Published in: EI2 2017 - 2017 IEEE Conference on Energy Internet and Energy System Integration
DOI: 10.1109/EI2.2017.8245292

Communications in Distributed Smart Grid Control: Software-Defined vs. Legacy Networks

Nils Dorsch, Fabian Kurtz, Christian Wietfeld
Communication Networks Institute
TU Dortmund University
{nils.dorsch, fabian.kurtz, christian.wietfeld}@tu-dortmund.de

***Abstract*—To deal with the challenges of increasingly fluctuating power flows in future energy systems, distributed control using a Multi-Agent System (MAS) is considered a promising solution. However, these agents require appropriate Information and Communication Technology (ICT) infrastructures to coordinate their actions. Software-Defined Networking (SDN) is a novel approach for dynamic and flexible configuration of communication networks, which enables integration of reliability and security enhancing measures, while optimizing network load and cost efficiency. In this work, the concept of SDN and traditional networking are compared regarding their applicability for establishing distributed power grid control. In particular, we discuss the aspects of security, reliability, transmission paradigms, topology detection and configuration effort. Using a typical transmission grid scenario, derived from the well-established New England Test System (NETS), we demonstrate the capabilities of SDN to improve significantly on the reliability of MAS communications, while incurring minimal administration overhead. Overall, our study indicates clear benefits of applying SDN for distributed power grid control.**

I. Introduction

To limit climate change, carbon dioxide emissions need to be reduced massively, with the energy system being a major factor. Hence, power generation is being shifted from fossil to renewable resources. This incurs more distributed, fluctuating feed-in, often in considerable distance from centers of energy demand. Moreover, the integration of Electric Vehicles (EVs), if not controlled properly, makes power consumption less predictable as well. In conclusion, these changes can destabilize the power system, provoking cascading outages, eventually causing complete black-outs [1]. To countervail this threat, real-time monitoring and control are required, mandating appropriate Information and Communication Technology (ICT) infrastructures [2].

As an alternative to overly complex and slow, centralized control systems, distributed solutions on basis of Multi-Agent Systems (MASs) are considered [3]. These excel at dynamic, real-time adaptation to variable grid conditions and enable the automated, coordinated deployment of countermeasures such as redispatch or activation of distribution grid flexibilities. For reliable MAS operation, agents need to exchange measurement and status data with adjacent units on a regular basis, as well as coordinate their actions. Therefore, we proposed the application of Software-Defined Networking (SDN) in previous work [4]. Building on this, we discuss advantages and disadvantages of this approach to distributed power grid control, in comparison to traditional Internet Protocol (IP) networks, in detail. SDN is a novel take on communication, separating the ICT network's data and control plane. Therefore, network control capabilities are extracted from networking devices and concentrated at a central instance, the SDN controller. The major benefit of this approach is the controller's programmability, which enables the integration of various approaches for ensuring hard service guarantees. In contrast, legacy IP networks are designed to provide best effort communications and are limited by a fixed set of functionalities. Hence, the fulfilment of service requirements is contingent on additional concepts such as Multi Protocol Label Switching (MPLS), which require significant administration efforts.

This paper is structured as follows: Section II describes the state-of-the-art in distributed power grid control and SDN for Smart Grids. Different communication approaches are introduced in Section III, followed by a comparison based on service criteria, such as reliability and security (Section IV). Next, an example of prioritization in a typical Smart Grid scenario is given in Section V. A summary and an outlook on future work in Section VI concludes the paper.

II. Related Work

In contrast to the traditional approach of centralized power grid control, current works propose distributed mechanisms [3][5]. Operating on basis of local measurements and data received from adjacent nodes, optimal utilization of reactive power is realized by distributed agents in [5]. Different concepts for preventing voltage collapse with the help of MAS are introduced in [6] and [3]. McArthur *et al.* describe in detail the requirements regarding MAS in energy systems, with standardized, flexible communication being a major enabler [7]. Specifications, defined by the Foundation for Intelligent Physical Agents (FIPA), are an important basis for this purpose [8]. In [9] a co-simulation of MAS for Smart Grids and corresponding communication systems is realized. Several works investigate the use of SDN for Smart Grid communications [10][11][4]. In [10] an Open Flow (OF)-enabled SDN infrastructure is compared to MPLS in the context of power system control. Cahn *et al.* implement automated substation configuration on basis of SDN [11]. SDN-enabled cyber security mechanisms are implemented and evaluated using International Electrotechnical Commission (IEC) 61850 communications in [12]. In previous work, we propose SDN to enhance the reliability of power system communications [4], which is refined by an interconnection between SDN controller and MAS [13]. Thus the communication network is dynamically tailored to the latter's requirements.

