<https://www.sciencedirect.com/science/article/pii/S0167404818311349>

百度百科：

雾计算（Fog Computing），在该模式中数据、（数据）处理和应用程序集中在网络边缘的设备中，而不是几乎全部保存在云中，是[云计算](https://baike.baidu.com/item/%E4%BA%91%E8%AE%A1%E7%AE%97/9969353)（Cloud Computing）的延伸概念，由[思科](https://baike.baidu.com/item/%E6%80%9D%E7%A7%91/454822)（Cisco）提出的。这个因“云”而“雾”的命名源自“雾是更贴近地面的云”这一名句。

雾计算和云计算一样，十分形象。云在天空飘浮，高高在上，遥不可及，刻意抽象；而雾却现实可及，贴近地面，就在你我身边。雾计算并非由性能强大的服务器组成，而是由性能较弱、更为分散的各类功能计算机组成，渗入工厂、汽车、电器、街灯及人们物质生活中的各类用品。

SCADA(Supervisory Control And Data Acquisition)系统，即数据采集与监视控制系统。SCADA系统是以计算机为基础的DCS与电力自动化监控系统；它应用领域很广，可以应用于电力、冶金、石油、化工、燃气、铁路等领域的数据采集与监视控制以及过程控制等诸多领域。

在电力系统中，SCADA系统应用最为广泛，技术发展也最为成熟。它在远动系统中占重要地位,可以对现场的运行设备进行监视和控制，以实现数据采集、设备控制、测量、参数调节以及各类信号报警等各项功能,即我们所知的"四遥"功能.RTU(远程终端单元),FTU(馈线终端单元)是它的重要组成部分．在现今的变电站综合自动化建设中起了相当重要的作用．

一、物联网概念

物联网可以定义为“一个无处不在的网络，它可以通过收集，处理和分析由传感器或智能对象生成的数据来监视和控制物理环境”。

物联网应用于工业环境时，它被称为工业物联网（IIoT）。

二、DDoS攻击和缓解

DDoS攻击以发送大量流量或占用服务器资源的方式，消耗了网络带宽和处理能力，并阻止了向合法用户的网络服务。

云计算具有灵活的计算功能，但是基于云的DDoS防御方法无法充分满足实时操作要求。

为了有效克服现有缓解解决方案的缺点，以分布式和协调方式开发DDoS缓解方法存在挑战，包括低检测效率，高误报率，长时间延迟以及高计算能力和成本。

这项工作的主要贡献是在IIoT环境中应用Fog计算方法，通过在运行过程中分配更近的计算能力，并通过三级缓解架构在系统中分配工作量来减轻DDoS攻击。

1）在现场控制级别，防火墙用于根据已知的攻击流量特征反向过滤攻击数据包。

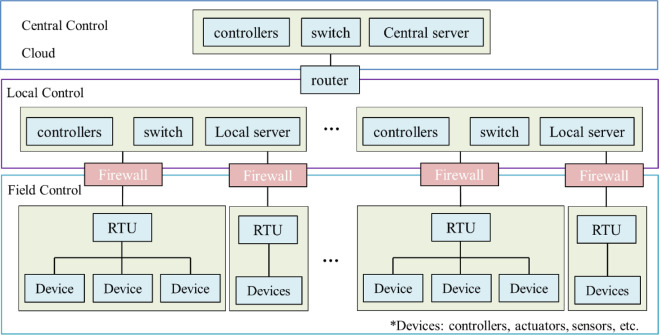
2）在本地控制级别，利用服务器通过实例化虚拟网络功能（VNF）来检查流量，以执行基于规范的流量检测。

3）在云级别，中央服务器将来自多个位置和来源的信息关联并合并，以进行更准确的检测决定。

三、DDoS缓解方案的设计

1、基于雾计算的DDoS缓解架构

基于Fog计算的DDoS缓解方案通过三级架构（即现场，本地和云级）提供了对恶意网络行为的深入调查和分析。该方案利用了现有的传统系统基础结构，例如防火墙和站点服务器，以提供流量监控方面的额外功能。



基于典型工业SCADA系统的DDoS缓解架构

2、基于雾计算的DDoS缓解方案

1）基于规则的数据包过滤

2）基于规范的DDoS检测方案

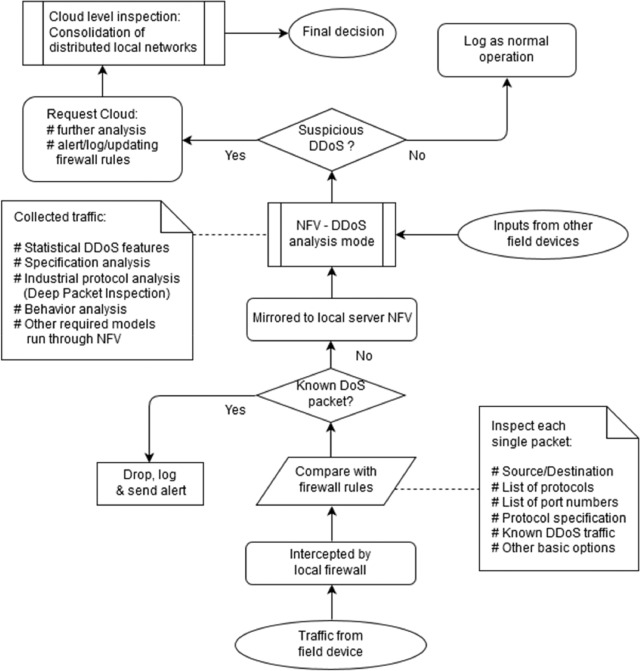
3）基于合并和关联的决策

3、缓解计划的运作程序

阶段1：通过现场防火墙进行初始过滤

阶段2：本地级DDoS检测

阶段3：集中整合和分析



四、实验实现

（在现有的SCADA系统测试平台之上实施该方案。）