CREDC
CYBER RESILIENT ENERGY
DELIVERY CONSORTIUM

Research Activity
Fact Sheet

Advanced Networking for Reliable Energy Delivery Systems

Website: http://cred-c.org/researchactivity/anreds

Researchers (Illinois/OSU): Sibin Mohan (Illinois), Rakesh Bobba (OSU), Smruti Padhy (Illinois, now at MIT), Rakesh Kumar (Illinois), Monowar Hasan (Illinois), Ashish Kashinath (Illinois), Rafid Al-Mahdi (OSU)

Industry Collaboration:

- Currently seeking industry collaborators who make computing and networking equipment for EDS
- Also looking for collaborators from national labs, power companies, etc., to test deployment.

Description of research activity: This activity is split into two distinct, yet related projects. Software Defined Networking (SDN) can help improve the security of networks in energy delivery systems – SDN provides a global view and mechanisms to manage flows as a whole (instead of individual packets at each router/switch). This enables the creation and management of carefully pre-engineered paths for packet flows in control networks as is being demonstrated in a related SDN project in collaboration with SEL. However, there are concerns about network consistency during security-incident induced updates (e.g., redirecting flows around areas of a network thought to be compromised, or under DDOS attack.) Further, SDNs still do not support provision of end-to-end real-time quality-of-service (QoS) that is needed to ensure on-time delivery of real-time messaging. Existing real-time QoS mechanisms in literature do not have the manageability that SDNs bring. Current state of the practice for ensuring reliable and timely delivery of critical control packets is mostly achieved through over-provisioning. In this activity, we aim to design and develop dynamic real-time QoS mechanisms for EDS control networks that are using SDN. Hence, we will develop mechanisms, algorithms and protocols for achieving QoS with real-time (i.e. end-to-end delay) guarantees and prioritization. Further, we will also investigate how to maintain isolation guarantees, especially among critical and non-critical flows during changes in the network (disruptions, failures, configuration changes etc.) These are essential for network resiliency, where non-critical connectivity services gracefully degrade in the face of security disruptions, but the network provides essential functions throughout the security incident.

How does this research activity address the Roadmap to Achieve Energy Delivery Systems Cybersecurity?
This work will help develop and implement new protective measures to reduce risk – by ensuring that timeliness of critical flows in EDS cannot be impacted by other flows/adversaries.

Summary of EDS gap analysis: Energy delivery systems lack guarantees for critical flows – in terms of end-to-end timeliness guarantees as well as maintaining the consistency of network flows when the system needs to be updated. This can impede the critical operations. Without such guarantees, the system may be vulnerable to multiple problems, for instance, *(a)* denial-of service attacks by an adversary, *(b)* sudden increases in debug/engineering flows (say due to failures or even due to adversarial activity), etc. As mentioned earlier, software-defined networks (SDNs) have unique properties that can help address such problems (the global visibility into the network for instance). Current SDN offerings though do not have this functionality yet. For instance, there is a lack of research in time-critical flows for EDS using SDNs. This research effort intends to fix this very gap.

Full EDS gap analysis: Most EDS require that network flows meet their end-to-end requirements. Without such resiliency guarantees, the correct operation of such systems could be at risk. Also, without the right safeguards in place (for the end-to-end requirements) malicious adversaries would impede the correct operation of such systems by preventing the network from providing the necessary guarantees. Such problems would fit into the “communications failures” as presented by the NESCOR failure scenarios document – in particular, DGM.2, DGM.7 and Generic.2 (along with AMI.18, WAMPAC.1, WAMPAC.11, ET.12, DR.1, Generic.1) [13]. In fact, one way to introduce instability in EDS would be to increase the amount of data pumped through the network for say, debugging/engineering traffic. While this could look like regular operation, a malicious adversary could increase such (and other) flows – this would then affect the end-to-end timing requirements for critical flows. Hence, we need to develop hardware/software mechanisms to isolate the critical flows and ensure that their end-to-end timing guarantees are met.

Current safety-critical systems often have separate networks (hardware and software) for the critical/non-critical of flows (for safety and sometimes security reasons). This leads to significant overheads (equipment, management, weight, *etc.*) and potential for errors/faults and even increased attack surface and vectors. Existing systems, *e.g.,* avionics full-duplex switched Ethernet (AFDX) [1], [3], [9], controller area network (CAN) [7], *etc.* that are in use in other critical domains are either proprietary, complex, expensive and might even require custom hardware. Even though AFDX switches ensure timing determinism, packets transmitted on such switches may be changed frequently at run- time when sharing resources (*e.g.,* bandwidth) among different networks [10]. In such situations, a dynamic configuration is required to route packets based on switch workloads and flow delays to meet all the high priority QoS (*e.g.,* end-to- end delay) requirements. In addition, AFDX protocols require custom hardware [4].

