2015

CPS security testbed federation: architectural design, implementation and evaluation

Anirudh Pullela
Iowa State University

CPS security testbed federation: Architectural design, implementation and evaluation

by

Anirudh Pullela

A thesis submitted to the graduate faculty

in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

Major: Computer Engineering

Program of Study Committee:
Manimaran Govidarasu, Major Professor
Douglas Jacobson
Venkataramana Ajjarapu

Iowa State University

Ames, Iowa

2015

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGEMENTS

Firstly, I would like to thank my parents, P.Y.N. Sastry and P. Suryaprabha, and my brother, Sandeep Pullela, whose role in my life brought me to where I am today and with whose support and inspiration the idea of pursuing my Master’s degree materialized.

I would like to thank my major advisor, Dr. Manimaran Govindarasu, for giving me the opportunity and privilege of working with him. He introduced me to how research is done and guided me at every step of this project. His belief in me was the source of inspiration to push harder when there were obstacles.

I would also like to thank Aditya Ashok of Iowa State University and Ryan Goodfellow of Washington State University, who worked with me on this project and made immeasurable contribution to this project. I have had a lot to learn from them during the course of this project and am grateful for their help.

I would like to thank my childhood friends, Vivek Balusu, Rajiv Gautham and Puneeth Reddy, and my friend Divija Kota, for their virtual presence during the course of my Master’s degree. Conversations with them always brought a smile to my face at whatever time or situation.

Finally, I would like to thank Iowa State University, the Department of Electrical and Computer Engineering, the faculty and the student community who all played a role in making this a wonderful journey of education and making me feel at home away from home.

ABSTRACT

Experimental testbeds play an important role in spearheading the advancements in any given field, be it technology testbeds, energy testbeds, manufacturing testbeds or transportation testbeds. Each of the testbeds has their own resources and capabilities but a lot more can be achieved if they are not as disconnected as they are. When two or more testbeds form a federation, the federated testbed offers more in terms of functionality and resources, thereby opening more possibilities and avenues of research. This thesis is based on the federation of a cyber-physical security testbed located in Iowa State University, PowerCyber, to a cyber-security testbed located in University of Southern California, DETERLab. This work is meant to address the milestones and challenges pertaining to the implementation, configuration and use-case scenarios of a Federated Testbed of this nature.

This thesis primarily discusses the architectural design of the proposed Federated Testbed and discusses the milestones involved in its implementation. Further, this work also portrays the functionality of the Federated Testbed post-implementation through a use-case scenario, in order to showcase the experimental capabilities of the testbed. This work also goes on to evaluate the Federated Testbed's metrics in terms of latency and volume of packet loss between the two testbed environments, PowerCyber and DETERLab and also compares the results to previous results in a non-federated environment. Finally, future work is suggested and conclusions are listed.

CHAPTER 1

BACKGROUND

Smart Grid – Power Infrastructure of the Future and its Vulnerabilities

Over the last few years, the power infrastructure in the country has had a vital facelift in terms of reliability, efficiency and resiliency and is on the path of transforming into a "smart grid". Steps are being taken to digitize large parts of the power grid to allow for two-way digital communication in place of the primitive one-way electromechanical power grid. While doing this brings a more sustainable power grid in the future, it also opens up new interdependencies and vulnerabilities. Integrating information technologies is essential to building a smart grid, but it is even more important to devise effective strategies to secure the computing and communication networks that form the core of the envisioned electric power infrastructure.

According to a report presented by National Institute of Science and Technology (NIST) [1] in 2010, the following were listed as the key points in the cyber-security strategy for smart grids –

1. Prevention – Required steps should be taken to perform continuous assessment of the grid components and ensure that the risk due to threats and vulnerabilities are minimum.
2. Detection – Action should be taken to detect anomalous behavior, intrusions, malicious code and events that may disrupt the normal functioning of the electric grid.

3. Response – Responsive measures should be taken to address immediate effects of an unforeseen incident, such as avoiding or reducing loss of lives and property.
4. Recovery – In the case of an incident, measures should be taken to restore the smart grid to its normal operating conditions as soon as possible.

In order to devise effective strategies to secure the smart grid, it is not wise to experiment on a real smart grid infrastructure. It is necessary to have an environment to that mimics a real smart grid environment and that can support researchers to perform attack-defense analysis and vulnerability assessment. This throws into relief, why Cyber-Physical Security testbeds are of growing importance.

PowerCyber – A Cyber-Physical Security Testbed

PowerCyber [2] is a smart grid testbed whose vision is to make significant contribution to ensure the security of critical power infrastructure against sophisticated cyber-attacks. With the use of automated control systems, i.e., use of the cyber network for grid communication, increasing in the electric power grid, it has become a challenge to protect the grid infrastructure from cyber threats. The attacks on grid infrastructure belong to a specific set of cyber-attacks. While the attacks take place on the cyber layer, the target of these attacks is not cyber devices but is the physical components of the grid. PowerCyber research is focused on Cyber-Physical Security, i.e., finding vulnerabilities for these specific set of cyber-attacks and includes impact estimation of such attacks and methods of mitigating such attacks.

Architecture

The architecture of PowerCyber consists of three entities –

1. Control System

2. Physical System
3. Cyber Layer

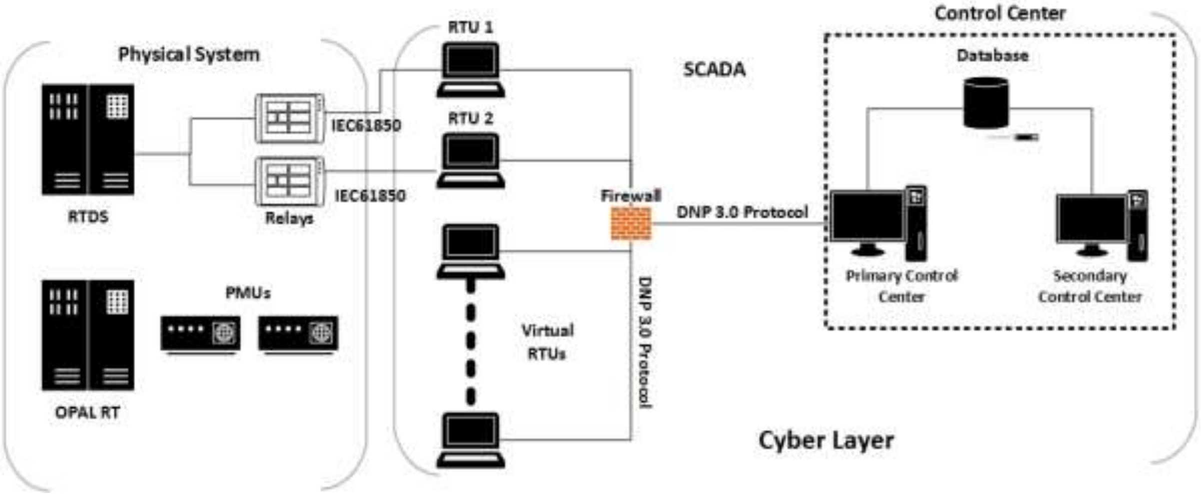


Figure 1 PowerCyber Architecture

<u>*Control System*</u>

The control of the grid is distributed between the functions of the control center and the functions of the substations.

Control Center is a combination of two individual control centers, which communicate to each through a common database which contains information regarding the communication specifications of individual substations and the physical devices they interact with. It serves as the SCADA server and enables SCADA communications with substations. It performs the SCADA functions of the grid such as device status indication, measurement collection and broadcasting operator commands to field devices.

Substation consists of an RTU and Intelligent Electronic Devices (IEDs). The substations interface to the power system simulations in the environment. The IEDs act as over-current protection relays and can pass on current and voltage measurements in the transmission lines to the RTUs. The RTUs accumulate this data and send it to the control center. Substations in the environment are of two kinds – 1) dedicated RTUs connected to physical IEDs, and 2) virtualized RTUs connected to virtual IEDs which are modeled by the power system simulation.

Physical System

The physical system of the testbed is deployed by the Real-Time Digital Simulator (RTDS) and OPAL RT. Both of them provide the testbed with the capability of performing real-time power system simulations and also allow integration with physical hardware. The power system model that they currently simulate is the Western Electricity Coordinating Council (WECC) 9-bus model. The real-time capabilities of the RTDS and OPAL RT allow the simulation to mimic the physical response characteristics of power system equipment in various scenarios.

Communication

The communication layer is the most crucial part of the grid, seamlessly integrating the physical system and the cyber components.

PowerCyber uses industry standard communication protocols, similar to the ones used in real smart grid environments. The communication scheme follows the Supervisory Control and Data Acquisition (SCADA) system.

The communication between the control center and substation uses the wide-area DNP3 protocol. The DNP3 protocol communication takes place over IP.

In the substation, the RTU and the IEDs communicate through the IEC 61850 protocol to transfer commands and status information. IEC 61850 GOOSE messages are casted over the Ethernet to facilitate power system protection mechanisms. These allow the IEDs to talk to each other with a very high response rate. Manufacturing Message Specification (MMS) protocols are used to transfer analog and binary values between the RTU and IEDs.

Research Applications

PowerCyber's multi-disciplinary environment gives way to the multiple research applications.

- Vulnerability Research – Inspect weaknesses within the environment
- Impact Analysis – Explore cyber-attack impact on physical systems
- Mitigation Research – Find mitigation strategies and verify their effectiveness
- Cyber-Physical Metrics – Develop metrics combining cyber-physical properties
- Data and Models Development – Exploration of innovative security approaches
- Security Validation – Evaluation of security posture of the system for self-assessment and compliance requirements
- Interoperability – Evaluation of how products support and connect with real-world systems
- Cyber Forensics – Explore ways to detect cyber-attacks specific to industry protocols and field devices
- Operator Training – Providing operators interaction to the power system controls during simulated cyber-attacks.

DETERLab – A large-scale Cyber Security Experimentation Testbed

The DETER project[3] was kicked off in 2004 at the Information Sciences Institute in University of Southern California, with the intention to provide researchers a platform to conduct cyber-security experiments within a controlled environment. It was built upon Emulab software, offering a wide range of tools and platforms for cyber-security experimentation. DeterLab experiments emulate real-world network complexity, allowing researchers to choose their environment to conduct sophisticated networking and cyber-security experiments.

The DETER testbed is laid out across University of Southern California and University of California at Berkeley, consisting of about 400 general purpose computers and 10 FPGA-based reconfigurable hardware elements, enabling a dynamically reconfigurable switched network.

