MEMORANDUM

Date: \_\_\_<due signed, before first thesis slot>\_\_\_

From:  \_\_\_\_\_\_\_\_\_\_<all student names, if more than one>\_\_\_\_\_\_\_\_\_\_\_

Section(s): \_\_\_\_\_\_\_\_\_\_<sections for above students>\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

To:  Program Officer, Computer Science

Via:  (1) Thesis Advisor, \_\_\_<title and name>\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(2) Co-Advisor or 2nd Reader: \_\_\_<title and name>\_\_\_\_\_\_\_\_\_\_\_\_

(3) SFS Program P.I.

(4) Academic Associate, CS Department

(5) Chair, CS Department

Subj: THESIS PROPOAL

Encl: (1) Computer Science Thesis Proposal

(2) Institutional Review Board (IRB) Student Research Checklist

1. Tentative Title of Proposed Thesis: Development and Implementation of Information Assurance Protocol for Low Bandwidth Nanosatellite Communications

2. General Area of Proposed Thesis Research: IP based communicaitons information assurance

3. Enclosure (1) is the Thesis Proposal with a milestone plan of dates and events for research and thesis completion.

4. I expect that my thesis will be considered[[1]](#footnote-1) UNCLASSIFIED.

5. I reviewed the IRB webpage concerning the use of humans in research. This research does NOT <alternatively: DOES> involve human subject research.

6. I anticipate NO travel or other extraordinary requirements. <Alternatively, I anticipate the following travel or other extraordinary requirements: \_\_\_\_\_\_\_\_\_.>

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Student Signature Second Student Signature <if joint thesis>

1. Forwarded, recommending approval: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_

Thesis Advisor Date

2. Forwarded, recommending approval: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_

Co-Advisor or 2nd Reader (circle) Date

3. Forwarded, recommending approval: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_

Cynthia Irvine, SFS P.I. Date

4. Forwarded, recommending approval: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_

Academic Associate, CS Dept Date

5. Forwarded, recommending approval: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_

Chair, CS Department Date

6. Approved, and retained:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_

Program Officer, CS Department Date

COMPUTER SCIENCE THESIS PROPOSAL

A. General Information

1. Name: <Enter all students, First MI Last>

2. Email: <Ordered for all students above>

3. Curriculum: Computer Science (368)

4. Thesis Advisor: <title and name>

5. Co-Advisor or 2nd Reader: <title and name>

6. Academic Associate, CS Department: Dr. Man-Tak Shing

7. Chair, CS Department: Dr. Peter J. Denning

8. Date of Graduation: <date>

B. Area of Research

This thesis will conduct an investigation into the development of a low-bandwidth reliable network protocol that supports a high assurance cryptographic system for encrypted communications between base stations on Earth, and nanosatellites, namely CubeSats. This protocol will use commercial off-the-shelf (COTS) components in continuation of the precedent set by CubeSat developers, will be easy to reproduce and manufacture, will allow for a high degree of assurance in the information being relayed from the satellite to the base station, and will include functionality that facilitates the retransmission of lost packets while reducing the data overhead typically associated with the transport control layer (TCP) protocol to maximize the bandwidth usage.

Currently the largest limitation in relaying information between nanosatellites and base stations on Earth is the limited power available to the telecommunications systems. This limitation places a burden on the bandwidth of communication available between the base station and the satellite. Due to the popularity and increasing use of CubeSats, several protocols to ensure the communication between the CubeSat and the ground station exist. While some of these protocols take into consideration the limited operational bandwidth, there is no clear protocol that integrates encryption with bandwidth efficiency. One such protocol is the AX.25 Amateur Packet-Radio Link-Layer Protocol which provides a mechanism for the reliable transport of data between two signaling terminals. The CubeSat Space Protocol (CSP) is in place to facilitate network and transport layer delivery of internet protocol packets from CubeSats to the corresponding base station. The CSP is analogous to the TCP/IP model used in networking today, and contains a lightweight 32-bit header with the appropriate information for relaying. The CSP also includes capabilities of using a block cipher for encrypted packets with XTEA block cypher in counter mode. While these are two examples of nanosatellite communication schemes, there is no clear standard for communication with these devices that is bandwidth efficient and secure.

