Abstract— Synchrophasor systems are being added to modern power systems to facilitate improved wide area monitoring and wide area protection schemes. As synchrophasor systems are installed utilities must decide if new cyber devices, phasor measurement units and phasor data concentrators, will be declared as The US National Electric Reliability Council (NERC) Critical Infrastructure Protection (CIP) cyber critical assets. This paper explores the potential impact of reconnaissance attacks, packet injection attacks, and denial of service attacks on wide area monitoring systems and wide area protection systems. This paper was written to accompany a panel presentation and discussion and was not intended to provide new research results.

Index Terms— synchrophasor, phasor measurement unit, phasor data concentrator, cyber security

I. INTRODUCTION

Modern power systems are being upgraded with the addition of synchrophasor systems which include phasor measurement units (PMU) and phasor data concentrators (PDC) to facilitate wide area transmission system situational awareness. PMUs will measure voltage and current phasors 30, 60, or 120 times per second and transmit these measurements to PDCs which will interpolate for missing data, provide sample rate matching functionality, and reformat and forward multiple synchrophasor measurement streams as a single stream which is then forwarded to energy management systems which perform state estimation operations and present synchrophasor data to human operators in utility control centers. Synchrophasor data will also be shared with neighboring utilities, independent system operators, and other regional entities.

Two primary application groups are wide area monitoring systems and wide area protection systems. This paper explores cybersecurity threats to wide area monitoring systems and wide area protection systems. The threat classes considered in this paper are reconnaissance attacks, packet injection attacks, and denial of service attacks. This paper will be organized as follows. First, a background section provides a brief description of wide area monitoring, protection, and control systems (WAMPAC). Second, the three classes of threats are discussed with information on their implications to WAMPAC systems and recommendations for securing WAMPAC systems. Third, a discussion on cybersecurity testing of PMU and PDC is included.

II. BACKGROUND

Electric utilities and transmission operators are adding phasor measurement units (PMU) and phasor data concentrators (PDC) to bulk power transmission systems to increase wide area power system visibility and control. PMU measure current phasors, voltage phasors and frequency 30, 60 or 120 times per second. PMU are placed at multiple bus locations to provide optimal power system visibility. Measurements from different PMU are synchronized to within 1 microsecond to facilitate accurate state estimation.

PMU transmit measurements, aka synchrophasors, to PDC. PDC connect to multiple PMU and concentrate them into for retransmission to other PDC or to other end points; energy management systems, historians, and other synchrophasor applications. PDC concentration includes accepting multiple individual PMU measurement packets and creating a single packet with multiple measurements included in the single packet. As part of the concentration process the PDC may also interpolate for missing data and apply algorithms to adjust reporting rates (e.g. adjust a 30 sample per second stream to 60 samples per second). PDC may also implement local area control or power system event detection applications.

PMU and PDC use the IEEE C37.118 communication standard for data transmission. PMU are preconfigured with network connection information and measurement frequency details. When PDC are connected to a PMU configuration information is requested from the PMU. After the configuration frame is sent PMU begin transmitting a continuous stream of data frames to the PDC. IEEE C37.118 configuration, command, header and data frames do not include integrity (digital signature) or confidentiality (encryption) features. Researchers have shown that IPSEC can be used in conjunction with IEEE C37.118 communication to provide cyber security integrity and confidentiality features [5]. IEC 61850 90-5 is a communication standard currently in preparation which allows...
transmission of synchrophasor data and includes a digital signature to provide authentication and tamper detection and optionally provides encryption to provide confidentiality.

A. Wide Area Monitoring Protection and Control Systems

Wide Area Monitoring, Protection, and Control Systems (WAMPAC) systems leverage Wide Area Measurement Systems (WAMS) to implement System Integrity Protection Systems (SIPS) and Special Protection System (SPS).

