应用网络可靠性模型，预测灾难事件导致的停机

Ahmad M. Jrad, 美国朗讯
Jean Meng LWS

摘要

朗讯网络可靠性和安全性咨询服务能够为网络服务提供商分析网络上存在的各类风险，量化网络的可靠性和安全性，设计网络业务的抗损能力，从而全方位地提高网络的可靠性，安全性. 在本文中，我们介绍了一种保证网络业务连续性计划（Business Continuity Process）模型，用于确定由于灾难事件、常见软硬件故障导致的预期停机时间。我们还将展示，在常见故障条件下能够行之有效的某些技术，在灾难事件中却显得无能为力。我们还将提出弥补这些不足、确保网络即使在恶劣条件下（恰好也是最需要网络的时候）仍能保持高可用性的补救方法。最后，我们还将说明，由于灾难事件的可预见性，以及按照一定规律发生的事实,我们在预期网络可靠性时，迫切需要制定就绪的业务连续性计划（BCP）.

1. 导言

对大多数公司而言，网络的可靠性和可用性都极为重要，对电信供应商尤其如此。实际上，电信客户经常会请求服务提供商维持业务可用性，在某些情况下，如果达不到这些要求，则可能导致严厉的经济惩罚。鉴于这一点以及当前电信市场的激烈竞争，服务提供商必须根本、透彻地了解他们的网络，以及他们能够提供和保证的预期业务可用性和可靠性。

目前，在传统的可靠性建模中，通常主要依据硬软件故障率来计算电信网络的预期可用性。其实，这种方法忽略了一个事实：在很多情况下，网络故障很可能由通常未被视为可用性影响因素的外部事件导致。特别是，恶劣的天气环境和自然灾难等事件在决定实际的网络可用性过程中起着重要作用。这些事件通常受服务提供商设施所在位置的影响。

在通常情况下，服务提供商会为备份设备提供备选路径以保持运行，并将原有设备和备用设备放置在同一位置，造成对安全性的错觉。在计算网络可靠性时，备份设备的实施位置通常会被忽略。但是人们仍然很容易明白，导致原有设备故障的灾难事件，很有可能导致处于同一位置的备用设备也会出现故障，进而导致长时间的业务中断。

在本文中，我们介绍了一种新模型，可以预测由于灾难、外部事件导致的网络故障，与传统网络体系结构软硬件设备的可靠性予以全盘考虑。我们通过 BCP 分类法，量化了灾难和外部事件对网络的预期影响。

2. 背景

传统网络的可靠性模型是从设备制造商的角度构建的，重点强调硬软件故障。人们最熟知的度量标准是网络可用性或网络停机时间。网络可靠性模型使用的输入数据包括：网元的故障率、修理/恢复率。故障时间分布呈现 Poisson Arrival 模型。该模型对两种类型的故障进行建模：软件和硬件

故障。对于硬件故障，Poisson Arrival(泊松到达)曲线从理论上讲, 是在软硬件稳定运行状态下对软硬件故障率的观察. 。对于软件故障，故障事件的 Poisson Arrival 分布(泊松到达)也是在这一假设前提分布曲线。进行这种假设的合理依据是：在清除了 Bug 后，每个软件版本都到达一个稳定的故障率，这个过程通常称为可靠性增长阶段。一旦估计得出单个网元的软硬件故障率，就可以简单计算出网络的可用性或停机时间。常见方法是采用参考连接数据计算网络的可用性。使用这种方法，通过网络的参考连接数据（网络结构中的呼叫路径）的端到端可用性，是通过对呼叫路径中经过网络的各个网元或各个网段的可用性进行计算后得出的。如果人们希望通过停机时间计算，则端到端的停机时间就是呼叫路径中网元的停机时间总和。

粗略浏览实际的网络可用性数据，我们便可以发现：导致网络故障的原因多种多样，不仅是硬件和软件故障。图 1 显示了导致光网中断的各种根本原因，它是依据我们对 2001 FCC 停机报告的分析得出的[5]。显而易见，大多数光网停机时间由于光纤截断所致。本文重点论述了网络运行人员无法控制的类似的意外事件的建模。

图 1：光网停机时间原因分类

3 定义

可用性：系统或网络的可用性指它们在指定时间内及时执行规定的功能的概率。[5]
停机时间：停机时间是以分钟/年为单位计算的，公式如下：（1-可用性）X（每年累计的分钟数）。
MTTF：即平均故障时间。它是稳定状态故障率的倒数，它是假设网络稳定运行条件下的故障时间分布。

