

https://dspace.org/

An investigation into jamming GSM systems through exploiting weaknesses in the control channel forward error correction scheme

Timm, Gareth

2017

http://hdl.handle.net/10539/23620

Timm, Gareth Lloyd (2017) An investigation into jamming GSM systems through exploiting weaknesses in the control channel forward error correction scheme, University of the Witwatersrand, Johannesburg, http://hdl.handle.net/10539/23620

Downloaded from a DSpace repository. https://dspace.org/

Abstract

The ability to communicate effectively is of key importance in military scenarios. The ability to interfere with these communications is a useful tool in gaining competitive advantages by disrupting enemy communications and protecting allied troops against threats such as remotely detonated explosives. By reducing the number of corrupt bits required by using customised error patterns, the transmission time required by a jammer can be reduced without sacrificing effectiveness. To this end a MATLAB simulation of the GSM control channel forward error correction scheme is tested against four jamming methodologies and three bit corruption techniques. These methodologies are aimed at minimising the number of transmitted jamming bits required from a jammer to prevent communications on the channel. By using custom error patterns it is possible to target individual components of the forward error correction scheme and bypass others. A random error approach is implemented to test the system against random errors on the channel, a burst error approach is implemented to test the convolutional code against burst errors, and two proposed custom error patterns are implemented aimed at exploiting the Fire code's error detection method. The burst error pattern approach required the least number of transmitted jamming bits. The system also shows improvements over current control channel jamming techniques in literature.