WAMS allow state estimators to approach linearity by using synchrophasor measurements [2]. WAMS place PMU at various locations within a power system to collect voltage and current phasors. The increased volume of phasor data allows WAMS to detect power system events in advance of contemporary state estimators. WAMS will likely augment existing state estimators with new data rather than replace existing SCADA based measurement sources. PMU are typically placed within a power system to provide overlapping visibility. The continuing presence of existing measurement devices and the overlapping visibility of individual PMU lead some utilities to argue that WAMS are not cyber critical systems as defined by NERC CIP [1] and therefore PMU and PDC need not be treated as cyber critical assets (CCA). WAMS data will also be used for new visualization systems and stored in historians for post incident analysis [3]. WAMS may also include power system event classification applications such as semantic driven knowledge discovery algorithms [3]. Use of synchrophasor based visualization applications and event classifiers to inform control center operator control decisions will likely lead to CCA status for PMU and PDC devices.

SIPS and SPS are control schemes which use remote data from synchrophasor systems to provide system level protection and control applications. SPS detect changes in load, generation, or system configuration and attempt to take control actions to maintain system stability. SIPS include SPS, remedial action schemes, under voltage, under frequency, and out of step schemes [4]. SIPS and SPS both leverage synchrophasor data from WAMS to provide event detection then take control actions based upon identified events. SIPS and SPS control actions include load shedding, high speed reactive voltage compensation, generation control, and congestion mitigation. SIPS and SPS schemes rely on accurate data to make real time control decisions and actions. According to [4] some SIPS and SPS control actions require as little as 50 milliseconds for event detection and mitigation and many schemes require 200 or less milliseconds. SIPS and SPS will most definitely be classified as critical assets and therefore will result in CCA status for PMU and PDC devices which source synchrophasor data to SIPS and SPS systems. The integrity and availability of synchrophasor data used by SIPS and SPS systems is critical.

B. Cybersecurity Threats

1) Reconnaissance Attacks

Reconnaissance attacks allow cyber attackers to reconnoiter a system before attacking. Attackers use Reconnaissance attacks to identify connected systems and then fingerprint the connected systems. Fingerprinting allows an attacker to learn which ports are open, the identity and version of the remote operating system, and the identity and version of remote network stack daemons. With this information the attacker can plan a more effective attack.

2) Packet Injection Attacks

Packet injection can be classified into two subgroups; sensor measurement injection and command injection.

Sensor measurement injection attacks inject false sensor measurement data into a control system. Since control systems rely on feedback control loops before making control decisions, protecting the integrity of the sensor measurements is critical. Sensor measurement injection can be used by attackers to cause control algorithms to make misinformed decisions.

Command injection attacks inject false control commands into a control system. Control injection can be classified into 2 categories. First, human operators oversee control systems and occasionally intercede with supervisory control actions, such as opening a breaker. Hackers may attempt to inject false supervisory control actions into a control system network. Second, remote terminal units (RTUs) and intelligent electronic devices (IEDs) protect, monitor and control grid assets. The protection and control algorithms take the form of ladder logic, C code, and registers that perform calculations and hold key control parameters such as high and low limits, comparison and gating control actions. Hackers can use command injection attacks to overwrite ladder logic, C code, and remote terminal register settings.

3) Denial of Service Attacks

Denial of Service (DOS) attacks attempt to disrupt the communication link between the remote terminal and master terminal or human machine interface. Disrupting the communication link between master terminal or human machine interface and the remote terminal affect the feedback control loop and makes process control impossible. DOS attacks take many forms. A common DOS attack attempts to overwhelm hardware or software so that it no longer responsive.

