Modeling Telemetry Networks for Cyber Security Analysis

Wondimu Zegeye{Wondimu.zegeye}@morgan.edu

Advisors: Dr. Richard Dean, Dr. Farzad Moazzami, Dr. Mulugeta Dugda

Morgan State University, Electrical and Computer Engineering Department

ABSTRACT

This paper presents the modeling of the networks supporting today’s telemetry. The incorporation of networking features has significantly enhanced the capability and performance of modern telemetry systems. The development of the Integrated Network Enhanced Telemetry protocols and the use of networked telemetry applications has introduced a host of potential cyber security risks inherent in modern networking. This paper will investigate how telemetry applications are uniquely structured with wide area, local area, and micro area networks that represent modern telemetry solutions. The development of these models and the traffic on these networks will enable analysis into the unique threats and vulnerabilities of telemetry networks.

Key words: iNET, Telemetry Networks, cyber-attacks, SCADA

1. INTRODUCTION

Components of future Networked Telemetry include network enabled instrumentation, network enabled ground stations, mission control rooms as well as ground support equipment. These components are considered a high-level subsystem of integrated Network Enhanced Telemetry (iNET) [1]. iNET is portrayed as a networked telemetry data system that can provide developmental flight tests.
Figure 1 shows telemetry network instrumentation and a test article (TA) to ground station (GS) telemetry system proposed by Tom Young [1]. This single TA to single GS communication is the basic building block for multiple distributed sites that consists of multiple TAs and GSs. The iNET paradigm is shown to have the benefits of test/data and spectrum efficiency as well as long-term sustainability and interoperability. In our effort to develop a telemetry network testbed, we build upon the concepts and implementation ideas developed for iNET and beyond.

In modeling a Telemetry network, we consider the ground station to comprise traditional enterprise network and Supervisory Command and Data Acquisition (SCADA) systems. This allows us to build on the many studies of cyber vulnerabilities in SCADA networks. SCADA systems are one of the most widely used Industrial Control Systems (ICS) that enable controlling and monitoring of process equipment on multiple sites which spread over large distances [2]. SCADA systems are cyber physical systems with communication networks interfacing the monitoring and control system with the hardware and these could have multiple supervisory systems, Programmable Logic Units (PLCs), Remote Terminal Units (RTUs), Human Machine Interface (HMIs), process and control instrumentation, sensors, and actuator devices over a large geographical area. SCADA systems make use of both new and legacy systems including traditional information systems [3]. SCADA systems are not only as vulnerable as any other networked computer systems, but their legacy systems create another layer of threat. Since many of these systems have existed for decades, their cybersecurity risks are unknown and challenging to analyze as well. These SCADA systems resemble much of the Networked Telemetry systems that we intend to model and therefore represent a good starting point.

The goal of this paper is to provide an architectural framework for telemetry networks for our testbed that meets the current and future requirements of network operations. It describes and classifies the current modules and components of a telemetry network system. It outlines the system architecture to help set a working foundation for telemetry network system vulnerability analysis that leads to a security solution. This is our contribution to the general Telemetry Cybersecurity community, where we capture the scope of these networks and
frame this environment. This architecture will also allow us to explore Machine Learning and Artificial Intelligence for real time streaming of data to predict unique patterns in traffic in telemetry networks.

**Figure 1.** Telemetry network instrumentation and a test article aircraft [1]

2.1. Test Article and Ground Station

2.1.1. Onboard Instrumentation System

The onboard instrumentation system on a TA consists of a networked system of devices communication via different protocols such as ethernet, WiFi, Bluetooth/BLE, ZigBee, and Zwave. These protocols belong to a class of IoT protocols. Hence, the onboard instrumentation can be viewed as a network of communication equipment that sends data from the IoT network. Where the IoT devices mainly include different sensors on the Test Article. The flight onboard testbed also consists of the Telemetry Network System (TmNS) that includes TmNS Recorder, TmNS Radio, TmNS data acquisition units, TmNS switch.

The data encrypted by the TA’s network is processed and displayed for real-time and offline visualization by the Mission Control System of the ground station. This control system is described in detail in the SCADA system, section 3.1.
2.1.2. Ground Communication System

The ground segment contains the Antenna system that creates a link to the TA or multiple TAs as shown in Figure 1. The current link paradigm relies on a TM link which is efficient in spectrum to increase the availability of required bandwidth. In addition, it is also efficient in providing improved test data and test efficiency.

2.2. Test and Resource Management Center

The Test Resource Management Center (TRMC) is the manager of the Joint Mission Environment Test Capability (JMETC). This subsection describes the architectures of the test and training environment that integrates the live and virtual environments [4-5]. Several perspectives of this environment are captured below from prior work that will allow us to develop our testbed model.

2.2.1. Test and Training Environment

Figure 2 shows the kind of network framework that we envision for our cybersecurity test environment. At the top in Figure 2 is shown some physical assets. These physical assets are connected through networks below them. We have a simulated environment below the networks. These physical and simulated real environments are somehow interfaced to virtual assets such as Big Data Storage, Big Data Analytics and Visualization through the Middleware called Test and Training Enabling Architecture (TENA).

