基于 APT 潜伏攻击的网络可生存性模型与分析

姚 苏[1,2],关建峰[3],潘 华[2],张宏科[1]
(1. 北京交通大学电子信息工程学院,北京 100044;2. 中国航空综合技术研究所,北京 100028;
3. 北京邮电大学,北京 100876)

摘 要: 基于传统网络攻击模式和高级持续性威胁(Advanced Persistent Threat,简称 APT)攻击模式提出网络可生存性的评估模型. 建立网络攻击场景,仿真验证提出的网络可生存性模型,并比较两种模式的性能. 得到的结论:提出的评估模型合理刻画了网络可生存性的两个重要参数,网络攻击传播速率和网络修复速率;基于 APT 潜伏攻击模式下的网络可生存性性能低于传统攻击模式.

关键词: 潜伏攻击;网络可生存性;评估模型;马尔科夫链
中图分类号: TP393.0 **文献标识码:** A **文章编号:** 0372-2112 (2016)10-2415-08
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2016.10.020

Modeling and Analysis for Network Survivability of APT Latent Attack

YAO Su[1,2], GUAN Jian-feng[3], PAN Hua[2], ZHANG Hong-ke[1]
(1. *School of Electronics and Information Engineering, Beijing Jiaotong University, Beijing* 100044, *China*;
2. *China Aero-Polytechnology Establishment, Beijing* 100028, *China*;
3. *Beijing University of Posts and Telecommunications, Beijing* 100876, *China*)

Abstract: The paper proposes the model of network survivability based on the patterns of normal network attack and APT attack. The model is demonstrated by constructing the simulation scenarios of network attack to analyze their performances. The results show that this evaluation model can effectively reflect two parameters: the speeds of network attack propagation and network recovery, and the performance of network survivability of APT attack pattern is lower than that of normal attack pattern.

Key words: APT; network survivability; evaluating model; Markov chain

1 引言

高级持续性威胁(Advanced Persistent Threat,简称 APT)是目前计算机网络安全界关注的最热门话题之一[1]. 特别是 2010 年谷歌宣布遭受极光攻击[2],伊朗核设施遭受震网(Stuxnet)病毒攻击等一系列极具破坏性的事件[3],打破了人们对传统网络攻击的认识,如震网病毒已经造成伊朗核电站推迟发电. 从图 1 所示的 APT 攻击[4],可以看出,APT 攻击已经成为近年来网络攻击的主要手段之一.

"潜伏性和持续性"是 APT 攻击最主要的特征[5]. "潜伏性"表示 APT 攻击并非进入用户网络中就立即发动攻击,通常会有一个潜伏期,这个潜伏期可长可短. 在潜伏期内,不断收集各种信息,直到收集到重要情报,能彻底掌握所针对的目标人、事、物. 因此,APT 攻击模式实质上是一种"恶意商业间谍威胁". "持续性"体现在网络攻击者不断尝试各种攻击手段,以及渗透到网络内部后长期蛰伏,继而不断发动攻击,从而达到破坏用户网络的目的[5].

目前,针对 APT 网络攻击的研究还处于初级阶段,

稿日期:2014-10-28;修回日期:2015-10-30;责任编辑:郭游
基金项目:国家 973 重点基础研究发展规划(No. 2013CB329101);国家自然科学基金(No. 61232017, 61003283);国家科技重大专项(No. 2013ZX03006002)

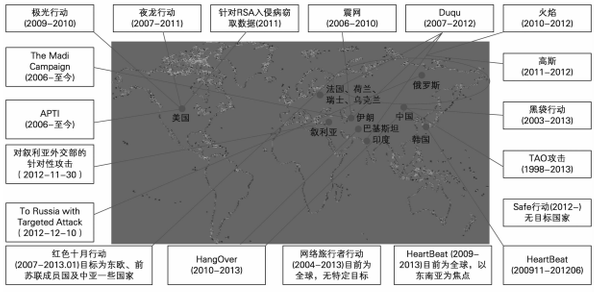


图1 近年的主要APT攻击分布[4]

开展的研究主要在 APT 攻击的案例分析[7]、特征值提取[8]、检测机制[9]等方面,并没有从网络可生存性的角度分析.

网络可生存性(Network Survivability)[10]泛指网络在出现故障损坏、遭受攻击或不可预知的事故时,仍然能够及时完成关键任务(提供服务)的能力,它属于网络安全性和可靠性的一部分. 目前,国内外对于网络可生存性并未有统一的定义,不过得到广泛共识的是美国国家标准学会(American National Standards Institute,简称 ANSI) T1A1.2 网络可生存性标准委员会给出的定义[11],网络可生存性包括两个方面:(1)在网络出现故障的情况下,通过各种恢复技术,来维持或恢复网络服务使之达到可接受的状态;(2)网络通过应用预防技术,从故障节点中减轻或预防服务失效. 可生存性通常用生存率来表示,即当某条链路或者节点出现故障时,可从其它链路上疏通的业务量与该链路所传送的业务量之比. 图 2 给出的可生存性量化指标的说明[12]. X 轴表示时间,Y 轴表示网络的可生存性. 该曲线刻画了网络遇到故障或者攻击时,网络可生存性度量值即阻塞概率随着时间产生的变化. 在故障或攻击发生之前,阻塞概率为 m_a;故障或攻击发生后,经过时间 t_r 后,阻塞概率为 m_r;经过时间 t_R 后,阻塞概率恢复到 m_a.

