CSC7575 Reivew - Power Substation Network Dynamics

Rob Gillen

Main Contribution

This paper aims to study the actual behavior of SCADA network traffic at real-world power substations with the goal of confirming (or refuting) the current assumptions made by those designing security systems for those networks. The authors begin by explaining some of the challenges of research in the SCADA area (lack of real-world data, overrelaince on synthetic data and lack of validation of that synthetic data). They then describe their study which is a 3-year longitudinal study with an emphasis on a single substation and then a survey of the results from that station with two others.

The primary contributions of the paper are the data and models they present regarding the traffic on these systems. They highlight the inconsistencies of traffic, the underpoweredness of various embedded processors in the fielded systems and how, even in a heavily over-provisioned network environment there is great variability in the observed traffic patterns.

Related Problems Yet Unresolved

There are a handful of questions that arise when reading this paper. Some of these questions were addressed by the authors while others were not. Some of these include:

1. The authors hint that they feel they might be able to characterize and identify individual devices on the network purely by their behavior (response times, interaction patterns, etc.) quite similar notionally to what NMAP does for IT devices. This is an issue that should be expanded and studied as it would have broad implications if actually feasible.
2. The authors only studied a single company's networks. This leads one to wonder how much of the trouble they saw was simply due to the equipment that company had used, how they configured it, or some other factor. They acknowlege this as a weakness and indicate that they would like to do more, but that is still outstanding.
3. An indepth study of the devices that are producing the variance in response is warrented. The authors make a solid case for their assertion of the source, but it would be adantageous to confirm this emperically by studying the devices directly (rather than indrectly via their network traffic footprint).

Strengths/Weaknesses

The fact that the authors were able to monitor a powerstation for such a long period of time is a great thing and provides great insight to the research community. Adding to this that they were able to compare the results from that station with that of others is also of great benefit.

The fact that these were all from the same operations company is a weakness... being able to compare/contrast across multiple companies would lend credence (or not) as to the generalizeability of their results. As it stands, you are left wondering if this is a mistake or symptomatic only of issues at that one company.

The fact that there were network upgrades/infrastructure changes during their monitoring period is also a strength. This adds additional value to their results especially those that remained constant regardless of those changes.

Additional Publications by the Same Author(s)

The following are more recent papers by the author, though none of them are directly related to traffic modeling.

- David Formby, Milad Rad, and Raheem Beyah. Lowering the Barriers to Industrial Control System Security with GRFICS. To appear in the USENIX Workshop on Advances in Security Education (ASE), Baltimore, Maryland, August 2018.
- Qinchen Gu, David Formby, Shouling Ji, Hasan Cam, and Raheem Beyah. "Fingerprinting for Cyber Physical System Security: Device Physics Matters Too." To appear in the IEEE Security & Privacy Magazine.
- Celine Irvene, Samuel Litchfield, David Formby, and Raheem Beyah. "HoneyBot: A Honeypot for Robotic Systems." Proceedings of the IEEE, Vol. 106, Issue 1, Jan. 2018.
- Xiaojing Liao, Preethi Srinivasan, David Formby, and Raheem Beyah. "Di-PriDA: Differentially Private Distributed Load Balancing Control for the Smart Grid." IEEE Transactions on Dependable and Secure Computing, 2017.
- Samuel Litchfield, David Formby, Jonathan Rogers, Sakis Meliopoulos, and Raheem Beyah. "Rethinking the Honeypot for Cyber-Physical Systems." In the IEEE Internet Computing Magazine - Special Issue on Cyber-Physical Security and Privacy, Vol. 20, No. 5, Sept.-Oct. 2016.

Review Questions

- According to the paper, the assertion that SCADA network traffic is consistent and reliable (in contrast to IT network traffic). [True/False]

  FALSE. This is the most important take-away from the paper.

- To what do the authors attribute the largest aspect of the systems instability?

  Underpowered/mis-configured embedded systems attempting to handle IP/network stacks

- How many power substations were studied in this paper? How many different power companies?

  3, 1