Experiment Modeling

DeterLab experiments allow users to describe their environment by creating network topology and complexity of their need and let them generate, route and decide the bandwidth of their traffic in every section of the experiment. Typically, as far as the experimenter is concerned, every experiment has a life cycle that contains the following stages –

1. Design
2. Instantiation
3. Execution
4. Analysis

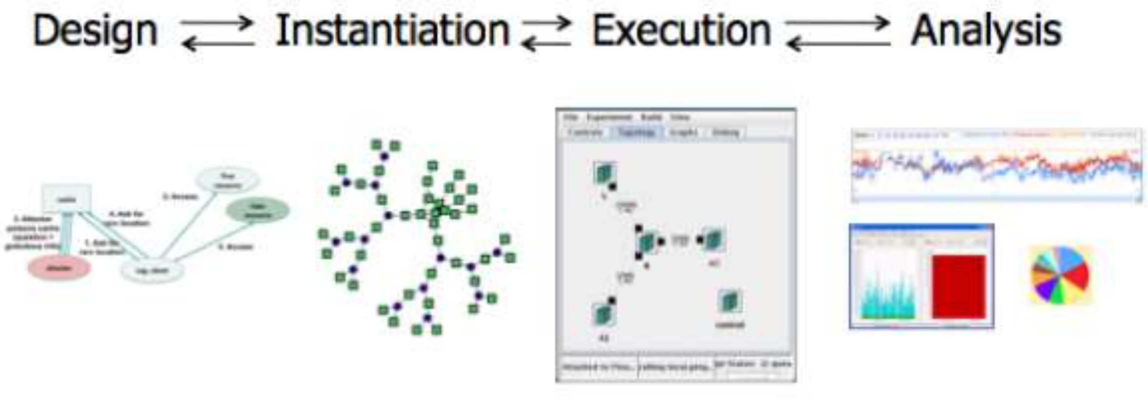


Figure 2 Experiment Cycle in DeterLab [3]

This provision from DeterLab makes it easier for users to focus on the design and running of their experiments and not worry about the backend events happening within DETER.

In the backend, once the user creates an experiment, DeterLab allocates resources to the experiment model by leveraging the DeterLab "Containers" System [3]. Depending on the modeled experiment, the Containers System provides experiment resources of varying scale and fidelity, i.e. allotting whole computers as high fidelity when necessary and virtual machines when high resolution is not necessary, making the experiment scalable and dynamic for the experimenter.

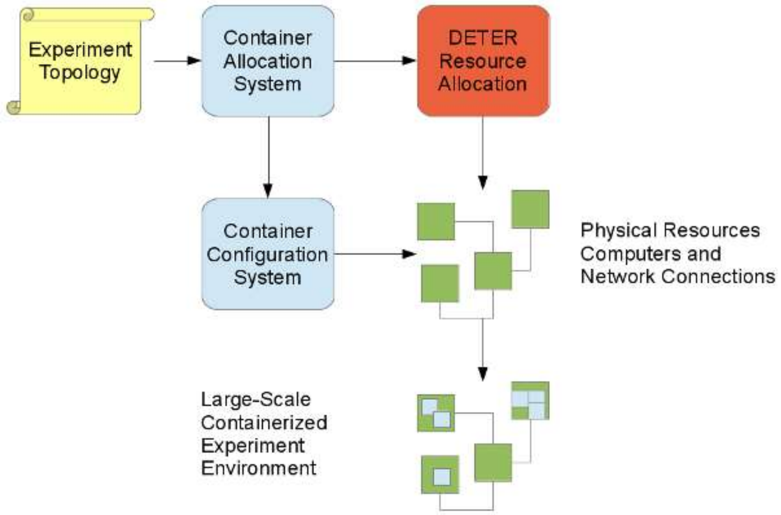

Experiment Topology
Container Allocation System
DETER Resource Allocation
Container Configuration System
Physical Resources Computers and Network Connections
Large-Scale Containerized Experiment Environment

Figure 3 DETER Containers System [4]

Custom Modeling of Experiment Nodes

The nodes within DeterLab are designed to allow users to choose what exactly they want to do with them. From choosing to OS of nodes to choosing startup applications and running custom initiation scripts, DeterLab allows users to fully customize each node to suit their need.

By default, DeterLab offers the following OSes to run on nodes –

1. Free BSD 8 and Free BSD 9
2. CentOS 5 and CentOS 6
3. KALI 1
4. Ubuntu 10.04, 11.04, 12.04
5. Windows XP SP3

Further, uses can use RPMs or TARballs to add custom features to any node at the time of design. If the customizations cannot be contained within a TARball, then the users can also create their custom OS and upload it to nodes as needed.

Example Experiment Topology

Each experiment created within DeterLab involves, designing the network topology in an NS file or using the DeterLab GUI that allows drawing the topology.

After placing nodes as needed, users can load them with the required OSes and get them to run custom TARs within. In case of an NS file, these parameters are filled in while creating the node itself.

Each experiment contains a node named ‘control’ which is not connected to topology but is part of the environment and is the node through which users control their experiment.

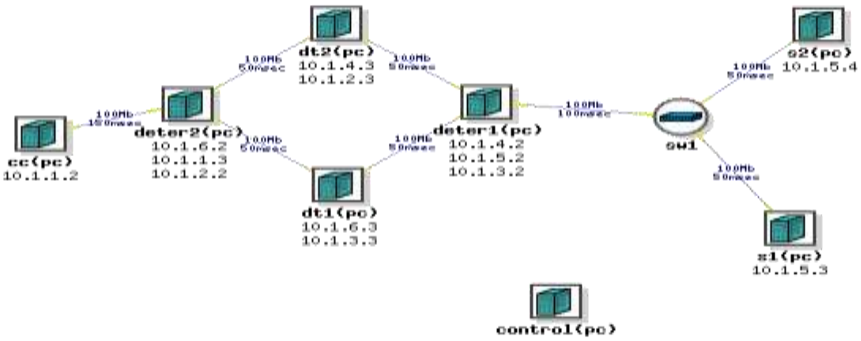


Figure 4 DETER Experiment Topology

Further, users can define the link characteristics and delay characteristics for each part of the network and gain total control over the experiment.

Motivation for Testbed Federation

Testbed federation is being highly encouraged in the research community. Federation provides testbeds with expanded functionality. Especially in the case of cyber-security and cyber-physical security testbeds, such as PowerCyber and DeterLab, federation provides a higher level of experimentation. Some of the motivations of putting together a Federated Cyber-Physical Testbed are as follows –

1. Provides scope real-time wide-area experimentation
2. Provides scalability to the cyber-physical environment as the cyber network is larger after federation.
3. Resource-sharing removes limitations in terms of hardware for experimentation and saves cost.
4. Larger cyber-physical systems can be spawned for experimentation as there is almost no limitation in terms of number of nodes, after federation.
5. A large federation of testbeds can potentially be the platform for the research community to perform remote experimentation, in spite of not having their own resources, thereby helping the research community at large.

The above motivations stand good for almost any testbed federation and apply to the PowerCyber and DeterLab federation as well.

CHAPTER 2

RELATED WORK

The purpose of this section is to discuss literature on work that has been done to achieve testbed federation, or which contributes to the same.

Network Domain Federation – An Architectural View on How to Federate Testbeds

This work [5] describes a generic approach to federating domains from a networking standpoint. On a broad scale, this article discusses domain federation as a model for establishing large-scale infrastructure for communication technologies, services and applications. With that said, testbed federation is used as a concrete example to display the architectural specifics of domain federation.

The article addresses that the issue with testbed federation or domain federation is the heterogeneous nature of two or more given environments. The article refers to federation as not just a connection between two or more environments but as a balance between efficiency and fine grained management, while imposing minimum overhead. With this view, a generic approach is suggested for domain federation which is, in turn, used to present a concept for domain federation.

The article presents domain federation in two steps –

- Achieving Federation Connectivity
- Enabling tools for utilizing the federation as an infrastructure

Federation Connectivity

Federation Connectivity is provided as a solution to the most common interconnection problems between two environments. Federation Connectivity aims to achieve one of the main objectives of imposing minimum requirements on individual domains. The solution proposes to use Gateways at the border of each domain, acting as converging points and establish dynamic VPN links between each domain.

The article also suggests a central federation control unit that ensures connectivity between the Gateways and the respective domain resources. The VPN technology allows for setting up a more secure overlay instead of utilizing the lesser secure network links.

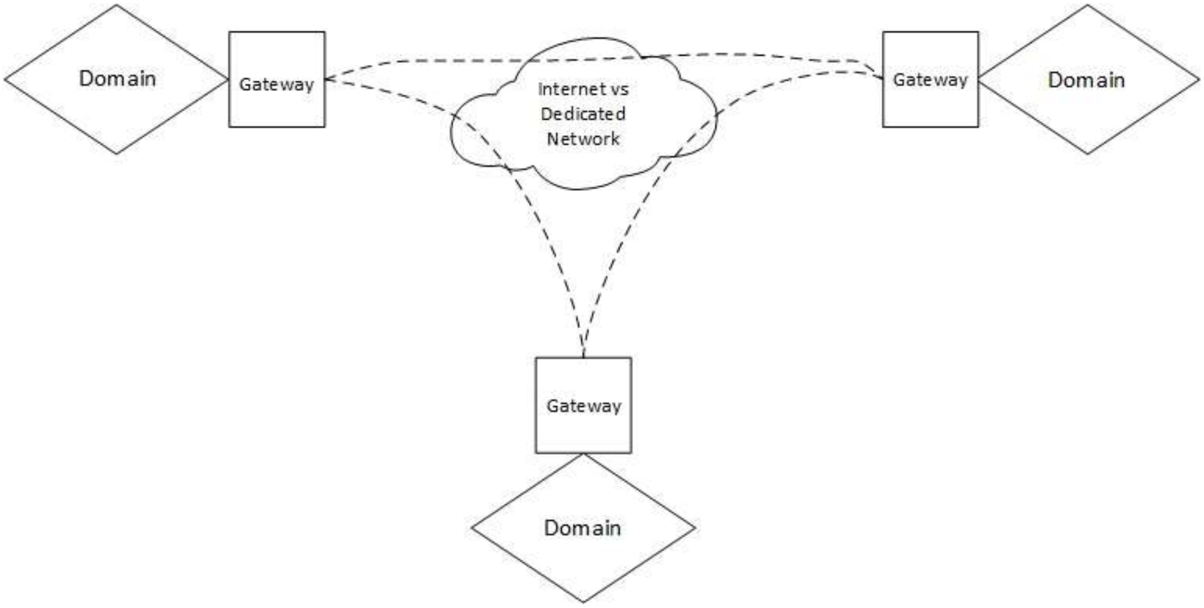


Figure 5 Federation Connectivity [5]

Enabling Tools for Federation

A federation is not complete if there are no tools/services that either leverage or enable the functionality of the federation. This article presents a centralized approach to federation, where most of the functionality is provided by the centralized control unit. The article addresses distributed peer-to-peer control as well, but explained that centralized approach would be the best method when multiple testbeds are involved since functionalities such as authentication and establishment of trust might be more feasible and controllable using the centralized approach.