![Figure 2. Virtual Test and Training Environment (R. Norman [5])](image-url)
Figure 2 shows a virtual test and training environment, JMETC, which reflects our objective in modeling a telemetry network. This test environment abstraction shows the many aspects of the future of telemetry [6].

JMETC provides a robust and secure distributed testing environment, including several government and industry range labs, cybersecurity testing and evaluation (T&E), and TENA. JMETC supports T&E Infrastructure Interoperability. One of the challenges in the original design of the DoD test range infrastructure was the lack of interoperable between different systems. TENA is a flexible infrastructure design for T&E operation with mature and continuously improving software architecture with integration capability [5].

JMETC has a hybrid network architecture:

1. The JMETC Secret Network (JSN), which is the T&E enterprise network solution for Secret testing is based on the Secret Defense Research and Engineering Network (SDREN).

2. The JMETC Multiple Independent Levels of Security (MILS). Whereas The T&E Enterprise network solution for all classifications and cyber testing is Network (JMN).

JMETC supplies tools, services, and support that are all institutionally funded capabilities. JSN and JMN engineering and event support services are free to the user. JMETC capabilities are driven by user requirements and JMETC provided tools and services are based on user input. TENA is an Architecture for Ranges, Facilities, and Simulations to interoperate, to be reused, & to be composed into greater capabilities [5].

3. General Networked Telemetry Architecture

This section outlines the general telemetry architecture envisioned in this paper. Our approach models telemetry systems as Industrial Control System (ICS) SCADA. These systems have received significant attention, so analysis and conclusions of this work will apply directly to our efforts to model telemetry systems for cyber security purposes. The architecture consists of a typical enterprise network and ICS/SCADA representation of a telemetry system ground station as shown in Figure 3. Here the emphasis is on the ICS-SCADA representation of telemetry systems which is described in detail in section 3.1. Section 3.2 presents the core of this paper which is the general networked telemetry architecture. The SCADA system architecture evolution is as shown in Table 1 and the model we consider will be the Purdue reference architecture.

| Table 1. Scada System Architecture Evolution |
The ICS model includes three independent layers: the Enterprise layer, the Supervisory layer and the Field layer. The Industrial Control System (ICS) network model maps telemetry Test Range control elements into the ICS Supervisory layer and the telemetry Test Article into the ICS Field layer. The ICS system’s Field Layer can be connected to the enterprise network for management purposes via the supervisory layer separated by a Firewall [7-8].

The ICS is different from a traditional enterprise system due to its close connections to the physical layer of devices. For example, if we consider a single telemetry ground station, the sensors distributed on a Test Article consist of the Intelligent Electronic Devices (IEDs) in the ICS model.

Figure 3. ICS Network Architecture
3.2 General Integrated Networked Telemetry (iNET) Architecture

The telemetry architecture described in this section models the telemetry network test sites which includes an Enterprise level that follows the SCADA model Control and Field network levels. This architecture as shown in Figure 4 has two Test Sites (T&E Centers) each of which have three SCADA levels. The Global Grid is the DoD Internet connected to both Test Sites and the T&E Resource or Center through high-speed internet. Interfaces between two connected sites are secure connections. There are telemetry radio links between the Test Sites and Test Articles, which can be aircraft or ships. Those communications links are targets of cyber threats such as denial of service on the radio network, or intrusion on the Enterprise, Control, or Field Networks or on the Test Article [9-10].

The general telemetry architecture proposed in this article is shown in Figure 4. It consists of different Test and Evaluation centers that are interconnected via the global grid. Figure 4 also shows two T & E centers connected to the global grid. The detail of each T & E site consists of the ICS- SCADA control room and enterprise network that is described in Figure 3. The two T & E centers can communicate via the internet, which is secured via VPN, across the global grid. It also shows a joint test space made up of two test articles communicating via a reliable link, but they belong to two different T & E centers.
4. CONCLUSIONS
In this paper we have captured a network enhanced telemetry architecture for the purpose of modeling and analysis for cyber security risks. We show how Telemetry Systems can be modeled as an ICS-SCADA system that merges with an enterprise network. In addition, it shows how this architecture can be transformed into an IoT reference architecture to make use of the cloud service capabilities. The main goal of this paper is to lay a network foundation to explore cyber security issues with an integrated network enhanced telemetry architecture. This cyber domain is going to include vulnerabilities associated with ICS-SCADA, Enterprise network, and Cloud network.

ACKNOWLEDGEMENT
This work is funded by a grant from International Foundation for Telemetering (IFT). Author and other WiNetS laboratory members in the School of Engineering at Morgan State University thank IFT for their support of this research.

REFERENCES
5. Norman, R. Improving Distributed Test & Evaluation with JMETC & TENA. Joint Mission Environment Test Capability (JMETC) Program Overview; JMETC Program in; Test


8. Guide to Industrial Control Systems (ICS) Security Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC), NIST Special Publication 800-82 Revision 2. Available online: http://dx.doi.org/10.6028/NIST.SP.800-82r2 (accessed on 1 December 2020).


10. Stouffer, K.; Falco, J.; Kent, K. Guide to Supervisory Control and Data Acquisition (Scada) and Industrial Control Systems Security; Sp800-82; NIST: Gaithersburg, MD, USA, 2006.