**基于MININET的CPS仿真项目**

# 基本概况

为支撑配电网CPS仿真的重点研发项目，探讨基于MININET的CPS仿真平台的系统原理、实现方式，以及验证基于MININET的CPS仿真平台的运行情况，特制定本方案。

## 主要背景

配电系统转向以传统电力供应、分布式新能源发电、储能、信息通信设备和各类用电负荷为主的物理系统与信息系统深度耦合的配电网信息物理系统（CPS）。

与传统配电网相比，CPS具有如下显著特征：

1）多源异构、网络复杂

负荷的分散性和新能源发电的间歇性，不仅改变了传统功率单向流动的特点，而且分布式电源和储能的种类繁多，各种设备性能各异；随着电力系统的信息化建设，大量传感器、通信设备加入，导致系统的物理网络拓扑结构愈加复杂，规模愈加庞大，整个系统的动态特性具有明显的非线性、不确定、时变、异构性等特征。

2）交互频繁、易受攻击

随着智能电表、分布式电源和储能设备的大量接入，为了完成海量信息采集、传输、优化控制及需求侧响应等功能，电力流与信息流交互频繁，信息感知的深度、广度及密度大幅提高，使得信息安全的问题也愈发突出，而通信协议的开放化、标准化，也给调度自动化、继电保护和安全装置自动化、负荷控制、用户信息采集等领域带来了新的安全隐患。

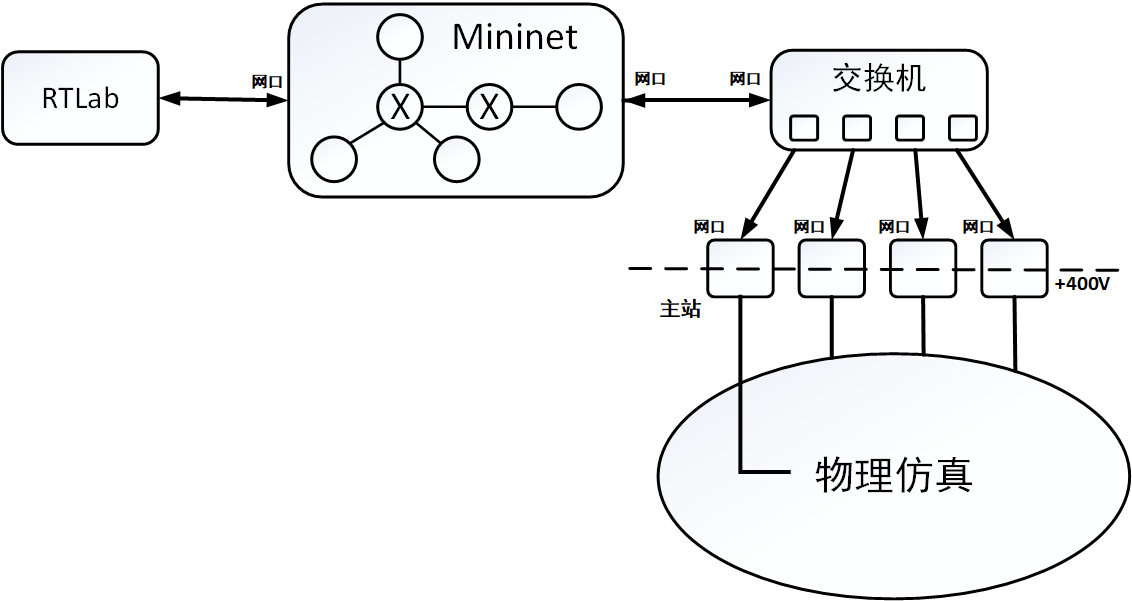
3）分层调度、防护困难

单一的集中式、分散式控制方法，无法综合考虑投资成本、控制性能、可靠通信等指标，而分布式控制能较好地满足系统要求，但电网的分层式调度结构，使得系统严重依赖通信网络的可靠性和完备性，增加了优化控制难度和安全防御风险。