C. NERC CIP Requirements

The US National Electric Reliability Council (NERC) Critical Infrastructure Protection (CIP) Standards 002 through 009 [1] requires utilities to identify cyber critical assets (CCA). CCA must be housed within physical and electronic security perimeters. The physical security perimeter must include physical access control, must include a monitoring system which alerts for unauthorized physical access, must include a visitor control program, and must log and retain records of all physical access. The electronic security perimeter must deny access by default, ensure the authenticity of remote access parties, monitor electronic access, detect and alert for invalid electronic access attempts, and only allow network traffic on required ports. CCA systems must disable unused and unnecessary ports and services, must support security patching were feasible, must support anti-virus and malware detection where feasible, must support user account...
management with individual based passwords and roles where feasible, must support minimum password complexity requirements, and be disposed of securely. Finally, declaration of a device as a cyber critical asset leads implementation of multiple compliance steps including personnel training, implementation of physical and electronic access controls and records retention. Declaration of a cyber asset is seen as an expensive proposition and therefore utilities perform careful assessments of to determine CCA status. As PMU and PDC are added to utility systems utilities must decide if PMU and PDC are CCA. This decision will ultimately depend upon applications which use synchrophasor data.

D. NISTIR 7628 Recommendations

NISTIR 7628 volume 2 [7] includes a process for deriving cyber security requirements and recommendations for smart grid subsystems. The NISTIR provides a method for utilities and responsible entities to derive impact levels for confidentiality, integrity, and availability (CIA) for a given subsystem type and its associated interfaces. Based upon the derived CIA impact levels which can be high, medium, or low for each CIA component users can derive requirements and recommendations for access control, awareness and training, audit and accountability, security assessment and authorization, configuration management, continuity of operations, identification and documentation management, incident response, smart grid information system development and maintenance, media protection, physical and environmental safety, planning, security program management, personnel security, risk management and assessment, smart grid information system and services acquisition, smart grid information system and communication protection, and smart grid information system and information integrity [7]. WAMS and PMU are covered directly by the NISTIR. WAMPAC systems are not covered explicitly by the NISTIR, however, can be addressed indirectly through the recommendations related to the WAMS interface to SCADA systems and to energy management systems.

This NISTIR was used by the authors to derive cybersecurity requirements and recommendations for a American and Reinvestment and Recovery Act funded synchrophasor project at a utility in the United States. Twenty eight individual requirements and recommendations were derived from this source for a WAMS system. These recommendations provides a solid foundation for discussion, but, were necessarily vague and required engineering analysis by a cross function team to move from recommendation to acceptable project requirement.

The NISTIR provides a more comprehensive set of cyber security recommendations and requirements than NERC CIP. However, much of the output of the NISTIR process are recommendations which means cyber security engineers are left with the burden of convincing utility management and vendors of the need to implement individual recommendations.

III. CYBERSECURITY TESTING OF PHASOR MEASUREMENT SYSTEMS AND PHASOR DATA CONCENTRATORS

A series of tests were performed against commercial PMUs and PDCs to search for vulnerabilities which may be exploited to enable the aforementioned threats. A MU Dynamics MU-4000 Analyzer [6] was used to perform denial of service testing including; network congestion testing, testing known denial of service vulnerabilities, and protocol mutation testing. Testing also included packet injection demonstrations including; command injection, sensor measurement injection, and man-in-the-middle attacks. NMAP [8] was used to perform reconnaissance attack against PMU and PDC to identify open ports and services. Reconnaissance testing also included a MODBUS address scan and MODBUS point scan.

A. Denial of Service Testing

The MU-4000 Network Analyzer was used to perform network congestion testing. The MU-4000 denial of service test suite includes tests for multiple network protocols across all network OSI layers. The denial of service tests validate a device’s ability to withstand large volumes of traffic directed at the device. The test engineer should identify relevant network protocols for testing.

Each network congestion test attempts to stress a separate portion of the device’s network stack. The tests target a device’s ability to process large volumes of a single type of network traffic across all network layers. Many substation network appliances contain limited memory which can be exhausted and lead to operating system exceptions, cause services to stall, and or cause the device to reset itself.

All devices tested eventually became unresponsive when the traffic volume increases beyond that devices ability to process packets. Some devices may hang or reset themselves when subjected to high packet rates. Many devices are unresponsive during the test, but, become responsive again when the packet rate returns to acceptable levels.

