Proceedings of the 7th International Conference of Control Systems, and Robotics (CDSR'20)
~~Niagara Falls, Canada~~ Virtual Conference – November, 2020
Paper No. 127
DOI: 10.11159/cdsr20.127

Covert Communication Using MODBUS Protocol in IoT Devices

Sashaa Nagrikar[1], Saeed Alshahrani[2], Daryl Johnson[3]
[1]Rochester Institute of Technology
1 Lomb Memorial Drive, Rochester, US
sn1945@rit.edu; sa7762@rit.edu; daryl.johnson@rit.edu

Abstract **-** Internet of Things (IoT) is a part of Cyber Science that has been gaining popularity exponentially. IoT are generally referred to as smart devices since the carry out their operations with minimal human intervention. The IoT devices are connected to each other via a device such as a centralized modem. Through this method, IoT helps provide an easier life for its consumers. Even so, these smart devices are flawed and face privacy challenges and can be exploited at the physical level to obscurely perform information exchange that they are not intended to do. This is known as a covert channel. By definition, a covert channel is some form of a medium which is used by exploiting its functionalities to secretly send and receive messages which they are not originally programmed to do so. Hence following the above definition, "MODBUS Protocol" was chosen to be used as a communication protocol in a Master-Slave model for a covert channel. The MODBUS protocol uses a Master and Slave system model where the Master sends functional instructions to the slaves and the slaves return the output corresponding to the instruction. By exploiting this feature of the Master-Slave architecture, we have built a covert channel wherein the receiver maps each character of the covert message into an instruction and sends it to the slave and the slave strips off the data in that instruction and sends it to the intended receiver, where the receiver maps the instruction back to the character and prints out the message.

Keywords**:** MODBUS, Master, Slave