下一代网络信息安全防护体系的核心防护机制

（来源：网络安全和信息化公众号，2019-11-08）

随着各国加快 5G 建设，车联网、工业互联网等人们期待已久的垂直行业应用正逐步走入生活,5G 时代定义的三大应用场景——eMBB、URLLC 和 mMTC 带来的不仅是技术的进步,更是工作生活方式的颠覆。

与此同时，这些应用场景也给网络带来了前所未有的承载压力，网络的物理极限阈值正从理论上的可能性逐步变为现实存在的系统性风险。为解决这一风险，以雾计算为代表的新兴网络技术正在成为构建下一代大数据监管系统及网络信息安全防护体系的基石。但是雾计算的八大支柱特性本身也是一柄双刃剑，而解决这一问题的关键在于构建与下一代网络特点相适应的防护机制。

一、雾计算支柱特性的天然弱点

根据已经发布的雾计算标准 IEEE 1934，雾计算具有 8 大支柱特性，分别为安全性、可扩展性、开放性、自主权、可靠性、灵活性、层次性和可编程性。雾计算的支柱特性既是其优势所在，也是其弱点所系。

在这些支柱特性中，安全性、可扩展性、自主性和层次性与下一代监管系统及网络信息安全防护体系的技术演进趋势相契合，但开放性、可靠性、灵活性和可编程性也会使得威胁网络信息安全的恶意行为可以直接通过网络远程实施，轻则造成数据泄露，重则直接对物理世界产生破坏。

开放性实现了资源共享，使得应用内部的生产设施能够直接连接

到远程维护服务提供商和其它合作伙伴，也为非授权的访问行为打开了方便之门。

可靠性既为远程维护和预测维护功能实现提供了便利，也为非授权获取数据等恶意行为的实施提供了土壤。

灵活性允许雾计算节点实时检测和处理故障、自行调整生产线，也让破坏物理世界的恶意行为可以通过网络远程实现。

可编程性赋予雾计算节点的编程能力，使其可以创建动态的价值链，并分析现场的数据，而不是将其发送到云；也使上述恶意行为可以长期隐藏在雾计算节点中，持续威胁网络信息安全。

雾计算支柱特性的天然弱点不仅使其自身存在安全隐患，也直接影响了边缘计算层和云计算层的安全防护。从节点层次来说，雾计算处于构建边缘计算-雾计算-云计算的多层次网络信息安全防护的枢纽位置，起着承上启下的重要作用。边缘计算中的计算和存储资源相对有限、云计算中的网络边缘能力不足都需要通过雾计算解决。一旦雾计算节点遭到破坏，将直接引发相邻边缘计算节点与云计算节点的连锁反应。

总体来说，雾计算既是构建下一代大数据监管系统及网络信息安全防护体系的基石，也是下一代网络信息安全防护的要害。

二、面向下一代网络的核心防护机制

如何解决雾计算的天然弱点产生的安全隐患，关键在于构建与下一代网络特点相适应的防护机制。

这一防护机制不同于以往的防护机制，需要匹配下一代网络的两项基本特征：一是全程全网，即不同位置、不同层次、不同规模异构节点共同汇聚于一个网络；二是节点有别，即不同层级、不同类别节

点之间的差异性将会显现，同时节点的分层化趋势也逐渐凸显。因此面向下一代网络的防护机制需要具备两项能力，一是基于节点的差异和分层匹配不同的安全防护策略，二是在部分节点出现问题时能保障网络总体不受影响。根据其外在表现形式，可以将这一防护机制命名为闭锁机制。

闭锁机制，其外在表现形式为将问题节点或节点内出问题的功能模块与其他节点或功能模块隔离开来，防止在网络中的进一步扩散或联动。根据隔离的程度和技术实现方式，可以进一步分为四种类型：

物理闭锁，即节点在网络中运行时只允许远程访问，所有功能模块均不可修改。

刚性闭锁，即节点在网络中运行时只允许特定的远程操作，只允许修改部分功能模块。

灰度闭锁，指在一定范围的网络中始终只有部分节点和功能模块处于允许远程操作的状态，并且预先配置不相容节点和功能模块。即在部分节点和功能模块处于允许远程操作状态时，始终有另一部分节点和功能模块禁止远程操作，而且预设数据校验，由后者校验前者，监测异常行为。

拟态闭锁，指节点和功能模块在网络中运行时不断切换远程操作规则与权限、基于内生机理的主动闭锁，必要时可以模拟出物理闭锁、刚性闭锁或灰度闭锁的拟态伪装。实现这一闭锁需要节点配备拟态防御技术，使其具备动态异构冗余的内生安全特性，并可根据需要模拟成物理闭锁、刚性闭锁或灰度闭锁的蜜罐，配合追踪溯源等技术进行有效的主动诱捕。