电网CPS是一个比较新的概念，在配用电信息的智能同步与采集、监控设备智能化与数字化等方面取得了一些初步成果。但是对于如何分析和理解电力系统与信息系统的交互机理，如何建立综合计及能量流、信息流和业务流的安全防御体系，如何充分利用前沿信息与通信技术增强配电系统的安全性、可靠性、自适应和自愈能力等问题，还没有形成系统的理论体系，现有的研究成果也相当初步。

# 项目整体方案

如下图所示，针对本课题的需求，设计了如下架构将RTLAB、实际设备（及物理仿真）、Mininet进行融合。



图：部署示意图

如上图所示，Mininet可进行相关的配电网拓扑以及节点的仿真。Mininet与RTLAB之间通过网口连接，Mininet可为RTLAB提供配电网通信状态及配置信息，RTLAB可直接下发命令控制Mininet中的任何一个节点。Mininet可外接交换机，通过交换机与相关实际设备（主站、终端）等连接。主站的网口接入交换机，连接通信网络。主站的非网口（电口）接入物理仿真部分。

基于上述部署环境，虚实结合的实验环境可实现如下功能：

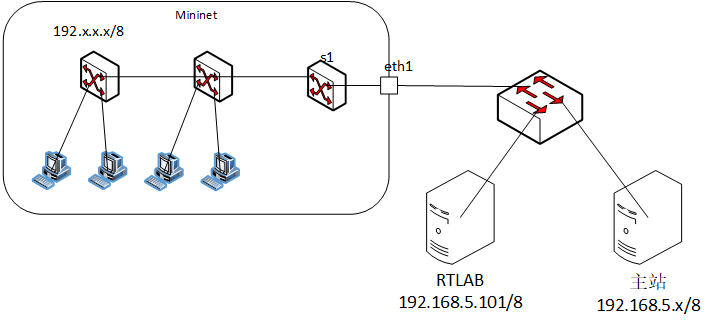
* 配电网通信网络的仿真，包含模拟仿真以及与实际设备结合的仿真
* 各种真实攻击的再现式仿真（可使用真实网络中的攻击发生器进行实际攻击，与真实网络几乎无差别）
  + DDOS攻击：可使用真实的DDOS攻击程序进行攻击。
  + 中间人攻击：可实施典型的中间人攻击。
  + 病毒攻击（模拟病毒传播）:模拟病毒去感染相关机器，这些机器发出一些异常包或者瘫痪等过程。也可以模拟伊朗“震网”病毒的传播模式，病毒在某些机器隐藏、及隐秘传播，只等到相关的关键词出现进行攻击。
  + 网络控制中心侵入的攻击：模拟网络中的控制节点被控制，从而修改网络中的路由策略影响整个网络的连通性。整个网络大多数节点无法按照要求发送到预期的目标。
* 网络动态防御功能的仿真
  + 针对DDOS攻击进行网络的动态配置，降低攻击的危害：在发现可能的攻击流之后，对网络边缘的节点进行控制，从而将相关可疑流导入到模拟的安全设备。
  + 基于网络隔离技术：通过配置虚拟网络，实现网络的分片，从而实现多分区隔离网络。在各个隔离网络的节点，无法访问到其他网络的信息，从而实现安全性。

# 系统设计

## 3.1. 系统搭建之网络通信方案部署

mininet内部网络需要和外部网络进行通信，所以可以将mininet所在主机网口和mininet内部虚拟交换机绑定，如此，可以借助通向外部网络的交换机实现内部结点与外部网络通信。

