MODELING AND CUSTOM DATASET GENERATION OF THE DNP3 SCADA PROTOCOL

BY

ARTURO CUEVAS

THESIS

Submitted in partial fulfillment of the requirements

for the degree of Master of Science in Electrical and Computer Engineering

in the Graduate College of the

University of Illinois Urbana-Champaign, 2023

Urbana, Illinois

Adviser:

Professor David M. Nicol

ABSTRACT

DNOP is

ACKNOWLEDGEMENTS

I would like to express my deepest gratitude to my thesis advisor Professor David M. Nicol for his invaluable guidance and support in my graduate studies. Professor Nicol displayed immense patience, consideration, and kindness to me during the completion of my degree that I hope I can repay to the future generation of researchers.

As well I would to thank the support of my fellow research group members at the Information Trust Institute: David Emmerich, Matthew Needham, and Logan Marlow, for their support and expertise in the completion of my thesis. I also would like to thank the endless support from my family and friends who made this possible.

TABLE OF CONTENTS

[Chapter 1 INTRODUCTION 1](#_Toc139888878)

[1.1 START 1](#_Toc139888879)

[Chapter 2 BACKGROUND 1](#_Toc139888880)

[2.1 DNP3 Protocol 1](#_Toc139888881)

[2.2 Previous Methods for Traffic Generation 1](#_Toc139888882)

[2.3 Cycle Detection 1](#_Toc139888883)

[2.4 DTMC 1](#_Toc139888884)

[2.5 Role of Scapy in Traffic Analysis 1](#_Toc139888885)

[Chapter 3 MOTIVATION 1](#_Toc139888886)

[Chapter 4 DNP3 Library 1](#_Toc139888887)

[Chapter 5 CYCLE DETECT 1](#_Toc139888888)

[Chapter 6 DTMC 2](#_Toc139888889)

[Chapter 7 EVALUATION 2](#_Toc139888890)

[Chapter 8 CASE STUDY/DISCUSSION 2](#_Toc139888891)

[Chapter 9 CONCLUSION RERFERENCES 2](#_Toc139888892)

# **INTRODUCTION**

## 1.1 START

Bring up all terms

# **BACKGROUND**

## 2.1 DNP3 Protocol

## 2.2 Previous Methods for Traffic Generation

## 2.3 Cycle Detection

## 2.4 DTMC

## 2.5 Role of Scapy in Traffic Analysis

# **MOTIVATION**

3.1 Importance of DNP3 Traffic Analysis

3.2 Current Challenges in DNP3 Traffic Analysis

3.3 Proposed Methodology for Analysis

# **DNP3 Library**

# **CYCLE DETECT**

# **DTMC**

# **EVALUATION**

# **CASE STUDY/DISCUSSION**

# **CONCLUSION RERFERENCES**