Detection of Malicious Base Station Attacks Through the Carrier Analysis

D. Fernández*(1), A. V. Alejos(1), and M. García Sánchez(1)
(1) Radio Systems, University of Vigo, Pontevedra, Spain

In 2G and 3G mobile standards there are vulnerabilities caused by the use of false Base Station (BS). In 3G security architecture offers protection against BS attacks, however when the User Equipment (UE) is configured in automatic GSM/3G mode this UE can accept connections coming from GSM/GPRS BSs that are configured as an attacker finally establishing a connection with such malicious BTS located within the UE's coverage area. Even without the use of a frequency jammer, potential attack danger exists because the connection between an UE and the fake BTS can be achieved if the BS is transmitting with more power than the real base station, and the UE enters in the handover process imposed by the 2G standard.

In this paper we explain how an attack from a false GSM/GPRS BTS can be detected in an early stage through the detection of the transmitted carrier given that it becomes distinguishable from actual carriers. We present measurements done with a spectrum analyzer valid to determinate if a carrier can be potentially malicious. A setup was configured using two carriers: one from an actual BTS at the frequency of 1845.2 MHz corresponding to the ARFCN 712, and the false BTS carrier working at 1863.8 MHz or equivalently ARFCN 805.

Although the receiver power level depends on the relative locations of the BTSs and the UE, the malicious BTS needs transmitting with large power, to be primarily detected. Two procedures can be used to determine the presence of the malicious BTS. A first way of detection is comparing time slots of Time Division Duplex (TDD) which remain empty for the fake BTS. The second form of detection is checking the power control of the signal. The signal from an actual BTS performs a power control loop, whilst the malicious BTS does not have this power control capability to force a handover by power, so it would be possible to determine that the carrier potentially belongs to an illegitimate carrier.

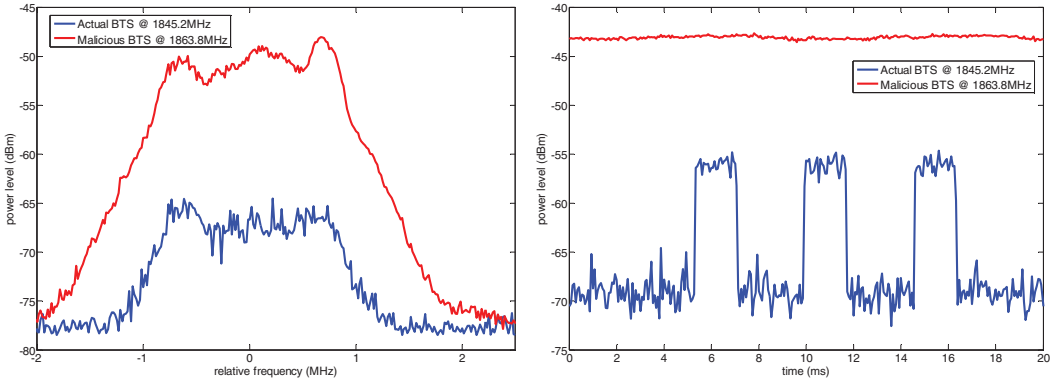

Fig. 1. Comparison of spectra and power control of actual and malicious BTSs.