名通信协议的抗攻击性,可以从阻断或延缓攻击过程和防御攻击方法两个方面来进行研究。

4.1 阻断攻击过程

在攻击的信息收集阶段,尽可能的减少攻击者能收集到的信息是一个重要的阻断手段。

1) 保护节点源地址信息

因为 AMIMR 的节点采用了源地址扩展,IPv4 环境下节点可以使用伪造源地址,IPv6 环境下节点可以使用伪造源地址或者通过 DHCPv6 获得多个源地址[14],使得攻击者在收集系统信息的时候复杂度上升,并且无法获得真实的节点地址信息。

2) 消除数据流特征

为了消除数据流特征,一般匿名协议可以通过建立多条链路或者发送掩饰流来达到这个效果。但是建立多条链路会引入新的问题,例如建立多条链路会导致合作节点的数量大幅度增加,节点失效会导致在出口节点处无法组合出完整的数据流或者效率下降。通过掩饰流来隐藏数据流特征也会导致通信效率的下降,在低延迟匿名通信中的适用范围有限。

AMIMR 引入混淆环路,通过多个中转节点组成环路来消除从发送者到出口节点的数据流特征。因为环路中的节点都以中转节点的形态存在,而且每个节点都借助于环路进行匿名通信。

3) 消除连接特征

为了消除连接特征,AMIMR 引入有向不可逆环路。对于攻击者来说,匿名通信行为的发起者、中转节点、出口节点不再存在连接特征。而对于发起者和接收者两端的上层应用来说,逻辑上的双向连接仍然存在。

4) 限制用户申请中转节点的数量和频率

通过限制用户节点申请中转节点的数量和申请频率,使攻击者一方面无法在短期内获得大量的节点地址和服务端口等信息,另一方面也无法判断出通信发起者的邻居节点和选择的中转节点信息。

5) 保护目录服务器和全局数据

因为 AMIMR 需要一个或多个目录服务器来进行全局数据的保存以及用户节点的注册和资源申请,所以 AMIMR 可以说是有中心的。有中心存在也就是有弱点存在。为此 AMIMR 使用了 Fast-flux[15]保护目录服务器免受封锁攻击。Fast-flux 的基本原理是利用一些具有公共 IP 地址的主机作为代理(flux-agent),服务器域名被解析为这些 flux-agent 的 IP 地址,真实的目录服务器隐藏在 flux-agent 背后提供服务。为保持可用性和隐蔽性,和域名关联的 flux-agent 的 IP 地址一直不停地变化。Fast-flux 带来的主要好处就是非常好的隐蔽性,使得目录服务器难以被跟踪和发现。从而抵抗封锁攻击对目录服务器的影响。

4.2 防御被动攻击方法

1) 防御水印攻击

在会话中数据包如果不改变编码的话,攻击者很容易通过对信息流进行重新编码打上水印来追踪到信息,AMIMR 采用常

用包结构将每个经过的匿名数据包重新打包。在数据包重新路由的时候,每个数据包都会改变编码结构。如此则可以使水印攻击失效。

2) 防御本地协作攻击

当 AMIMR 的目录服务器进行混淆环路创建时,环上的节点尽量属于不同的自治域。这样本地协作攻击是无法获得环路上更多信息的。

3) 防御时间攻击

AMIMR 使用了扩展源地址,动态源端口和动态目的端口。从数据流的角度来看不存在两个连续的数据包。攻击者不能确定哪些数据包属于同一个数据流。这样就使时间攻击失效。

4) 防御前驱攻击

AMIMR 的信道采用的是单向环路结构,数据包的源地址采用了扩展源地址,恶意节点是无法通过猜测前驱节点的真实地址来获得前驱的位置的。

5) 防御流量分析攻击

和时间攻击一样,AMIMR 消除数据流特征的特性决定了恶意节点是无法判断哪些数据包属于同一个数据流。因此,恶意攻击者也无法进行流量分析。

6) 防御回溯攻击

AMIMR 采用了扩展源地址。每个节点对于自身的上一跳节点的真实地址是无法确定的。因此,无法通过地址的收集进行回溯。

4.3 防御主动攻击方法

1) 防御路径选择攻击

AMIMR 的中转节点会定期随机生成服务端口号,使攻击者收集到的节点信息定期失效。同时限制用户申请中转节点的数量和频率。这样可以减少攻击者收集到的信息,使可供使用的路径信息无法满足路径选择攻击的需要。