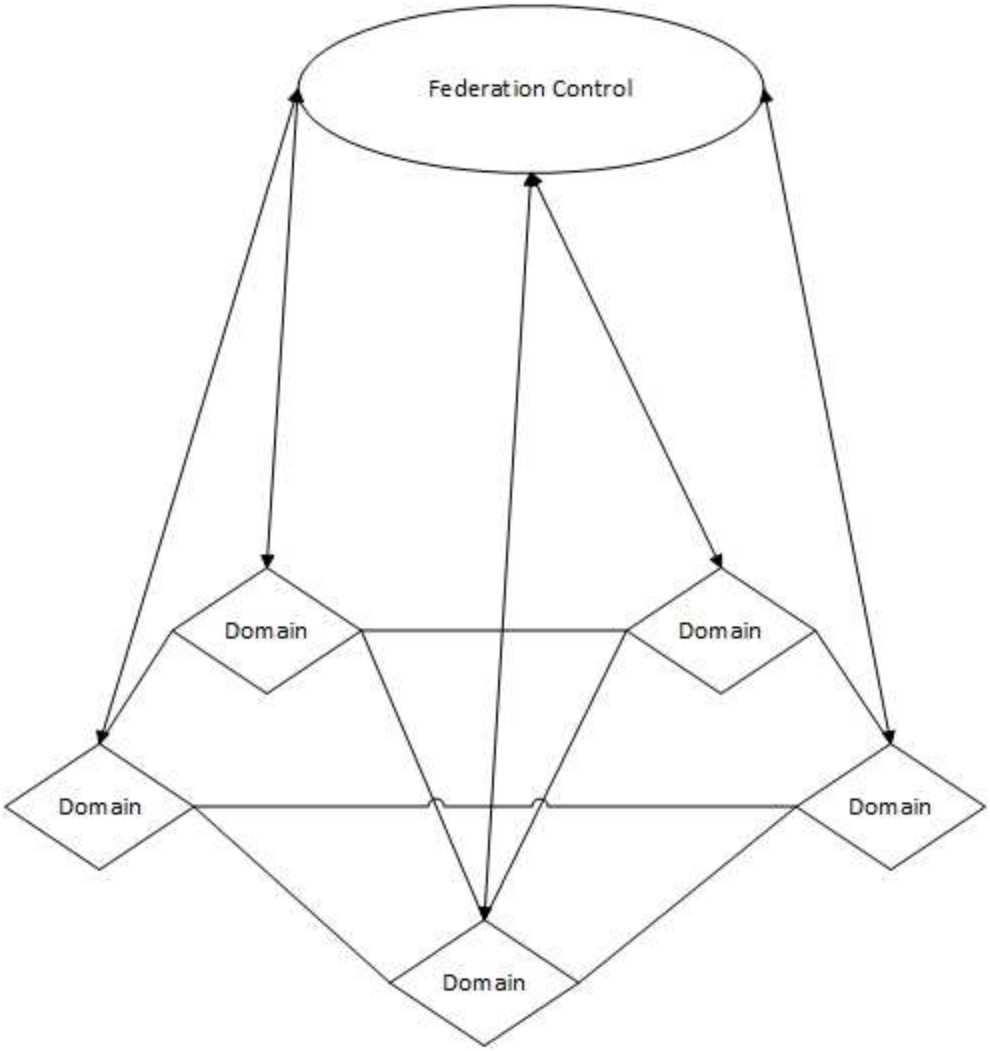


Figure 6 Centrally-controlled Domain Federation [5]

The above figure shows the proposed architecture for a federated testbed across multiple domains, along with the central federation control unit and its control flow across the domains.

This work highlights the main issues to be addressed with regards to networking for federated testbeds and illustrates practical implementation with the proposed architecture.

An Architecture for International Federation of Network Testbeds

This work discusses the challenges involved in International Federation [6] of networking testbeds and proposes an architecture based on the GENI project, which is a product of the US National Science Foundation.

The paper identifies the key challenges involved in an international federation to be establishment of trust and user access policies while maintaining the autonomy and abstractions of individual testbeds.

The paper starts off by discussing the growing need for federated networking testbeds since they present a platform for researchers to investigate the future of the internet architecture.

SFA Architecture

The paper proposes an architecture named ProtoGENI [6] which is based off the GENI framework. This leverages the granular "Slice-based Federation Architecture" (SFA) [7] which was developed by the GENI community. According to SFA, a "slice" is a partition in the physical facility of the testbed. Each slice can be running a different network architecture or experiment within it. A slice contains a set of "slivers" which could be a virtual machine, VLAN, virtual circuit or entire physical components (PCs, routers, switches, links, etc.). Each GENI facility contains an Aggregate Manger (AM) which manages all the resources or components in that facility. A user can create slices spanning across multiple AMs for experiments. There also exists a Registry which stores the mapping of resources to their corresponding GID. The Registry is also responsible for issuing certificates and credentials to entities and resources.

With respect to international federations, ProtoGENI consists of three entities built upon the GENI-based SFA – Identity Providers (IdPs), Slice Authorities (SA) and Clearinghouse (CH).

IdPs provide identity to users by provisioning them with unique names and issuing user certificates.

Slice Authorities are responsible for manipulating slices. They create slice names and grant users necessary credentials to perform actions within a slice.

Clearinghouse is used as a mechanism to establish trust in a large-scale federation, which is an issue in case of an international federation of multiple testbeds. It publishes certificates of its own federate that are used to establish trust. It can also discover certificates of other federates. Discovering certificates does not mandate the Clearinghouse to trust the federate; a federate may choose not to trust certificates or may also trust additional certificates that are not present in the Clearinghouse. The Clearinghouse simply makes the process of establishing trust more convenient.

The flow of interaction within a federation is depicted in the figure below –

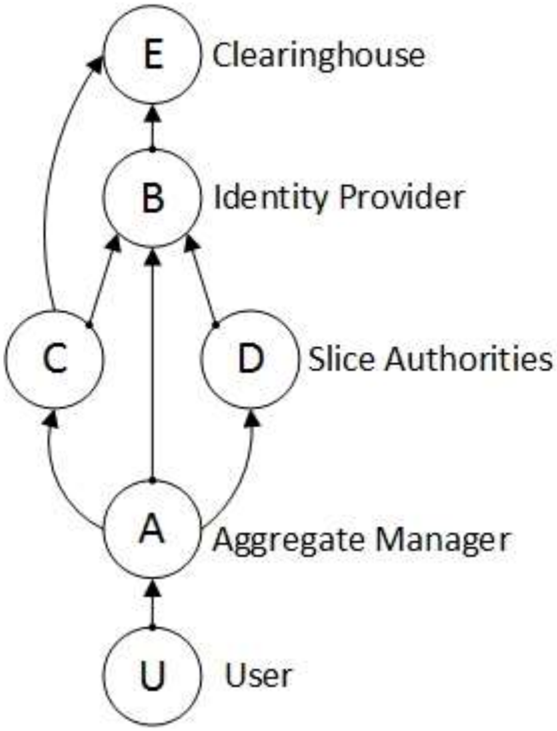


Figure 7 Flow of interaction in ProtoGENI Federations [6]

Proposed Architecture for International Federation

The proposed architecture starts off by defining an “Inter-Federation” to be a federation whose member are federations themselves. Utilizing the ProtoGENI architecture, the inter-federation architecture consists of a “Global Clearinghouse”, a single Clearinghouse for the entire federation.

There are two cases for establishing trust in an inter-federation –

1. Single root of trust per federation, and
2. Multiple roots of trust per federation

The methods of establishing trust for each of these cases is at the will of each federate.

Single root of trust is easier implemented when each federate's certificate is included in the Clearinghouse, indicating that trusting the Clearinghouse means trusting all the members of the federation. When this is not the case and there are exceptions in the trust certificates in the individual federates, then the multiple roots of trust scenario is the way to go.

The paper sums up by talking about the design challenges involved in federations, especially with international federations, due to issues related to operational and policy autonomy that is required by federations from different nations. The paper goes on to highlight that the proposed architecture has been implemented on a dozen testbeds and the results suggest that it is a practical route to performing international federations.

CHAPTER 3

FEDERATION ARCHITECTURE

The federation between PowerCyber testbed and DeterLab testbed is primarily to share resources and to add functionality to both testbeds. The federation provides cyber-physical security experimentation functionality to the DETER environment and provides real-time networking latency between the control center and substation communication in PowerCyber as that in real smart grid environments, thus adding accurate measurements to the experiments.

The motivations behind the federation are listed as under –

- Using DETER to perform large-scale experiments as part of PowerCyber's cyber-attack assessment
- A combination of PowerCyber's components and DETER's components can pave way to setting up a large-scale cyber-physical security testbed that can be used by the broader research community for remote experimentation, much like how DeterLab is being used today.

DETER Federation Architecture (DFA)

The DETER Federation Architecture [8] was designed to enable researchers to conduct what DETER calls "Federated Experiments". According to DETER, a federated experiment enables researchers to connect two or more distinct testbeds, which may or may not be of the same nature, in order to share resources and run meaningful experiments leveraging the capabilities of these testbeds.

DeterLab accomplishes a federation by using what they call a ‘Fedd Client’. In a two-way federation between two testbeds, Fedd Clients are present on either sides of the federation, routing traffic back and forth between the two environments and allowing sharing of resources.

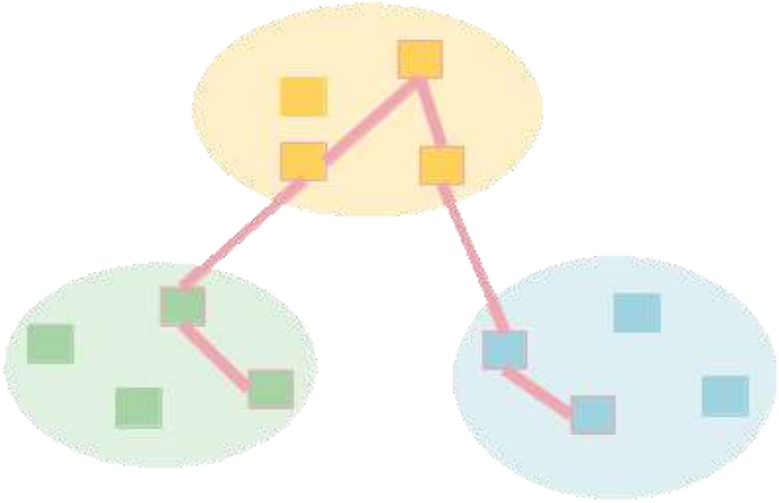


Figure 8 DETER Federation Architecture [8]

The Fig. 8 shows what it would look like to have a federation of multiple testbeds with the Fedd Client being the underlying fabric of connectivity. The advantage of this kind of federation is that only resources that are necessary for the experiment can be shared and others can be cut out to avoid unwanted communication within the federated experiment.

The DFA was used to implement the federation between PowerCyber and DeterLab by placing Fedd Clients in each of the environments.

The federation was completed with three milestones along the way.

1. Milestone 1 – Setting up communication between the two testbeds and using the DETER environment to route wide-area traffic from the Control Center to Substation
2. Milestone 2 – Setting up the PowerCyber experiment within DeterLab

3. Milestone 3 – Designing a meaningful use-case scenario and run it on the federated testbed to showcase the functionality

Milestone 1

The first step of the federation is to ensure that there is communication between components in both testbeds. Once traffic can be routed through to DETER, the DETER environment can be used for wide-area networking fabric for the SCADA communication between the Control Center and the Substations.

