Secure Communication Interface Design for IoT Applications, Using the GSM Network

Andrew Wightwick and Basel Halak
School of Electronics and Computer Science
Faculty of Physical Sciences and Engineering
University of Southampton, Southampton SO17 1BJ, United Kingdom

Abstract—In this work, a secure short messaging service (SMS)-based communication interface is designed. The interface has applications in the internet of things (IoT) such as machine to machine (M2M) communications, and human-operated remote system management. The case study of waking a personal computer remotely is considered, and a complete proof-of-conceptis implemented for this purpose, using a field-programmable gate array (FPGA)-based receiving device and an Android-based transmitting device. On the Android device, SMS messages are generated in software using a "rolling code" system based on linear feedback shift registers (LFSRs), then encrypted with the extended tiny encryption algorithm (XTEA) cipher. The FPGA employs both hardware XTEA decryption, and hardware systems to validate incoming messages.

Index Terms—decryption, encryption, FPGA, GSM, IoT, security