网络环境搭建方案如下：



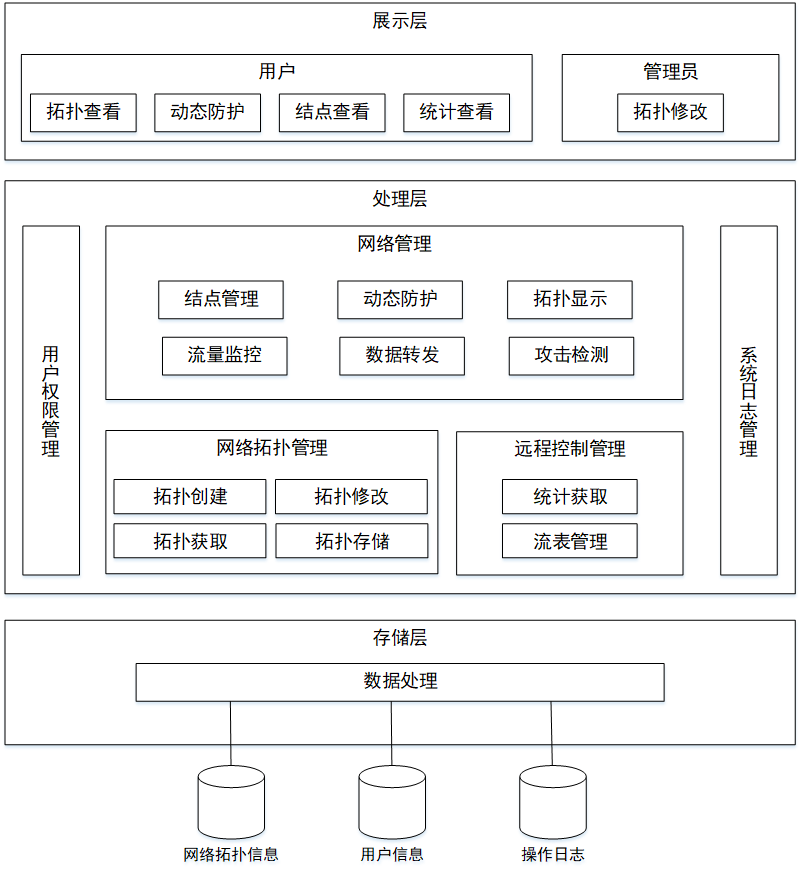
图：网络通信部署图

上述的网络环境搭建方案中，mininet网络可以采用不同的子网段，由于mininet是采用主机的网口和外部网络进行通信，所在主机的IP地址属于同一子网，本方案实验中采用的是192.0.0.0/8该子网，可以支持2^24-2台主机。

## 3.2. 系统功能结构

### 3.2.1. 系统功能结构框图

以下为网络仿真系统的模块结构图。如图所示，系统由三层架构组成，展示层、处理层、存储层组成。



图：系统模块架构图

如图所示，最上层的展示层对应系统架构的系统客户端界面，由用户模块和管理员模块组成，主要实现用户对系统操作的界面；中间层的处理层对应系统架构的服务器的处理层，由网络管理模块、网络拓扑管理、远程控制管理模块以及用户权限管理模块和系统日志管理模块组成，主要实现系统对用户需要的任务所进行的具体操作；底层的存储层对应服务器的存储层，由数据处理模块和数据源组成，主要实现系统对数据的可持久化。

### 3.2.2. 系统功能组件定义

下面将对上图中的各个模块的功能和主要实现方法作简要说明。

**数据处理**模块主要实现对持久化数据的一系列操作，网络拓扑信息、用户信息和操作日志的查询，以及针对这些信息的修改。

**网络拓扑管理**模块主要实现仿真系统中网络拓扑的创建以及修改，此外还包含了对拓扑信息的获取和存储功能。网络拓扑管理模块由拓扑创建、拓扑获取、拓扑修改、拓扑存储子模块构成。

**远程控制管理**模块主要实现仿真系统中网络通信中的一系列控制操作和统计信息的获取，具体可获取通信过程中实时流量信息和累计流量信息，以及针对网络中有限制的通信，可通过控制流表的操作实现。远程控制管理模块由统计获取和流表管理子模块构成。

**网络管理**模块主要实现仿真系统中对网络一系列操作，对网络结点信息的管理，网络拓扑的显示，以及针对网络攻击所实施的动态防护功能；此外，还有流量监控功能，控制网络结点数据转发的功能和结点攻击检测的功能。网络管理模块由结点管理、动态防护、拓扑显示、流量监控、数据转发、攻击检测子模块构成。