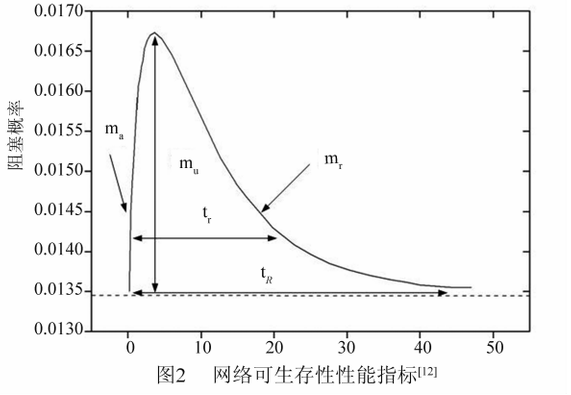


图2 网络可生存性性能指标[12]

目前,针对网络可生存性的研究主要集中在故障或者意外事故前提下开展的研究[13,14]. 如文献[13]提出了一种基于飓风灾难条件下的网络可生存性模型,采用连续时间马尔科夫链的分析方法,详细分析了灾难传播和恢复过程,并总结了三种不同的灾难恢复机制. 文献[14]改进了文献[13]提出的连续时间马尔科夫链分析方法,并提出了一种基于地震灾难条件下的网络可生存性模型,并与实际情况比较,验证了该模型的合理性. 文献[15]在注重提高网络可生存性的同时,也兼顾服务可区分性的要求,提出了一种主动服务漂移的模型,增强了对不同网络环境的可生存性适用性. 文献[16]针对大规模网络场景下提出了一种提高网络可生存性方法,文献[17]给出了网络可生存的评估体系. 可以看出,针对网络攻击特别是新的网络攻击(诸如 APT 攻击)的特点,而开展的网络可生存性研究较少. 本文结合 APT 攻击的隐蔽性特点,即网络中的节点被攻击后有潜伏期特点,构建 APT 攻击下的网络可生存性模型,并对分析了其网络可生存性性能.

本文第二节叙述 APT 攻击下的网络生存性模型;第三节简要介绍在 APT 攻击下使用该模型对网络生存性分析;第四节验证网络可生存性模型的正确性,仿真 APT 攻击下的网络生存性指标并与传统攻击模式进行比较;第五节提出建议并进行总结.

2 模型建立

2.1 网络可生存性模型

由于攻击是包含时间序列的单个事件,为了评估和分析网络遭受攻击时的可生存性,本文研究定量评估模型,给出一种网络可生存性模型.

假设该攻击初始于接入网的某个子网,之后攻击传播到下一个子网,之后依次传播. 这种传播可以称作攻击传播,它是一种级联状行为. 不同于故障的传播特点,网络攻击传播可以发源于内部网络,并且有多个状态.

此外,网络可以被看作有一个包含节点和有向边的有向图. 节点表示网络中基础设施(终端、路由设备等),有向边表示信息传播的方向. 网络系统的脆弱性表现为攻击的初始状态和传播状态都是基于某个随机事件. 因此,这种传播过程可以被视为随机过程.

假设网络的节点数量为 n,攻击事件将有以下几个步骤. 不失一般性,网络攻击最初发生于节点 1. 接着,在一个随机时间内,攻击从被感染的节点传播到下一个节点,节点间的攻击传播视为有向边. 这种传播被视为“无记忆”性的,攻击事件从一个节点传播到另一个节点仅依赖于当前的系统状态,而与系统的历史状态无关. 由于攻击的传播速度和方向是

由外部攻击源等条件决定的因此遭受攻击的节点可以在一个随机时间内被修复. 假设攻击的传播速率和修复时间服从指数分布,本文的研究重点在网络初始被攻击,攻击传播直至网络系统完全被修复的传播时段,其过程符合连续时间的马尔科夫随机过程的约束条件.

假设在有限状态空间 $S=\{1,2\cdots,n\}$ 中$\{X,t>0\}$表示网络系统中的各个节点的状态. 每一个接入网都有 n 个不同区域的子网组成. 网络攻击在整个网络中传播. 在任意时刻 t,网络系统的状态可以由以下 n 维向量表示

$$X(t)=(X_1(t),X_2(t),\cdots X_n(t)),t\geqslant 0 \tag{1}$$

对于子网 $k\in\{1,2,\cdots,n\}$,$X_k(t)$表示在时刻 t 子网 k 的状态. 对于子网 k,它有两种状态,一种是遭受攻击的状态“0”,另一种是正常状态“1”. 当网络攻击未发生时,此时子网 k 状态为正常状态“1”;当子网 k 在时刻 t 遭受攻击时,此时子网状态由正常状态“1”变为“0”;经过时间 t',子网 k 由状态“0”修复为“1”.

$$X_k(t)=\begin{cases}1,\text{正常状态,子网未被攻击}\\0,\text{感染状态,子网被攻击}\end{cases} \tag{2}$$

此外,每次只能对一个子网发动攻击;在本文中,子网作为最小的网络系统单位,只有当子网完全被攻击后,子网才开始修复过程;攻击和修复的传播过程只取决于当前子网状态,而与到达当前状态的路径没有关系.

