work on multiple fronts.

II. TECHNICAL PAPERS AND KEYNOTES

The program of DISN’2015 consists of 3 technical papers and 2 keynotes, briefly described next.

The first paper “SeReNe: On Establishing Secure and Resilient Networking Services for an SDN-based Multi-Tenant Datacenter Environment” is by Chun-Jen Chung, Tianyi Xing, Dijiang Huang, Deep Medhi, and Kishor Trivedi. The authors describe the Secure and Resilient Networking (SeReNe) service model to establish a programmable and dynamic defensive mechanism that can reconfigure itself and adjust the system’s networking resources such as topology, bandwidth allocation, traffic/flow forwarding policies, among others, according to the perceived security threats. The objective of SeReNe is to develop an orchestrated and resilient defensive mechanism that uses well-established quantifiable metrics, models, and evaluation methods. The proposal involves both a Moving Target Defense (MTD) framework and an Adaptive Security-enabled Traffic Engineering (ASeTE) approach to select optimal countermeasures and network bandwidth allocation, to minimize the intrusiveness to the applications and also the cost.

The second paper “Video on Demand Hosted on Private Clouds: Availability Modeling and Sensitivity Analysis” is by Rosangela Melo, Maria Clara Bezerra, Jamilson Dantas, Rubens Matos, Ivanildo Melo, and Paulo Macial. The authors investigate how cloud computing can be best used to host multimedia services, in particular video streaming. Cloud-based services can take advantage of scalability and elasticity that are intrinsic to the environment. The authors use hierarchical analytical models to evaluate the availability of a video streaming service hosted on a typical cloud environment. Both Reliability Block Diagrams (RBDs) and Markov chains were employed to execute a sensitivity analysis, used to determine the parameters that cause the greatest impact on the availability. Among the results, the authors show by using Parametric Sensitivity Analysis and Reliability Importance that the most important component of the system in terms of reliability is the Frontend module. Strategies to improve the availability are discussed.

The third paper “Implementation of a Failure Detector Based on Network Function Virtualization” is by Rogerio Turchetti and Elias P. Duarte Jr. In this paper the authors propose NFV-FD: a NFV to detect process and link failures. NFV-FD relies on an OpenFlow controller from which information about the network is obtained. With this information, NFV-FD was implemented and experimental results are reported for the amount of resources required by the virtual function, as well as the quality of the failure detection and notification service.

The first keynote “Software Network Security” is by Otto C. M. B. Duarte. In the near future, the number of “software networks” could reach thousands of networks running over a physical infrastructure composed by interconnected data centers. In this keynote, the speaker will discuss the security and privacy challenges of software network environments, which include different new technologies such as virtualization, cloud, software defined networking, and big data. Virtualization system vulnerabilities are described. Proposals for software network isolation, virtual machine authentication, and secure virtual machine migration are provided. Denial of service as well as consistency problems during state transition
on software defined networking are also assessed. The inter-university network testbed FITS (Future Internet Testbed with Security) is also described which provides a management interface for OpenFlow and Xen networks. The tool is based on a service-oriented architecture and dynamically allows monitoring and configuring software network.

The second keynote “NetPaxos: Consensus at Network Speed” is by Robert Soule. In this keynote, the speaker explores the possibility of implementing the widely deployed Paxos consensus protocol in network devices. Two different approaches are presented: (i) a detailed design description for implementing the full Paxos logic in SDN switches, which identifies a sufficient set of required OpenFlow extensions; and (ii) an alternative, optimistic protocol which can be implemented without changes to the OpenFlow API, but relies on assumptions about how the network orders messages. Although neither of these protocols can be fully implemented without changes to the underlying switch firmware, the speaker argues that such changes are feasible in hardware today. An evaluation is presented that suggests that moving Paxos logic into the network would yield significant performance benefits for distributed applications.

ACKNOWLEDGMENTS

The Chairs of DISN’2015 would like to express their gratitude to the Workshop Chairs of DSN’2015, Marco Vieira and Fabiola Greve, and to the General Chairs of DSN’2015, Eliane Martins and Regina Moraes. We would also like to thank David de Andrés Martínez for his help with the publication procedure. Finally we would like to thank the TPC members for their support.