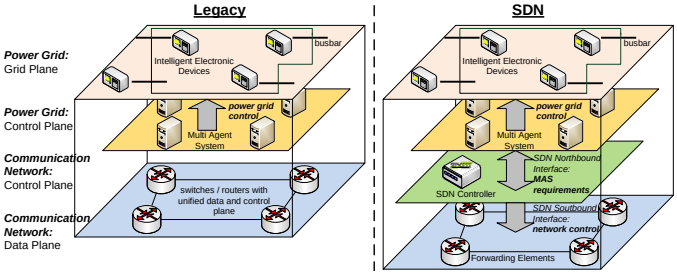

Figure 1: Comparison of legacy and SDN architectures for MAS communications

III. Concepts for Power Grid Control and Communications

This section introduces the principles of distributed, MAS-based power grid control and provides an overview of the different communication solutions for this purpose.

A. Multi Agent System-based Power System Control

The MAS consists of multiple agents, located at substations of the power grid. To devise control actions, agents rely on local measurements as well as information from other substations. It is sufficient for an agent to interact with other agents in adjacent substations within a defined observability area, as a complete system view is not required. Interaction comprises exchanging data using so-called *StateInformMessages* and coordinating control actions between agents. Local measurements are combined with data gained from *StateInformMessages* to perform distributed topology analyses. Based on the results, each agent derives a model of the surrounding system and its current state. To keep this model up-to-date, new state information needs to be incorporated and evaluated regularly. Subsequently, control actions are deduced and implemented with the help of connected assets at the respective substation. Actions involve for example changing the set point of High Voltage Direct Current (HVDC) converters and power flow controllers. Moreover, coordinated redispatch of flexible load and generation can be initiated to relieve overloaded transmission lines. Reactive power is provided by acting on shunt capacitors or flexible distribution systems. If the system is close to voltage collapse, agents may shed loads to maintain system stability. Compared to centralized grid control, major benefits of this distributed approach are quick adaption to unforeseen grid conditions such as (N-k)-cases and improved real-time capability. Low-latency communication networks are essential in enabling these functionalities.

B. Communication Approaches

Regarding agent communication, we compare applying traditional IP and SDN-based infrastructures, as shown in Fig. 1.
Legacy: The *legacy* approach uses traditional IP networks, involving best effort transmission of packets and decentralized routing. Therefore, each agent needs to identify its relevant neighbors, respectively its observability area independently, both on power system and ICT infrastructure level. With regard to the communication network this includes for instance determining the IP addresses of adjacent agents. To establish interaction, each agent is required to explicitly contact its communication partners using their IP addresses. Every substation infrastructure needs to encompass a router to direct packets towards other substations on the wide-area network. Due to the decentralized paradigm, routers perform network topology detection and packet forwarding case by case according to their routing tables. As traditional IP networks do not inherently provide hard service guarantees, further protocols and applications need to be added for stable power grid operation.
SDN: As a consequence of splitting the communication network's data and control plane, topology detection and routing are handled centrally by the SDN controller. To fully exploit the benefits of SDN, the MAS is coupled with the SDN controller via its Northbound Interface (NBI). Hence, agents are able to notify the SDN controller of their communication requirements, both for initial configuration and dynamic adaptation. Moreover, agents no longer require information on the ICT infrastructure, such as IP addresses of destinations. Instead of addressing specific neighbors directly, connectivity to neighboring agents is provided transparently. As the SDN controller receives information on the power grid topology, it establishes forwarding rules at the network elements, considering the individual observability area of each agent. Hence, agents simply need to send out their messages, which are then delivered to their destinations automatically. At the same time, the SDN controller monitors and ensures the fulfillment of service guarantees.