根据上述假设,攻击传播过程中的子网状态 $X(t)$ 可以被看作为一个连续时间的马尔科夫链,它的状态空间为:

$$\Omega=\{(X_1,X_2,\cdots,X_n),X_1,X_2,\cdots,X_n\in(0,1)\} \tag{3}$$

状态空间 Ω 总共包含 $N=2^n$ 个状态. 子网状态 $X(t)$从$(0,1,\cdots,1)$开始,结束于$(1,1,\cdots,1)$,这表明网络中所有子网都依次遭受到攻击,并且依次恢复到正常状态.

简而言之,网络可生存的模型可以归纳为以下几点:

(1)在某时刻 t,子网的状态只有两种状态$\{0,1\}$;

(2)在初始时刻 $t=0$,第一个子网遭受攻击,此时网络的状态为$(0,1,\cdots,1)$;

(3)攻击从子网 $k-1$ 传播到子网 k 服从泊松随机过程,传播的速率为 λ_k;

(4)每个子网只有一次修复过程并且子网中的终端都可以同时被修复完成,子网 k 的平均修复速率服从指数分布值为 μ_k.

根据上述的假设,在状态空间 S,子网的修复过程可以从数学上建模为时间上均匀分布的连续时间马尔科夫链(Continuous-Time Markov Chain,CTMC).

对每个状态而言,有 $t\geqslant 0$ 和 $i\in S$,我们定义 t 时刻处于状态 i 的概率为:

$$\pi_i(t)=\Pr\{X(t)=i\} \tag{4}$$

假设 $X(t)$的传播概率的列向量为

$$\pi(t)=[\pi_1(t),\pi_2(t),\cdots,\pi_N(t)] \tag{5}$$

当系统处于状态 $i\in S$,ψ_i 为系统的回报率. 因此,根据连续时间马尔科夫链的状态空间,系统的回报率也可用列向量表示为:

$$\psi=[\psi_1,\psi_2,\cdots,\psi_N] \tag{6}$$

根据上述模型,可以有多种测算方式来测算网络的可生存性性能. 由于无法在系统修复期间准确预估系统的状态,我们考虑从正常工作的网络系统中获取性能指标的预估值. 在我们的模型中,系统的回报作为系统性能的重要指标. 在时刻 t 网络可生存性性能由系统瞬时的预估回报 $E[M(t)]$表示:

$$E[M(t)]=\sum_{i\in\Omega}\gamma_i\pi_i(t) \tag{7}$$

假设系统是有序的,在状态 $1,2,\cdots,k$ $(k<N)$有故障传播,在状态 $k+1,k+2,\cdots,N$ 系统处于恢复状态. 此时,$\{X(t),t\geqslant 0\}$的转移矩阵为

$$P=\begin{pmatrix}p_{11}&\cdots&p_{1k}&\cdots&p_{1N}\\\vdots&\ddots&\vdots&\ddots&\vdots\\p_{k1}&\cdots&p_{kk}&\cdots&p_{kN}\\\vdots&\ddots&\vdots&\ddots&\vdots\\p_{N1}&\cdots&p_{Nk}&\cdots&p_{NN}\end{pmatrix} \tag{8}$$

其中,p_{ij}表示状态 i 转移到状态 j 的转移概率.

根据状态转移矩阵 P,连续时间马尔科夫链的动态行为可以由柯式差分微分方程表示:

$$\frac{d\pi(t)}{dt}=\pi(t)P \tag{9}$$

则状态转移概率矩阵 $\pi(t)$为

$$\pi(t)=\pi(0)e^{Pt}=\pi(0)\sum_{i=0}^{\infty}e^{-\alpha t}\frac{(\alpha t)^i}{i!}Q^i \tag{10}$$

2.2　APT 潜伏攻击模式的网络可生存模型

APT 潜伏攻击模式,网络攻击并非一触即发的,通常会潜伏在所攻击的网络系统,并在某个时刻触发,方才发动攻击,它的攻击更具有隐蔽性并且破坏性更强. 因此,不同于正常状态,对于子网 $k\in\{1,2,\cdots,n\}$,$X_k(t)$表示在时刻 t 子网 k 的状态. 此时,对于子网 k,它有三种不同状态:(1)健康状态“1”;(2)遭受 APT 攻击后的休眠状态“0”;(3)遭受 APT 攻击后的活跃状态“0′”[18].

$$X_i(t)=\begin{cases}Hea.,\text{健康状态.}\\Inf.,\text{感染状态}\begin{cases}Act.,\text{活跃状态,}\\Dor.,\text{休眠状态.}\end{cases}\end{cases} \tag{11}$$

如图 3 所示,当网络攻击未发生时,此时子网 k 状

态为健康状态“1”;当子网 k 在某时刻 t 遭受攻击时,此时子网状态由健康状态“1”进入休眠状态“0”;再经过时间 t',子网 k 由休眠状态“0”进入活跃状态为“0′”;此时,子网探测到来自外部的 APT 攻击,开始进行修复;经时间 t'',子网 k 由活跃状态修复为健康状态.

