**A Commercial Off the Shelf (COTS) Packet Communications Subsystem for the Montana EaRth-Orbiting Pico-Explorer (MEROPE) CubeSat**

The Montana EaRth Orbiting Pico-Explorer (MEROPE) CubeSat is a Montana Space Grant Consortium CubeSat built by the Space Science and Engineering Laboratory (SSEL) at Montana State University[pg.474]. This satellite is built using mostly commercial off the shelf (COTS) components to reduce its cost and complexity. Due to the technical experience limitations of the MEROPE team, the communication subsystem design goal was to have a device that was as “plug-and-play” as possible, and communicate over common VHF uplink and individual UHF downlink bands.

Looking at the design specification of the MEROPE CubeSat, the authors focus primarily on the volume and physical properties of the communications subsystem rather than the software packet delivery mechanisms of the subsystem. The subsystem operates at a power output of 1 Watt RF, and has a target data rate of 1200 bits per second, or approximately 100 Kilobytes of telemetry and payload data per pass [pg.475]. The architecture is based on “store-and-forward” scheme, meaning that upon contact with the ground station, MEROPE will dump the contents of its memory into the terminal node controller (TNC). The TNC will then take the data, convert it into packets and transmit them into the base station[pgs.473,475]. This architecture is noteworthy because it not only uses COTS components to carry out this transmission of data, but also because the data is stored in the satellite memory before being dumped, made into discrete packets of a specific size, and then transmitted. It should be noted that the architects chose the AX.25 packet radio protocol to transmit the data, and that the data transmission is only triggered after an encrypted message is sent from the ground station to MEROPE. While the message to trigger the data transmission is explicitly described as encrypted, there seems to be no encryption scheme or information assurance mechanism on the payload data.

This mechanism for data transmission is described as effective and inexpensive by the authors. The payload data is designed to be a discrete fragment of the data collected by MEROPE, making the packets analogous to the current Internet Protocol packet infrastructure. In this transmission scheme the ground station assembles the packets and recreates the contents of MEROPE’s memory. This mechanism is an open transmission of packet payloads with no built in security mechanisms preventing an unauthorized recipient from collecting the data. The only security mechanism in place is the encrypted message sent to MEROPE by the ground station to trigger the transmission of data. The specifications are unclear on what protections this mechanism has against a replay attack or on the strength of the encryption.

This communications subsystem is an ideal candidate for integrating a one-time-pad (OTP) encryption mechanism protocol. The subsystem already takes data and fragments it into discrete packets for transmission over UHF as raw bytes. The development of an encryption submodule that takes the stored data by MEROPE and encrypts it using a OTP before fragmenting could provide a high level of assurance to the data transmitted at a small processing and data overhead cost. The processing cost arises from the time needed to encrypt the stored data before transmission, while the data overhead would be minimal assuming a throughput of 100 Kilobytes per pass. In order to transmit information of the position of the OTP being read, the encryption mechanism could use 3 bytes at the start of each payload indicating the starting offset of the OTP being used. This would provide increase security without adding too much complexity to the transmission subsystem.

The authors do caution that the functionality and performance of the communications subsystem is untested in high radiation environments [pg.477]. High radiation environments and cosmic rays could cause some problems in flipping bits and corrupting the data being transmitted or the OTP, and radiation shielding or hardening can only provide so much protection as these environmental factors can also cause an increased noise in the signal being transmitted. This would present a problem if the data stream was encrypted or compressed. Despite the environmental noise, a OTP encryption mechanism would limit the error propagation to a single byte as each byte is encrypted independently.