IV. Communication Aspects of Distributed Power Grid Control

In this section, relevant criteria for communications of distributed power grid control systems are discussed in detail.

A. Topology Detection

Both power system and communication network require topology detection mechanisms. On the power system level, this involves determining each agent's observability area, i.e. adjacent agents to interact with. In the ICT infrastructure, routes for exchanging messages between agents need to be identified. This is particularly relevant in case of topology changes such as the addition or failure of agents, switches and communication links.
Legacy: In case of legacy communication networks, each agent must determine both topologies and create its own local view of the system. Therefore, it broadcasts discovery messages, including information about the respective agent, its IP address and control capabilities, to detect adjacent substations. Reaching the other agents presupposes the substation router to discover the network topology beforehand, using common routing protocols such as Routing Information Protocol (RIP) or Open Shortest Path First (OSPF).
SDN: In contrast, with SDN, detection of the communication network topology is handled by the controller. Moreover, it receives identity information from each agent. Thus the controller is capable of grouping agents by their position and capabilities within the grid. Hence it provides connectivity exploiting its holistic view of both communication and power

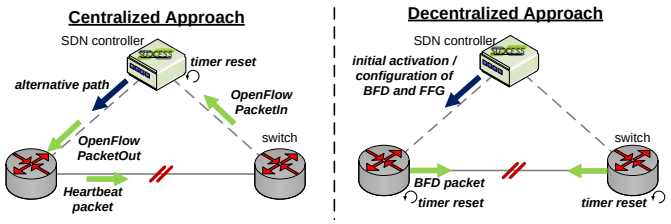

Figure 2: Comparison of SDN-based Failover Approaches

system. As a result, agents can interact without further knowledge of the underlying communication infrastructure.

B. Reliability

The reliability of a communication network involves fault tolerance as well as ensuring service guarantees.

1) Fault Tolerance: In communication infrastructures fault tolerance refers to the ability of maintaining operation in the presence of failed network elements such as switches and links. In case of SDN this also involves errors of the SDN controller. Fast recovery from failures in the communication network of power systems is particularly important as delayed or missing data may obstruct timely resolution of power imbalances, causing cascading outages.

Legacy: Standard IP networks do not possess any mechanisms for fast failover. To achieve sufficiently fast recovery, additional protocols such as MPLS and Resource Reservation Protocol (RSVP) Traffic Engineering (TE) need to be introduced. MPLS uses labels to direct traffic to specific paths, establishing end-to-end connections over packet-switched networks. In combination with RSVP TE this enables pre-configuration of backup paths, to which the traffic is switched in case of failures [14]. Such backup paths originate at points of local repair, where they separate from the main path, and rejoin downstream at merging points. By minimizing deviations between main and backup path, additional configuration overhead is to be reduced. Joint deployment with Bidirectional Forwarding Detection (BFD) [15] for fast local failure detection, allows for recovery within a few milliseconds [15][16]. However, despite attempts to reduce overhead, MPLS-based local protection incurs significant configuration and administration efforts [10].

SDN: In SDN-enabled infrastructures, fast recovery approaches can be implemented at the SDN controller directly. As soon as it is notified of a failure, the controller computes and conveys alternatives paths to the switches, shown in Fig. 2 (left side). By introducing a controller-based heartbeat mechanism for fast failure detection, recovery times of about $30\,\mathrm{ms}$ can be achieved [17]. Such delays are sufficient for distributed power grid control, whereas other energy system functions have even stricter time requirements. IEC 61850, which is a common standard for the communication in power grids, defines maximum delays below $10\,\mathrm{ms}$ for time-critical protection functions [18]. For this purpose, local failure detection and recovery mechanisms can be configured using the SDN controller. Again, BFD is deployed for identifying failed links. It is combined with OF's Fast Failover Groups (FFGs), which automatically switch traffic to backup paths, pre-defined by the SDN controller, in case the respective primary output port is not available (c.f. Fig. 2 (right side)). In contrast to MPLS-based solutions for legacy networks, this approach facilitates configuration significantly. Details on SDN-enabled fast failover for communication link failures can be found in [17]. In addition, failures of the SDN controller itself need to be considered. Typically, this is regarded as a single point-of-failure problem. However, in practical implementations it can be avoided easily by deploying multiple controller instances, which are required for scalability and security reasons as well.