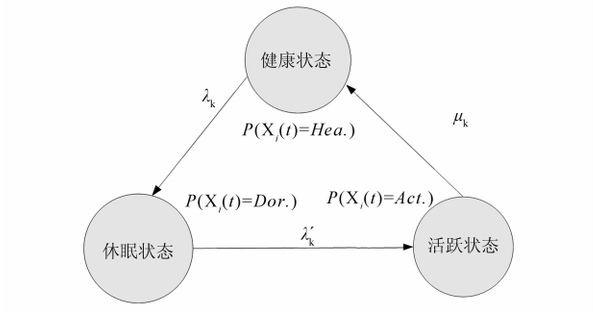


图3 APT攻击模式下节点状态转移

同样,APT 攻击下的攻击传播过程中的子网状态 $X(t)$ 也可以被看作为一个连续时间的马尔科夫链,它的状态空间为:

$$\Omega=\{(X_1,X_2,\cdots,X_n),X_1,X_2,\cdots,X_n\in(0,0',1)\} \tag{12}$$

状态空间 Ω 总共包含 $N=3^n$ 个状态. 子网状态 $X(t)$ 从(0,1,…,1)开始,结束于(1,1,…,1). 攻击从正常状态子网 $k-1$ 传播到休眠状态子网 k 服从泊松随机过程,传播的速率为 λ_k;同样,攻击从休眠状态子网 $k-1$ 传播到活跃状态子网 k 服从泊松随机过程,传播的速率为 λ_k'.

3 攻击实例

本节基于上述模型,构建攻击场景,分析和评估攻击和修复状态的传播过程.

攻击场景的示意图如图 4 所示. 该网络系统由核心网和接入子网组成. 接入子网由接入路由器接入核心网中,为简化分析和评估过程,假定只有两个接入子网,每个子网中的终端数量分别为 N_1 和 N_2. 初始状态,假设接入子网 1 遭受攻击,紧接着攻击传播至接入子网 2.

3.1 传统攻击模式

在上述攻击场景的传统攻击模式下,状态空间 $S=\{S_0,\cdots,S_\theta\}(\theta=2^2-1)$ 有四种不同状态,其传播状态可以用 (X_1,X_2) 表示,其中子网状态 $X_i\in\{0,1\}$. 可能存在的传播状态为:

$S_0=(11),S_1=(10),S_2=(01),S_3=(00)$.

如图 5 所示,假设接入子网 1 被攻击,子网 1 所有的终端都将与接入路由器断开连接. 此时,接入子网

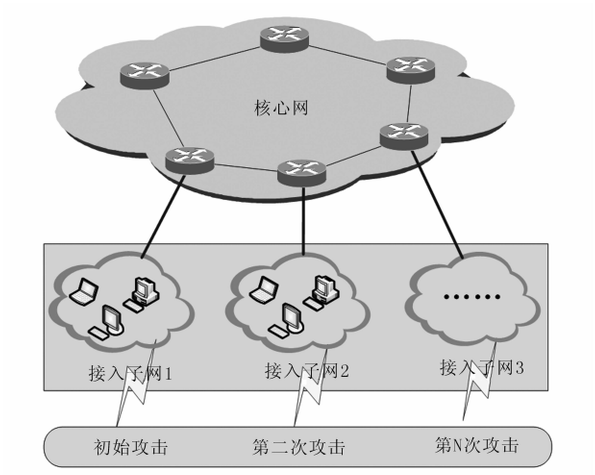


图4 攻击场景示意图

空间的状态为(01). 在该状态,若接入子网 2 继续被攻击,且攻击传播速率为 λ_2,子网进入(00)状态;若接入子网 1 被修复,且修复速率为 μ_1,子网恢复至健康状态(11). 同样,如果初始时刻,子网 2 遭受攻击,子网空间状态则为(10);在该状态,若子网 1 被攻击,则进入(00)状态;若子网 2 被修复,则进入健康状态(11).

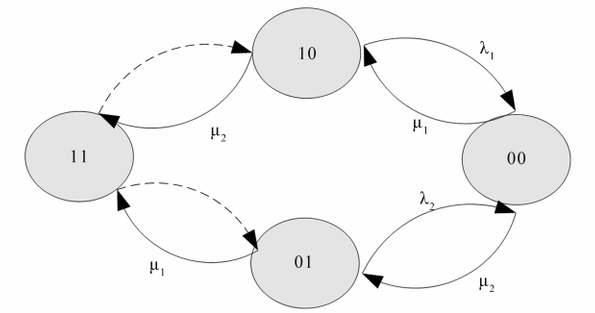


图5 传统攻击状态空间转移

当子网状态为(00),它只能进入修复过程;当修复速率为 μ_1,子网状态恢复至(10);当修复速率为 μ_2,子网状态恢复至(01).