Heine *et al.* proposed a design and built a real-time middleware system, CONES (COnverged NEtworks for SCADA) [6] that enables the communication of data/information in SCADA applications over single physical integrated networks. That work leveraged some of the existing IP technologies such as Multiprotocol Label Switching (MPLS) and DiffServ for network resource reservation/management, and is based on iDSRT [11] that uses Earliest deadline first scheduling algorithm (EDF) for scheduling of network traffic and CPU time based on the deadline requirements.

There have been some prior attempts at provisioning SDNs with worst-case delay and bandwidth guarantees. Azodolmolky *et al.* proposed a NC-based model [2] for a single SDN switch that provides an upper bound on delays experienced by packets as they cross through the switch. Guck *et al.* used mixed integer program (MIP) based formulation [5] for provisioning end-to-end flows that provide delay guarantees – they do not provide a solution of what traffic arrival rate to allocate for queues on individual switches for a given end- to-end flow. A QoS-enabled management framework to allow end-to-end communication over SDN is proposed in literature [12]. It classifies flows into two levels, *i.e.,* QoS flow and best- effort. It uses flow priority and queue mechanism to obtain QoS control to satisfy the requirement.

While there exist some SDN offerings from industry that target this space [14], they still lack the mechanisms and protocols for offering end-to-end QoS guarantees for critical flows. The main focus (in terms of resiliency) in such switches is link failures and automatic backup path configurations.

All of the above related work has deficiencies in providing the right kinds of guarantees for critical network flows in energy delivery systems. Hence, we have started work on designing such a system using software-defined networking (SDN) [8].

Bibliography:

[1] ARINC Specification 664, Part 7, Aircraft Data Network, Avionics Full Duplex Switched Ethernet (AFDX) Network. 2003.

[2] S. Azodolmolky, R. Nejabati, M. Pazouki, P. Wieder, R. Yahyapour, and D. Simeonidou. An analytical model for software defined networking: A network calculus-based approach. In *Global Communications Con- ference (GLOBECOM), 2013 IEEE*, pages 1397–1402. IEEE, 2013.

[3] H. Charara, J. L. Scharbarg, J. Ermont, and C. Fraboul. Methods for bounding end-to-end delays on an AFDX network. In *18th Euromicro Conference on Real-Time Systems (ECRTS'06)*, pages 10 pp.–202, 2006.

[4] C. M. Fuchs. The evolution of avionics networks from ARINC 429 to AFDX. *Innovative Internet Technologies and Mobile Communications (IITM), and Aerospace Networks (AN)*, 65, 2012.

[5] J. W. Guck and W. Kellerer. Achieving end-to-end real-time quality of service with software defined networking. In *Cloud Networking (CloudNet), 2014 IEEE 3rd International Conference on*, pages 70–76. IEEE, 2014.

[6] E. Heine, H. Khurana, and T. Yardley. Exploring convergence for SCADA Networks. In *ISGT 2011*, pages 1–8, Jan 2011.

[7] N. Instruments. Controller Area Network (CAN) Overview.

[8] Rakesh Kumar, Monowar Hasan, Smruti Padhy, Konstantin Evchenko, Lavanya Piramanayagam, Sibin Mohan,Rakesh B. Bobba. Dependable End-to-End Delay Constraints for Real-Time Systems using SDNs. arXiv:1703.01641 [cs.NI]

[9] I. Land and J. Elliott. Architecting arinc 664, part 7 (afdx) solutions. XILINX, 2009.

[10] Z. Li, Q. Li, L. Zhao, and H. Xiong. Openflow channel deployment algorithm for software-defined afdx. In *2014 IEEE/AIAA 33rd Digital Avionics Systems Conference (DASC)*, pages 4A6–1. IEEE, 2014.

[11] H. Nguyen, R. Rivas, and K. Nahrstedt. *iDSRT: Integrated Dynamic Soft Real-Time Architecture for Critical Infrastructure Data Delivery over WLAN*, pages 185–202. Springer Berlin Heidelberg, 2009.

[12] C. Xu, B. Chen, and H. Qian. Quality of service guaranteed resource management dynamically in software defined network. *Journal of Communications*, 10(11):843–850, 2015.

[13] National Electricity Sector Cybersecurity Organization Resource (NESCOR) Technical Working Group 1. Electric Sector Failure Scenarios and Impact Analysis.

[14] Schweitzer Engineering Laboratories (SEL). Software-Defined Network Switch. SEL 2740-S. https://selinc.com/products/2740S/