2) Service Guarantees: For the transmission of critical MAS traffic, it is fundamental to guarantee defined service levels. Otherwise, capacities may be insufficient for exchanging measurement values with appropriate resolution or delivering switching commands in time, provoking outages of the power system. Hence, measures for providing hard service guarantees need to be integrated, in particular with regard to throughput (data rate) and latency.

Legacy: Common IP networks offer best effort transmissions without any service guarantees. To improve upon this situation, several approaches have been proposed, e.g. Differentiated Services (DiffServ), Integrated Services (IntServ) and MPLS. DiffServ enables rough service provisions on basis of traffic classes using the Type of Service field of IP packets. In contrast, IntServ implements fine-grained prioritization of packets on certain connections by reserving resources at routers with the help of RSVP. Yet, this approach requires all relevant network devices to support resource reservation. Also, configuration is quite static and requires significant efforts in comparison to DiffServ [19]. MPLS allows for traffic prioritization on basis of different labels by incorporating RSVP-based resource reservation. Configuration of this combination of protocols involves considerable overhead as well [10].

SDN: The SDN controller directly controls traffic streams and configures network elements. Thus, fine-grained prioritization is established, selecting appropriate routes and queues. Queues can be set-up at the switches with different priorities, minimum and maximum data rates. Low priority traffic is re-directed dynamically or dropped in case of sudden network overload [4]. Also, applications are enabled to request service guarantees via the SDN controller's NBI [13]. Prioritization can be further advanced by the introduction of network slicing, which provides isolated slices of resources for different applications. One might argue, that SDN increases overall network latencies due to the involvement of the SDN controller. Yet, this delay occurs just initially during the set-up of new flow rules. Typically, in infrastructures such as the power system, established rules are changed only occasionally. Moreover, even the initial delay may be avoided if communication demands are conveyed in advance, so that static rules can be implemented at the switches before the actual transmission starts [13].

C. Security

Due to the threat posed by cyber attacks, secure transmission of critical data becomes extremely important for power system communications. In both, traditional and SDN-enabled net-

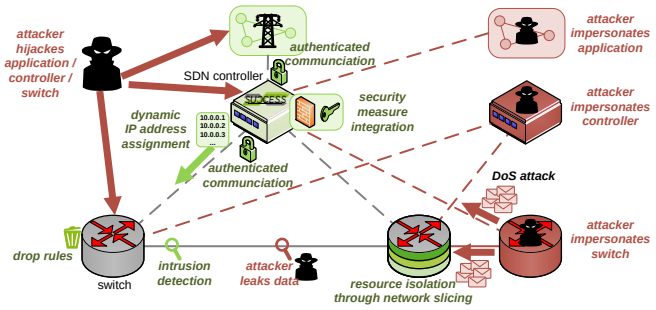

Figure 3: SDN-induced security breaches and measures

works, measures for authentication and encryption have to be taken. IEC 61850 applies the standard IEC 62351 for securing the transmission of critical data in power grids. This involves for example using Transport Layer Security (TLS) procedures and algorithms for the Transport Control Protocol (TCP)/IP-based Manufacturing Message Specification (MMS) service. As MAS communication relies on TCP/IP messaging as well, these security measures may be easily adopted. Hence, in the following, we focus on advantages and threats introduced by the SDN architecture [20][21], visualized in Fig. 3.