MTTR：平均修复时间，也称为平均恢复时间。它是发生故障后，恢复业务所需的平均时间。

4 计算传统的可用性

4.1 网络结构图

为了评估网络的可用性和可靠性，我们首先将提供单个业务的网络表示成为呼叫流程图。我们将网络表示为结构图，并抽取在网络结构中提供某一特定业务的呼叫流进行研究。如果网络能够能够承载大量不同的业务, 不同网络结构中的的呼叫路径不同, 很可能导致不同的预期停机时间。因此，当我们谈及网络的可靠性时，我们总要说明某一种业务的可靠性评估。

例如，我们假设一个简单的无线网络，并展示如何对它们进行建模。该网络是现有和实际无线网络的简化版本。无线网络的选择无关紧要，我们可以很容易地在任何指定通信网络（如 PSTN、数据网和光网等）中，进行相同的分析。

我们首先研究网络的构件（构件视图），如图 2 所示。该视图显示了不同的网络组件是如何互

连，哪些组件在传输和建立网络业务时进行交互。

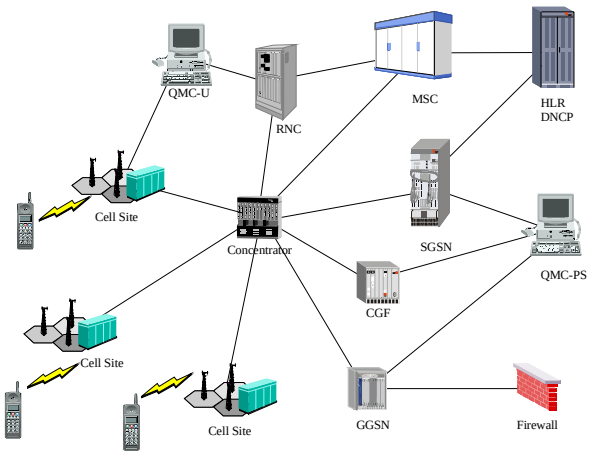


图 2：网络视图：网络结构图

4.2 获得呼叫路径视图

根据网络结构图，我们开发了网络的呼叫路径视图，并将其用作确定整个网络的可用性的依据。如前所述，在网络中我们根据指定业务路径，通过以业务为中心的方式，对网络进行研究，从而评估出网络的可用性。例如，假设一个无线网络，我们设定网络中的一个无线用户向另一个无线用户发出呼叫，而两个用户由不同的 MSC 提供服务，则端到端的网络视图如图 3 所示。在多数情况下，网络有一个以上的呼叫路径视图。通常，一种业务具有一种呼叫路径视图。因此，如果业务类型不同，那么网络的可用性也会有所差异。

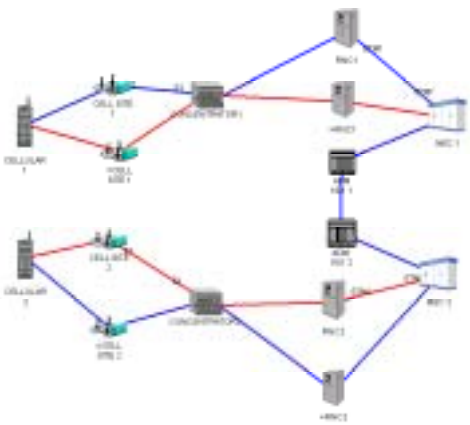


图 3：网络视图：呼叫路径视图

如图 3 所示，我们假设所有小区站点之间有冗余。因此，如果其中一个小区站点出现故障，邻近的其他站点可以承载故障站点的部分流量。在本例中，我们假设 60%的流量将被继续传输，剩余的 40%将被阻塞。在现用和备用设备共置的实时备用系统中，RNC 受到保护。在图 3 中，主路径用蓝色显示，冗余路径以红色显示。