Due to the lack of standard and understanding of the bandwidth limitations of the UHF and VHF frequencies employed by these satellites, nanosatellites have been using TCP/IP connections to transmit their data. While TCP is a connection driven protocol that ensures all of the data arrives, it also comes at a cost of bandwidth. Every packet sent by the server to the client has to be acknowledged by the client with an ACK response. Otherwise the server assumes the packet was lost and will automatically retransmit the packet if there is a timeout. What the developers of the nanosatellites fail to take into consideration is the fact that TCP packets require a steady and reliable connection that is not often available in UHF and VHF signals being sent by these satellites. Furthermore, due to the large volume of noise and error rates in the packets due to interference, TCP requires a large number of retransmissions from the server on the satellite to the client on the ground. This can be either from delayed or lost ACK packets or from lost or delayed payload packets being sent from the server. These retransmits further saturate the bandwidth and thus decreases the amount of data that is received by the ground station.

The research presented in this thesis will do a comparison of the vulnerabilities of the current CSP, namely the vulnerabilities in the block cipher XTEA, and the processing power required to execute encryption of arbitrarily long messages that can fit within the payload of the CSP packet, and compare it to the processing and security attributes of using a one-time pad. The thesis will also research the development of a standard protocol that combines the reliability of TCP, but focuses on reducing the data overhead from large number of ACKs and large TCP headers. This protocol will combine the low data overhead of the user datagram protocol (UDP) with the reliability of TCP. For this research the protocol developed will be classified as a reliable UDP (RUDP) and will seek to provide a network layer solution for nanosatellite communications. The thesis research will also support the development of a lightweight easily accessible and distributable encryption scheme that will allow nanosatellites to use much stronger encryption schemes, potentially allowing them to be deployed as space assets and be used to relay the data they collect in a secure manner. This encryption scheme will be able to be used independent of the RUDP protocol, but the RUDP protocol will have the encryption scheme as a central tenet of its standard.

Notably, the current usage of UHF, VHF, and S-Band radio frequencies to communicate with satellites is of interest to this research. The focus on these frequencies is due to the fact that these are the frequencies wherein the bandwidth capabilities to communicate with a nanosatellite are the most limited. The bandwidth for these satellites can be below 10 Kbps (kilobits per second) upwards to 2 Mbps (megabits per second). Using higher frequencies allows the base stations to operate with higher bandwidths and ranges, and this is largely the focus of larger, more expensive satellites.

Tangentially, there is the application of using these devices and algorithm as a modern take on old number stations from the Cold War era days. The intelligence community may set up an IRC server listening on a specific IP address, and have the traffic directed to the decryptor. Meanwhile an agent in the field with access to an insecure connection, low bandwidth, and a USB drive with the one-time pad, can relay home over unencrypted and heavily monitored channels, in the most cryptologic secure method over a device whose presence on the internet is maintained to a minimum to reduce the possibility of compromise

C. Research Questions

The thesis will develop and examine the feasibility of a low-cost (processing-wise) high assurance encryption scheme that can be deployed in short-lived nanosatellites with low bandwidth operating at the UHF, VHF, and S-Band frequencies by using COTS components and one-time pads. The resulting encryption protocol will provide high confidentiality of the cybersecurity triad (confidentiality, integrity, availability) in communication channels with these satellites. Furthermore, the thesis will develop a standard for reliable communications with nanosatellites that reduce the data overhead and has an encryption algorithm built into the protocol. These research goals will seek to answer:

* What are the processing and storage costs associated with using a one-time pad for encryption in nanosatellite communications?
* Is it feasible to use one-time pads as a standard for encrypted communications in low-bandwidth communications with these satellites?
* What is the feasibility of developing and implementing a new network standard that combines the reliability of TCP with the low data overhead of UDP, and integrates security from a one-time pad?

D. Discussion

Cybersecurity of nanosatellites is important as these devices are becoming a cheap alternative for research and development. Currently CubeSats communication is achieved largely through the use of UHF, VHF, and other radio frequencies, and there is no clear or decisive authority on communication standards of CubeSats or nanosatellites. As these nanosatellites become more prominent and less expensive, the confidentiality of the data transmitted needs to be taken into consideration. To this end, satellite encryption can be done using the most secure cipher of all, a one-time pad. One-time pad ciphers are the strongest ciphers since they are based on randomly generated symbols for each of the characters that the packet wishes to relay and can only be decoded by the other individual that has the same one-time pad. The drawback to the mass deployment of one-time pads in day to day operations is the fact that both individuals need to physically exchange the one time pad before it can be used. This drawback has led to other verification mechanisms like public key infrastructure, Diffe-Hellman key exchange methods, and other bandwidth-heavy mechanism.