SDN-induced security threats: Potential vulnerabilities of the SDN architecture are the controller itself, as well as its connections to network devices and external applications. First of all, an attacker may impersonate the SDN controller, gaining direct access to network resources. Thus, flow rules and resulting network behavior could be modified. To avoid this threat, protocols such as TLS need to be applied, ensuring that only rules from authorized controllers are accepted by switches. The use of TLS is proposed by the OF specification already. However, since it is an optional feature, it has not been widely adopted yet [20]. Second, controllers or switches can be hijacked by attackers, resulting in comparable consequences as above. Multiple controller instances, which should be deployed for high availability regardless, help mitigate this issue. Thus, suspicious behavior of controllers and switches can be detected, decisions may be double-checked and malicious devices excluded from network control. Also, applications such as the MAS may be compromised or malicious ones can be introduced to influence network behavior. To forgo this issue, prior authentication of applications can be demanded. Further, permissions may be limited and applications' activity checked against a log of malicious processes. Using a man-in-the-middle attack, an attacker can intercept the communication between switches, controllers and applications. Again, device authentication is the key to prevent successful attacks. Data leakages may help attackers to determine network behavior and deduce flow rules. According to [20], no effective solutions have been proposed for resolving this issue. Finally, Denial-of-Service (DoS) attacks endanger reliable communication infrastructure operation and hence the power system. If switches or controllers are flooded with requests, they may collapse, rendering parts of the network inoperable. To preclude such situations, the number of requests, sent to the controller, can be limited. The controller may check the validity of source addresses and install rules to drop packets from invalid sources. Also, virtualized controller instances can be scaled according to network load, potentially minimizing the impact of DoS attacks.

SDN-induced security advantages: Despite these threats, SDN may improve communication network security. In particular, the SDN controller's global view and its capability to determine network behavior can help identify and mitigate attacks. By integrating existing intrusion detection systems, the SDN controller is enabled to recognize and mitigate malicious patterns. This includes for example machine learning approaches to detect anomalies. Hence, the impact of attacks such as DoS or worm propagation can be diminished by installing drop rules at the network devices. Firewall applications for checking packets can be integrated into the SDN controller, avoiding additional components and middle boxes. By assigning virtual IP addresses dynamically, the controller can protect network devices. Thus, actual addresses are hidden, complicating target identification for the attacker. The SDN controller may also establish fine-grained access control by authenticating switches, hosts and applications. Being based on isolating network resources, SDN-enabled slicing may not only ensure hard service guarantees, but also prevent unauthorized access. Finally, due to its programmability the SDN controller can adapt to new security issues quickly.

D. Multicast

Multicast deals with the joint transmission of packets to multiple destinations, by using common paths as long as possible. Thus, network load can be reduced massively. This technique is essential for the transfer of measurement, status and command messages in IEC 61850 substation environments. It can be extremely useful for the exchange of information within groups of control agents as well.

Legacy: In traditional IP networks, the most common approach for publishing information to user or device groups is the application of Virtual Local Area Networks (VLANs). Therefore, inefficient broadcast transmission is used within the respective VLAN, which is identified by the VLAN tag in Ethernet packets. However, efforts for the set-up and management of VLAN groups are comparably high.

SDN: Multicast transmission of packets is facilitated significantly by SDN. Applications may use the SDN controller's NBI to define groups of devices for participating in multicast along with patterns for identifying corresponding packets. In contrast to VLAN-based multicast, patterns are arbitrary, i.e. any packet header field may serve for multicast identification. For example typical fields, such as MPLS or VLAN tags, can be used, but also very general patterns like IP source addresses are applicable. Definitions of multicast groups are stored at the controller, which determines optimal routing trees and establishes corresponding rules at the devices within the network. Thus, administration effort is minimized, while group definitions can be adapted flexibly.

E. Configuration

Configuration efforts play a major role in the choice of communication solutions as these affect directly the Operational

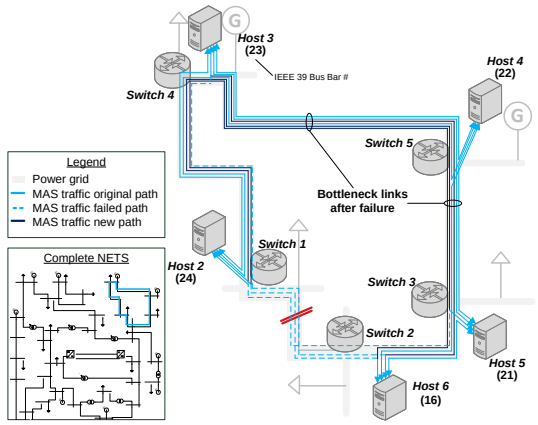

Figure 4: ICT infrastructure mapping of excerpt from NETS

Expenditures (OPEX) of the infrastructure.