在时刻 t 的传输状态概率为

$$\pi(t)=[\pi_{(0,1)}(t)\cdots\pi_{(X_1,X_2)}(t)\cdots\pi_{(1,1)}(t)] \tag{13}$$

根据状态转移图我们容易得到,传统攻击模式下的状态转移矩阵为:

$$\Lambda=\begin{pmatrix}-\lambda_1-\mu_2 & 0 & \lambda_1 & \mu_2\\ 0 & -\lambda_2-\mu_1 & \lambda_2 & \mu_1\\ \mu_1 & \mu_2 & -\mu_1-\mu_2 & 0\\ 0 & 0 & 0 & 0\end{pmatrix} \tag{14}$$

根据上述的差分微分方程 $\frac{d\pi(t)}{dt}=\pi(t)\Lambda$,我们可以得到以下方程组:

$$\begin{cases}\dfrac{d\pi_1(t)}{dt}=-(\lambda_1+\mu_2)\pi_1(t)+\mu_1\pi_3(t)\\ \dfrac{d\pi_2(t)}{dt}=-(\lambda_2+\mu_1)\pi_2(t)+\mu_2\pi_3(t)\\ \dfrac{d\pi_3(t)}{dt}=\lambda_1\pi_1(t)+\lambda_2\pi_2(t)-(\mu_1+\mu_2)\pi_3(t)\\ \dfrac{d\pi_0(t)}{dt}=\mu_1\pi_1(t)+\mu_2\pi_2(t)\end{cases}\tag{15}$$

3.2　APT 攻击模式

在 APT 攻击模式下,子网空间状态有正常、休眠和活跃三种. 基于上述攻击场景的连续马尔科夫链的状态转移图如图 6 所示,该转移图有 9 个节点. 因此,转移矩阵为 9 * 9 向量空间,初始概率向量 R = (1,0,0,0,0,0,0,0,0).

定义向量空间 $S=\{S_0,\cdots,S_\theta\}(\theta=3^2-1)$,每个状态空间可以由$(X_1,X_2)$表示,其中 $X_i\in\{0,0',1\}$. 状态空间的九个状态分别为:

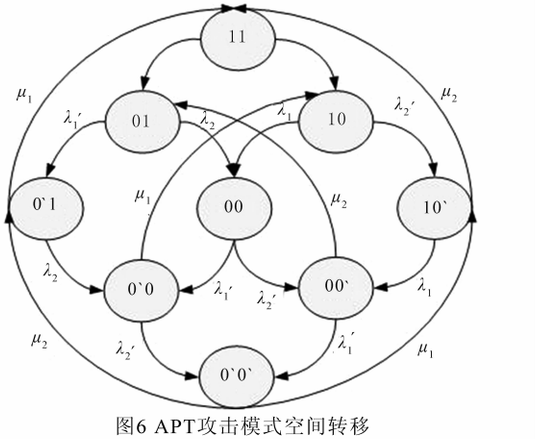


图6 APT攻击模式空间转移

$$\Pi=\begin{Bmatrix}-\lambda_1'-\lambda_2 & 0 & \lambda_1' & \lambda_2 & 0 & 0 & 0 & 0 & 0\\ 0 & -\lambda_1-\lambda_2' & 0 & \lambda_1 & \lambda_2' & 0 & 0 & 0 & 0\\ 0 & 0 & -\mu_1-\lambda_2 & 0 & 0 & \lambda_2 & 0 & 0 & \mu_1\\ 0 & 0 & 0 & -\lambda_1'-\lambda_2' & 0 & \lambda_1' & \lambda_2' & 0 & 0\\ 0 & 0 & 0 & 0 & -\mu_2-\lambda_1 & 0 & \lambda_1 & 0 & \mu_2\\ 0 & \mu_1 & 0 & 0 & 0 & -\mu_1-\lambda_2' & 0 & \lambda_2' & 0\\ \mu_2 & 0 & 0 & 0 & 0 & 0 & -\mu_2-\lambda_1' & \lambda_1' & 0\\ 0 & 0 & \mu_2 & 0 & \mu_1 & 0 & 0 & -\mu_1-\mu_2 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\end{Bmatrix}\tag{17}$$

根据上述的差分微分方程$\dfrac{d\pi(t)}{dt}=\pi(t)\prod$,我们可以得到以下方程组:

$$S_0=(11)S_1=(01)S_2=(10)S_3=(0'1)S_4=(00),$$
$$S_5=(10')S_6=(0'0)S_7=(00')S_8=(0'0')$$

接入子网初始处于正常状态(11),当遭受 APT 攻击后,攻击源潜入子网中,此时,接入子网进入(10)或者(01)状态. 以状态(01)为例,在此状态,攻击源可从子网 1 传播至子网 2,并在子网 2 中潜伏,此时子网状态为(00),攻击传播速率为 λ_2;若攻击源在(01)状态被激活,此时对子网 1 发起 APT 攻击,则子网状态为(0'1),攻击传播速率为 λ_1'.

在状态(00),两个子网均被 APT 攻击潜伏,在此状态下,若攻击传播速率为 λ_1',则表示子网 1 被攻击,子网状态进入(0'0);若攻击传播速率为 λ_2',则表示子网 2 被攻击,子网状态进入(00').