DETER as a wide-area networking fabric

According to the PowerCyber setup, all components are present on the same local area network (LAN) which means that all communication within the environment, though using the real-world grid control protocols and mechanisms, is still local traffic. The unrealistic part of this is that the latency of communication between the control center, substations and the power system components is very small. In a real smart grid environment, the substations are laid out across different geographic locations, so the communication latencies that we see in PowerCyber are the ideal case and not what we see in the real-world. In order to overcome this, an experiment was created within DeterLab which routes control center communication through nodes inside the experiment and brings it back to PowerCyber's substations. The architectural concept of this milestone is represented in the diagram below –

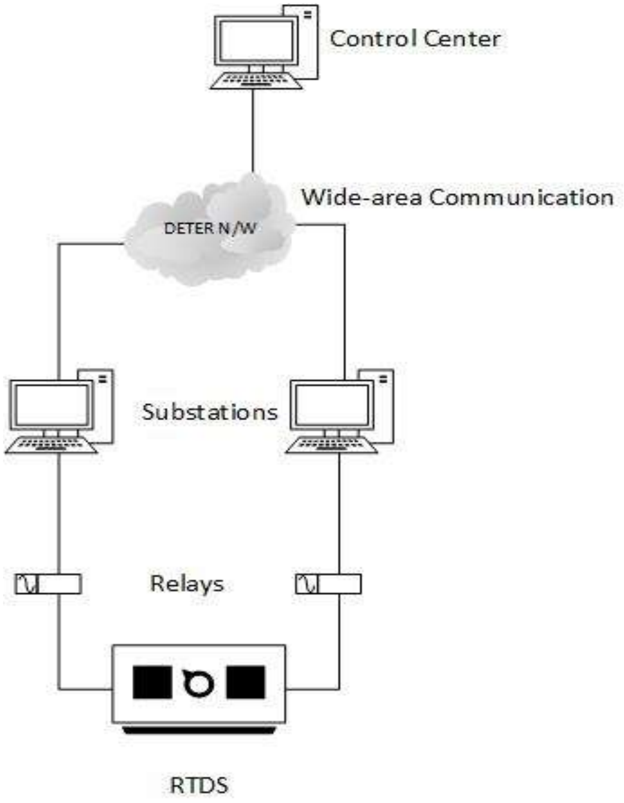


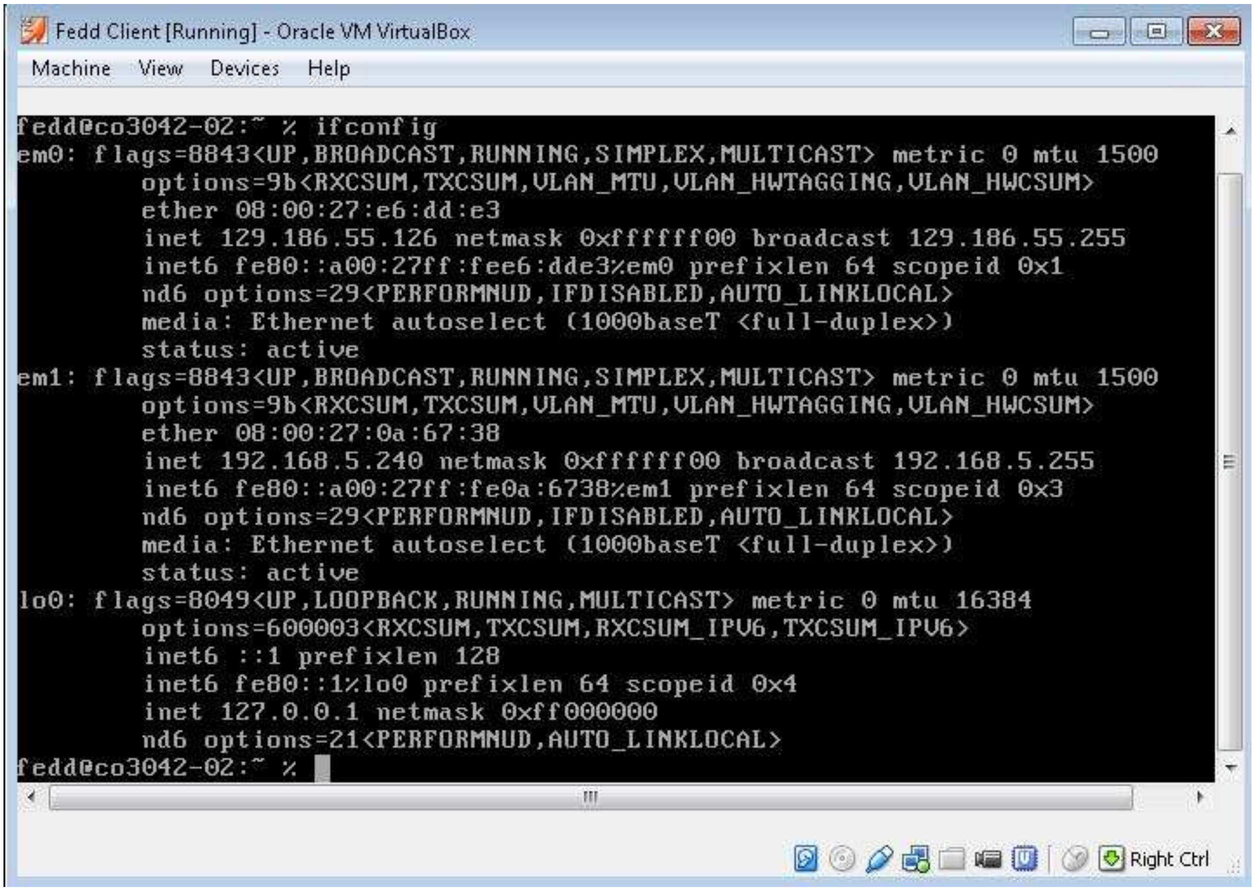
Figure 9 DETER as a wide-area networking fabric

Fig. 9 represents that the DETER network lies between the Control Center and Substation communications, channeling the wide-area traffic between them, to emulate the real-world grid control scenario. The diagram is meant to convey that once control center sends a command to one of the substations, the traffic is routed to a node within DETER and routed through a complex network of the DETER experiment before returning back to PowerCyber and reaching the substation. This adds real-time latency of wide-area communication to the PowerCyber environment.

DETER Federation Architecture (DFA) and Fedd Client

The communication between the two testbeds was setup using the DETER Federation Architecture (DFA). Fedd Clients were used on either end to route traffic between the testbed components.

The Fedd Client machines run Free BSD 9 OS. Each of them has two Network Interface Cards (NIC), one card to connect to each other through the Internet and one card to connect to the components of their respective environments.


Fedd Client [Running] - Oracle VM VirtualBox
Machine View Devices Help
Right Ctrl

```
fedd@co3042-02:~ % ifconfig
em0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 08:00:27:e6:dd:e3
        inet 129.186.55.126 netmask 0xffffff00 broadcast 129.186.55.255
        inet6 fe80::a00:27ff:fee6:dde3%em0 prefixlen 64 scopeid 0x1
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
em1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 08:00:27:0a:67:38
        inet 192.168.5.240 netmask 0xffffff00 broadcast 192.168.5.255
        inet6 fe80::a00:27ff:fe0a:6738%em1 prefixlen 64 scopeid 0x3
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
        options=600003<RXCSUM,TXCSUM,RXCSUM_IPV6,TXCSUM_IPV6>
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x4
        inet 127.0.0.1 netmask 0xff000000
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
fedd@co3042-02:~ %
```

Figure 10 Fedd Client Machine

Each Fedd Client is basically part of both the internet and their respective testbeds. They talk to each other through the internet and set up a tunnel for the traffic flowing between the two testbeds. Traffic also has to be statically routed between the testbeds so the devices know where to send response to commands or requests. For example, the PowerCyber LAN is on one subnet and the DETER experiment LAN is on another subnet. When a machine in PowerCyber communicates with the relay asking for its status, the relay knows exactly what to do, but if the request has to go inside the DETER environment first and then get routed back to PowerCyber, then the communication has to be routed accordingly. So all traffic must be statically routed to the Fedd Client and then routed from the Fedd Client on the other end, and then return back through the Fedd Client in DeterLab to the Fedd Client in PowerCyber.

Milestone 2

This part involved getting the SCADA components of the PowerCyber testbed, i.e., the Control Center and Substations, to run within DETER and route the SCADA communication through the Fedd Client to talk to the physical system present in PowerCyber.

Virtual PowerCyber inside DETER

The control center and substations of PowerCyber run industry standard software that enables the SCADA environment. In order to get the same environment running inside DeterLab, images of these machines were created and packed as virtual machines. As was previously mentioned, DeterLab has the capability to run custom OSes or images of custom OSes on its nodes. So these virtual machines were made to boot on three DeterLab nodes within the experiment.

The architecture of the setup after achieving this milestone is as under –

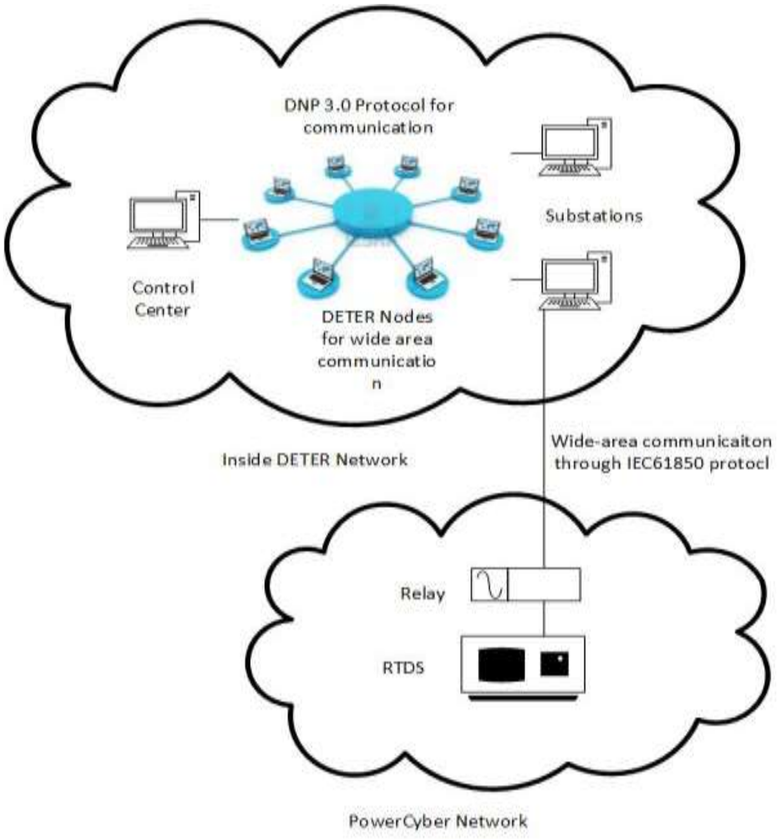

DNP 3.0 Protocol for communication
Substations
Control Center
DETER Nodes for wide area communicatio n
Inside DETER Network
Wide-area communicaiton through IEC61850 protocl
Relay
RTDS
PowerCyber Network

Figure 11 PowerCyber within DETER

The Fig.11 describes the concept of running a SCADA environment similar to PowerCyber's within DeterLab. Since the control center and substation machines within the DeterLab experiments are images of the actual machines within PowerCyber, they have to be reconfigured to suit the DeterLab environment in order to be functional. Most of these changes are IP-based and require changes in the IP address and the way the traffic is routed within the network.