A second method to test for denial of service vulnerabilities is through protocol mutation, also known as fuzzing. Protocol mutation creates network packets with random contents. Each field in a packet’s header, payload, and trailer is assigned a set of variant values. Variant values for a field may include legal values and illegal values. The protocol mutation tester creates a set of packets which include all combinations of all fields with all variant values. The number of combinations grows quickly and protocol mutation can be a slow process. The benefit of protocol mutation is that combinations of fields which may not be thought of by a human can be tested to confirm that the device network stack does not hang or reset when the test packet is processed. Protocol mutation is intended to discover vulnerabilities before they are discovered by an adversary and become exploited zero day vulnerabilities.

The selection of protocols for mutation testing was based on port scanning and device manual review results. All communication protocol supported by a device should be tested. Mutated protocols for the PMU and PDCs included
B. Packet Injection Testing

Protocol mutation testing identifies individual packets which cause device failures including hanging network stacks or causing the device under test to reset itself. Protocol mutation testing may also identify combinations of packets which cause similar device failures. In both cases careful study is required to determine the root cause of the failure. Mitigation of detected vulnerabilities can be achieved with a firewall or signature based intrusion prevention system (IPS) rules to block problem traffic. Vulnerabilities identified using protocol mutation should also be reported to the device vendor. Protocol mutation identified multiple issues on devices tested for this work. Issues included crashing of individual network services, crashing of applications running on devices, and unintended soft resetting of affected devices.

Finally, the MU-4000 includes a database of known denial of service vulnerabilities including LAND attacks, tear-drop attacks, ICMP attacks, etc. PMU and PDC devices were subjected to the known denial of service attacks. Results of known denial of service attacks were similar to protocol mutation results.

B. Packet Injection Testing

IEEE C37.118 packets do not include a cryptographic signature to prevent packet spoofing, transmission of unauthorized or altered network packets. The authors of this paper have demonstrated the ability to inject invalid sensor measurements in the form of altered IEEE C37.118 data frames.

Ettercap was used to create a man-in-the-middle node which captured and altered C37.118 data frames transmitted from a PMU to PDC. In this demonstration ettercap provided captured data frames to a separate script which altered the packets by doubling the magnitude of all captured phasors. Upstream PDC were not able to distinguish altered packets from unaltered packets. Furthermore, the alteration process happened within PDC data frame life time requirements, therefore altered packets were not marked old and dropped. Ettercap can also be used to alter C37.118 command, configuration, and header frames. Many PMU include MODBUS or DNP3 interfaces to allow remote monitoring and control. MODBUS and DNP3 packets do not include cryptographic signatures, as such, these packets may also be altered by a man-in-the-middle attack.

C. Reconnaissance Testing

Many PMU and PDC require password authentication prior to remote access and control. In laboratory testing the wireshark network protocol analyzer [10] was used to capture plaintext passwords in flight between remote systems and PMU and PDC.

Additional information can be gathered from eavesdropping on IEEE C37.118 network traffic. IEEE C37.118 frames include configuration information, substation names, and GPS coordinates. Attackers could use such information to learn the physical location of PMU within a transmission system. Learning the location of multiple PMU may enable large scale attacks designed to fool a state estimator [11].

Also in laboratory testing NMAP was used to scan networks with connected PMU and PDC to identify open ports and services. PMU and PDC use commercial operating systems. US-CERT was searched for known vulnerabilities associated with open ports which may provide vectors for system penetration or privilege escalation.

IV. CYBER SECURITY THREATS AND RECOMMENDATIONS FOR WIDE AREA MONITORING, PROTECTION, AND CONTROL SYSTEMS

A. Reconnaissance

Reconnaissance attacks allow an attacker to identify potential targets. PMU and PDC are not intended to be placed in every substation, rather, they will be placed sparsely in configurations which allow maximum system visibility with minimal cost. Eaves dropping attacks against PMU can be used to map the synchrophasor system within a transmission system. Such a map can be used to enable large scale attacks which cause invalid state estimator results.