在状态(00'),若子网 1 被激活成活跃攻击状态,则进入(0'0')状态,攻击传播速率为 λ_1';若子网 2 被修复,修复速率为 μ_2,则子网状态进入(01). 同样,在状态(0'0),子网状态既可进入(0'0'),也可修复为(10).

在状态(0'0'),子网只可进入修复过程. 但其修复过程有两种不同路径,一种先修复完成子网 1,经过修复速率 μ_1 子网状态进入(10'),最终到达完全正常状态(11);另一种是先修复完成子网 2,经过修复速率 μ_2 子网状态进入(0'1),最终到达完全正常状态(11).

在时刻 t 的传输状态概率为

$$\pi(t)=[\pi_{(0,1)}(t)\cdots\pi_{(X_1,X_2)}(t)\cdots\pi_{(1,1)}(t)]\tag{16}$$

根据图 6 我们容易得到,APT 攻击模式下的状态转移矩阵为:

$$\begin{cases}\dfrac{d\pi_1(t)}{dt}=\mu_2\pi_7(t)-(\lambda_1'+\lambda_2)\pi_1(t)\\ \dfrac{d\pi_2(t)}{dt}=\mu_1\pi_6(t)-(\lambda_1+\lambda_2')\pi_2(t)\\ \dfrac{d\pi_3(t)}{dt}=\lambda_1'\pi_1(t)+\mu_2\pi_5(t)-(\mu_1+\lambda_2)\pi_3(t)\\ \dfrac{d\pi_4(t)}{dt}=\lambda_2\pi_1(t)+\lambda_1\pi_2(t)-(\lambda_1'+\lambda_2')\pi_4(t)\\ \dfrac{d\pi_5(t)}{dt}=\lambda_2\pi_3(t)+\lambda_1'\pi_4(t)-(\mu_2+\lambda_1)\pi_5(t)\\ \dfrac{d\pi_6(t)}{dt}=\lambda_2'\pi_4(t)+\mu_1\pi_8(t)-(\mu_1+\lambda_2')\pi_6(t)\\ \dfrac{d\pi_7(t)}{dt}=\lambda_2'\pi_4(t)+\lambda_1\pi_5(t)-(\mu_2+\lambda_1')\pi_7(t)\\ \dfrac{d\pi_8(t)}{dt}=\lambda_2'\pi_6(t)+\lambda_1\pi_7(t)-(\mu_1+\mu_2)\pi_8(t)\\ \dfrac{d\pi_0(t)}{dt}=\mu_1\pi_3(t)+\mu_2\pi_5(t)\end{cases} \tag{18}$$

4 仿真与分析

为了进一步揭示网络攻击时的网络可生存性传播模型及规律,通过 MATLAB 软件仿真,取得了该模型的传播曲线,并设定不同参数验证了该模型的正确性. 同时,为了方便比较,突出 APT 攻击时网络可生存的特点,将传统攻击和 APT 攻击时的传播曲线放在同一张图中对比.

在这里,我们考虑用网络中活跃用户数百分比作为网络生存性的一个标准化性能指标[19],这个指标可以准确反映网络中终端被中断服务的比例. 该百分比可以用公式(7)的预期瞬时回报率表示. 因而,预期的瞬时回报率可以描述在 t 时刻网络中的终端被攻击的情况.

假定子网 i 的用户数为 N_i,可以得到每个状态的回报率. 例如,传统攻击模式下的回报率为:

$$\gamma_0=1,\gamma_1=\frac{N_2}{N_1+N_2},\gamma_2=\frac{N_1}{N_1+N_2},\gamma_3=0$$

考虑到每个 C 类 IP 地址最多可连接 254 台主机,因而我们设置子网 1 连接的终端数 $N_1=150$,子网 2 连接的终端数 $N_2=200$. 根据文献[20],我们可以得到网络攻击的传播速率和修复速率. 通常,网络的修复速率会比网络攻击速率低一个数量级. 因而,设定的网络攻击传播速率和修复速率如表 1 和表 2 所示.

下面从两个维度来检验本文提出的网络可生存性模型. 首先假设子网初始状态的攻击传播速率均为 $2hours^{-1}$,修复速率均为 $0.2hours^{-1}$,如表 1 所示. 通过增大子网攻击传播速率,如图 7 所示. 从图中可以看出,网络在遭受攻击时,子网中活跃用户数明显下降. 但随着时间的推移,子网中的终端逐渐被修复,直至完全被修复(子网的活跃用户百分比为 1). 根据表 2 中的参数,当保持子网中修复速率不变,增大子网的攻击传播速率,可以看出,子网中初始活跃用户数不断下降,同时,子网达到完全被修复状态所需要的时间也不断增加. 在 150hour 时刻,初始状态已完全修复,但状态 4 只修复至 0.8.