Legacy: Overhead for administration and configuration is comparably small in traditional IP networks. Yet, as lined out previously, such infrastructures are designed for best effort transmissions. Hence, neither hard service guarantees nor sufficient fault tolerance can be provided without integrating additional protocols. These measures for prioritization, fast recovery and security, however, demand high efforts for configuration and continuous administration.

SDN: Compared to best effort IP networks, the set-up of the SDN controller requires additional configuration. Nevertheless, these efforts are significantly lower than those of decentralized approaches such as MPLS as all measures are concentrated at the SDN controller. Therefore it is sufficient to implement software modules at the controller, which configure and interact with switches remotely. Also, the NBI enables convenient access for external applications. Hernandez-Valencia *et al.* estimate that SDN in combination with Network Function Virtualization (NFV) allows for reductions of network operation efforts in the range of 14 to 31 % [22].

V. Case Study: Smart Grid Prioritization

This case study serves to support the above-discussed comparison between SDN-based and legacy infrastructures empirically, using the example of prioritizing MAS traffic.

A. Application Scenario

An excerpt from the IEEE 39 bus system / NETS, a well-established reference power grid, is used as scenario for the case study, as shown in Fig. 4. We assume a fiber-optic network, matching the power system with communication links being carried along power lines. Agents, situated at substations 16, 21, 22, 23, 24 collaborate to control the corresponding part of the grid. Hence, measurement and status data is exchanged between these agents. Due to an outage of the power line between substations 16 and 24, the agents need to coordinate counter measures, increasing communication demands significantly. Yet, simultaneous to the power line failure, the associated communication link is disrupted as well. Subsequently, all traffic is shifted to the remaining network links, causing network overload on the consecutive links between substations 21,22 and 23.

B. Testing Environment

The testing environment, used for experimental validation of our algorithms, consists of three separate networks. The data network is deployed for actual data transmissions between distributed agents. It consists of five 48 port Pica 3297 baremetal switches (bSwitches), running PicOS 2.6.32. In the SDN case Open vSwitch (OVS) v2.3.0 is used as OF-enabled switch on top, whereas in the legacy scenario the switches are operated in layer 2/3 mode. The switches connect five Intel Celeron J1900, equipped with a two port I210-LM NIC each, which host the agents of the MAS. The MAS is created on basis of the Java Agent DEvelopment (JADE) framework [23], which conforms to FIPA [8] specifications and includes libraries to facilitate the implementation and deployment of agent systems. For measurement orchestration and configuration the hosts are connected to a separate management network. The third network is applied for the SDN case only, establishing connectivity between the switches and the SDN controller. The latter is realized by our Software-Defined Universal Controller for Communications in Essential Systems (SUCCESS) framework (forked from the Java-based Floodlight controller [24]), which we tailored to the specific requirements of Smart Grid communications [13]. OF v1.3 is used for controller-switch interaction.

C. Evaluation Results

Fig. 5 compares the performance of legacy and SDN-enabled infrastructures, before and after the simultaneous failure of power line and communication link between substations 16 and 24. Under normal network conditions, MAS messages, transmitted between these two substations, experience a mean delay of about 350 μs, independent of the applied network technology. After the failure, however, delay increases to more than 10 s in the legacy case as the network is overloaded and no appropriate prioritization mechanisms are available. In contrast, latencies increase only slightly if SDN-based dynamic prioritization and queuing are applied.