NMAP can be used by an insider or network penetrator to identify IP addresses of connected PMU and PDC. Different PMU and PDC vendors provide different network services on PMU and PDC. The combination of identified services can be used fingerprint PMU and PDC and distinguish between vendors and potentially model numbers and firmware versions. Such information can be used to enable future attacks.

Utilities can defend against reconnaissance attacks by using SSL or IPSEC to encrypt network traffic. Many industrial firewalls include SSL or IPSEC features. Such as system has been proposed in [5]. Enabling IPSEC or SSL between a firewall at the substation and the remote control room will encrypt traffic between electronic security perimeters (ESP). However, such a configuration will not encrypt traffic within the control room LAN or within the substation LAN. As such, IPSEC or SSL between ESP still allows attacks within an ESP or from within one ESP to within another ESP. Ideally, PMU and PDC should include SSL or IPSEC features. Most commercial PMU and PDC do not include SSL or IPSEC features. Alternatively, IEC 61850 90-5 will include optional encryption service. PMU and PDC which support IEC 61850 90-5 should enable this service.

B. Packet Injection

WAMS systems create a feedback control loop from the PMU which provides process measurements through a visualization platform which displays synchrophasor measurements to a human operator. In the WAMS case the human operator is in the feedback control loop and acts as the controller. WAMPAC replace the human operator in the loop with automated control algorithms. In both cases integrity of synchrophasor measurements presented to the human operator or automated controller is critical. Synchrophasor measurements altered by a man-in-the-middle attack or other means can lead to incorrect control actions.
Researchers have identified attacks which use false data injection to manipulate state estimator results [11] [12]. Such attacks can be used to confuse an operator and lead to incorrect control actions by the operator. The authors of [11] present constrained and unconstrained attacks which allow manipulation of targeted state estimator variables without detection by bad data detection. These attacks require manipulation of measurements from multiple locations within a network to avoid trigger a false data detection algorithm such as presented in [13]. Such an attack can be achieved by compromising multiple PMU or by compromising a single PDC. Compromising multiple PMU will require penetration of multiple ESP. Penetrating a network at multiple points is more complex than a penetration at a single location. However, the regularity of utility firewall rules, hardware vendors, and firmware versions may replication of a successful attack within a utility network feasible. PDC accept streams of synchrophasor data from multiple PMU and concentrate the streams into a single output stream. This makes the PDC an ideal penetration target to manipulate large amounts of synchrophasor measurements.

In addition to fooling state estimators WAMPAC can be fooled by manipulating synchrophasor data provided to newly proposed tools for detecting power system events such as semantic driven knowledge discovery algorithms [3]. These systems use classifiers such as stream data mining algorithms to detect events. Altered data could be used to force such algorithms to trigger alarms for small signal oscillations, under frequency alerts, under voltage alerts, system imbalance, etc.

Many PMU are implemented as optional add-ons to existing protection relays. IEEE C37.118 and IEC 61850 90-5 include fields to imbed control signals to the parent relay. Command injection attacks could be used to illicitly trip relays and or modify relay configuration.

As mentioned above, IEEE C37.118 frames do not include a cryptographic signature to prevent frame manipulation in flight and authenticate frame origin. The previous section discussed the use of SSL or IPSEC to provide confidentiality features. SSL or IPSEC can also be used to provide integrity features to prevent frame manipulation. As with the confidentiality case, SSL and IPSEC should be added at the end nodes, PMU and PDC to maximize effectiveness. IEC 61850 90-5 includes cryptographic signatures to prevent frame manipulation and authenticate endpoints. Systems which IEC 61850 90-5 and IEEE C37.118 should be configured to use IEC 61850 90-5 to take advantage of the cryptographic signatures.

C. Denial of Service

Denial of service attacks against synchrophasor systems can cause a loss of system visibility. For both WAMS and WAMPAC denial of service attacks break the feedback control loop. Denial of service attacks may stop delivery of synchrophasor measurements to controllers (operators or software), may stop delivery of control actions, or both.