表 1 子网攻击传播速率参数

状态类型	子网 1 攻击传播速率(λ_1)	子网 2 攻击传播速率(λ_2)
初始状态	$2\ hours^{-1}$	$2\ hours^{-1}$
状态 1	$3\ hours^{-1}$	$3\ hours^{-1}$
状态 2	$4\ hours^{-1}$	$4\ hours^{-1}$
状态 3	$5\ hours^{-1}$	$5\ hours^{-1}$
状态 4	$6\ hours^{-1}$	$6\ hours^{-1}$

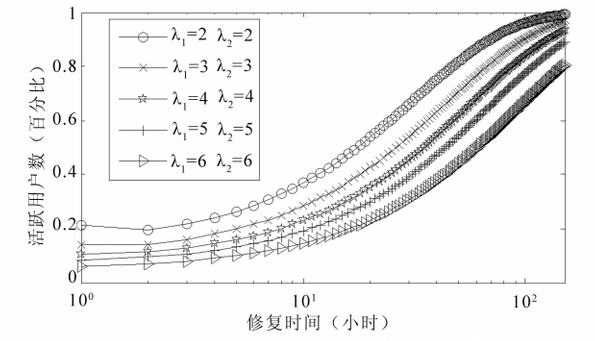


图7 攻击传播速率对网络可生存性的影响

根据表 2 中的参数,当子网的攻击传播速率保持不变,通过增大子网的修复速率,如图 8 所示,子网中初始活跃用户数不断增加,由初始状态 0.2 增加至状态 4 的 0.4. 同时,初始状态需要经过 100hour 才可完全修复,然而状态 4 在经过 10hour,已经修复至 0.9,可见子网修复速率的提升.

表 2 子网修复速率参数

状态类型	子网 1 修复速率(μ_1)	子网 2 修复速率(μ_2)
初始状态	$0.2\ hours^{-1}$	$0.2\ hours^{-1}$
状态 1	$0.3\ hours^{-1}$	$0.3\ hours^{-1}$
状态 2	$0.4\ hours^{-1}$	$0.4\ hours^{-1}$
状态 3	$0.5\ hours^{-1}$	$0.5\ hours^{-1}$
状态 4	$0.6\ hours^{-1}$	$0.6\ hours^{-1}$

由此可知,网络的可生存性性能不仅取决于网络攻击的传播速率,还与网络的修复速率相关.

在 APT 攻击模式下,将网络攻击传播速率和修复速率参数设置一致,与传统攻击模式的可生存性曲线比较. 如图 9 所示,APT 攻击模式下的网络修复速率比

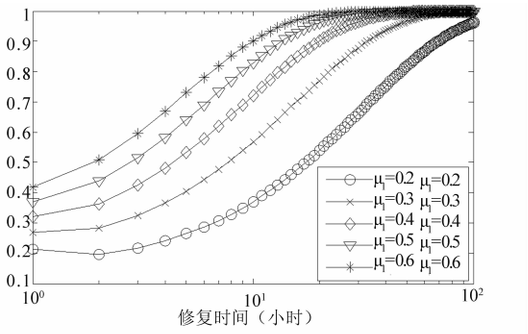


图8　子网修复速率对网络可生存性的影响

传统模式下稍低. 这是因为在 APT 攻击模式下,网络中的攻击具有潜伏性,这样在潜伏期网络攻击不容易被发现,致使网络的可生存性比传统模式要差. 但随着时间的推移,网络的活跃用户数也修复至正常水平,从而验证了模型的正确性. 但总体上,APT 攻击对网络的可生存性是有影响的. 综上所述,本文提出的模型有效的刻画了基于 APT 攻击的网络可生存性特点,具有一定的现实指导意义.

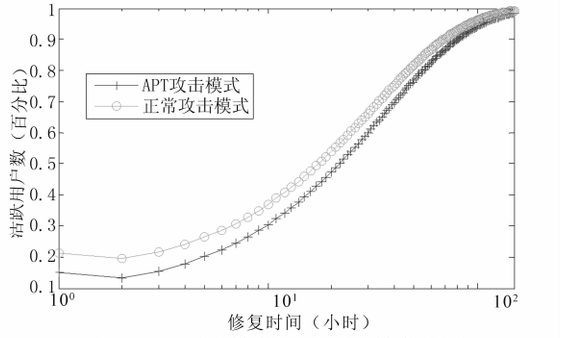


图9　APT攻击模式与传统攻击模式的比较

5　结论

本文基于连续马尔科夫链,建立网络可生存性模型,并通过攻击实例,验证了模型的正确性. 总结了影响网络可生存性的两个重要因素,网络攻击传播速率和网络修复速率. 更进一步,通过仿真验证 APT 攻击模式下,网络可生存性的特点. 可以看出,网络修复速率是影响 APT 攻击模式下的网络可生存性性能关键指标,是防御 APT 攻击的重要保证. 下一步,需要继续研究攻击潜伏周期长短对网络可生存性的具体影响,以及针对多个子网发动同时攻击的模型构建和安全策略.

参考文献

[1] Jeun I, Lee Y, Won D. A practical study on advanced persistent threats [J]. Computer Applications for Security, Control and System Engineering, 2012, 11: 144 – 152.

[2] Zetter K. Google hack attack was ultra sophisticated, new details show[J]. Wired Magazine, 2010, 14: 33 – 36.

[3] Langner R. Stuxnet: dissecting a cyberwarfare weapon[J]. IEEE Security & Privacy, 2011, 9(3): 49 – 51.

