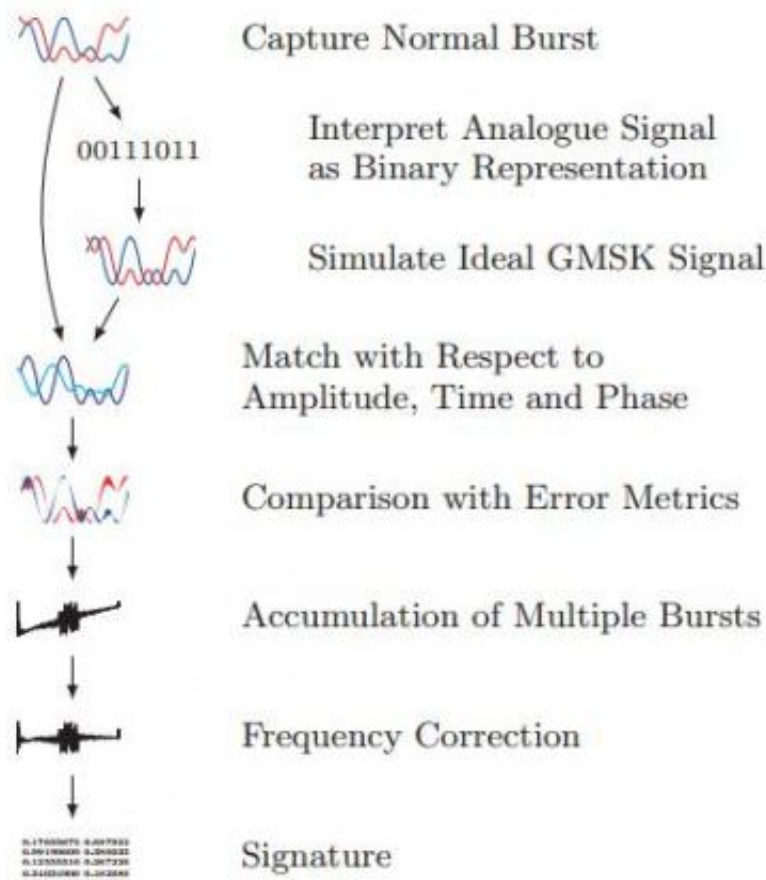


Engineers discover unique fingerprint for cell phones

August 2 2013, by Bob Yirka



Overall Procedure of Feature Extraction. Credit: Forensic Identification of GSM Mobile Phones, Jakob Hasse et al.

(Phys.org) —Law enforcement officials may soon have a new tool at their disposal—a device that can distinguish between cell phones based

on their digital signal. In the never ending game of cat-and-mouse between law enforcement and criminals, this new advancement may give the good guys the upper hand—all due to a discovery by a team of engineers in Germany.

The development of the cell phone has led to new advances in both law enforcement and criminal evasion. Police officers use cell phones to communicate with one another, as do criminals. It didn't take long, however, for the police to figure out that they could track criminals as they talk on their cell phones using triangulation of cell towers. To keep from getting caught, criminals began using new evasion tactics such as modifying the built-in ID code on their cell phone or swapping out SIM cards—doing so made it nearly impossible for [law enforcement](#) to track them down by their cell phone signals alone. This new advance by the engineers in Germany appears likely to thwart that strategy.

Working at the Technical University of Dresden, engineers Jakob Hasse, Thomas Gloe and Martin Beck found that each of the separate components inside a cell phone has a degree of error. When all of the errors are taken together, as seen in the digital signal sent to a cell tower, the result can be read as a unique digital signal—or fingerprint. That means that no matter what criminals do to their cell phone—short of swapping out internal components—their phones will continue to emit a unique signal that can be read by a device and used to separate it out from all the other [cell phone](#) signals. Once that's done the location of the phone—and possibly the [criminals](#)—can be calculated using triangulation of [cell towers](#).

Unfortunately, a device to read and recognize the unique signature of cell phones is still in the research and development stage, though the engineers on the project report a nearly 98 percent success rate in correctly identifying a signal. Law enforcement would surely like to see that number bumped to 100 to avoid finding themselves occasionally

raiding the wrong house.

More information: Forensic Identification of GSM Mobile Phones,
Jakob Hasse et al. ([PDF](#))

via [Newscientist](#)

© 2013 Phys.org

Citation: Engineers discover unique fingerprint for cell phones (2013, August 2) retrieved 19
April 2024 from <https://phys.org/news/2013-08-unique-fingerprint-cell.html>

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.