The final architecture of the Federated Testbed is as shown below –

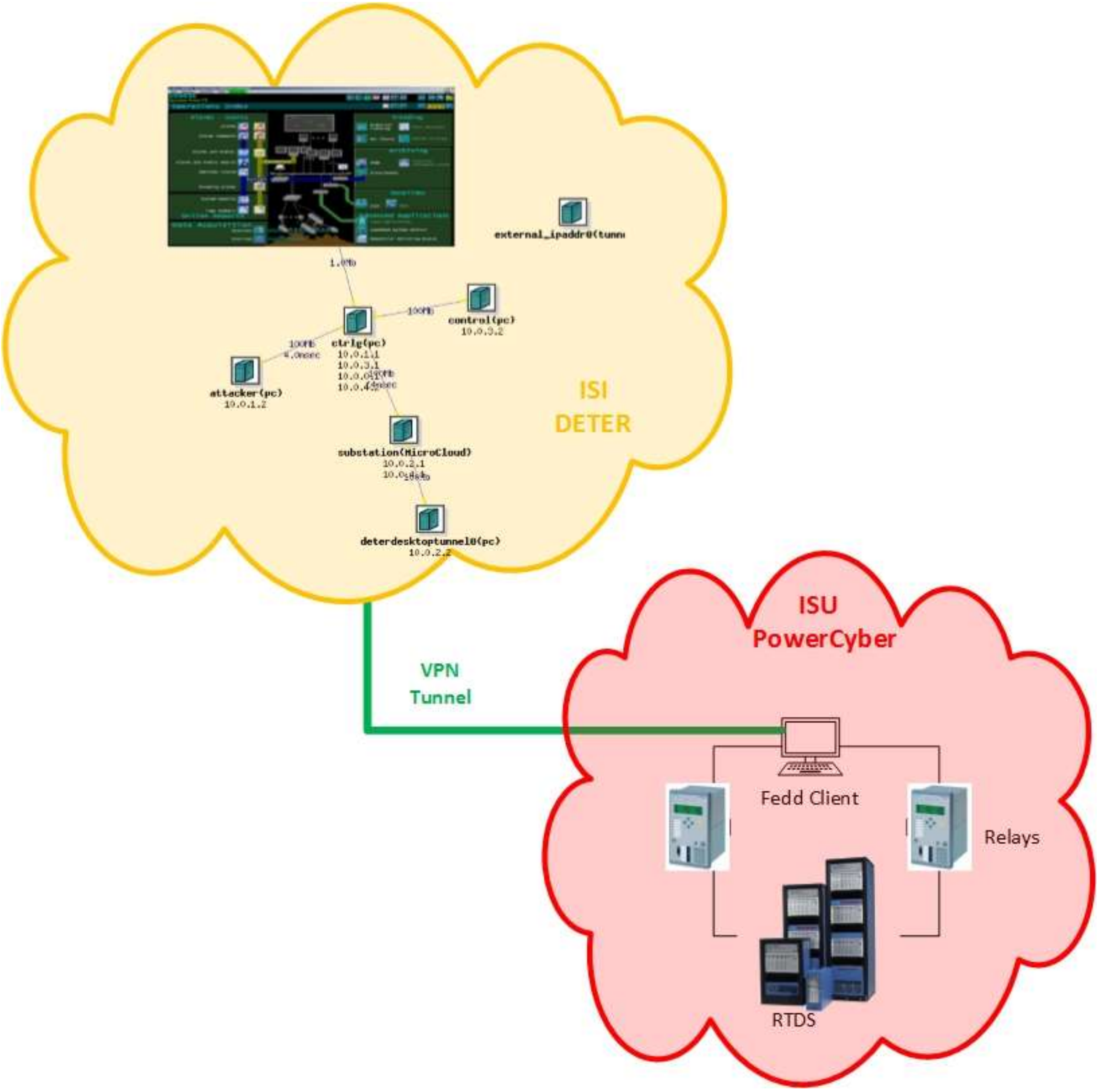


Figure 12 Architecture of Federated Testbed

Milestone 3

This is the most important part of the federation. No federation is complete without the ability to do meaningful experiments to show the new capabilities of the federated testbed.

Once the SCADA environment is setup inside DeterLab and is able to talk to the physical system in PowerCyber, i.e., the relays and RTDS, an attack-defense scenario was designed to showcase the functionality of the federated testbed. The architecture of this experiment looks as under –

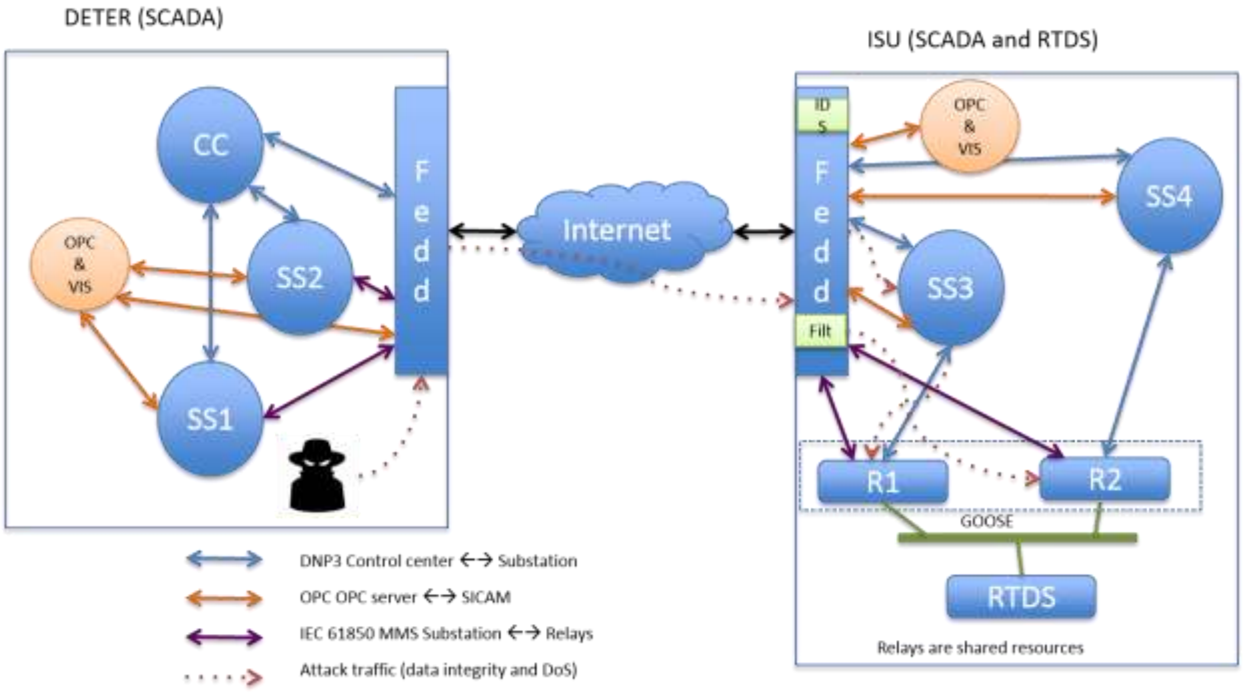

DETER (SCADA)
CC
OPC & VIS
SS2
SS1
Fedd
Internet
ISU (SCADA and RTDS)
IDS
OPC & VIS
Fedd
Filt
SS3
SS4
R1
R2
GOOSE
RTDS
Relays are shared resources
DNP3 Control center ←→ Substation
OPC OPC server ←→ SICAM
IEC 61850 MMS Substation ←→ Relays
Attack traffic (data integrity and DoS)

Figure 13 Experiment Architecture

In the Fig. 13 above, the left part indicates the DETER environment and the right part indicates the ISU PowerCyber environment. As was accomplished in the previous milestones of the federation, PowerCyber Control Center and Substations run as nodes within the DeterLab experiment. The substations within PowerCyber are also interfaced with the control center VM running within DeterLab. As the Fig. 13 depicts, the DETER environment is running the SCADA system of the smart grid and PowerCyber is running a combination of the SCADA system and the physical system, since some of the substations in are still part of the SCADA environment.

All communication between the two environments runs through the Fedd Clients on either end. Each of the substations within the two environments is interfaced to the relays R1 and R2, which are present in PowerCyber. The RTDS simulates the power system to be used and the relays R1 and R2 are interfaced to the power system.

Attacks are generated on the federated testbed to destabilize the power system and defense mechanisms (Intrusion Detection System and Traffic Filtering) are employed to stop the system from destabilizing, in the case of likely attacks.

The scenario also contains a visualization engine running on a Google Earth frontend, to showcase the events happening in the federated testbed, as they occur. This visualization engine is useful in depicting the federated testbed as a single entity where experiments can be carried out.

CHAPTER 4

EXPERIMENTATION

The experiment scenario chosen to depict the functionality of a federated testbed includes a power system, an attack scenario and a defense mechanism to nullify the effects of the attacks generated on the power system. It is a classic example of a cyber-physical security experiment on a federated testbed.

Physical System

The physical system of the experiment is contained within PowerCyber and consists of an RTDS, which spawns the power system, and two relays which are integrated as part of the power system. The power system is protected by a wide-area protection scheme to keep it stable in the event of an anomaly.

Power System

The power system spawned by the RTDS is the WECC 9-bus system shown in the diagram below –

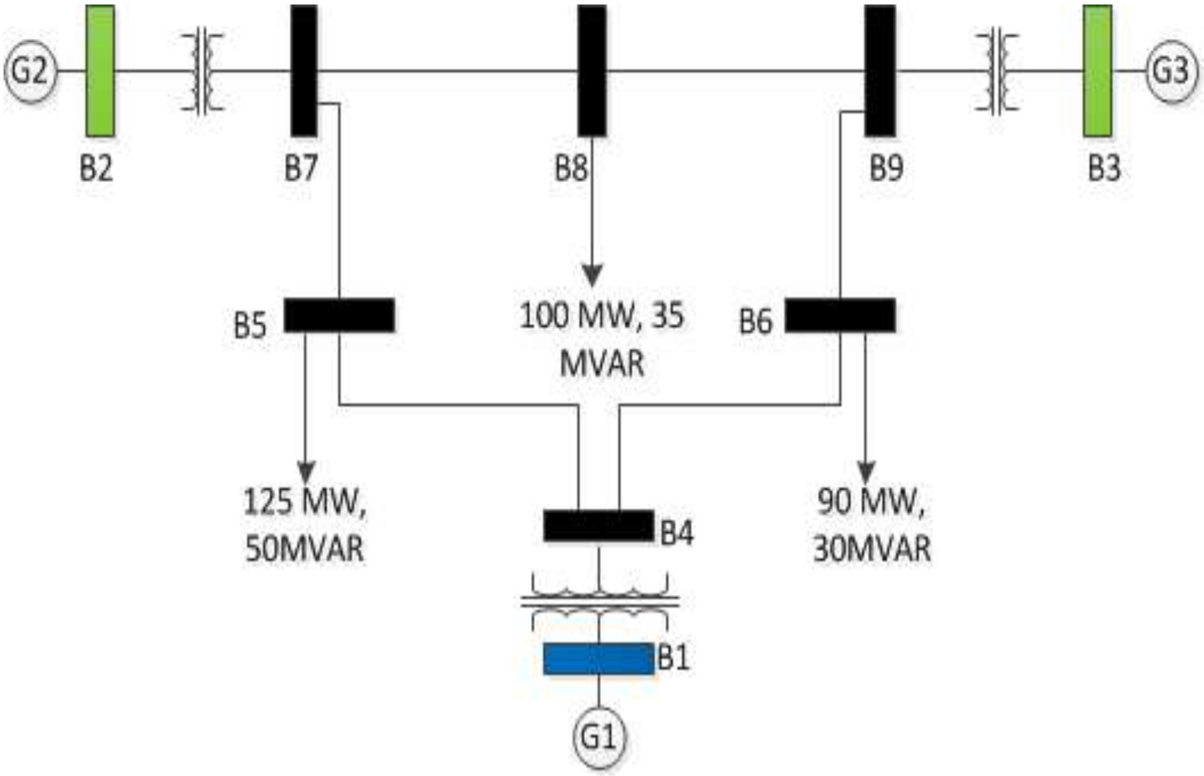


Figure 14 Physical System – WECC 9-bus model [1]

The system consists of three generators, G1, G2 and G3, supplying loads at buses B5, B6 and B8. Virtual relays are placed in the system as breakers with the logic that they trip out whenever the transmission line they control get overloaded. The overload conditions can be defined within the RTDS. The physical relays R1 and R2 are integrated as part of the system – Relay R1 acts as the breaker for the transmission line between buses B5 and B7 and Relay R2 is present as part of the protection scheme that is employed by the power system.

Protection Scheme

In real conditions, multiple events of anomaly may occur to destabilize a power system. In order to make the system resilient, it is necessary to protect the system from destabilizing due to such events. The power system in this scenario is protected by a wide-area protection scheme called the Recommended Action Scheme (RAS) [9]. The relay R2 is present in the power system as the RAS Controller which performs the function of avoiding overload during events of anomaly.

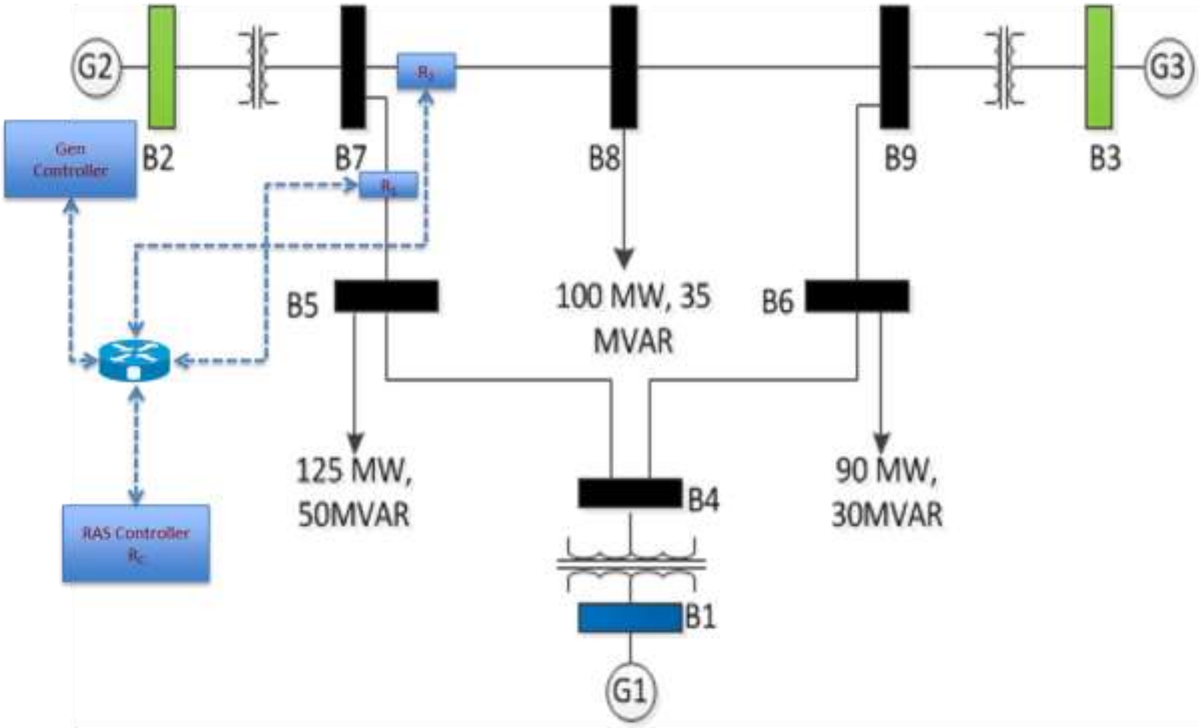


Figure 15 9-bus model with RAS Controller

Consider Fig. 15. The Relay R1 is the breaker for the transmission line between B5 and B7. If an event, such a cyber-attack or any natural cause, causes the relay to trip, then the line between B5 and B7 is removed. As a result, the line between buses B7 and B8 gets overloaded due to the same amount of generation by generator G2. As per the protection scheme, when an event such as this occurs, the RAS controller, i.e., Relay R2 sends a GOOSE message to the generator G2 to ramp down its generation. When the generator receives this message, it ramps down the generation accordingly in order to keep the transmission below the threshold of the transmission line and the system stabilizes.

Attack Scenario

Considering the protection scheme that the power system possesses, the attack scenario should be such that the in spite of the protection scheme, it should be able to destabilize the system. There are two steps involved in the attack scenario – tripping the relay R1 and performing a DOS attack on the relay R2.

Data Integrity Attack

The data integrity attack is intended to trip the relay by fabricating a packet that instructs the relay to trip. The relay does not require any sort of authentication when the trip command is sent to it, so it is vulnerable to this kind of attack.

When this attack targets relay R1, the relay, which is the breaker for the transmission line between buses B5 and B7, will trip out and cause that line to be out of the power system.

Denial of Service (DOS) Attack

According to the wide-area protection scheme of the power system, when a line gets tripped out, the RAS Controller sends a message to the generator that feeds that line, to ramp down its generation. However, if the RAS Controller, i.e., relay R2, is subject to a DOS attack, it will be unresponsive on the network and will not be able to communicate the GOOSE messages, thereby causing the command to never reach the generator.

Coordinated Attack Vector

The attack scenario that is being implemented is what can be a called a “Coordinated Attack Vector”, where two parts of the system are simultaneously hit and a third event occurs in the system causing what is known as a “Cascaded Outage” in the power system.

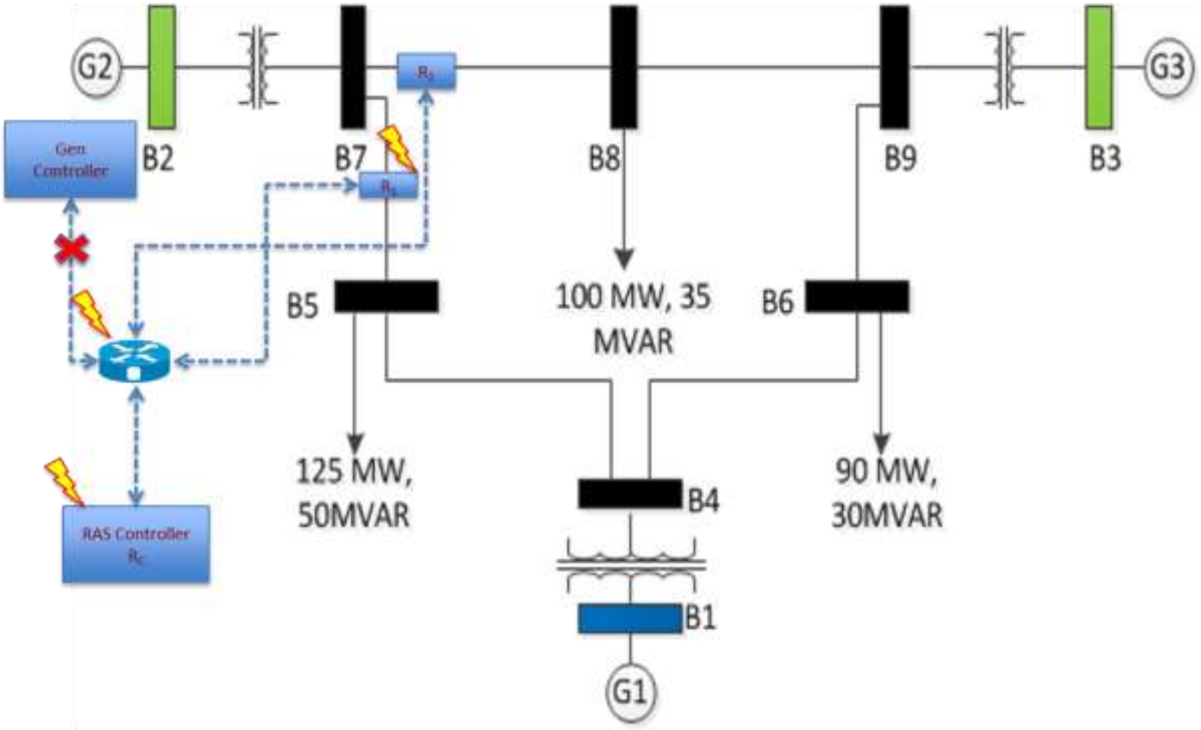


Figure 16 Attacking the Protection Scheme

The attack scenario is started off with the data integrity attack, which trips relay R1. This causes the transmission line between buses B5 and B7 to be disconnected. Simultaneously, the relay R2 is subjected to a DOS attack so it cannot communicate to the generator G2 to ramp down its generation and failing it from performing its role as the RAS Controller. As a consequence of both these attacks, the transmission line between buses B5 and B7 is disconnected from the system and the generator G2 is still generating at its original capacity. This causes the line between buses B7 and B8 to be under overload and once the overload extends a certain period of time, the breaker logic in the transmission line causes the line to trip out. The final consequence of this attack is that the generator G2 is isolated from the power system and there is a discrepancy in the frequency of operation of the power system.

Defense Scenario

The defense scenario is crafted to be a cyber-defense scenario and deals with the cyber-attacks that take place on the system. The environment is equipped with what is called as “Perimeter Defense” mechanism, which when deployed, filters attack traffic before entering the PowerCyber environment.

The Perimeter Defense mechanism is equipped with an Intrusion Detection System (IDS) which sets rules for whitelisted communication and a Traffic Filter which filters high amounts of traffic heading towards a single destination, which is what, happens during a DOS attack.

The Perimeter Defense mechanism can successfully stall the Coordinated Attack Vector that was discussed previously. However, the IDS rules for whitelisted communication can be easily bypassed by mechanisms like IP spoofing. Even in that case, the Traffic Filter will ensure that the DOS traffic is blocked before entering the PowerCyber environment, in which case, even if the data integrity attack goes through, the RAS Controller will remain operational and the power system remains stable.

As Fig. 17 shows, the defense mechanism is protecting the power system at the points where it is vulnerable and prevents any cases of outage or cascaded outage and succeeds in keeping the power system stable under all conditions.

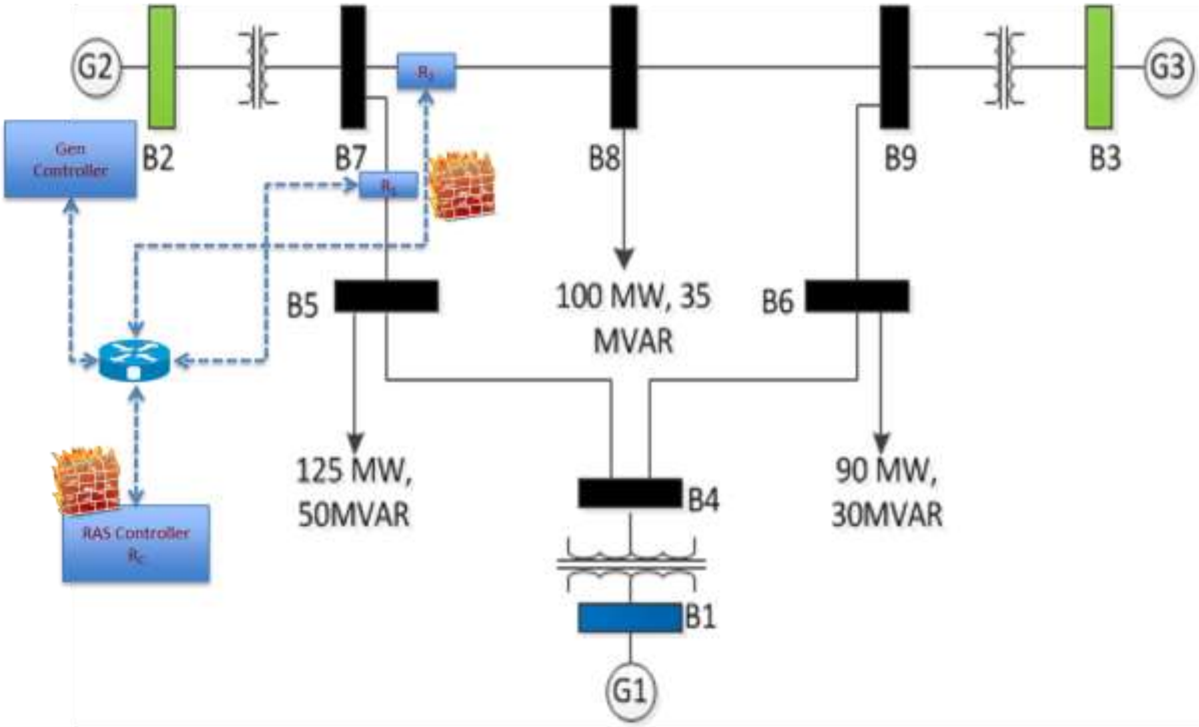


Figure 17 Defending the RAS Controller

Visualization Engine

In a federated testbed, a lot of the events, while occurring concurrently, are not easy to portray. The visualization engine helps in displaying the events in the federated testbed in a coherent fashion.

Every event that occurs within the federated testbed has a visual feedback on the visualization engine.

Frontend

The frontend was made on the Google Earth API. A model of the 9-bus system is mapped on the state of Iowa with realistic locations of generators and substations. The entire frontend was designed using Keyhole Markup Language (KML) [10]. The KML file consists of geographic information of all objects that are mapped onto the UI. The components on the UI appear and disappear according to the events occurring on the Federated Testbed. For example, when the DOS attack initiates, a visual attack icon appears and the component being attacked turns into red color indicating that it is unresponsive in the system. Transmission lines, generators and breakers change color to indicate status. The color coding for the transmission lines is setup as – green for normal operation, yellow for overload and red for line-out. This color convention applies to most components of the UI.

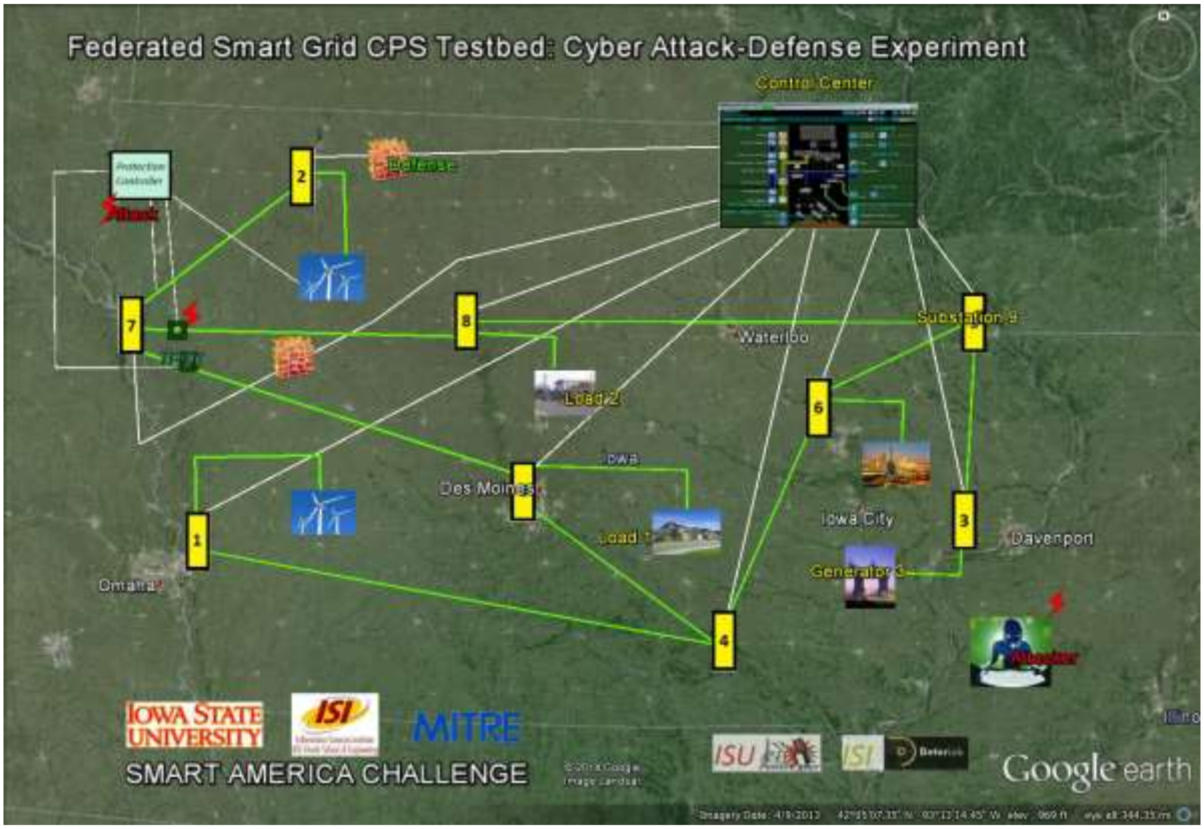


Figure 18 Frontend UI on Google Earth

Backend

The backend architecture of the visualization is shown in Fig.19.

The backend consists of two servers constantly polling for information and refreshing the KML file that displays the components in Google Earth. A python script continuously runs in the background, obtaining the changes in the state of the testbed components and writes them to a KML file at regular intervals, which is then loaded into Google Earth, so that the UI reflects the changes in the environment.

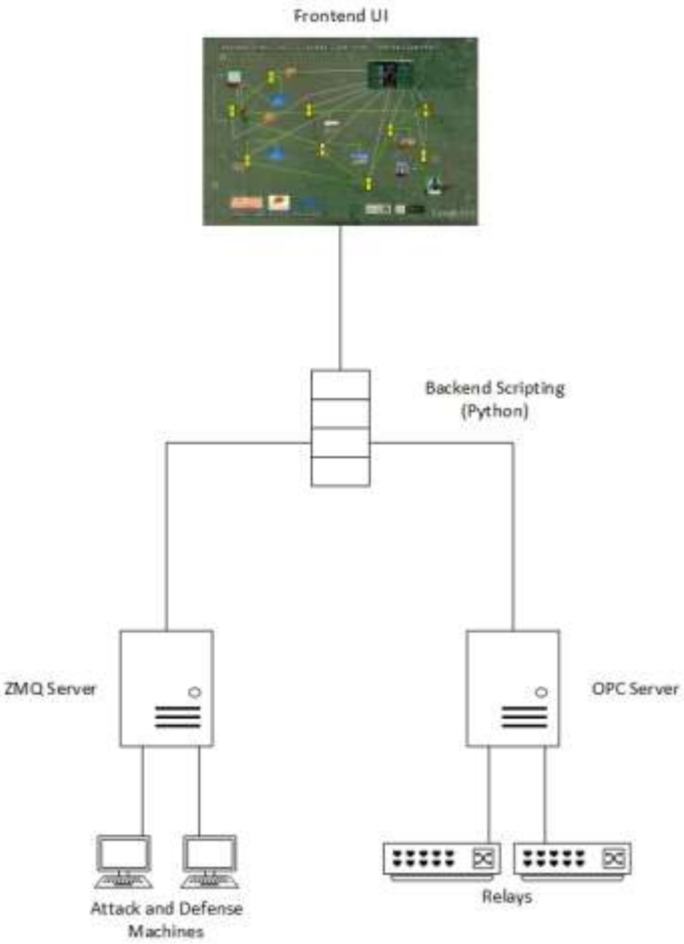


Figure 19 Visualization Architecture

OPC Server

The OLE Process Control (OPC) [11] server obtains the statuses of the relays inside PowerCyber constantly. When there is a change in the status of any of the relays (trip, close), the backend script, which is constantly polling the server, notices the change and writes to the KML file accordingly. So when a relay is tripped, the corresponding transmission line for which it is a breaker will turn red indicating that the line is now open.

ZMQ Server

The ZMQ server is used to monitor the attack and defense machines in the DETER environment so that whenever an attack is initiated or the defense mechanism is turned on, the event will be visible on the front end. What the ZMQ server does is, when an attack is initiated, it receives a message indicating the start of the attack and passes it on to the backend script, which then writes to the KML file to turn on the visibility of the attack objects along with the necessary color coding to indicate the initiation of the attack.