三、基于闭锁机制的下一代网络闭锁矩阵

考虑到下一代网络的发展趋势，主要有两类因素影响节点采用相应的闭锁机制。

一是对真实世界的物理影响。随着车联网、工业互联网等垂直行业应用的发展，节点将逐渐从传统意义上 IT 域拓展到 OT 域，节点越趋向 OT 域，越可能对真实世界产生物理影响。

二是节点功能的复杂度。随着旨在实现万物互联的下一代网络建设，从功能单一的传感器，到功能复杂的无人驾驶汽车，各类设备都可以成为网络中的节点。

因此，基于闭锁机制的下一代网络闭锁矩阵如下图所示：

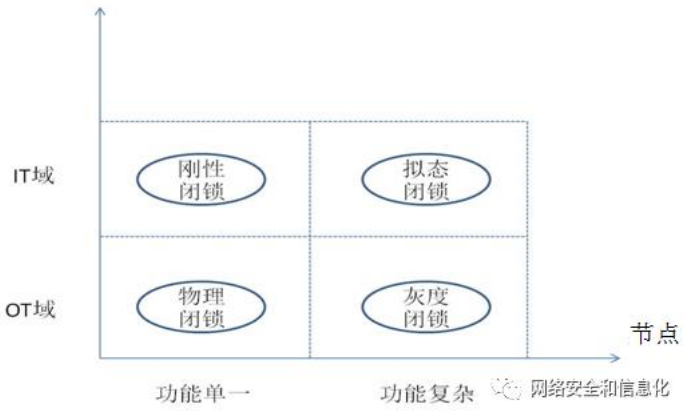

图 1 基于闭锁机制的下一代网络闭锁矩阵

在闭锁矩阵中，闭锁类型与节点特点相对应，表示的是某类节点以采用某类闭锁机制为主。当节点功能单一且趋向 OT 域应用时，以采用物理闭锁为主，例如工业互联网中的运动控制器。当节点功能单一且趋向 IT 域应用时，以采用刚性闭锁为主，例如物联网中的传感器。当节点功能复杂且趋向 OT 域应用时，以采用灰度闭锁为主，例如工业机器人。当节点功能复杂且趋向 IT 域应用时，以采用拟态闭锁为主，例如智能车间的中央控制室。

在现实应用中，各类节点中部署的闭锁机制往往是组合式的，通

过闭锁组合提升闭锁效果。例如，基于配合追踪溯源等技术需要也可能在功能单一且趋向 OT 域的节点中配置采用拟态闭锁的特定节点。

此外，节点所在的网络层次、节点的部署成本等因素也会影响闭锁机制的选择，闭锁矩阵还可以作进一步的维度拓展。

四、基于闭锁矩阵的下一代大数据监管系统建设

基于闭锁矩阵，可以将基于物理极限维度的下一代大数据监管系统的概念架构作进一步拓展，根据节点功能的复杂度和对真实世界的物理影响进一步明确监管节点对采用不同闭锁机制节点的监管重点。

1. 对采用物理闭锁节点，监管重点为是否出现超出设置范围的异常数据，关注节点的物理运行状态。

2. 对采用刚性闭锁节点，监管重点为是否出现数据的异常流动，关注非授权获取数据的恶意行为。

3. 对采用灰度闭锁节点，监管重点为节点的物理运行数据和数据的异常流动，关注节点是否已被远程侵入和操纵、预设数据校验是否能控制异常物理运动。

4. 对采用拟态闭锁节点，监管重点为对节点遭遇的恶意行为进行特征提取和追踪溯源。监管节点自身的闭锁机制也以拟态闭锁为主，保障监管节点的安全可信。

在大数据监管系统的建设中，这些监管重点与边缘计算层-雾计算层-云计算层配备的技术深度融合，分层分类分配各项监管任务，配备的技术包括 TLS/SSL 等协议、入侵防护技术、流量识别技术、追踪溯源技术、新型加密技术（混合加密、同态加密等）、安全审计技术、数据匿名化技术、基于数据失真和加密的技术、数据挖掘技术、访问控制技术、区块链、拟态防御等。

其中，雾计算的关键节点需要以拟态闭锁为核心构建防护，从而保障其在面临与云计算层或边缘计算层设备失联时的极端情况下的自主处置权能够正常运转。

五、基于闭锁机制的下一代网络信息安全防护体系构建

构建下一代网络信息安全防护体系，既要充分运用雾计算等新兴网络技术，也要建立与之相适应的核心防护机制——闭锁机制，更要提高人们对网络信息安全的认识与意识，实现人机协同的一体式防护，及时闭锁问题节点与功能模块，将风险遏制在网络的末梢上。

原文链接：https://mp.weixin.qq.com/s/MPskAzW7kNZWQLrqy-QbMA ，转载请注明。