Cyber Security Concerns for Dynamic Line Rating

Addressing the security challenges of making a smarter grid

Owen Parkins
New Mexico Institute of Mining and Technology
Mentor: Jake Gentle (D520)

Overview

- Dynamic Line Rating (DLR) increases the ampacity of transmission lines due to environmental conditions (Bhattarai, 2018).
- Requires weather data to be collected and transmitted.
- Needs the data to be secure to prevent a malicious adversary from manipulating it.

Objectives

- Identify and create a mitigation plan for the vulnerable points that are present in a system that uses DLR (see figure 1).
- The scope is limited to the DLR data processor only. Securing field sensors and operator terminals is not in the scope.

Process

- The threat statement was determined to include all threats except for a malicious insider.
- Possible attack vectors were identified, and mitigation plans were prepared.

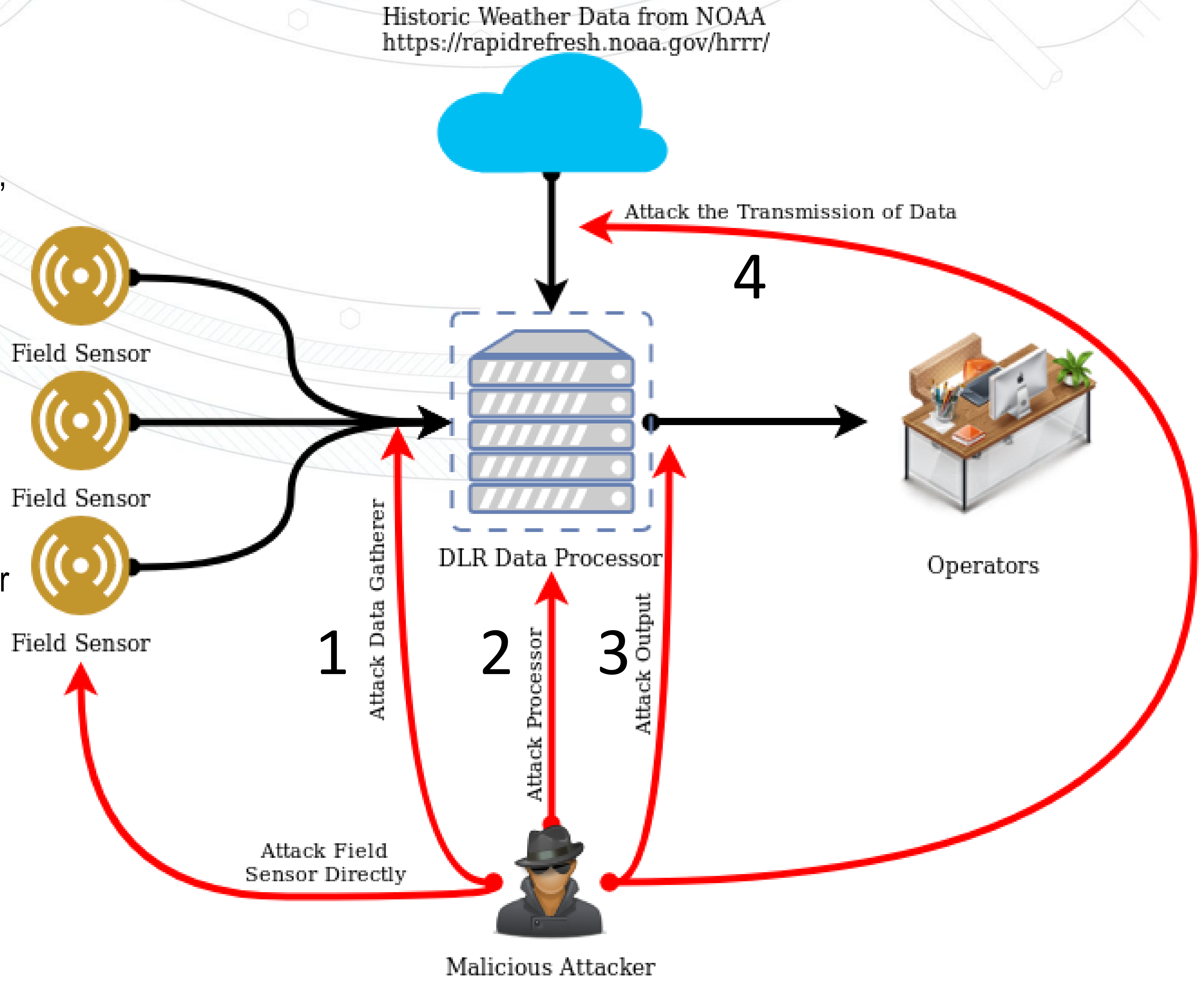

Figure 1) This diagram shows the flow of data through a DLR system with the black arrows. The red arrows show possible attack vectors that a malicious attacker could use to disrupt or influence the DLR system. Not all possible attack vectors are shown. To simplify the diagram, other software packages that DLR systems implement are not shown.

References:
B. P. Bhattarai *et al.*, "Improvement of Transmission Line Ampacity Utilization by Weather-Based Dynamic Line Rating," in *IEEE Transactions on Power Delivery*, vol. 33, no. 4, pp. 1853-1863, Aug. 2018.
R. Langner, "Stuxnet: Dissecting a Cyberwarfare Weapon," in *IEEE Security & Privacy*, vol. 9, no. 3, pp. 49-51, May-June 2011.

Security Concerns and Mitigations

- Inserting fake data (See Point 1 on Figure 1) could make the calculated ampacity rating too high for safe operations. An anomaly detection system can be used to detect the falsified data.
- The executable will be signed to prevent unauthorized modifications (See Point 2), and the machine will verify the signatures before running the executable. The Stuxnet attack happened because code was not signed (Langer, 2011).
- By only allowing the DLR Data Processor account write access to the output directories, it prevents bad data from being sent to the operators (See Point 3). Adding another anomaly detection system can add a layer of protection.
- Manipulating the historic weather data source (See Point 4) could be easier than directly manipulating the DLR system. The external system should be upgraded to provide integrity services by signing the checksums of the data. The Linux repository system uses this methodology.

Future Work

Ensuring that these concerns are handled properly in running systems and looking at a wider scope would increase the overall security of the system.