For WAMS systems this loss of system visibility may mask power system events and cause an operator not to take timely control actions. For WAMPAC denial of service attacks may cause automated event detection algorithms not to operator and may block automated actions from transmission.

Laboratory testing demonstrated that PMU and PDC network interfaces can become unresponsive and temporarily stop transmitting synchrophasor measurements when subjected to large volumes of network traffic. Understanding the packet rate which causes a device to become unresponsive is important for system planning and for creating an effective denial of service mitigation approach. Figure 1 shows a typical availability chart for a single denial of service test against a device. The availability shows the percent availability (Y-axis), percentage of time that a device is able to respond to instrumentation requests, versus packet transmission rate (X-axis).

Utility engineers and network administrators can use the availability chart to define a maximum threshold for traffic congestion at the switch or router within the substation for the different traffic types.

For WAMS systems the high volume of traffic attack would likely be detected and mitigated before causing significant problems. Also, WAMS systems will augment existing state estimation from SCADA sources. The SCADA sources could serve as a back up to this attack during such an attack. For WAMPAC some algorithms require as little as 50 milliseconds to operate and many require less than 200 milliseconds for operation [4]. A short term high volume of traffic attack could cause a WAMPAC to not operate if timed correctly.

It is recommended that utilities monitor network traffic volume in control system networks to detect transmission of high volumes of traffic. Monitoring systems should alert a human administrator to enable mitigation. Routers in the control system network may be configured to limit traffic sent to the PMU or PDC or may be configured to close ports sourcing offensive amounts of network traffic. Automatically closing router ports is potentially dangerous since critical traffic may use the port. A thorough system review should be performed before enabling automatic port closure.

![Figure 1: Availability Chart from Congestion Testing](image)

PMU and PDC transmit continuous streams of measurements at 30, 60, or 120 samples per second. Measurements are time stamped with 1 microsecond accuracy.
relative to universal time coordinated (UTC) time. It is important to understand PMU and PDC behavior after DOS event completes. Testers should confirm that tested devices and network appliances in the route do not queue large volume of IEEE C37.118 data packets which then leads to a synchrophasor stream which is perpetually delayed. PDC hold data from on time PMU to wait for data packets from late arriving PMU streams. A denial of service attack can have a persistent effect if the attacked PMU’s data stream becomes consistently late after the attack. PDC eventually drop old data packets and begin to interpolate. PMU and PDC which recover from a denial of service attack should clear their transmit queues to avoid the aforementioned effects.

Protocol mutation attacks and high volumes of network traffic can lead to longer lasting affects for PMU and PDC. Laboratory testing resulted in systems resetting themselves and in network stacks which were no longer operational. Such attacks can lead to long term loss of visibility for WAMS systems and long term loss of visibility and control for WAMPAC systems. Protocol mutation testing should be performed for all new PMU and PDC and new firmware prior to production installation. Identified vulnerabilities should be reported to PMU and PDC vendors to enable fixes for the entire industry. Protocol mutation vulnerabilities may often also be addressed by adding firewall rules to detect and drop mutated packets. However, firewall rules will only drop packets which originate outside the ESP. Adding intrusion detection and or intrusion prevention systems within an ESP, especially within substations, are also recommended.

V. CONCLUSIONS

Synchrophasor systems are being added to modern power systems to implement wide area monitoring systems (WAMS) and wide area protection and control systems (WAMPAC). Both WAMS and WAMPAC are feedback control loops. Reconnaissance, packet injection, and denial of service attacks against these systems can lead loss of power system visibility and control. Phasor measurement units (PMU) and phasor data concentrators (PDC) are hardware and software devices which will be used to implement these systems. PMU and PDC should undergo cyber security testing to discover and mitigate reconnaissance, packet injection, and denial of service vulnerabilities before use in production WAMS and WAMPAC systems. Finally, WAMS and WAMPAC systems should include SSL or IPSEC features to ensure confidentiality and integrity. WAMS and WAMPAC systems should also include mechanisms to prevent, detect, and mitigate denial of service attacks.

VI. REFERENCES: