Proceedings of the 2017 Winter Simulation Conference
W. K. V. Chan, A. D'Ambrogio, G. Zacharewicz, N. Mustafee, G. Wainer, and E. Page, eds.

A CONCEPTURAL FRAMEWORK TO FEDERATE TESTBEDS FOR CYBERSECURITY

Lavanya Ramapantulu
Yong Meng Teo
Ee-Chien Chang

Department of Computer Science
National University of Singapore
SINGAPORE

ABSTRACT

The transition to a "smart city" necessitates an increase in interdependencies between critical infrastructures and information technologies. Moreover, such interdependencies are across multiple domains. However, these interdependencies expose critical infrastructures to cybersecurtiy threats. Furthermore, the availability of domain-specific simulators everywhere motivates the need for federation of interoperable cybersecurity and cyberphysical testbeds to validate cybersecurity threat resiliency. This paper presents some key issues and challenges in accomplishing such a federation of testbeds. While there are multiple modeling and simulation approaches in specific domains, none of these works address the challenges of federating across multiple domains such as federation between cyberphysical testbed and cybersecurity testbed to enable validation of cybersecurity resilience. We outline a reference architecture, DEFT (feDerate tEstbeds For cybersecuriTy) with design considerations that stem from the key issues highlighted.

1 INTRODUCTION

Essential systems or assets that are part of a nation's economy, security, and health are termed as critical infrastructure (Görbil and Gelenbe 2009). Critical infrastructures are relying heavily on information technology and increasingly becoming interdependent on each other. This interdependency among critical infrastructures make them more vulnerable to cybersecurity attacks and threats. Thus, it is becoming increasingly important to study and model such system of systems and their interdependency to increase their cybersecurity resiliency (Rome et al. 2014, Tolone et al. 2008, Martí et al. 2008, Bagheri and Ghorbani 2006). The critical infrastructures are typically modeled using individual cyberphysical testbeds and these stand-alone models do not suffice to validate these infrastructures across all types of attacks.

Concurrently, there is an availability of a wide range of cybersecurity testbeds to conduct security experimentation and to improve cybersecurity resilience (Benzel 2011, Sklower and Joseph 2007). While the National Cybersecurity Lab testbed (NCL 2017) at Singapore is made available for cybersecurity experimentation, a cross-domain federation of this testbed with cyberphysical testbeds representing critical infrastructure is a challenge. The availability of such cybersecurity testbeds coupled with the necessity to address cybersecurity challenges in critical infrastructures introduces new opportunities to create a "unified cybersecurity testbed" or federation. Such a unified testbed federation consisting of heterogeneous federates representing different systems (cyberphysical or simulators) addresses the need for modeling interdependencies between critical infrastructure system components.

Figure 1 shows a "smart city" with four critical infrastructure systems, namely a water plant, hospital, power distribution unit and telecommunication services (Formicola et al. 2014). The inter-dependencies among critical infrastructures are shown with arrows from the source of the service. A single denial of service attack on one of these infrastructures is bound to impact disruptions on others and this can lead to cascading effects of multiple failures (Di Pietro et al. 2015). Such inter-dependencies translate to a

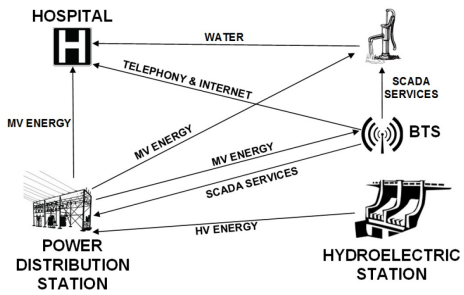


Figure 1: Interdependency of Critical Infrastructure (Di Pietro et al. 2015)

"weak link" that can be easily exploited by both external and insider cybersecurity threats. Additionally, a breakdown or malfunction in any one infrastructure can cause disruption in other infrastructure services thus causing havoc in daily operations. Hence, modeling these inter-dependencies is crucial to understand cascading effects of failure (Jenkins and Burmester 2015, Howser 2015).

A federation consists of heterogeneous cyberphysical systems called federates, wherein each of these individual federates represent different critical infrastructure systems belonging to different domains. Thus such a cross-domain federation models and simulates a "smart city". From a cybersecurity perspective, such a modeling and simulation approach using cross-domain federation is important to study (i) cybersecurity training and attack management, (ii) cybersecurity resilience mechanisms and (iii) evaluating past breakdowns due to cybersecurity attacks and avoiding them. However, a cross-domain federation constituting of various systems with each of them having disparate interfaces and objectives gives rise to many interoperability issues that need addressing, especially with executing multiple federates each having its own representation model. This paper addresses some of these issues with the following outline.

In Section 2, we highlight key issues with respect to cross-domain federation of critical infrastructures and cybersecurity testbeds. Section 3 reviews the current state-of-the-art on federated modelling and simulation for critical infrastructures using four examples covering different application domains, (i) High-Level Architecture (HLA) standard for military domain simulations, (ii) DIESIS framework with respect to interoperability among other critical infrastructure testbeds, (iii) DeterLab a cybersecurity testbed and (iv) GENI architecture for distributed networks. In Section 4, we propose a layered architecture, DEFT (feDerate tEstbeds For cybersecuriTy) that addresses the research gaps for cross-domain federation between heterogeneous federates and we present the conclusion in Section 5.

2 KEY ISSUES AND CHALLENGES

While federated modeling and simulation of critical infrastructures is very important to gain useful insights on dynamic effects within the interconnected complex system or to understand cascading effects of failures, there are a multitude of challenges that need addressing (Nieuwenhuijs et al. 2008, Setola et al. 2008). Firstly, a federation requires multiple individual simulators (dynamic) or models (static) of the underlying components that constitute individual federates. Secondly, these multiple infrastructures are quite domain-specific and modeling or simulating these heterogeneous behaviours as a single integrated environment is non-trivial. Thirdly, the inter-dependencies to be modeled are not only among these heterogeneous federates but also between the external environment and each of these federates necessitating the need for clear interfaces. Thus to achieve a federation goal key implementation issues that need addressing include: (i) exchange of data across domains pertaining to individual federates, (ii) syntactic interoperability among these heterogeneous federates, (iii) semantic interoperability across heterogeneous domains, (iv) global time management and (v) security and privacy aspects of the federation. In this section, we discuss in detail some of these key issues with respect to federation among cross-domain testbeds.

2.1 Cross-Domain Interoperability

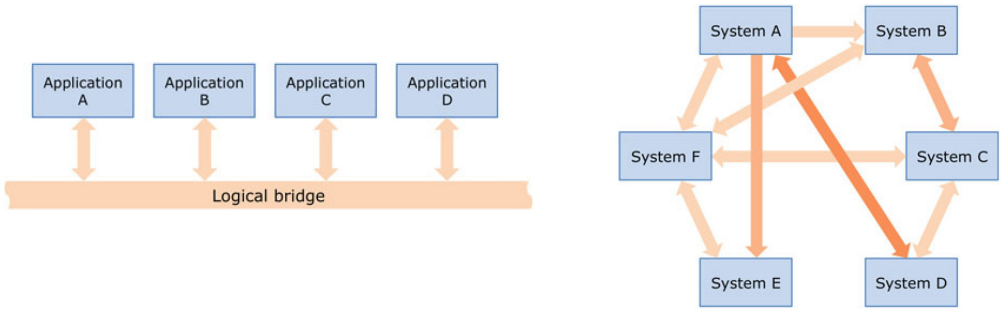
A cross-domain federation constitutes of individual federates wherein each federate is a model or simulation that is applicable to a specific domain. An example of cross-domain federation is that of a cyber-security testbed with a wireless sensor testbed, where the programming interfaces between the participating federates

are designed separately for each domain and it is difficult to standardize them across all domains. For such cases of cross-domain federation to be interoperable, a federation bridge may be employed. Such a bridge is expected to provide a mechanism for both syntactic and semantic translation across each of the domain-specific federates. There are three considerations for cross-domain federation, access, transfer and multilevel. While access refers to federation users able to connect to the individual federates, transfer refers to exchange of information between the users and the federates and among federates. The multilevel aspect refers to the different levels of authorizations and permissions needed for a successful federation between users and federates. Traditionally federation consisted of federates from the same domain and hence the multi-level security policies and access controls were similar contextually. But in cross-domain federation, multi-level authorization and resource sharing is a key challenge that needs to be addressed.

2.2 Syntactic Interoperability

For effective interoperability among federates, there should be both a technical or **syntactic** connection as well as a **semantic** connection. The syntactic connection refers to the ability of federates to exchange information among them using a common language, with a common data structure and syntax for the underlying data being exchanged within that data structure. On the other hand, there is a need for common definitions on the context of the data being exchanged between federates which refers to the semantic connection.

Figures 2(a) and 2(b) illustrate two topologies of connecting simulators, namely, central coupling



(a) Centrally Coupled Architecture (b) Lateral Coupled Architecture

Figure 2: Topology Architectures for Connecting Simulators (Rome et al. 2014)

and lateral coupling respectively. Examples of central coupling topology architecture include HLA (IEEE 2010b, IEEE 2010a), OpenMI (Gregersen et al. 2007). This topology is particularly useful when all the participating federates adhere to a standard format for exchanging data and the central coupling logical bridge is implemented as middleware based on this standardized format. Such a topology supports easy integration of new federates as the middleware is ready and the new federate should just implement the interface with the logical bridge. While it is simple to use, due to the possibility of all federates not able to implement a common interface, it is not practical to use. In addition, the central coupling topology does not address the time synchronization challenge discussed in Section 2.4 as it requires a common central bridge among all federates and for heterogeneous federations with models and simulators, the time scales cannot be matched.

To overcome this challenge of time-synchronization among heterogeneous federates in central coupling, a pairwise coupling is proposed. In contrast to central coupling a distributed and scalable peer-to-peer approach involves lateral coupling (Tofani et al. 2010), where only two or few federates exchange information as shown in Figure 2(b). A disadvantage of this lateral coupling is the development of multiple mini-federate managers adhering to the many different interoperable peer-to-peer links, and is less tenable to the addition of new federates. To overcome this, a hybrid approach could possibly use pair-wise coupling between two federates, and these two federates could in turn consist of many federates communicating via central coupling.

2.3 Semantic Interoperability

While syntactic interoperability can be achieved by using a standardized protocol or interfacing rules to communicate among federates, semantic interoperability is more challenging especially in a cross-domain and heterogeneous federation. Interoperability defined as per the Third Generation Partnership Project (3GPP) is: *"the ability of two or more systems or components to exchange data and use information"* (Van der Veer and Wiles 2006). While the syntactic interoperability is concerned with data exchange, the challenges with usability of this data as information and processing it is dealt by semantic interoperability.

This is an issue in cross-domain federation due to the necessity of representing the knowledge contained in the data using a single abstract across all domains of the participating federates. For example, the interdependencies between the critical infrastructures depicted in Figure 1, shows that the telecommunication dependency of the hospital from the Base Transceiver Station (BTS) is inter-dependent on the energy from the power distribution station which in turn is dependent on the hydroelectric station. Thus, to understand the effect of failure of the BTS system it is important to model the dependency of the hydroelectric station which does not have any physical communication link with the BTS. This syntactic interoperability issue in using a single modeling entity to model such complex interdependencies needs to be addressed to achieve a successful testbed federation of critical infrastructures.

2.4 Time Management

One of the major challenges in federation is the synchronization of time between the distributed federates and the maintenance of a single clock (global simulation view) time across them. This is a major challenge because each of the participating federates will have different operating clock frequencies and different processing capabilities due to the amount of computations that need to be done in a single simulation time-step. Thus resulting in inaccuracies of either missing communicating events among the federates or losing the temporal order among these events, especially in the case of a discrete-event simulation.

A conservative approach prevents participating federates from missing events by absolutely ensuring that a federate processes only safe events. A received event at a federate is termed safe by a federation manager by ensuring that this federate will not receive the same event at a later point in time by using computing algorithms to determine lookahead simulation events of other federates. This approach simplifies the implementation of individual federates but it is challenging to develop the lookahead algorithms for all the federates and implement them in the federation manager.

On the other hand, the optimistic approach allows the individual federates to process unsafe events but the federates should have the ability to roll-back to a state before the event happened to ensure the correct order of events. Thus in contrast to the conservative approach, the challenge lies in the implementation of all the federates being able to effectively roll-back without any side effects after processing an event to a state that has not seen the same event. This also increases the memory used for each federate to effectively store all the preceding states for a clean roll-back but simplifies the task of the federation manager.

2.5 Federation Security

A federated experiment consisting of a testbed of testbeds requires the issue of security to be addressed at multiple levels. Firstly, the user requesting for a federated experiment should be identified correctly by the appropriate authentication. Next, the the user must have the necessary permissions with respect to authorized access to the requested federates as resources. While a user might have access requests, there should be proposer checks to ensure that the federation controller, who might be a different user has control authorization rights over the requested testbed resources. Thus the layers of authentication for the user logging in must be separated from the layer of authorization for access and control to ensure agility during a federated experiment execution.

3 REVIEW OF STATE-OF-THE-ART

In this section, we review the state-of-the-art with respect to the key issues discussed in Section 2 and discuss four approaches in detail: (i) the High Level Architecture (HLA) (IEEE 2010a) proposed by the US Department of Defence to address the challenges for multi-user simulation of realistic combat training,

(ii) the Design of an Interoperable European Federated Simulation Framework for Critical InfrastructureS (DIESIS) (Usov et al. 2010) which specifically addresses the coupling of heterogeneous simulation systems to identify risks and analyze the cascading effects cross-domain dependencies, (iii) a testbed federation approach based on the DETER testbed (Faber et al. 2007) federating with other co-located or co-implemented DETER subsystems and, (iv) the distributed virtual laboratory for at-scale experiments in network science, services, and security, namely Global Environment for Networking Innovation (GENI) (McGeer et al. 2016) based federation architecture.

3.1 HLA

To address the need for interactive simulators combat-training, Defense Advance Research Projects Agency (DARPA) initially implemented the SIMNET to interconnect different military simulators like airplanes, tanks etc. The successful usability of SIMNET led to the IEEE standard 1278, called Distributed Interactive Simulation (DIS) which defines how simulators should interact among each other by interpreting the data sent and received in a standard manner (semantic interoperability). However, a few drawbacks of the DIS are (i) the semantics strictly adhere to the syntax of network-based link protocol and all participating federates must adhere to this for meaningful exchange, (ii) it causes network congestion as it is based on every federate broadcasting its current state to every other federate and (iii) it does only supports real-time simulation.

To overcome these, the High Level Architecture (HLA) standard was proposed by the US Department of Defence and it defines how simulators interact by communicating data and synchronize among each other. While DIS is always with respect to a user, HLA supports simulations with out human users too. The first usage of the word "federate" came about with the introduction of a HLA-compliant simulator and the simulation with multiple federates is a federation. HLA consists of three main components namely,(i) the common format for interoperability and reuse of federates and their manager, called the Object Model Template (OMT), (ii) the rules for the federate and federation to be HLA-compliant, and (iii) the run-time interface which is a communication layer between the federates and the run-time infrastructure (RTI).

3.1.1 Federation Examples

In this section we discuss two examples of federations using HLA and RTI for different application domains. Next, we discuss the shortcomings of HLA and show an example which uses some implementations based on the HLA-approach and implements a new interoperable framework. The Extensible Modeling and Simulation Framework (XMSF) (Brutzman et al. 2002, Pullen et al. 2005), which aims at executing a HLA-compliant distributed federation. There are many follow-up research works on distributed federation that make use of XMSF, such as Web Services Internet Management (WSIM) (Morse et al. 2004). While both XMSF and WSIM have their applications in the military domain, in the networking domain, an example architecture for a communication network simulation federating two instances of the Network Simulator (ns). To overcome the challenge with respect to the high difference between real-time and simulation time, this architecture distributes the simulation across multiple processors thus meeting the high compute resource demand. They use a federation architecture based on HLA with the Run TIme Infrastructure (RTI) implemented as a FDK library to take care of data passing and synchronization of events among federates.

While HLA and RTI provide an approach for homogeneous federation as shown by the above two example implementations, interoperability using HLA for heterogeneity among federates when they use different languages is a major challenge. Another follow-up research similar to HLA but not using HLA is using the XMSF and developing an interoperable framework as a middleware for homeland security application is the Interoperable Distributed Simulation Framework (IDSIM) (Fitzgibbons et al. 2004). The IDSIM software architecture with implements a communication middleware based on the open standard Open Grid Service Infrastructure (OGSI) for communication among the participating federates. Simulators interface through a remote server that manages federation state and provides all simulation-related services. XML repositories containing XMSF-based documents provide simulation models and configuration information needed to instantiate the framework. A storage service provides a method to commit a log of events that transpire during the course of an execution (Fitzgibbons et al. 2004).

While IDSim enables distributed federation in the homeland security domain, Java based framework such as ASimJava (Sikora and Niewiadomska-Szynkiewicz 2007) and the Integrated Modeling Environment (IME) (Tolone et al. 2008) enable federation of large-scale physical systems. Other frameworks such as I2Sim (Martí et al. 2008) abstract the technical details of individual critical infrastructures thus not only preserving their privacy but also reducing the domain expertise needed for users running a federation experiment. Another approach that uses abstraction to analyze the complex behaviour of critical infrastructures is the AIMS workflow (Bagheri and Ghorbani 2006, Bagheri et al. 2007). They have a set of component templates that users can use to create instances of the model and the interactions between them. Furthermore the AIMS framework has a special middleware that supports Visualization, Manipulation and Analysis protocol that enables users of the federation to dynamically change the models and scenarios in a federated experiment (Rome et al. 2014). Another example of simulation of critical infrastructure using agents to represent subsystems and modeling the interdependencies between two simulators representing power transmission and network communication is demonstrated in SimCIP (Usov and Beyel 2008) environment of the IRRIIS project (Klein et al. 2008).

3.2 DIESIS

To overcome the interoperability challenges due to the "one size fits all" approach of HLA (Reid and Powers 2000), a lateral coupling strategy was proposed by the EU project Design of an Interoperable European Federate Simulation network for Critical InfrastructureS (DIESIS) (Usov et al. 2010). This approach is also a feasible solution for heterogeneous federates and cross-domain federation. In addition to lateral coupling, DIESIS also introduces separation between the technical and semantic interoperability layers. While a single RTI proposed by HLA is suitable for domain-specific federation, a generic RTI does not work if these federates do not adhere to a single interface standard. Additionally, having a global standard interface for all types of heterogeneous federates may not give reasonable performance and slow down the entire federation. To address heterogeneous federates across domains, a lateral coupling architecture might be more efficient as specific efficient links could be established between the federates that exchange data and these links could be different from other such pair-wise links between other inter-operable federates and so on. For these pair-wise or laterally couple links to work, both the syntax and semantic definitions have to be clearly specified.

DIESIS uses Ontology Web Language (OWL) and the Semantic Web Rule Language (SWRL) to define the infrastructures, their dependencies and relations between them for a seamless federation. Similar to the three object model templates for interoperability defined in HLA, DIESIS also defines three ontology templates, (i) World Ontology (WONT) to define the infrastructures, the possible inter-dependencies and behaviours, (ii) Infrastructure Ontology (IONT), to describe each specific critical infrastructure including its domain-specific properties. It does not detail the individual infrastructure but pertains to a description that is necessary for interacting with other federates, and (iii) the federation ontology (FONT) that models the dependencies among federates. Thus, using these three ontologies the DIESIS approach aims to capture all possible semantic interactions between the federates as a different abstraction from the physical coupling links between them. Apart from the ontologies, DIESIS defines four types of coupling links based on functionality, data, control and time to help reusability and develop light weight functionality. While the links provide for semantic interoperability among critical infrastructures based federates, there is a need for a middleware that considers the syntactic connectivity details and provides for the right translation using adapters between federates implemented on different languages. DIESIS is a flexible approach that provides for federation between heterogeneous critical infrastructure and study their inter-dependencies. But it does not consider security and authentication aspects. Next, we study some federation approaches specifically addressing cyber-security testbeds.

3.3 DETER Federation Architecture

Federation of testbeds have different objectives compared to federation of critical infrastructures. Federation of critical infrastructures help mitigate interdependency risk and study cascading effects of failure. In contrast, federation of testbeds is to allow for large-scale experimentation not feasible with a small testbed and in

addition gain larger geographical distribution using the testbed federation. A key challenge with respect to federation of testbeds is that these resources are shared by many experimenters and the sharing of the testbed resources are managed in a very independent manner at each testbed level. Thus, it is non-trivial to manage federation of multiple testbeds at the same time wherein each testbed has its own sharing policy. While the previously discussed related works do not consider security with respect to authentication, the Deterlab based federation architecture has an Attribute Based Access Control (ABAC) engine that ensures federation with the many layers of possible privileges users typically have in a testlab environment. The federator which manages the federants has a separate plugin for each of the different testlabs being federated and uses the ABAC engine to control whether the user has the necessary privilege and authenticate the users to design experiments in each federant. Some of the key challenges addressed by the Deterlab federation architecture include, (i) identification techniques to maintain individual testbed experiment scope in the federated experiment setup, (ii) management of access control of varying levels for the experimenter and only one level for the project in a testbed environment, (iii) differentiating between global objects accessible for inter-testbed and local objects with the testbed, and (iv) resource allocation across federating testbeds. Currently, the National Cybersecurity Lab (NCL) testbed hosted in Singapore (NCL 2017) implements and supports customized auto-provisioning of host and network, similar to the DeterLab (Benzel 2011) cybersecurity experimentation. However, currently both NCL and Deterlab do not address cross-domain federation issues specifically federation between cybersecurity testbeds and cyberphysical testbeds.

3.4 GENI Federation Architecture

The definition of a federation from the GENI project is " A collection of people and institutions who agree to share resources and abide by common procedures in order to share resources in a reliable, mutually beneficial manner." (McGeer et al. 2016). The Slice-based Federation Architecture (SFA) extends the GENI initiative and defines two key abstractions, components and slices. Components are actual resources like hardware and multiple components are grouped as aggregates which are accessed via interfaces and controlled by aggregate managers. One of the main purposed of the GENI project is to enable trusted exchange of resources. Resources in the GENI context refer to infrastructure based resources such as storage, networking, compute infrastructure and the GENI architecture tries to mediate between the two parties involved in the resource exchange, providers and consumers. While both the providers and consumers of resources are motivate to exchange or share them, there are many barriers for effective exchange such as the providers and consumers not aware of each others existence in terms of how much demand for th e resource for the providers and resource capacity and availability for the consumers. Secondly, there are trust issues among them in terms of reliability of service provided for the consumers and service misuse for the providers. Some of these challenges are addressed by the GENI Clearinghouse, where the Clearinghouse is a trusted third party that provides for reliable exchange of resources which is non-trivial when the number of providers and consumers are large (McGeer et al. 2016). The GENI federation architecture mainly consists of three software services, the clearing house, the aggregate manager and the client tools. While the clearinghouse manages policies regarding trust and authorization, the aggregate manager (AM)) uses AM APIs to actually allocate the requested resources from the provider to the consumer. The client tools are the users of the federation services provided using GENI architecture.

3.5 Summary

In summary, while each of the discussed approaches addresses federation goals specific to a certain domain, none of these suffice to achieve federation of both cybersecurity testbeds and cyberphysical testbeds representing critical infrastructure. With the increase in the interdependency between both types of testbeds, namely cybersecurity and cyberphysical, there is a need to federate between them to model and simulate such interdependencies. While DIESIS approach considers different critical infrastructures, and GENI considers cloud and networking infrastructure, neither of them suffice for federation of critical infrastructures and cloud-based infrastructures due to the syntactic and semantic interoperability issues discussed in Section 2. Thus, in the next section, we propose a layered federation architecture, DEFT that enables such a cross-domain federation of testbeds.

4 CONCEPTUAL ARCHITECTURAL FRAMEWORK

The objective of this paper is to design a scalable federation architecture framework that enables users to build a federated experiment. Such a federation provides a unified view to users and enables to study interdependencies among critical infrastructures. Users select the necessary federate to combine as part of the single unified testbed and the federation should enable only those users that have the required authentication to use and control the selected federates during experiment execution. In this context, a scalable testbed (federation) consists of testbeds (federates) that are connected to achieve a testbed goal and the federation management defines how interconnected federates are created, join, etc. Before we design a reference architecture it is important to outline the objectives and the key design considerations which form the basis of the conceptual framework. We consider three aspects, management, interoperability and elasticity of a federation for the design of the conceptual framework. With respect to management, we consider an approach that enables scalability, i.e. ease of creating new federates and dynamically managing their execution during the federated experiment. As this conceptual framework being proposed is for a testbed consisting of heterogeneous testbeds, "testbed of testbeds", ease of management is an important design consideration.

To study and model a federation consisting of multiple heterogeneous testbeds with each testbed being either a physical system or a simulator, it is important that the participating federates across domains can easily communicate and inter-operate among each other. While a common API is necessary for communication across federates, the context of data exchanged is also an important design criterion. Furthermore, it is increasingly important to model sequence attacks to validate intrusion detection tools that are sequence aware (Caselli et al. 2015). Thus, a federation design should be elastic to incorporate both ease of scalability for new federates joining in and the flexible interoperability with meaningful context-aware data exchange among the participating federates. With these design considerations of ease of federation management, scalability, flexibility and elasticity of a federation, we propose a reference architecture, DEFT.

4.1 DEFT Federation Architecture

The design of the proposed federation architecture, DEFT is to achieve some of the goals of a successful federation from the perspective of both users and the participating federates. Given a set of physical resources in terms of cybersecurity testbeds or cyberphysical systems modeling critical infrastructures, the reference architecture is a layered approach with increasing level of abstraction to give a unified testbed infrastructure as a federation to the user. We use the separation of concerns design principle in the proposed layered cybersecurity testbed federation architecture. The proposed architecture, DEFT is outlined in Figure 3 , wherein the operational concerns of the federation including monitoring and billing is separate

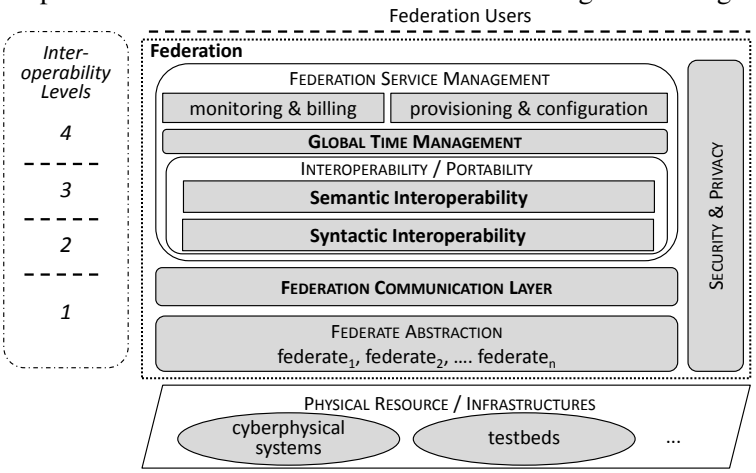


Figure 3: DEFT - A Layered Cybersecurity Testbed Federation Architecture

from the interoperability among federates. Such a layered approach with different abstractions for achieving

different design considerations help in making the federation more scalable and elastic both from a user and federation management perspective.

Level 1: Cross-domain interoperability The federate abstraction layer is used to address the issue of cross-domain interoperability and abstracts away the domain-specific features of a federate, keeping only a component level view of a federate as an entity. This specification of each domain-specific federate as an entity can be easily achieved by using the Object Management Group's (OMG) open standard, Model Driven Architecture (MDA) (Mellor 2004, OMG 2003). Using this abstracted model the reference architecture uses the separation of concerns between the model and how the models communicate with each other using the federation communication layer.

This communication layer defines interactions between the federates abstracted as models, for instance using a UML sequence diagram. While the models representing the federates define the source and sink of the individual federate data, the sequence of exchange of data among the models is done by the communication layer. Using separation of concerns, the actual protocol for the exchange of data and the meaning of the data being exchanged is defined in the higher interoperability layers. Thus, this layered reference architecture is analogous to the networking stack wherein the federation communication layer is similar to the flow of bits in the physical layer of the network stack.

Level 2: Elasticity via Distributed Control Using the analogy of the networking stack, the syntactic interoperability layer is then similar to the data link layer of the Open Systems Interconnection model (OSI model). The syntactic interoperability layer defines the protocol for communication between the federates. To achieve a scalable architecture and accommodate for legacy federates, we propose using lateral-coupling or a peer-to-peer connectivity. For ease if syntactic interoperability, we should be able to use a light-weight adapter that converts legacy protocol to the current protocol implemented in the federation. For example, eXtensible Markup Language (XML) maybe used for specifying the syntactic interoperability between federates and defines the types of data being exchanged. The data can be exchanged among only those federates connected to each other by a physical connectivity as defined in the communication layer of the federation.

Level 3: Rule-based Semantics for interdependency modeling While the type of data being exchanged is defined by the syntactic layer, the meaning of this data with the cascading effects of such data interactions among the federates is defined by the syntactic interoperability layer. The communication layer and the syntactic layers only consider which federates talk to each other and what type of data is being exchanged respectively. The modeling of interdependencies among the federate models is defined in the semantic layer by using interaction rules between the federates. An example of defining these interaction rules and interdependencies is by using a tree-like data structure where the data generated by a parent node will have cascading effects on all of its subsequent children nodes. Thus this data structure captures both interdependent critical infrastructure as well as independent systems. Such a tree like structure need not be same across all the syntactic connections possible between the interacting federates and could be written as different rules per type of connection, thus enabling a unified model constituting of complex interactions between testbed of testbeds.

Level 4: Unified view and control Using the separation of concerns as the basis for the reference architecture design, the service management layer has a global view of the federated experiment and is used for logging, monitoring and managing the global time of the experiment. This management layer is also responsible for providing a clear user interface with a global view of the available physical resources and the management of the requested resources via authentication. While the security issues dealing with exchange of information is managed at each level of interoperability, the global authentication of the possibility for a particular experiment requested by a specific user is managed by this layer.

Table 1 summarizes the four different federation approaches, HLA, DIESIS, DeterLab, GENI and compares these with DEFT our proposed federation architecture using the design consideration factors for cross-domain federation.

Table 1: Federation Approaches

Factors	HLA (Van Hook et al. 1996) (Zeigler et al. 1999) (Riley et al. 2004) (Xie et al. 2005)	DIESIS (Rome et al. 2009) (Bologna et al. 2009) (Masucci 2012) (Usov et al. 2010)	DeterLab (Faber et al. 2007) (Benzel 2011) (Sklower and Joseph 2007) (Liu and Srivastava 2015)	GENI (Elliott 2008) (McGeer et al. 2016) (Berman et al. 2014) (Jeong and Bavier 2010)	DEFT Proposed Testbed Federation Architecture
Cybersecurity	no	no	yes	yes	yes
Cross-Domain Interoperability	no, only military simulation	limited, only cyberphysical	no, cybersecurity only	limited, networked testbeds	yes
Elasticity	no, central	yes, lateral	no,central	no, central	yes, lateral
Interdependency Semantics	yes, Run-time Infrastructure	yes, Simple Object Access Protocol	no, MAGI messaging substrate	no Common Federation API	yes, modeling interaction rules
Global Time	yes, Time Stamp Order Time Advance Grant	yes, Time Management Module	no	no	yes, unified view & control
Federation Security	no	no	yes, ABAC engine	yes, Clearinghouse	yes, inter-layer

5 CONCLUSIONS

While individual testbeds provide researchers with the environment to create and execute novel models, the increasing interdependencies of critical infrastructure makes federation of multiple testbeds an invaluable approach for validating security resilience. Federation not only provides a means to perform experiments for crisis management but also serves as a decision support system tool to perform "what-if" analysis for emergency management. In this paper we have highlighted some of the key issues in cross-domain federation and exposed the gaps by an extensive review of the current state-of-the-art. Addressing these gaps, the paper proposes DEFT, a novel reference architecture for federation. DEFT is a conceptual federation framework that enables a federation of testbeds to address the limitations of current federation approaches by using a layered approach and separating the various levels of interoperability. Thus, the DEFT framework uses separation of concerns across the layers such that it can be easily applied for cross-domain federation due to the abstraction of the domain in the bottommost layer and the inter-domain dependencies addressed by the semantic layer. The issue of security is handled by applying the user authorization and authentication at the federation management layer and transferring the credentials downwards to each of the interoperability layers. While this paper identifies key issues and challenges in cross-domain federation of testbeds for cybersecurity and proposed DEFT, a four-tier conceptual framework, the next step will be to prototype the framework and validate it against a use-case.

ACKNOWLEDGEMENTS

This research is supported by the National Research Foundation, Prime Minister's Office, Singapore under its National Cybersecurity R&D Program (Award No. NRF2015-NCRNCR002-001) and administered by the National Cybersecurity R&D Directorate.

REFERENCES

2003. "Object Management Group (OMG), Model-driven Architecture (MDA)". http://www.omg.org/mda/.

Bagheri, E., H. Baghi, A. A. Ghorbani, and A. Yari. 2007. "An Agent-based Service-oriented Simulation Suite for Critical Infrastructure Behaviour Analysis". *International Journal of Business Process Integration and Management* 2 (4): 312–326.

Bagheri, E., and A. Ghorbani. 2006. "A Service Oriented Approach to Critical Infrastructure Modeling". In *Workshop on Service Oriented Techniques*: National Research Council, Canada.

Benzel, T. 2011. "The Science of Cyber Security Experimentation: the DETER Project". In *Proceedings of the 27th Annual Computer Security Applications Conference*, 137–148. ACM.

Berman, M. et al. 2014. "GENI: A Federated Testbed for Innovative Network Experiments". *Computer Networks* 61 (0): 5 – 23. Special issue on Future Internet Testbeds Part I.

Bologna, S., E. Gelenbe, E. H. Luiijf, and V. Masucci. 2009. "DIESIS: An Interoperable European Federated Simulation Network for Critical Infrastructures". *proc. EURO SIW*.

Brutzman, D., M. Zyda, J. M. Pullen, and K. L. Morse. 2002. "Extensible Modeling and Simulation Framework (XMSF): Challenges for Web-based Modeling and Simulation".

Caselli, M., E. Zambon, J. Petit, and F. Kargl. 2015. "Modeling Message Sequences for Intrusion Detection in Industrial Control Systems". In *International Conference on Critical Infrastructure Protection*, 49–71. Springer.

Di Pietro, A., S. Panzieri, and A. Gasparri. 2015. "Situational Awareness Using Distributed Data Fusion with Evidence Discounting". In *International Conference on Critical Infrastructure Protection*, 281–296. Springer.

Elliott, C. 2008. "GENI-global Environment for Network Innovations". In *LCN*, 8.

Faber, T., J. Wroclawski, and K. Lahey. 2007. "A DETER Federation Architecture". In *Proceedings of the DETER Community Workshop on Cyber Security Experimentation and Test on DETER Community Workshop on Cyber Security Experimentation and Test 2007*, 11–11. USENIX Association.

Fitzgibbons, J. B., R. M. Fujimoto, D. Fellig, S. D. Kleban, and A. J. Scholand. 2004, July. "IDSim: an extensible framework for Interoperable Distributed Simulation". In *Proc of International Conference on Web Services*, 532–539.

Formicola, V., A. Di Pietro, A. Alsubaie, S. DAntonio, and J. Marti. 2014. "Assessing the Impact of Cyber Attacks on Wireless Sensor Nodes that Monitor Interdependent Physical Systems". In *International Conference on Critical Infrastructure Protection*, 213–229. Springer.

Görbil, G., and E. Gelenbe. 2009. "Design of a Mobile Agent-based Adaptive Communication Middleware for Federations of Critical Infrastructure Simulations". In *International Workshop on Critical Information Infrastructures Security*, 34–49. Springer.

Gregersen, J., P. Gijsbers, and S. Westen. 2007. "OpenMI: Open modelling interface". *Journal of Hydroinformatics* 9 (3): 175–191.

Howser, G. 2015. "Using Information Flow Methods to Secure Cyber-Physical Systems". In *International Conference on Critical Infrastructure Protection*, 185–205. Springer.

IEEE 2010a, Aug. "IEEE Standard for M & S HLA – Framework and Rules". *IEEE Std 1516-2010 (Revision of IEEE Std 1516-2000)*:1–38.

IEEE 2010b, Aug. "IEEE Standard for M & S HLA – Object Model Template Specification". *IEEE Std 1516.2-2010 (Revision of IEEE Std 1516.2-2000)*:1–110.

Jenkins, J., and M. Burmester. 2015. "Runtime Integrity for Cyber-Physical Infrastructures". In *International Conference on Critical Infrastructure Protection*, 153–167. Springer.

Jeong, S., and A. Bavier. 2010. "Geni Federation Scenarios and Requirements". *GENI: Global Environment for Network Innovations*:1–16.

Klein, R., E. Rome, C. Beyel, R. Linnemann, W. Reinhardt, and A. Usov. 2008. "Information Modelling and Simulation in large interdependent Critical Infrastructures in IRRIIS". In *International Workshop on Critical Information Infrastructures Security*, 36–47. Springer.

Liu, R., and A. Srivastava. 2015. "Integrated Simulation to Analyze the Impact of Cyber-attacks on the Power Grid". In *Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES), 2015 Workshop on*, 1–6.

Martí, J., C. Ventura, J. Hollman, K. Srivastava, and H. Juarez. 2008. "I2Sim Modelling and Simulation Framework for Scenario Development, Training, and Real-time Decision Support of Multiple Interdependent Critical Infrastructures during large Emergencies". In *NATO (OTAN) MSG-060 Symposium on How is Modelling and Simulation Meeting the Defence Challenges out to 2015*.

Masucci, V. 2012. "Semantic Interoperability among Federated Simulators of Critical Infrastructures–DIESIS project". *WIT Transactions on State-of-the-art in Science and Engineering* 54.

McGeer, R., M. Berman, C. Elliott, and R. Ricci. (Eds.) 2016. *The GENI Book*. Cham: Springer.

Mellor, S. J. 2004. *MDA distilled: Principles of Model-Driven Architecture*. Addison-Wesley Professional.

Morse, K. L., R. Brunton, J. M. Pullen, P. McAndrews, A. Tolk, and J. Muguira. 2004. "An Architecture for Web-services based Interest Management in Real Time Distributed Simulation". In *Proc of 8th DS-RT*, 108–115.

NCL 2017. "National Cybersecurity Lab Testbed, Singapore". *https://ncl.sg/testbedInformation*.

Nieuwenhuijs, A., E. Luiijf, and M. Klaver. 2008. "Modeling Dependencies in Critical Infrastructures". In *International Conference on Critical Infrastructure Protection*, 205–213. Springer.

Pullen, J. M., R. Brunton, D. Brutzman, D. Drake, M. Hieb, K. L. Morse, and A. Tolk. 2005. "Using Web Services to Integrate Heterogeneous Simulations in a Grid Environment". *Future Generation Computer Systems* 21 (1): 97–106.

Reid, M. R., and E. I. Powers. 2000. "An Evaluation of the High Level Architecture (HLA) as a Framework for NASA Modeling and Simulation".

Riley, G. F., M. H. Ammar, R. M. Fujimoto, A. Park, K. Perumalla, and D. Xu. 2004. "A federated approach to distributed network simulation". *Trans. on Modeling and Computer Simulation* 14 (2): 116–148.

Rome, E., S. Bologna, E. Gelenbe, E. H. Luiijf, and V. Masucci. 2009. "DIESIS: an Interoperable European Federated Simulation Network for Critical Infrastructures". In *Proceedings of the 2009 SISO European Simulation Interoperability Workshop*, 139–146. Society for Modeling & Simulation International.

Rome, E., P. Langeslag, and A. Usov. 2014. "Federated Modelling and Simulation for Critical Infrastructure Protection". In *Networks of networks: the last frontier of complexity*, 225–253. Springer.

Setola, R., S. Bologna, E. Casalicchio, and V. Masucci. 2008. "An Integrated Approach for Simulating Interdependencies". In *ICCIP*, 229–239. Springer.

Sikora, A., and E. Niewiadomska-Szynkiewicz. 2007. "A Federated Approach to Parallel and Distributed Simulation of Complex Systems". *IJAMCS* 17 (1): 99–106.

Sklower, K., and A. D. Joseph. 2007. "Very Large Scale Cooperative Experiments in Emulab-derived Systems". In *DETER Community Workshop on Cyber Security Experimentation and Test 2007*.

Tofani, A., E. Castorini, P. Palazzari, A. Usov, C. Beyel, E. Rome, and P. Servillo. 2010. "An Ontological Approach to Simulate Critical Infrastructures". *Journal of computational science* 1 (4): 221–228.

Tolone, W. J., E. W. Johnson, S.-W. Lee, W.-N. Xiang, L. Marsh, C. Yeager, and J. Blackwell. 2008. "Enabling System of Systems Analysis of Critical Infrastructure Behaviors". In *International Workshop on Critical Information Infrastructures Security*, 24–35. Springer.

Usov, A., and C. Beyel. Novemeber/December 2008. "Simulating Interdependent Critical Infrastructures with SimCIP". *European CIIP Newsletter 4(3)*:6–8.

Usov, A., C. Beyel, E. Rome, U. Beyer, E. Castorini, P. Palazzari, and A. Tofani. 2010, Aug. "The DIESIS Approach to Semantically Interoperable Federated Critical Infrastructure Simulation". In *Proc. of 2nd SIMUL*, 121–128.

Van der Veer, H., and A. Wiles. 2006. "Achieving Technical Interoperability - The ETSI Approach". *https://www.itu.int/dms_pub/itu-t/oth/06/02/T06020000040002PDFE.pdf*.

Van Hook, D. J., S. J. Rak, and J. O. Calvin. 1996. "Approaches to RTI implementation of HLA Data Distribution Management Services". In *Proceedings of the 15th DIS Workshop*, 535–544.

Xie, Y., Y. M. Teo, W. Cai, and S. J. Turner. 2005. "Servicing Provisioning for HLA-based Distributed Simulation on the Grid". In *Proc. of 19th Workshop on PADS*, 282–291.

Zeigler, B. P., G. Ball, H. Cho, J. Lee, and H. Sarjoughian. 1999. "Implementation of the DEVS Formalism over the HLA/RTI: Problems and Solutions". In *Simulation Interoperation Workshop (SIW)*, Volume 99.

AUTHOR BIOGRAPHIES

LAVANYA RAMAPANTULU is a Research Fellow at the National Cybersecurity R&D Lab, Singapore. Her email address is lavanya@comp.nus.edu.sg.

YONG MENG TEO is an Associate Professor with the Department of Computer Science at the National University of Singapore (NUS), and an Affiliate Professor at the NUS Business Analytics Center. He heads the Computer Systems Research Group. His email address is teoym@comp.nus.edu.sg.

EE-CHIEN CHANG is an Associate Professor with the Department of Computer Science at the National University of Singapore (NUS). His email address is changec@comp.nus.edu.sg.