[4] 肖新光. 恶意代码对抗体系演进的四部曲[EB/OL]. http:// www. antiy. net/papers/.
Xiao X G. The tetralogy of defending malicious code[EB/OL]. http:// www. antiy. net/papers/. (in Chinese)

[5] Bencsáth B, Pék G, Buttyán L, et al. The cousins of stuxnet: duqu, flame, and gauss [J]. Future Internet, 2012, 4(4): 971 – 1003.

[6] Lee J D. Targeted cyberattacks: a superset of advanced persistent threats[J]. IEEE security & privacy, 2013, 11(3): 54 – 61.

[7] Giura P, Wang W. A context-based detection framework for advanced persistent threats [A]. International Conference on Cyber Security [C], Washington, 2012. 69 – 74.

[8] Dube T E, Raines R A, Grimaila M R, et al. Malware target recognition of unknown threats[J]. IEEE Systems Journal, 2013, 7(3): 467 – 477.

[9] Johnson J R, Hogan E A. A graph analytic metric for mitigating advanced persistent threat [A]. IEEE International Conference on Intelligence and Security Informatics [C], Seattle, 2013. 129 – 133.

[10] Sterbenz J P G, Hutchison D, ? etinkaya E K, et al. Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines [J]. Computer Networks, 2010, 54(8): 1245 – 1265.

[11] ANSI T1A1. 2 Working Group on Network Survivability Performance. Technical Report on Enhanced Network Survivability Performance [S], ANSI, Tech. Rep. TR No. 68, 2001.

[12] Heegaard P E, Trivedi K S. Network survivability modeling[J]. Computer Networks, 2009, 53(8): 1215 – 1234.

[13] Xie L, Heegaard P E, Jiang Y. Network survivability under disaster propagation: Modeling and analysis [A]. Wireless Communications and Networking Conference (WCNC) [C], Shanghai, 2013. 4730 – 4735.

[14] Xie L, Jiang Y, Heegaard P E. Modelling and analysis of the survivability of telecommunication networks[A]. 15th International Symposium on Software Reliability Engineering[C], 2004, 367 – 377.

[15] 赵二虎,阳小龙,彭云峰,隆克平. CPSM:一种增强 IP 网络生存性的客户端主动服务漂移模型[J]. 电子学报, 2010, 38(9): 2134 – 2139.
Zhao E H, Yang X L, Peng Y F, Long K P. CPSM: client-side proactive service migration model for enhancing IP network survivability [J]. Acta Electronica Sinica, 2010, 38(9): 2134 – 2139. (in Chinese)

[16] Izaddoost A, Heydari S S. Enhancing network service survivability in large-scale failure scenarios[J]. Journal of Communications & Networks, 2014, 16(5): 534 – 547.

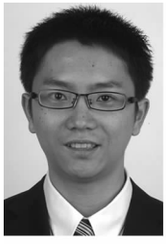
[17] 王鹏飞,赵文涛,张帆,邹荣念. 网络系统可生存能力量化评估的指标体系研究[J]. 计算机工程与科学, 2014, 36(6): 1050 – 1056.
Wang P F, Zhao W T, Zhang F, Zou R N. Research on index system of quantitative evaluation for network systems viability[J]. Computer Engineering&Science, 2014, 36(6): 1050 – 1056. (in Chinese)

[18] Wen S, Zhou W, Zhang J, et al. Modeling propagation dynamics of social network worms[J]. IEEE Transactions on Parallel and Distributed Systems, 2013, 24(8): 1633 – 1643.

[19] Zolfaghari A, Kaudel F J. Framework for network survivability performance[J]. IEEE Journal on Selected Areas in Communications, 1994, 12(1): 46 – 51.

[20] Camtepe S A, Yener B. Modeling and detection of complex attacks[A]. Third International Conference on. IEEE Security and Privacy in Communications Networks and the Workshops[C]. Nice, 2007. 234 – 243.

作者简介



姚 苏 男,1986 年 12 月出生,安徽舒城人,中国航空综合技术研究所工程师,现为北京交通大学在读博士. 目前主要从事网络安全标准应用技术的研究工作. 获中航工业集团奖励多项,参与多项国家和军队技术基础研究项目.
E-mail: yaosu@bjtu.edu.cn.

关建峰 男,1982 年 2 月出生,河南巩义人. 2004、2010 年分别毕业于东北大学、北京交通大学获得学士、博士学位. 2010 年进入北京邮电大学网络技术研究院,主要从事移动互联网、网络安全等方面的研究工作.
E-mail: jfguan@bupt.edu.cn.

潘 华 女,1965 年 10 月出生,安徽界首人;1988、1991 年分别于北京航空航天大学获得学士、硕士学位,现为中国航空综合技术研究所研究员,主要从事信息技术标准化的研究工作,主编多项国家军用标准,并多次获得军队和中航工业集团奖励.

张宏科 男,1957 年 9 月出生,山西大同人,北京交通大学教授,博士生导师. 目前主要从事下一代信息网络关键理论与技术的研究工作,作为首席科学家主持国家 973 项目"智慧协同网络理论基础研究"的研究工作.