2) 防御针对拥塞攻击

AMIMR 利用目录服务器统计环标识号的对应的环长度并建立环标识号与发送者的对应关系表。当一个发送者试图建立超过目录服务器授权中转节点数长度的环时,目录服务器判定该发送者是恶意节点,并标识出该发送者。当环标识号没有对应的发起者时目录服务器判定该建环请求为恶意,并拒绝建环验证。这样拥塞攻击也会因此减少。

3) 防御封锁攻击

AMIMR 加强了对目录服务器的保护,封锁攻击试图攻击目录服务器的威胁降低了。而因为扩展源地址的存在,入口节点地址泄露的几率也会降低。这样能有效的防御封锁攻击。

5 模拟试验

假设系统中存在 N 个节点。所有 N 个节点的通信行为在理想情况下使每个节点被确定作为发送方的几率是 $1/N$。系统熵的计算公式为:

$$H(X) = -\sum_{i=1}^{N} p_i \log_2 p_i = \log_2 N \tag{1}$$

然而,恶意节点在 P2P 系统中是不可避免的。假设 N 个节点中恶意节点占总节点数比例为 p。如果我们不考虑其他特殊攻击战略,系统熵的计算公式为:

$$H(X) = \log_2(1-p) \times N \tag{2}$$

那么存在 M 个恶意节点的匿名系统的匿名度为:

$$D(X) = \log_2(1-p) \times N/\log_2 N \tag{3}$$

因为 AMIMR 中的节点具有扩展源地址特性,假设一个正常的节点可以使用 R 个扩展的源地址,并且第 4 节的分析显示 AMIMR 可以有效地抵御被动攻击。如果一个恶意节点进入环路,它只能获得其继任者的真实地址。那么恶意节点比例为 p 的 AMIMR 的匿名度可以用下式表示:

$$D(X) = \frac{H(X)}{H_{\max}}(X) = \frac{\log_2(N \times (1-p) \times (R \times (1-p) + p))}{\log_2(N \times (R \times (1-p) + p))} \tag{4}$$

当系统的节点中存在受限节点时,假设受限节点占总节点比率为 q。那么匿名系统的匿名度可以用下式表示:

$$D(X) = \frac{H(X)}{H_{\max}}(X) = \frac{\log_2(N \times (1-p) \times ((1-q) \times (R \times (1-p) + p) + q))}{\log_2(N \times ((1-p) \times (R \times (1-q) + q) + p))} \tag{5}$$

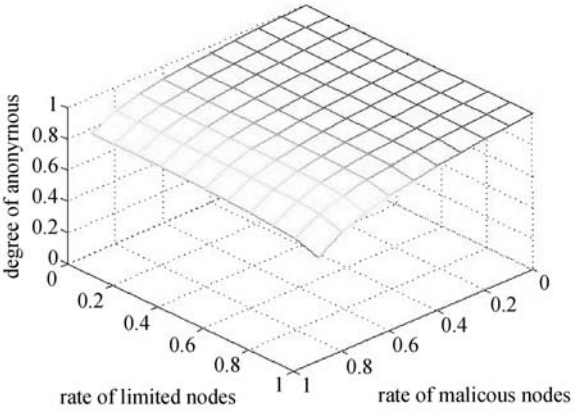

图 1 节点数为 1000 时系统的匿名度变化

我们使用 MATLAB 对 AMIMR 系统的匿名度进行了模拟,在节点数达到 1000,源扩展地址的长度为 255 时,恶意节点比率和受限节点比率从 0 到 1 变化,步长为 0.1。可以从图 1 中看到,恶意节点比率和受限节点比率都会影响系统的匿名度。恶意节点比例在 0.6 以上时系统的匿名度才会明显下降到 0.8 以下。受限节点比例对系统的匿名度的影响不是很明显,仅在比例非常高的时候才会影响到系统的匿名度。