4.3 Markov 模型

系统可靠性结构图中的每个网元都使用图 4 的 Markov 模型进行评估。该模型是 Telcordia SR-1171 中的 Markov 模型的延伸[6]。状态（1）是 N+1 子系统的正常工作状态，此处的 N 表示激活装置的数量。子系统能够通过多种方式从状态（1）中退出。如果 N 个激活装置中的任意一个装置出现故障，备份装置会自动激活。这个过程表示为从（1）到（2）的转换。转换（故障）率是 $Nc\lambda$，C 表示成功进行故障切换的概率，λ则表示装置故障率（通常使用 TR-332 评估）[7] 。要从 (2) 恢复到 (1)，需要委派技术人员来更换故障设备。这是晴天场景（sunny-day scenario）。雨天场景（rainy-day scenario）就是备份装置的故障切换操作失败，如(1) 到(5)所示。 发生这种情况的概率为 $N(1-c)$，c *代表*成功的故障切换的可能性。状态（5）红色是下降状态（业务受到影响）。从状态（5）退出，通常不需要委派额外的专业人员，因为操作人员可以远程进行故障切换。该过程如(5) 到 (2)所示。

下面我们假设备份装置为晴天场景。当备份装置出现故障时，故障可以被检测出来，并派遣技术人员去更换该装置。该过程如(1) 到 (6)的转换所示。转换（故障）率为 $d\lambda$， d 表示检测备份装置故障的概率，λ*表示装置故障率*。雨天场景是“ 静故障 ”，如(1) 到 (4)的转换所示。当系统处于状态（4）时，激活装置正处于工作状态，但系统却未

感知备份装置已经不能使用。因此，如果激活装置失败，系统将处于停机状态，如状态（3），那么（4）就是易受攻击的状态。

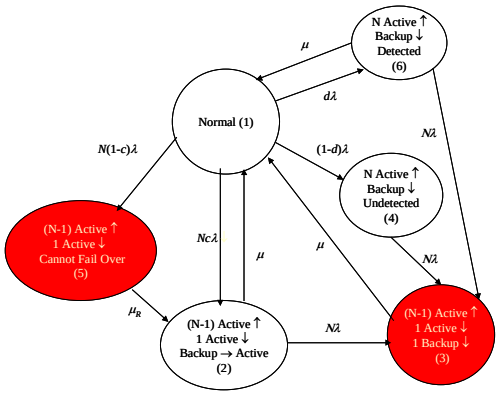


图 4：Markov 模型 N+1 受保护子系统

Markov 模型分析公式的推导非常简单。

4.4 平行路径算法

冗余设置的可用性通过以下方法计算。假设我们有图 5 中所示的冗余设置。

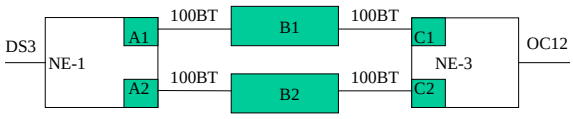


图 5：冗余的平行配置

假设 A 表示(A1 – B1 – C1) 或 (A2 – B2 – C2)中的任一路径的可用性，为简单起见，我们假设两种路径具有相同的可用性。平行路径的可用性的计算方法如下：

$$Ap = A + pA(1 - A)$$

P 表示激活设备到备用设备成功实现故障切换的概率。

5 预测灾难发生

5.1 灾难类型

我们根据灾难发生的方式及其产生的整体影响[9]进行分类，大致将这些灾难分为三大类：

- 自然灾难
- 技术故障
- 人为威胁

5.1.1 自然灾难

自然灾难指世界上自然发生的、很大程度上由地理位置和自然环境引发的灾难事件。自然灾难的一些例子包括：飓风、龙卷风、洪水、地震、海啸等。众所周知，任何地区如果曾有重大灾难发生，就会有灾难的历史记载。

5.1.2 技术故障

技术故障经常会导致灾难性后果。这些灾难包括：由于我们所依赖的资源出现技术故障导致的灾难（如能源停机），以及一些可能导致环境威胁的资源出现故障引发灾难，如能源厂核辐射（如 1986 年 4 月发生的切尔诺贝利事件）、化学品泄漏事件。 这些事件发生的概率可结合以往事件的历史记录、技术的当前状态计算得出。

5.1.3 人为威胁

人为威胁通常指以故意破坏为目的的灾难类型。此类灾难的典型例子有 2001 年 9 月 11 日世贸中心发生的“ 9.11 事件 ”。尽管我们研究的网络可能不是故意袭击的目标，但它可能受到邻近事件的影响。此类灾难还包括怠工、恶意破坏、针对公司的攻击等。