**用户权限管理**模块主要实现对系统用户信息的操作，该模块仅限管理员操作，可进行用户的增加、删除，修改用户的密码及权限，限制用户是否具有查看拓扑、修改拓扑、查看日志等功能。

**系统日志管理**模块主要实现记录用户的各种操作及发生时间，例如登入、登出、修改拓扑、查询流量信息等。

**拓扑查看**模块主要实现用户查看仿真系统的网络拓扑信息，网络中各类结点个数，结点之间的连接关系通过图的形式展示。

**动态防护**模块主要实现网络拓扑中攻击的识别以及动态防护，并且实时展示防护过程，用户可以选择开启或者关闭入侵检测和网络动态防护以了解动态防护对于网络拓扑系统的保护效果，可以完成对网络拓扑中网络攻击的识别也就是系统入侵检测以及针对于入侵选择合适的防护策略以完成动态防护，并且实时展示防护过程中的信息流或者网络分区变化。

**结点查看**模块主要实现用户查看网络结点详细信息，包括host的类型和ip信息以及资源使用情况，还可查看switch的结点详细信息。

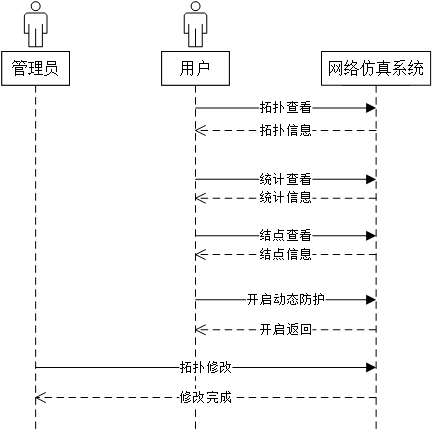
**统计查看**模块主要实现对网络中流量信息的统计功能，实时显示当前各个线路中流量大小，和每条线路中各个时段总流量大小。

**拓扑修改**模块主要实现管理员对网络拓扑中结点的增删和链路的增删操作。

## 3.3. 系统功能实现动态描述

### 3.3.1. 系统与外部交互

从系统整体的层面来看，下图动态地显示了系统与外部对象之间的交互关系：



图：系统与外部交互

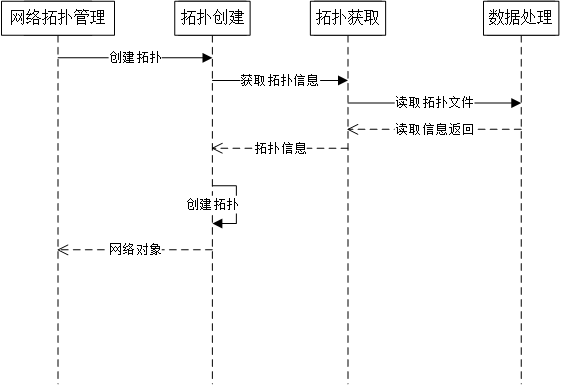
上图隐藏了系统的内部模块划分，重点在于显示出本系统与外部对象的动态消息交互关系，展现了各个消息之间的时序关系。其中，消息交互的序列简述如下：

1. 用户调用系统查看拓扑，系统返回网络拓扑信息，并将拓扑信息依据规定方式以图的形式展示出，并可继续查看拓扑中结点详细信息。
2. 用户调用系统统计查看，系统返回网络中当前时段各个区域流量累计总和，通过折线图形式展示给用户，以及实时返回每条链路的流量信息，在图中以颜色区分。
3. 用户调用系统结点查看，系统依据用户输入的参数，对结点信息进行查询并返回，还可查询结点当前cpu等资源使用情况。
4. 用户调用系统开启动态防护，系统即开启动态防护功能，对网络中的网络攻击进行检测并采取防护措施，返回提示用户功能已开启。
5. 管理员调用系统拓扑修改功能，对网络拓扑的结点和链路进行增删操作，系统修改完成并返回提示用户修改完成。

