Enhancing Cybersecurity in Electrical Power Substations via Cross-Substation Transfer Learning

Filip Natvig
Dept. of Electrical Engineering
Uppsala University
Uppsala, Sweden
filip.natvig@angstrom.uu.se

Göran N. Ericsson
Dept. of Electrical Engineering
Uppsala University
Uppsala, Sweden
goran.n.ericsson@uu.se

Lars Nordström
Div. of Electric Power and Energy Systems
KTH – Royal institute of technology
Stockholm, Sweden
larsno@kth.se

As the demand for electricity continues to rise, efficient management and control of electrical infrastructure become increasingly critical, leading to a rapid adoption of digital technologies within power systems. Central to this evolution is the IEC 61850 standard, which significantly influences the design, operation, and interoperability of substation automation systems (SAS). However, the gradual integration of this standard presents new challenges, particularly concerning information security.

Research indicates that within the communication network of IEC 61850 SAS, data availability emerges as a primary concern when contrasted with integrity and confidentiality. This underscores the urgent need to address threats such as Denial of Service (DoS). In response, numerous studies have proposed Intrusion Detection Systems (IDSs) tailored for IEC 61850 SAS, aligning with the recommendations of the IEC 62351 standard.

The majority of these proposed detection systems utilize anomaly-based methods, renowned for their effectiveness in detecting zero-day attacks by analyzing deviations from normal behavior. However, a significant challenge lies in compiling comprehensive datasets, partly due to the diverse array of potential substation states and the cost associated with building authentic IEC 61850 test rigs.

Recognizing these challenges, there's a growing interest in maximizing the utility of existing data. Rather than focusing solely on creating extensive new datasets from individual substations, a more efficient approach could be to leverage the wealth of information already collected from other substations.

Building upon this premise, our study investigates a novel approach to enhancing IDS performance across different substations. Specifically, we explore the feasibility of transferring knowledge gained from network traces captured in one substation to improve an IDS tailored for another substation with a different architecture.

Preliminary results indicate promising outcomes. Statistical analyses confirm that the improvement in IDS accuracy achieved through transfer learning is statistically significant, with a confidence level of more than 99.9%, highlighting its prospects in fortifying cybersecurity defenses against DoS attacks targeting IEC 61850 SASs.