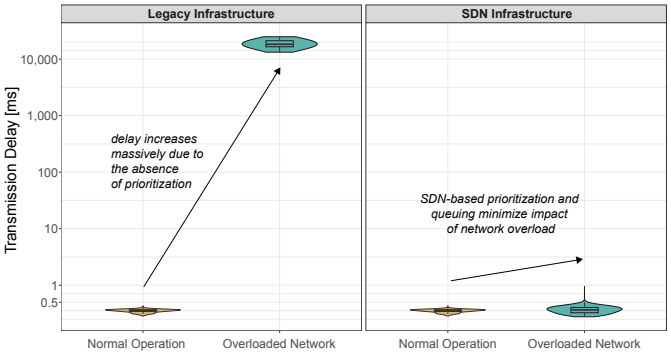

Figure 5: Impact of different network conditions on the fulfillment of MAS service requirements in legacy and SDN-enabled infrastructures

VI. Conclusion and Outlook

In this paper, we evaluated adequate communication solutions for distributed, real-time control of power grids. In contrast to centralized control systems, Multi-Agent Systems adapt quickly to changing grid conditions, while reducing calculation complexity. However, such a system relies on coordination and regular exchange of status and measurement data between the agents. Therefore, communication infrastructures are required, which are able to fulfill several different service requirements.

Table I: Comparison of MAS communication solutions considering different service criteria

Service Criteria	Best Effort IP network	MPLS-based network	SDN-enabled infrastructure
Topology Detection	○	○	+
Reliability: Fast Recovery	-	+	+
Reliability: Prioritization	○	+	+
Security	○	○	○
Multicast	○	○	+
Configuration	+	-	+

Table I summarizes these criteria and compares their realization in best effort IP, MPLS-based and SDN-enabled infrastructures. It becomes obvious that best effort IP networks are inferior to the other two solutions, in particular with regard to reliability, which was shown in an empirical case study. Network security may be enhanced significantly by integrating detection and mitigation mechanisms into the SDN controller, yet the SDN concept entails different threats. Compared to MPLS, the performance of SDN is similar regarding most criteria, though significantly less configuration efforts are required. Due to its centralized approach, new algorithms and fixes can be deployed more easily compared to legacy fixed-function networks, making SDN future proof.

In subsequent work, we aim at analyzing the impact of different communication solutions from the power system point-of-view. Also, advanced security measures will be integrated into our SUCCESS framework.

Acknowledgement

This work has been carried out in the course of research unit 1511 *'Protection and control systems for reliable and secure operations of electrical transmission systems'*, funded by the German Research Foundation (DFG) and the Franco-German Project *BERCOM* (FKZ: 13N13741) co-funded by the German Federal Ministry of Education and Research (BMBF).

References

[1] X. Fang, S. Misra, G. Xue and D. Yang, 'Smart Grid - The New and Improved Power Grid: A Survey', *IEEE Comm. Surveys and Tutorials*, vol. 14, no. 4, pp. 944–980, 2012.

[2] Y. Yan, Y. Qian, H. Sharif and D. Tipper, 'A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges', *IEEE Comm. Surveys and Tutorials*, vol. 15, no. 1, pp. 5–20, 2013.

[3] L. Robitzky, S. Dalhues, M. Albrecht, S. C. Müller, U. Häger and C. Rehtanz, 'Agent-based prevention of voltage collapse in electrical transmission systems', in *Power Sys. Comp. Conf. (PSCC)*, Jun. 2016, pp. 1–7.

[4] N. Dorsch, F. Kurtz, H. Georg, C. Hägerling and C. Wietfeld, 'Software-Defined Networking for Smart Grid Communications: Applications, Challenges and Advantages', in *IEEE Int. Conf. on Smart Grid Comm.*, Nov. 2014, pp. 422–427.

[5] W. Zhang, W. Liu, X. Wang, L. Liu and F. Ferrese, 'Distributed Multiple Agent System Based Online Optimal Reactive Power Control for Smart Grids', *IEEE Trans. on Smart Grid*, vol. 5, no. 5, pp. 2421–2431, Sep. 2014.

[6] S. R. Islam, K. M. Muttaqi and D. Sutanto, 'Multi-agent receding horizon control with neighbour-to-neighbour communication for prevention of voltage collapse in a multi-area power system', *IET Generation, Transmission Distribution*, vol. 8, no. 9, pp. 1604–1615, Sep. 2014.

[7] S. D. J. McArthur *et al.*, 'Multi-Agent Systems for Power Engineering Applications - Part I and II', *IEEE Trans. on Power Sys.*, vol. 22, no. 4, pp. 1743–1759, Nov. 2007.