### 3.3.2. 系统模块间交互

系统模块由网络管理模块、网络拓扑管理模块、远程控制管理模块和数据处理模块组成，网络管理模块由结点管理、动态防护、拓扑显示、流量监控、数据转发、攻击检测子模块构成；网络拓扑管理模块由拓扑创建、拓扑获取、拓扑修改、拓扑存储子模块构成；远程控制管理模块由统计获取和流表管理子模块构成。下面描述这几个模块在各种操作下它们之间的交互：

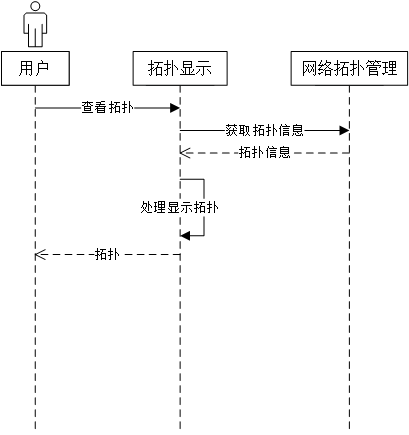
1. 拓扑创建模块交互



图：拓扑创建模块交互

上图描述了网络拓扑创建时，各系统模块间动态交互的时序；交互时序为：

1. 网络拓扑管理模块调用拓扑创建模块的创建拓扑接口；
2. 拓扑创建模块调用拓扑获取模块的获取拓扑信息；
3. 拓扑获取模块调用数据处理模块读取，读取拓扑文件并返回信息；
4. 拓扑获取模块将返回的拓扑信息返回给拓扑创建模块；
5. 拓扑创建模块获得拓扑信息，调用自身创建拓扑方法；并将创建后的网络对象返回给上级网络管理模块。
6. 拓扑显示模块交互



图：拓扑显示模块交互

上图描述了用户调用展示层的拓扑显示模块查看拓扑时，各系统模块间动态交互的时序；交互时序为：

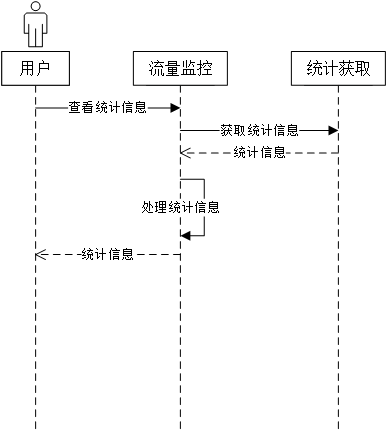
1. 用户调用拓扑显示模块的查看拓扑方法；
2. 拓扑显示模块调用网络管理模块的获取拓扑信息方法，网络管理模块返回拓扑信息；
3. 拓扑显示模块获得拓扑信息，根据拓扑信息处理显示并返回；
4. 用户可在界面上查看到网络拓扑。
5. 结点信息查看模块交互



