

Jamming LTE base stations easier than you may think

November 15 2012, by Nancy Owano



4G LTE single mode modem by Samsung. Credit: Wikipedia

(Phys.org)—This much everyone knows: As technologies break new ground in speed and performance, mischief-makers also break new ground in finding ways to disrupt. Now an academic research group has warned a U.S. government agency of their findings, which show that the LTE high-speed wireless data networks of today and tomorrow are vulnerable to a jamming technique that could destroy service across a city. They say it could take nothing more complex than a laptop and \$650 battery-operated radio unit aimed at portions of the LTE signal, to knock out an LTE base station, affecting large numbers of city residents.

Jeffrey Reed, director of wireless at Virginia Tech and graduate research assistant Marc Lichtman warned that any one of eight weaknesses in the LTE configuration, meaning eight different attacks are possible, can put a stop to all communications from a targeted base station.

The LTE signal is complex, made up of many subsystems. By taking out one subsystem, the entire base station goes with it. In spite of LTE's complexity, a [perpetrator](#) with the knowledge of a communications engineer could figure it out. As troubling, they pointed out that if an attacker added an inexpensive [power amplifier](#) to the rig, that person could take down an LTE [network](#) in a larger region.

The warning comes at a time of promotional ads touting speed paths possible with LTE. The term LTE stands for long-term evolution but the "long-term" seems just around the corner, with promoters saying that LTE is the choice high-bandwidth [mobile network](#) technology of today and tomorrow. Vendors of smartphones and carriers are promoting their intentions for a transition to LTE networks.

On November 7, Reed and Lichtman filed with the National Telecommunications and Information Administration, (NTIA) which advises the President on telecommunications and information policy issues.

The NTIA invited comments from experts on the feasibility of using LTE for the emergency responder initiative, First Responder Network Authority (FirstNet), as LTE has been proposed for next-generation systems for emergency response.

"If LTE technology is to be used for the air interface of the public safety network, then we should consider the types of jamming attacks that could occur five or ten years from now. It is very possible for radio jamming to accompany a terrorist attack, for the purpose of preventing

communications and increasing destruction," they wrote. They warned that terrorists could compromise an LTE network to confuse a response to an attack.

In the cover note to Lawrence Strickling, Assistant Secretary for Communications and Information, the US Department of Commerce, the researchers said the filing was a response to the FirstNet NOI (Notice of Inquiry) regarding the conceptual network architecture. "The focus on our comments is on the information assurance aspects of LTE and contains a summary of some of our preliminary analysis. This work is still in progress and we would be pleased to share details of our current and future findings on this issue."

More information: www.ntia.doc.gov/files/ntia/va_tech_response.pdf

via [TechnologyReview](#)

© 2012 Phys.org

Citation: Jamming LTE base stations easier than you may think (2012, November 15) retrieved 24 June 2024 from <https://phys.org/news/2012-11-lte-base-stations-easier.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--