5.2 灾难模型

为简单起见，我们首先假设自然灾难和技术故障为正常的 Poisson 分布[10]。我们还假设各种灾难都是独立发生的。

值得注意的是，并不是所有灾难都可以任意假定为拥有一个 Poisson 分布。我们特别说明下列情况：

- 自我组织管理的关键程度可以揭示灾难频率和后果之间的关系线索；
- Bak、Tang 和 Wiesenfeld[11]三人发现，模拟雪崩具有幂法则规模的分布特性，与 Gutenberg-Richter 定律接近。此外，雪崩的周期和发生次数也遵从幂法则时间分布。
-

如前所述，我们开始就进行了 Poisson 假设，但灾难模型（特别是资源缺失导致的灾难模型）是基于对所有已知的相关参数的了解，分别调整得出的。

我们假设灾难发生的概率为 Pd，该值定义在指定时段（T）里指定的灾难类型(Dj)在某个指定网元站点（Ei）发生的灾难次数（a）的概率，它基于两个基本的参数。第一个参数是 Rd 值，定义为在网元（Ei）所在的指定网络位置，指定灾难(Dj)发生的历史频率。第二个参数为 Ph，它表示灾难(Dj)直接影响精确位置上的网元(Ei)的比率。例如，某个城市龙卷风的发生率可能是根据历史数据得出的，这就是我们所说的“ Rd ”。但是已知龙卷风在袭击城市中的某幢特定街区或大楼的概率被定义为 Ph。假设城市所有邻近事物遭到龙卷风袭击的概率相等，则只需简单地将 Ph 当作根据城市位置划分的邻近位置计算。

如果现在已知 Rd 和 Ph，Pd 发生的概率计算公式如下：

我们还定义时间间隔 T 之间至少发生一次灾难的概率（但可能更多）。该概率可以通过下列公式

$$Pd_{(Ei,Dj)}(a,T)=e^{-(Rd_{(Ei,Dj)}*Ph_{(Ei,Dj)}*T)}\left[\frac{(Rd_{(Ei,Dj)}*Ph_{(Ei,Dj)}*T)^{a}}{a!}\right]$$

计算：

或简单计算

$$Pd_{(Ei,Dj)}(1+,T)=1-Pd_{(Ei,Dj)}(0,T)=1-e^{-(Rd_{(Ei,Dj)}*Ph_{(Ei,Dj)}*T)}$$

$$Pd_{(Ei,Dj)}(1+,T)=\sum_{k=1}^{\infty}Pd_{(Ei,Dj)}(k,T)$$

属于人为威胁的灾难则通过另一种不同方式处理。对于这些灾难类型，我们假定其发生的概率是一个数值极小但又有限的值，而不是将概率计算到最后 1 位数。我们主要研究在网络和设备遭到这些灾难袭击时产生的影响。

6 网元遭受灾难

6.1 网络图视图

网络的另一种视图称为网络图视图，我们通常用它来建立灾难对网络产生影响的模型。网络图视图显示的是网元的实际地域分布，如图 6 所示。我们可以从 图 6 中看到大量信息，这些信息在确定影响网络的灾难类型、如何为网元的这些灾难建模方面发挥了重要作用。例如，通过观察网络图视图，我们可以迅速决定网络的哪些部分处于主要水域的邻近地区。这些信息对模仿洪水、龙卷风和沿海地区的其他灾难具有重要作用。

图 6：网络图视图

图 6 显示的是平面背景地图，以便于查看。然而，通过在网络图视图上添加具有更多功能的层，我们可以确定海拔，以及对人类具有更大威胁的特定目标的接近程度。这些目标包括：飞机场、核电站、高风险基础设施。

图 6 还显示了网络中的不同站点的名称。两个主站点名为 N（北）和 S（南）。相临站点的名称是主机站点加上与其位置(相对于主机)对应的数字。N03 表示：以主机站点中心，大致处于 3 点钟指针位置的站点。