[8] *FIPA Specifications*, Foundation for Intelligent Physical Agents, 2009. [Online]. Available: http://www.fipa.org.

[9] F. Perkonigg, D. Brujic and M. Ristic, 'MAC-Sim: A multi-agent and communication network simulation platform for smart grid applications based on established technologies', in *IEEE Int. Conf. on Smart Grid Comm. (SmartGridComm)*, Oct. 2013, pp. 570–575.

[10] A. Sydney, J. Nutaro, C. Scoglio, D. Gruenbacher and N. Schulz, 'Simulative Comparison of Multiprotocol Label Switching and OpenFlow Network Technologies for Transmission Operations', *IEEE Trans. on Smart Grids*, vol. 4, no. 2, pp. 763–770, 2013.

[11] A. Cahn, J. Hoyos, M. Hulse and E. Keller, 'Software-Defined Energy Communication Networks: From Substation Automation to Future Smart Grids', in *IEEE Int. Conf. on Smart Grid Comm.*, 2013, pp. 558–563.

[12] H. Maziku and S. Shetty, 'Software Defined Networking enabled resilience for IEC 61850-based substation communication systems', in *Int. Conf. on Comp., Networking and Comm. (ICNC)*, Jan. 2017, pp. 690–694.

[13] N. Dorsch, F. Kurtz, S. Dalhues, L. Robitzky, U. Häger and C. Wietfeld, 'Intertwined: Software-defined communication networks for multi-agent system-based Smart Grid control', in *IEEE Inter. Conf. on Smart Grid Comm. (SmartGridComm)*, Nov. 2016, pp. 254–259.

[14] D. Awduche, L. Berger, D. Gan, T. Li, V. Srinivasan and G. Swallow, *RSVP-TE: Extensions to RSVP for LSP Tunnels*, Internet Engineering Task Force (IETF), 2001. [Online]. Available: https://tools.ietf.org/html/rfc3209.

[15] D. Katz and D. Ward, *Bidirectional Forwarding Detection (BFD) for Multihop Paths*, Internet Engineering Task Force (IETF), 2010. [Online]. Available: https://tools.ietf.org/html/rfc5883.

[16] Y. Lei, C.-H. Lung and A. Srinivasan, 'A Cost-Effective Protection and Restoration Mechanism for Ethernet Based Networks: an Experiment Report', in *Wkshp. on High Performance Switching and Routing*, 2004, pp. 350–354.

[17] N. Dorsch, F. Kurtz, F. Girke and C. Wietfeld, 'Enhanced Fast Failover for Software-Defined Smart Grid Communication Networks', in *IEEE Global Comm. Conf. (GLOBECOM)*, Dec. 2016, pp. 1–6.

[18] *IEC 61850: Communication Networks and Systems for Power Utility Automation*, International Electrotechnical Commission TC57.

[19] S. Shioda and K. Mase, 'Performance comparison between IntServ-based and DiffServ-based networks', in *IEEE Global Comm. Conf. (GlOBECOM)*, vol. 1, Dec. 2005, pp.–534.

[20] S. Scott-Hayward, S. Natarajan and S. Sezer, 'A Survey of Security in Software Defined Networks', *IEEE Comm. Surveys Tutorials*, vol. 18, no. 1, pp. 623–654, Firstquarter 2016.

[21] S. Shin, L. Xu, S. Hong and G. Gu, 'Enhancing Network Security through Software Defined Networking (SDN)', in *25th Int. Conf. on Comp. Comm. and Networks (ICCCN)*, Aug. 2016, pp. 1–9.

[22] E. Hernandez-Valencia, S. Izzo and B. Polonsky, 'How will NFV/SDN transform service provider OpEx?', *IEEE Network*, vol. 29, no. 3, pp. 60–67, May 2015.

[23] F. Bellifemine, A. Poggi and G. Rimassa, 'JADE - A FIPA-compliant agent framework', *Proceedings of PAAM*, vol. 99, no. 97–108, pp. 33–45, 1999.

[24] *Floodlight Controller Version 1.0*, Project Floodlight, 2015. [Online]. Available: http://www.projectfloodlight.org/floodlight/.