6 AMIMR 的局限性讨论

AMIMR 的局限性在于 AMIMR 协议会受到节点所处网络环境的影响。AMIMR 协议是在 Mix Rings 协议基础之上通过进行源地址扩展和单向化实现的环路不可见化。当 AMIMR 协议部署在不具有源地址扩展能力的受限节点上时,需要使用 pass 数据包并依靠环路节点的辅助才能实现数据包的匿名化。因此,受限节点在接受环路节点辅助时,负责转发 pass 数据包的节点如果是恶意节点,则受限节点完全失去的由匿名系统带来的地址匿名性。而且受限节点处于源地址扩展受限或者安全规则过滤的网络中,面临的被动攻击威胁的机会比正常节点要大。恶意节点伪装成受限节点对中转网络进行主动攻击也会对匿名系统的匿名性和性能产生比正常节点更大的影响。

为了保证整个匿名系统的匿名度,AMIMR 的中转网络需要由一定数量具有使用扩展源地址能力的正常节点组成。当正常

(下转第 35 页)

参 考 文 献

[1] Akyildiz I F, Akan B, Chen C, et al. InterPlaNetary Internet: State-of-the-Art and research challenges[J]. Computer Networks, 2003, 43(2):75-112.

[2] 熊永平, 孙利民, 牛建伟, 等. 机会网络[J]. 软件学报, 2009, 20(1):124-137.

[3] Grossglauser M, Tse Dnc. Mobility increases the capacity of ad hoc wireless networks[J]. IEEE/ACM Trans. on Networking, 2002, 10(4): 477-486.

[4] Juang P, Oki H, Wang Y, et al. Energy-efficient computing for wild life tracking: Design trade-offs and early experiences with ZebraNet[J]. ACM SIGARCH Computer Architecture News, 2002, 37(10): 96-107.

[5] Widmer J, Boudec J L. Network coding for efficient communication in extreme networks[C]//Proceedings of the 2005 ACM SIGCOMM Workshop on Delay-Tolerant Networking. Philadelphia: United States of America, 2005: 284-291.

[6] Wang Y, Jain S, Martonosi M, et al. Erasure-Coding based routing for opportunistic networks[C]//Proceedings of the 2005 ACM SIGCOMM Workshop on Delay-Tolerant Networking. Philadelphia: United States of America, 2005: 229-236.

[7] Chen L, Yu C, Sun T, et al. A hybrid routing approach for opportunistic networks[C]//Proceedings of the 2006 SIGCOMM Workshop on Challenged networks. Pisa, Italy, 2006: 213-220.

[8] Luo T Q, Zhang J, Wang Y. Fault-Tolerant Transfer Algorithm Based on Interweaving Code in Opportunistic Networks[J]. Applied Mechanics and Materials, 2011, 63-64: 341-344.

(上接第 4 页)

节点的数量不足和受限节点的比例过高时,都会影响整体系统的匿名性。

针对网络环境产生的局限性,我们采用受限节点认证的机制来降低恶意节点伪装成受限节点的几率。辅助受限节点的环路节点是恶意节点的情况目前还没有有效的方法解决,受限节点的地址信息无法匿名化,只能通过辅助节点随机化来降低风险。