图：结点信息

上图描述了用户利用展示层的结点查看模块查看网络结点信息时，各系统模块间动态交互的时序；交互时序为：

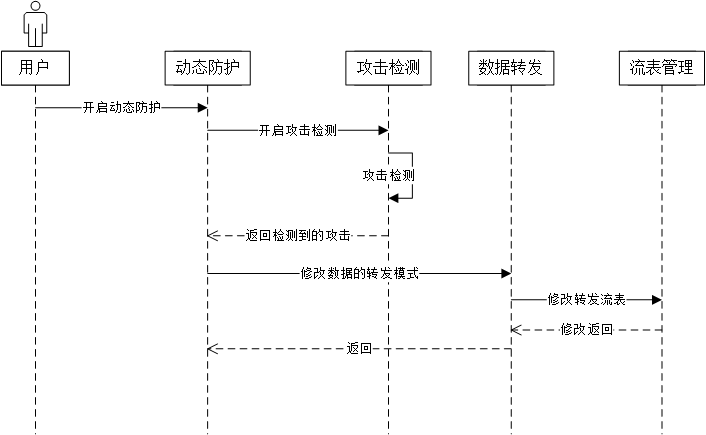
1. 用户调用结点管理的查看结点信息；
2. 结点管理模块调用网络拓扑管理的查看结点信息，网络拓扑管理模块将结点信息返回给上一级；
3. 结点管理模块将结点信息显示返回给用户；
4. 用户调用结点管理模块的查看结点资源信息；
5. 结点管理模块调用网络拓扑管理模块的查看结点资源信息方法；
6. 网络拓扑管理模块调用自身的查看结点资源信息方法，并将返回结果的资源信息返回上级；
7. 结点管理模块获得结点资源信息显示返回给用户。
8. 统计信息查看模块交互



图：统计信息查看模块交互

上图描述了用户利用展示层的统计查看模块查看网络统计信息时，各系统模块间动态交互的时序；交互时序为：

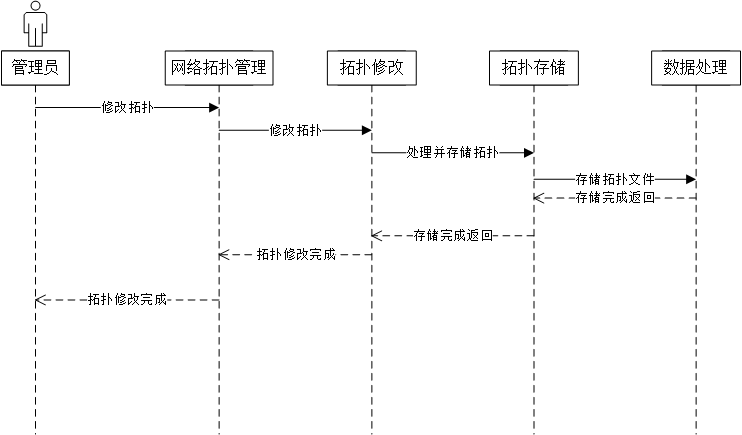
1. 用户调用流量监控模块的查看统计信息；
2. 流量监控模块调用统计获取模块的获取统计信息；
3. 统计获取模块执行方法后将统计信息返回上级；
4. 流量监控模块获取统计信息后，执行处理统计信息的方法，显示并返回给用户查看。
5. 动态防护模块交互



图：动态防护模块交互

上图描述了用户利用展示层的动态防护模块开启动态防护时，各系统模块间动态交互的时序；交互时序为：

1. 用户调用动态防护模块的开启动态防护；
2. 动态防护模块调用攻击检测模块的开启攻击检测方法；
3. 攻击检测模块开启攻击检测的方法，在检测到攻击后返回给动态防护模块；
4. 动态防护模块调用数据转发模块的修改数据的转发模式；
5. 数据转发模块调用流表管理模块的修改转发流表，流表管理模块修改完成后返回；
6. 数据转发模块修改转发模式后返回上级动态防护模块。
7. 拓扑修改模块交互



图：拓扑修改交互

上图描述了管理员利用展示层的拓扑修改模块对网络拓扑进行修改时，各系统模块间动态交互的时序；交互时序为：

1. 管理员调用网络拓扑管理模块的修改拓扑；
2. 网络管理模块调用拓扑修改模块的修改拓扑；
3. 拓扑修改模块修改完毕拓扑后调用拓扑存储模块的处理并存储拓扑方法；
4. 拓扑存储模块对拓扑信息依据规定方式处理拓扑信息，调用数据处理模块的存储拓扑文件；
5. 数据处理模块存储完成后返回上级，各级一次返回。