6.2 评估风险和停机时间

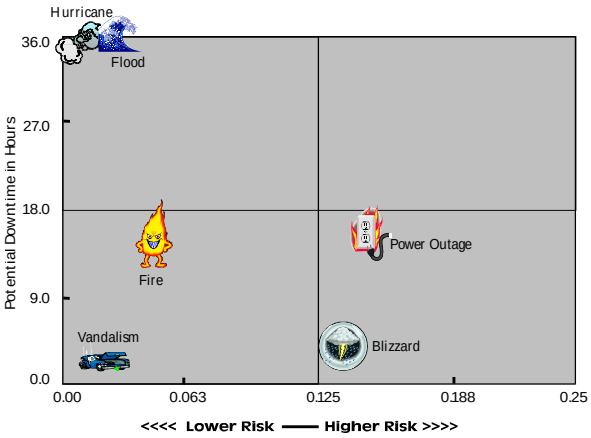
我们计算了每种灾难的风险和停机时间。该分布图显示了在水平方向网络（风险）遭到灾难攻击的概率，以及它在垂直方向灾难导致停机时间的概率。该风险可以定义为在指定时间内至少发生一次灾难的概率。这个时间段可能是几年，尽管 5 年是最常见的时间段，但它是电信通信服务提供商最常用的计划周期。停机时间按业务关键组件遭到灾难攻击后，修复或替换破坏组件需要的预期时间计算。

图 7 是我们研究的所有灾难类型和整个网络的风险-停机时间图的示例。它显示的是网络中所有站点在最坏情况（或者还可显示加权平均值）下的风险和停机时间。这就可以通过发生的概率和潜在预期停机时间，为那些可能出现高风险的地方提供很好的提示。

图 7 ：不同灾难类型的风险和停机时间

6.3 评估预期停机时间

我们可以通过风险—停机时间数据计算网络每年由于不同灾难（如图 8 所示）导致的预期停机时间。



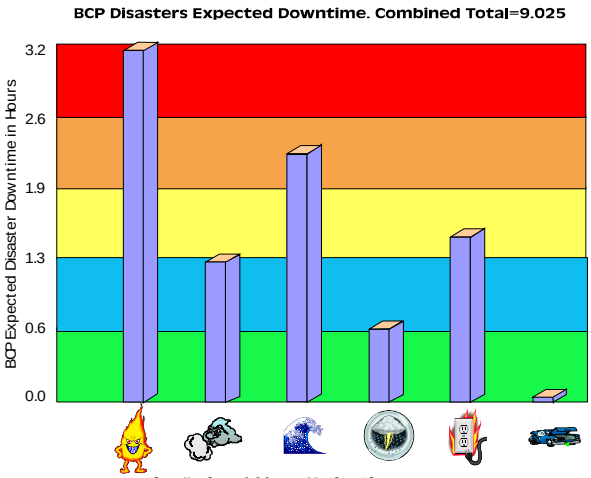


图 8：不同灾难类型的预期损失

BCP 灾难预期停机时间。总值-9.025
BCP 预期灾难停机时间（小时）

6.4 评估端到端的网络可用性

我们首先计算出指定呼叫路径视图中的不同组件在正常运行情况下的预期停机时间，从而决定端到端的网络可用性。将上面的停机时间相加，我们能够决定实际网络可用性的更加现实的数字。

呼叫路径中的不同组件的停机时间如表 1 所示。也可以参见图 3。

表 1：网元停机时间

网元	硬件停机时间	总的停机时间
节点 B	69 (分/年)	142 (分/年)
接头	12	29
RNC	3.5	14
MSC	5.4	12.5
Mux	0.94	4.7
总和	99	236

表 1 所示的总和表示：假定没有冗余的情况下，指定呼叫中的半个呼叫路径的总体停机时间。在小区站点添加冗余后（出现故障后，60%的流量可以通过），这会将小区站点的硬件停机时间降低到 20.8 分/年，总停机时间为 42.7 分/年。RNC 的冗余（出现故障后，98%的流量可以通过）将该组件的硬件停机时间降低至 0.08 分/年，总的停机时间为 0.31 分/年。

如果将图 3 中的全部预期停机时间和全部呼叫路径考虑进去，我们会发现，由于硬件故障导致的总停机时间是 77.86 分/年（可用性是 99.985%），由于软硬件和程序故障导致的总停机时间为 178.30（可用性为 99.966%）。

如果我们将上部分所述的由于灾难攻击导致的预期停机时间考虑进去，总的停机时间为：
停机时间=178.3 + 9.025*60 = 719.8 分/年
因此，更实际的预期可用性为 99.863%。

7. 结论

灾难随时可能发生，发生时会导致电信业务和其他服务行业的严重业务中断。在本文中，我们对网络和潜在的灾难类型模型进行了说明，同时提供使用这些模型的方法，以帮助电信服务提供商更有效地预测网络的停机时间。我们说明了如何利用该模型，量化灾难袭击网络任何位置的概率，以及灾难可能导致的业务停机时间。