Since nanosatellites are developed and deployed using COTS parts and assembled by the agency that seeks to capture the data, the challenge of both parties being present to exchange one-time pads is null, and therefore it can be used as a secure and light weight method to communicate over open channels. Such a cryptologic strength could be used to garner more support for the deployment of nanosatellites and the relay of sensitive information through them. Furthermore, the limited life-span of these satellites ensures that once the satellite’s operational life expires and reenters the atmosphere, the one-time pad will be destroyed and the communications will be indecipherable to an adversarial party.

Aside from the assurance and security of the data, the current issue with the limited and noisy bandwidth used by nanosatellites is the large data overhead that is consuming the bandwidth and reducing the total amount of data that the ground station can get from the satellite. The approach to send data from a satellite to a ground station has focused on using TCP over a connectionless internet protocol (IP) header, similar to those used by internet connections on the ground. While these protocols work with larger satellites, due to the low bandwidth and poor connection with the nanosatellites, TCP accrues a larger data overhead from retransmits and ACK messages that saturate the frequency on which it is communicating. Furthermore the TCP header has a minimum data overhead of 20 bytes, with a maximum header of 60 bytes. In order to mitigate errors from noise, these satellites focus on small payloads per packet, increasing the number of packets being sent over the connection. This exacerbates the problem since the data overhead is multiplied by every packet sent. By developing a standard that uses a lighter data overhead, reduces the number of ACK messages that need to be sent, but still allows for the reliability of retransmission of dropped packets, nanosatellites could send more data with the same limited bandwidth.

E. Scope of the Thesis

The thesis will focus on the amount of processing and size of packets generated with the encryption mechanism, seeking to reduce or maintain the size of the data being transmitted by these satellites while significantly increasing their security at the application data and packet payload layer at a minimal cost to processing power. In addition, the thesis will focus on researching and developing a new standard for nanosatellite communication that allows for packet retransmission at a lower bandwidth cost, and will natively incorporate the one-time pad encryption mechanism.

The success of this thesis will be largely determined by the comparison of data sizes of the ciphertext and the plaintext, the strength of the encryption mechanism and the processing power required to encrypt the plaintext, and the reduction of data overhead from TCP headers.

F. Methodology

1. Conduct literature review.
2. Review literature and manuals on current communication protocols and methods for nanosatellites.
3. Build encryption/decryption software platform prototype using python and TCP/IRC channel and netcat as a prototype and compare it to plain text generation.
4. Test robustness of the mechanism by adding noise to the signal and randomly inserting errors (deletion, replacement, insertion) and by verifying the strength of the encryption mechanism.
5. Testing encryption scheme using randomly generated data
6. Project the time needed to encrypt data and send data at various bandwidths and processing capabilities.
7. Development of RUDP to reduce the data overhead
8. Test RUDP in combination with randomly generated data for one-time pad
9. Simulate packet loss to trigger RUDP reliability mechanisms
10. Conduct small scale experiments using FM radio and minimodem using Raspberry Pi 3 model B.
11. Conduct usability study of encryption mechanism by analyzing the collected data sets.
12. Make analysis and recommendation of the encryption mechanism.

G. Chapter Outline

Tentative Chapter Outline:

I Introduction

A. Research Domain

B. Research Problem and Motivation

C. Research Questions

D. Scope

E. Approach

F. Thesis Structure

II Background

1. Problem Space: Low bandwidth in UHF/VHF/S radio frequencies
   1. Interference
   2. Packet Loss
2. Current communication standards with nanosatellites
   1. Data Overhead
   2. Connection problems
3. Chapter Summary

III Current Information Assurance in Nanosatellites

1. The need for cybersecurity in nanosatellites
   1. Data usage in nanosatellites
   2. Current nanosatellite communication protocol information security standards
2. Information security vulnerability assessment in nanosatellite communications
3. Chapter Summary

IV Encryption and One-Time Pads

1. Evaluating the Strengths of One-Time Pads
2. Limitations of One-Time Pads
3. Data Usage of Nanosatellite and Size of Pad
4. Chapter Summary

V Encryption Algorithm

1. Goals of Encryption Algorithm
2. Development of Encryption Algorithm  
   1. Platform development and description
   2. Performance over IP protocols
3. Measuring Performance  
   1. Data sizes of plaintext and ciphertext
   2. Processing time
4. Chapter Summary

VI Measuring Robustness to Error

1. Insertion of Data Errors
2. Deletion of Data Errors
3. Replacement of Data Errors
4. Chapter Summary

VII Mechanisms Developed to Overcome Error Propagation

1. Insertion of Data Errors
2. Deletion of Data Errors
3. Replacement of Data Errors
4. Data Loss Tolerances
5. Chapter Summary

VIII RUDP Development and Structure

1. Packet Structure
2. Reliability Mechanisms
3. Reducing Data Overhead
4. Benefits and Drawbacks to Other Protocols
   1. UDP
   2. TCP
   3. CSP
5. Chapter Summary

VIII FM Band Testing Results and Analysis

1. System Architecture
2. Testing Environment
3. Testing Results
4. Extrapolation to Larger Communication Schemes
5. Chapter Summary

IX Feasibility Study

1. System Performance and Evaluation
   1. Size of data being transmitted in comparison to existing plaintext protocols
   2. Usage of bandwidth
   3. Error robustness
2. System Costs
   1. Financial
   2. Processing Power Costs
      1. Processing Speed of AES, 3DES, and One-Time Pad on Raspberry Pi 3 Model B and Raspberry Pi Zero
      2. Analysis and comparison
3. Vulnerabilities
   1. Strength of encryption mechanism
   2. Impact on availability and integrity
4. Chapter Summary

X Conclusions and Recommendations

A. Main Conclusions and Recommendations

B. Main Contributions

C. Future Work

Appendices

Bibliography

1. Schedule

|  |  |
| --- | --- |
| **Thesis Stage** | **Completion Target Date** |
| Literature review | Mid April 2017 |
| Development of prototype encryption algorithm and robustness to error measurments completed | Mid April 2017 |
| Protoype is updated to account for error, RUDP development completed | May 2017 |
| FM Band Testing Complete | Mid May 2017 |
| Data analysis completed | June 2017 |
| Draft thesis to advisor(s): | July 2017 |
| Final thesis submission for signatures: | August 2017 |

1. Benefits of Study

The benefits of nanosatellites and picosatellites are still being discovered in research and development, education, and military applications. Unfortunately, due to their power constraints their communication capabilities are limited and amateur radio frequencies are largely used to send and receive both control and experiment data. The disadvantage of these frequencies is the large availability of potential listeners with access to equipment capable of listening to the broadcasts, sending malicious logic and data to the satellites, and the limited bandwidth and processing power of these satellites that are being built with commercial, lightweight, off the shelf components.

Using microcomputers like Raspberry Pi and Arduino, these satellites have limited processing capabilities, are designed to be low cost, and have varying mission life expectancies. To this end, a low processing power, low-bandwidth, high assurance encryption mechanism is needed.

Nanosatellites are still in their infancy, and are gaining popularity. They provide a cost effective alternative for space research, and could be deployed as potential assets even with short mission high altitude balloons. Currently the security of their communications has not been standardized and this could lead to potential theft of data, sabotage of satellites, or hijacking of the satellites for malicious purposes. By developing a high assurance standard that has the strongest and simplest encryption scheme, the operators of these satellites can be sure that the data is secure without having to worry about processing power.

Currently there is no clear standard for reliable, encrypted communication with nanosatellites. By researching the feasibility of developing a protocol with the desired characteristics that also reduces the current data overhead, researchers will be able to obtain larger amounts of data from nanosatellites using the strongest encryption possible.

Ultimately an encryption scheme like the one developed could also have multiple uses and deployments where low bandwidth and low power communications are desired. Uses could extend to covert operations messaging, or the development of picosatellites that are even smaller and yet have a high information security standard.

Preliminary Bibliography

Venturini, C., McVittie, T. (2014). *Current and Future Ground Systems for CubeSats Working Group*, Ground Systems Architecture Workshop 2014 Session 11C, NASA JPL-CalTech, Web 2017.

Insik, J., Kwon, K., Cho, D., Lee, S., Chung, H. (2016). *Construction of University Ground Station Using S-Band for CubeSat*, SpaceOps 2016 Conference, Republik of Korea Air Force Academy, Web 2017

Klofas, B., Anderson, J., Leveque, K. (2008) *A Survey of CubeSat Communication Systems*, California Polytechnic State University and SRI International, Web 2017

Henderson, P. (2009). *High Data Rate Radio Transmitter For Cube Satellites*, Master’s Thesis, Utah State University, Web 2107.

Challa, N., Bhat, G., Mcnair, J. (2012) *CubeSec and GndSec: a lightweight security solution for CubeSat communications*, 26th Annual AIAA/USU Conference on Small Satellites, University of Florida, Web 2017.

1. If classified, I have read Chapter V of NAVPGSCOLINST 5510.2, and the NPS Research Admin web page (http://intranet/ResAdmin/research1.html) concerning Classified Thesis. [↑](#footnote-ref-1)