Demonstration

The use-case scenario described above, along with the Visualization Engine, was demonstrated on June 11th, 2014 at the Smart America Expo [12] held at the Washington DC Convention Center in Washington DC. The Smart America Challenge was a White House Presidential Innovation Fellow project to combine research related to Cyber-Physical Systems from different sectors, such as Smart Manufacturing, Healthcare, Smart Energy, Intelligent Transportation and Disaster Response, and to portray the benefits they serve to the US Economy and to the daily lives of American citizens.

This Federation was achieved and demonstrated as part of the “Smart Energy CPS” team at the Smart America Expo. Members of the Smart Energy CPS team included MITRE Corporation, National Instruments, NREL, North Carolina State University, Penn State University, Scitor Corporation, University of North Carolina (Chapel Hill) and the Information Sciences Institute at University of Southern California.

CHAPTER 5

EXPERIMENTAL EVALUATION

Apart from showcasing the functionality of the Federated Testbed, an evaluation was performed to figure out how a DOS attack from the wide-area network would propagate and its impact on the Federated Testbed and the relay.

DOS Attack Evaluation

The DOS attack that was used for the evaluation was a UDP flood originating from the DETER environment and targeting the relay in PowerCyber. The attack was done with 80 byte packets and the rate of the flood was a parameter that could be changed. Each attack is aimed at bringing down the wide-area protection scheme of the power system by targeting the relay which is the RAS controller.

For each case, the DOS attack bombarded the relay for 30 seconds and for each rate, the attack was repeated 10 times.

The Fig.20 below presents a comparison of the bandwidth required to fail the protection scheme when the DOS attack is on PowerCyber's local network and when it originates from DeterLab on the Federated Testbed.

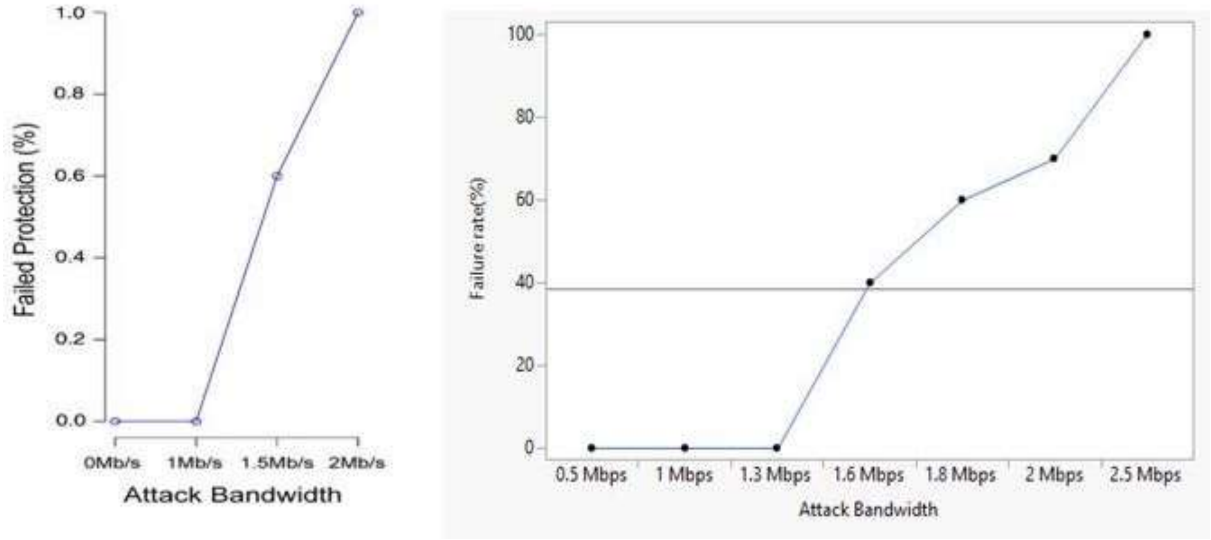


Figure 20 Comparison of local DOS attack and wide-area DOS attack. (Left) DOS analysis within PowerCyber [1] (Right) DOS analysis on the Federated Testbed

What is interesting to note here is that previous results showed that the relay shows a 100% failure rate when subjected to an attack bandwidth greater than two Mbps. However, those attacks were originated from within the local network of PowerCyber. These results show that a considerable amount of attack bandwidth is lost in the traversal over the wide-area network and hence, more bandwidth is required to fail the protection scheme in order to overcome the loss of packets.

Another point of concern is that the attack bandwidth must not be very high because traffic traverses between the environments through the tunnel between the Fedd Clients. If the attack traffic is very high, there were occasions where the Fedd Client would become unresponsive and stall all communication between the two testbeds.

The design of the DETER experiment is also important in terms of the location of the attack machine. It must have as less hops to the Fedd Client as possible so that the flood traffic does not go through a large number of nodes and flood the experiment itself. In the Federated Testbed, the attack machine is located one hop away from the Fedd Client on the DETER end.

Latency Evaluation

For cyber-physical systems, the latency in the network is a very important since power system components have a very fast response and the network should support the same in order to conduct meaningful experiments.

In the PowerCyber local network, the communication time between the control center, substation, RTDS and relays is always lesser than 1ms, which goes well with the fact that the response time of RTDS and relays is in the order of micro seconds. However, when it comes to the Federated Testbed, the latency becomes a very important factor since the communication has to go through the wide-area network which causes a much larger delay in the communication as compared to the local area communication.

Table 1 Communication Latencies within PowerCyber and on the Federated Testbed

Communication Components	Latency within PowerCyber	Latency in Federated Testbed
Control Center to Substation	<1ms	28.8ms
Substation to Relay	<1ms	66ms
Relay to RTDS	<1ms	<1ms

Since DETER nodes are laid out across a huge network of devices, the nodes within a single experiment may show a considerable amount of latency between each other, as in this case. In spite of the Control Center and the Substation being on the same network, the sheer complexity of the DETER network gives a communication latency of 28.8 ms. The substation to relay communication shows the amount of time it takes for traffic to reach from the DETER network to PowerCyber through the Fedd Clients and the wide-area network. The latency in the case of this experiment is not a huge concern because the most important part of the experiment is the protection scheme of the power system and the communication between the RTDS and the relay takes place in the local network of PowerCyber.

Control center-based applications such as Automatic Gain Control, can be employed in the Federated Testbed since the time constraints in these applications are not very tight and the latency of the Federated Testbed is still within the accepted range.

The latency, however, limits the kind of experiments that can be performed on the physical system of the Federated Testbed. For example, with this amount of latency, we cannot have a physical system that is spread across between two testbeds and form a Federated Testbed since a communication latency of greater than 50ms is not acceptable for employing wide-area protection schemes and state estimation based applications.

CHAPTER 6

CONCLUSION

Future Work

- The most challenging task ahead is to have a distributed power system on a Federated Testbed, supported by a suitable high-speed network. This means that multiple power system testbeds can spawn large-scale power systems and cyber testbeds can be the networking fabric, thus giving cyber-physical experimentation a very realistic platform.
- The federation paves way to large-scale cyber-physical security experiments. The huge cyber network of DeterLab can accommodate 100s of substations within its environment. This gives the scope for interfacing with large-scale power systems such as a 100-bus system, in place of the current 9-bus system, for experimental purposes.
- Create realistic experiments in the smart grid environment, large-scale protection schemes, and large-scale cyber-attack scenarios and provide the real platform to understand what it is like to protect a real smart-grid environment.

Conclusions

- Testbed federation is a growing buzzword in today’s research community, since it offers a large-scale experimentation platform to researchers and also extends functionality of current testbeds.
- Currently, there are very few cyber-physical experimentation testbeds and testbed federation could give rise to many large-scale cyber-physical environments through

sharing of resources. This work introduced one such environment and its experimental functionality.

- Both PowerCyber and DeterLab are well known testbeds in the field of cyber-physical experimentation and cyber-security experimentation, but this federation throws to light how their functionality can be taken to the next level.
- This federation gives scope for large scale cyber-physical experimentation in the future. The experimental analysis performed shows how experimentation is different in the case of a Federated Testbed as compared to the standalone testbed.
- It also shed light on some of the experiments which are feasible and those which are not feasible in this kind of an environment.
- The future prospects of the federation hold true for any federated cyber-physical testbed and not just PowerCyber and DeterLab.

REFERENCES

[1] NISTIR 7628: Guidelines to Smart Grid Cyber Security, NISTIR 7628, 2010.

[2] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu, "Cyber-Physical Security Testbeds: Architecture, Application, and Evaluation for Smart Grid, " IEEE Trans. on Smart Grid, vol.4 no.2, pp. 847-855, June 2013

[3] J. Mirkovic, T. V. Benzel, T. Faber, R. Braden, J. T. Wroclawski, and S. Schwab, "The DETER project: Advancing the science of cyber security experimentation and test," in Technologies for Homeland Security (HST), 2010 IEEE International Conference on. IEEE, 2010, pp. 1-7

[4] Terry Benzel, John Wroclawski, “The DETER Project: Towards Structural Advances in Experimental Cybersecurity Research and Evaluation”, Journal of Information Processing, Vol.20 No.4, pp. 824-832 (October 2012)

[5] Sebastian Wahle, Thomas Magedanz, “Network Domain Federation - An Architectural View on How to Federate Testbeds”, FIREworks Strategy Workshop, FIREweek September 2008

[6] Robert Ricci, Gary Wong, Leigh Stoller, and Jonathon Duerig, “An Architecture for International Federation of Network Testbeds”, IEICE Transactions on Communications E96-B (1), January 2013

[7] Slice-Based Federation Architecture, v 2.0. L. Peterson, Robert Ricci, Aaron Falk, Jeff Chase, July 2010 <http://groups.geni.net/geni/attachment/wiki/SliceFedArch/SFA2.0.pdf>

[8] Ted Faber, John Wroclawski, Kevin Lahey, “A DETER federation architecture, Proceedings of the DETER Community Workshop on Cyber Security Experimentation and Test” on DETER Community Workshop on Cyber Security Experimentation and Test, 2007, p.11-11, August 06-07, 2007, Boston, MA

[9] WECC remedial action scheme catalog summary, 2008

[10] Wilson, T., 2008, “OGC KML 2.2.0”, Document #07-147r2, Open Geospatial Consortium

[11] OPC Foundation, “*OPC Data Access Custom Interface Standard Version 3.00”*, March 2003 http://www.opcfoundation.org/DownloadFile.aspx?CM=3&RI=67&CN=KEY&CI=283&CU=12

[12] Smart America Expo, http://www.smartamerica.org/

[13] A. Hahn, G. Manimaran, S. Sridhar, B. Kregel, M. Higdon, R. Adnan, and J. Fitzpatrick, "Development of the PowerCyber SCADA Cyber Security Testbed," in Proc. Cyber Security and Information Intelligence Research (CSIIR) Workshop, Oak Ridge National Laboratory (ORNL), 4 pages, Apr. 2010