Signals from distant lightning could help secure electric substations

26 February 2019

Georgia Tech researchers Tohid Shekari, Raheem Beyah, Morris Cohen, and Lukas Graber hold an antenna and home-built recording equipment for the VLF radio receiver, known as AWESOME, which is capable of detecting lightning radio bursts from around the world. Credit: Christopher Moore, Georgia Tech

Side channel signals and bolts of lightning from distant storms could one day help prevent hackers from sabotaging electric power substations and other critical infrastructure, a new study suggests.

By analyzing electromagnetic signals emitted by substation components using an independent monitoring system, security personnel could tell if switches and transformers were being tampered with in remote equipment. Background lightning signals from thousands of miles away would authenticate those signals, preventing malicious actors from injecting fake monitoring information into the system.

The research, done by engineers at the Georgia Institute of Technology, has been tested at substations with two different electric utilities, and by extensive modeling and simulation. Known as radio frequency-based distributed intrusion detection system (RFDIDS), the technique will be described February 26 at the 2019 Network and Distributed System Security Symposium (NDSS) in San Diego.

"We should be able to remotely detect any attack that is modifying the magnetic field around substation components," said Raheem Beyah, Motorola Foundation Professor in Georgia Tech's School of Electrical and Computer Engineering. "We are using a physical phenomenon to determine whether a certain action at a substation has occurred or not."

Opening substation breakers to cause a blackout is one potential power grid attack, and in December 2015, that technique was used to shut off power to 230,000 persons in the Ukraine. Attackers opened breakers in 30 substations and hacked into monitoring systems to convince power grid operators that the grid was operating normally. Topping that off, they also attacked call centers to prevent customers from telling operators what was happening.

"The electric power grid is difficult to secure because it is so massive," Beyah said. "It provides an electrical connection from a generating station to the appliances in your home. Because of this electrical connection, there are many places where a hacker could potentially insert an attack. That's why we need an independent way to know what's happening on grid systems."

That independent approach would use an antenna located in or near a substation to detect the unique radio-frequency "side channel" signatures produced by the equipment. The monitoring would be independent of systems now used to monitor and control the grid.

"Without trusting anything at all on the grid, we can use an RF receiver to determine if an impulse occurred in the shape of an 'open' operation,"

Beyah said. "The system operates at 60 Hertz, and there are few other systems that operate there, so we can be sure of what we're monitoring."

However, hackers might be able to figure out how to insert fake signals to hide their attacks. That's where the lightning emissions known as "sferics" come in.

"When a lightning flash hits the ground, it forms an electrical path miles tall, potentially carrying hundreds of thousands of amps of current, so that makes for a really powerful antenna radiating energy," said Morris Cohen, an associate professor in the Georgia Tech School of Electrical and Computer Engineering. Each flash creates signals in the very low frequency (VLF) band, which can reflect from the upper atmosphere to travel long distances.

"Signals from lightning can zigzag back and forth and make it all the way around the world," Cohen noted. "Lightning from South America, for example, is easily detectable in Atlanta. We've even seen lightning echo multiple times around the world."

Security staff remotely monitoring substations would be able compare the lightning behind the 60 Hz substation signals to lightning data from other sources, such as one of the 70,000 or so other substations in the United States or a global lightning database. That would authenticate the information. Since lightning occurs more than three million times every day on average, there is plenty of opportunity to authenticate, he noted.

"Even if you could synthesize the RF receiver's data feed digitally, generating something realistic would be difficult because the shape of the pulse from lightning detected by our receivers varies as a function of the distance from the lightning, the time of day, latitude and more," Cohen said. "It would take a lot of real-time computation and knowledge of sophisticated physics to synthesize the lightning signals."

Working with two different electric utilities, the researchers—including graduate research assistant Tohid Shekari—analyzed the RF signals produced when breakers were turned off for substation maintenance. They also used computer simulations to study a potential attack against the systems.

"The signal from a lightning stroke is very distinct—it is short, around a millisecond, and covers a huge frequency range," Cohen added. "The only other process on Earth that is known to generate something similar is a nuclear explosion. The emissions from the power grid are very different and none of it looks like a pulse from lightning, so it is easy enough to separate the signals."

The researchers have filed a provisional patent on RFDIDS, and hope to further refine the security strategy, which independent of equipment manufacturer. Beyah believes there could be applications beyond the power industry for remote monitoring of other RF-emitting devices. The system could tell transit operators if a train were present, for example.

"The power grid is our most critical piece of infrastructure," Beyah notes. "Nothing else matters if you don't have electrical power."

In addition to those already mentioned, the research team also included recent master's degree graduate Christian Bayens and assistant professor Lukas Graber, both from Georgia Tech.

More information: Tohid Shekari, et al., "RFDIDS: Radio Frequency-based Distributed Intrusion Detection System for the Power Grid," (2019 Network and Distributed System Security Symposium).

Provided by Georgia Institute of Technology