7 结论和展望

本文的研究切入点是满足低延迟匿名通信协议抗攻击的需求。本文分析了目前低延迟匿名通信中的攻击过程和各种攻击方法,并整理了防御攻击的方法,描述了 AMIMR 协议[8]在节点、结构、拓扑、功能等方面的特性,对 AMIMR 协议从攻击过程,防御被动攻击和防御主动攻击方面进行抗攻击性分析。由分析可知通过有向混淆环路建立不可见匿名信道的 AMIMR 系统可以抵抗基于连接的低延迟匿名通信系统目前面临的各种被动攻击,对于恶意节点的主动攻击也有较好的抵抗能力。AMIMR 协议中节点的匿名性会受到所在网络环境影响,普通节点需要骨干节点的辅助,但是在利用混淆环路进行通信时整体系统的匿名性不会受到太大影响。受限制少的骨干节点加入网络能显著提高 AMIMR 的匿名性。AMIMR 作为一种低延迟匿名通信协议从节点特性、结构特性、拓扑特性、功能特性上获得了很好的抗攻击能力。

我们的下一步研究工作是解决 AMIMR 节点的激励机制问题,保证匿名节点的可信性和激励参与,避免 free-riding 等行为的产生。

参 考 文 献

[1] Serjantov, Sewell P. Passive attack analysis for connection-based anonymity systems[C]//Computer Security-ESORICS 2003. Springer-Verlag, LNCS (forthcoming), October 2003.

[2] Adam Back, Ulf Möller, Anton Stiglic. Traffic Analysis Attacks and Trade-Off in Anonymity Providing Systems[C]//Proceedings of Information Hiding Workshop (IH2001), 2001:245-257.

[3] Levine B N, Reiter M K, Wang C, et al. Timing Attacks in Low-Latency Mix-Based Systems[C]//Proceedings of the 8th International Conference on Financial Cryptography (FC'04), Florida, USA, 2004:251-265.

[4] Xinyuan Wang, Shiping Chen, Sushil Jajodia. Network Flow Watermarking Attack on Low-Latency Anonymous Communication Systems[C]//2007 IEEE Symposium on Security and Privacy (SP'07), 2007:116-130.

[5] Wright M K, Adler M, Levine B N, et al. The Predecessor Attack: an Analysis of a Threat to Anonymous Communications Systems[J]. ACM Transactions on Information and System Security (TISSEC), 2004, 7(4):489-522.

[6] Wiangsripanawan R, SusiloW, Safavi-Naini R. Design Principles for Low Latency Anonymous Network Systems Secure Against Timing Attacks[C]//Proceedings of the 5th Australasian symposium on ACSW frontiers, Victoria, Australia, 2007:183-191.

[7] Danezis G, Syverson P. Bridging and Fingerprinting: Epistemic Attacks on Route Selection[C]//Proceedings of the 8th International Symposium on Privacy Enhancing Technologies (PET), Leuven, Belgium, 2008:151-166.

[8] Burnside M, Keromytis A D. Low latency anonymity with mix rings[C]//Information Security, Proceedings 4176, 2006:32-45.

[9] Zheng Ming, Duan Haixin, Wu Jianping: Anonymous Communication over Invisible Mix Rings[C]//Proceedings of the 11th international conference on Algorithms and architectures for parallel processing-Volume Part I:182-193.

[10] Pappas V, Athanasopoulos E, Ioannidis S, et al. Compromising Anonymity Using Packet Spinning[C]//Proceedings of 11th Information Security Conference(ISC 2008), 2008:161-174.

[11] Hopper N, Vasserman E Y, Chan-Tin E. How Much Anonymity Does Network Latency Leak? [C]//Proceedings of the 14th ACM Conference on Computer and Communications Security(CCS), Alexandria, USA, 2007:82-91.

[12] Ding le dine R, Mathewson N. Design of a blocking resistant anonymity system [EB/OL]. 2007. [2009/04/20]. http://www.torproject.org/svn/trunk/doc/design paper/blocking.pdf.

[13] Kopsell S, Hilling U. How to achieve blocking resistance for existing systems enabling anonymous web surfing[C]//WPES 2004, Washington: ACM, 2004:47-58.

[14] Jia Z, Haixin D, Wu L, et al. A light-weighted extension of anonymous communications in IPv6 Network[C]//International Conference Green Circuits and Systems (ICGCS), 2010:404-408.

[15] Know Your Enemy: Fast-flux Service Networks[R]. The Honey net Project and Research Alliance, 2007.