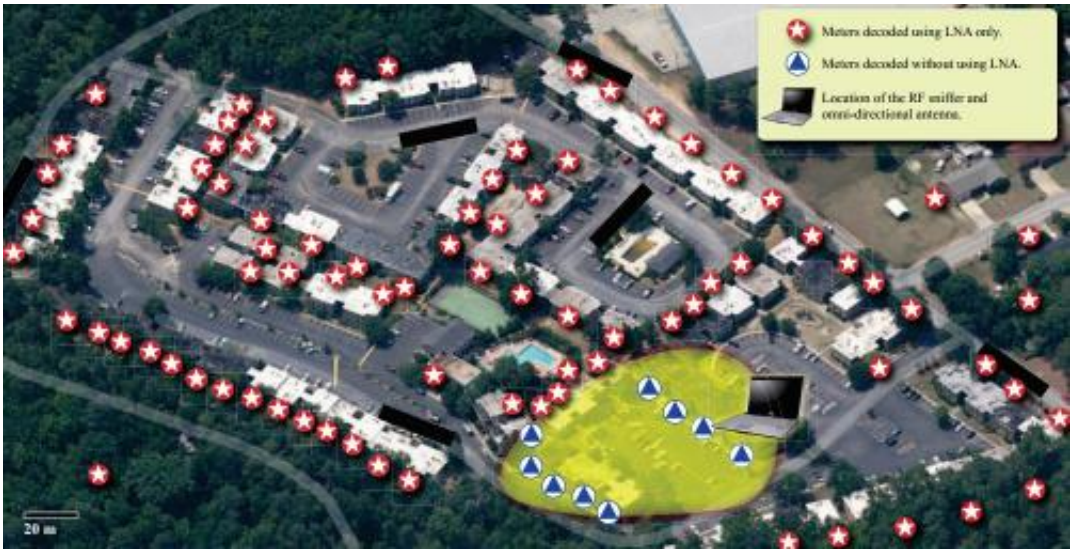
Automated meter reading systems make life easy for intruders

October 20 2012, by Nancy Owano



An aerial view of the neighborhood where the researchers performed their eavesdropping experiments. Each blue triangle or red star represents a group of four or five meters mounted in a cluster on an exterior wall. Using an LNA and a 5 dBi omnidirectional antenna, they were able to monitor all meters in the neighborhood. Some sniffed meters may be out of the scope of this view. Credit: Ishtiaq Rouf et al.

(Phys.org)—Intruders of the break-in and snooping variety have their work cut out for them by just picking up wireless signals that are broadcast by utility meters, say researchers from the University of South Carolina at Columbia, IEEE and Rutgers. As with many other technological advances that bring new pathways for criminals, advances

in meters have created concerns about intrusions. Millions of analogue meters to measure water, gas and electricity consumption have been replaced by automated meter reading (AMR) in the U.S. The newer method enables devices to broadcast readings by radio every 30 seconds for utility company employees to read as they walk or drive around with a receiver.

Intruders can tune into the same information, however, according to Ishtiaq Rouf and his colleagues, authors of a paper that delivers a security analysis of AMR systems.

More than 40 million meters in the United States have been equipped with AMR technology over the past years. The smart meters collect energy consumption data which could reveal sensitive personal information from homes, they said. Because energy usage often drops to near zero when a house is empty, the readings could be used to identify which owners are at work or traveling. Their work shows that currently deployed AMR systems are vulnerable to spoofing attacks and privacy breaches. The research was presented earlier this week at the 19th ACM Conference on Computer and Communications Security, which ran from October 16 to 18 in Raleigh, North Carolina.

The AMR meters that they studied make data publicly available over unsecured wireless transmissions. "They use a basic frequency hopping wireless communication protocol and show no evidence of attempting to ensure confidentiality, integrity, and authenticity of the data," added the research team.

They picked up transmissions from AMR meters operated by companies. They said that the communication protocol can be reverse-engineered with only a few days of effort. They made use of radio equipment and information available through online tutorials. They used software radio equipment publicly available for about $1,000 (GNU

Radio with the Universal Software Radio Peripheral). "We were able to both eavesdrop on messages as well as spoof messages to falsify the reading captured by a commonly used 'walk-by' reader," they said. Through wireless monitoring, they harvested consumption data from 485 meters within a 300m radius region.

As remedies, the authors suggested alternative schemes based on defensive jamming, which they said may be easier to deploy than upgrading meters themselves. Jamming could protect against the leakage of legacy devices and requires no modification of the deployed meters.

More information: Research paper: www.winlab.rutgers.edu/~grutes … ers/fp023-roufPS.pdf

via Newscientist