IEEE C37.118-2 Synchrophasor Communication Framework
Overview, Cyber Vulnerabilities Analysis and Performance Evaluation

Rafiullah Khan, Kieran McLaughlin, David Laverty and Sakir Sezer
Queen's University Belfast, Belfast, U.K.

Keywords: Smart Grid, Synchrophasor, Cyber Security, Vulnerability, IEEE C37.118.

Abstract: Synchrophasors have become an important part of the modern power system and numerous applications have been developed covering wide-area monitoring, protection and control. Most applications demand continuous transmission of synchrophasor data across large geographical areas and require an efficient communication framework. IEEE C37.118-2 evolved as one of the most successful synchrophasor communication standards and is widely adopted. However, it lacks a predefined security mechanism and is highly vulnerable to cyber attacks. This paper analyzes different types of cyber attacks on IEEE C37.118-2 communication system and evaluates their possible impact on any developed synchrophasor application. Further, the paper also recommends an efficent security mechanism that can provide strong protection against cyber attacks. Although, IEEE C37.118-2 has been widely adopted, there is no clear understanding of the requirements and limitations. To this aim, the paper also presents detailed performance evaluation of IEEE C37.118-2 implementations which could help determine required resources and network characteristics before designing any synchrophasor application.

1 INTRODUCTION

Synchrophasors are the measurements of electrical quantities across different parts of the power system synchronized using a common precise time source. For higher accuracy and utilizing a universal time source, synchrophasors are normally time-stamped using Global Positioning System (GPS) time. With the development of synchrophasor technology, numerous applications have been proposed. Today, synchrophasor technology is being used in Wide-Area Monitoring System (WAMS), Wide-Area Protection and Control System (WAPCS), islanding detection, determining stability margins, system dynamics visualization and recording, enhancing operator situational awareness, etc (Schweitzer et al., 2008).

The aim of synchrophasor technology is to represent power system condition/status in real time. This requires transmission of synchrophasor measurements across large geographical areas in real-time with very low latency. Using IP based communication is feasible where it utilizes already available high speed infrastructure. To transmit synchrophasor measurements over an IP network, a suitable communication framework is required. The IEEE C37.118-2 standard evolved as one of the most successful and widely adopted communication framework for synchrophasor applications. The IEEE C37.118-2 standard specifies messaging format but does not put any restriction on the choice of communication medium or transport protocol. Further, IEEE C37.118-2 standard does not addressed security features. The synchrophasor measurements are transmitted over insecure IP network which make IEEE C37.118-2 communication highly vulnerable to cyber attacks (Stewart et al., 2011).

This paper describes the IEEE C37.118-2 standard in details highlighting its main features and capabilities. It also explores how vulnerabilities can be exploited to launch different types of attacks on IEEE C37.118-2 communication system. In particular, reconnaissance, authentication/access, man-in-the-middle, replay/reflection and denial of service attacks are explored. These attacks alone or in combination may severely impact the synchrophasor applications. They may leave different components of the synchrophasor system not being able to communicate with each other or unintentionally performing wrong decisions. For most critical synchrophasor applications, cyber attacks could potentially cause severe damage to the physical equipment. Therefore, it is vital to effectively analyze and mitigate cyber vulnerabilities in the synchrophasor system. Most often, attackers try to exploit communication framework to

Khan, R., McLaughlin, K., Laverty, D. and Sezer, S.
IEEE C37.118-2 Synchrophasor Communication Framework - Overview, Cyber Vulnerabilities Analysis and Performance Evaluation.
DOI: 10.5220/0005745001670178
In *Proceedings of the 2nd International Conference on Information Systems Security and Privacy (ICISSP 2016)*, pages 167-178
ISBN: 978-989-758-167-0

launch attacks. To protect IEEE C37.118-2 communication framework against attacks, this paper recommends an effective security mechanism where security policy and keying material periodically change. Such refreshment of security credentials prevent attacker never being able to discover a valid secret key. Even if an attacker somehow discovers secret key through analyzing captured packets, it will no longer remain valid. In short, the main contributions of this paper include:

1. Analysis of vulnerabilities in IEEE C37.118-2 standard through different cyber attacks and their impact on the synchrophasor application.
2. Recommendation of an efficient security mechanism integrated in IEEE C37.118-2 standard and evaluation of its effectiveness.
3. Detailed performance evaluation of IEEE C37.118-2 standard to analyze requirements and limitations in a practical environment.

The rest of the paper is organized as follows: Section 2 addresses related work. Section 3 describes a generic synchrophasor system and its basic building blocks. Section 4 describes IEEE C37.118-2 standard, different types of defined messages, and communication modes and protocols. Section 5 analyzes cyber vulnerabilities in IEEE C37.118-2 standard and recommends a suitable security mechanism by addressing its unique features. Section 6 presents detailed performance evaluation of IEEE C37.118-2 implementations. Finally, Section 7 concludes the paper.

2 RELATED WORK

Synchrophasor technology got increasing popularity since its development. Its applications quickly progressed from simple data visualization and archiving or postmortem analysis to several real-time protection, monitoring and control applications. This is due to the capability of synchrophasors representing power system condition in real time and taking prompt control actions. The authors in (Schweitzer et al., 2008) described several advanced real-time synchrophasor applications developed over time. Several efforts were put to develop a suitable communication standard for synchrophasors. IEEE C37.118-2 evolved probably as the first most successful communication standard. It was originally based on IEEE 1344 standard and its evolution is explained in (Martin et al., 2008). The authors have also highlighted key differences between old and new versions and introduced several applications for IEEE C37.118-2 standard.

Since, most synchrophasor applications involve transmission of data across large geographic areas using non-reliable and insecure IP network, analysis of potential cyber vulnerabilities and threats drawn more and more research attention (Allgood et al., 2011). It is worth to mention that IEEE C37.118-2 standard does not include any security feature and making applications highly vulnerable to cyber attacks. Although cyber security research in general is not new, still implementation of experimental tools or strategies to effectively mitigate vulnerabilities for synchrophasor system is quite limited.

Authors in (Stewart et al., 2011) presented best practice techniques (such as firewall, Virtual Private Network (VPN)) and verified by experiments to overcome cyber vulnerabilities. Their main focus was to ensure information security between substation and control center. However, security within the substation LAN or within the control center LAN has negligible considerations. Authors in (Morris et al., 2011) evaluated the resilience of Phasor Measurement Units (PMUs) against denial of service attacks using IEEE C37.118. They flooded PMU with ARP request packets, IPv4 packets and PPPoE packets and monitored its unresponsiveness. Further, the authors evaluated resilience against malformed packets through protocol mutation tests. Several other efforts also tried to protect synchrophasor network against cyber attacks (Sikdar and Chow, 2011).

Along with information security, several research efforts also focused on ensuring PMU and Phasor Data Concentrator (PDC) security (D'Antonio et al., 2011). A further work analyzing PMUs vulnerabilities using IEEE C37.118 protocol was performed by (Coppolino et al., 2014). Synchrophasor applications require high time synchronization which is normally achieved through GPS. GPS spoofing may leave severe impact on any synchrophasor application. This is analyzed by authors in (Shepard et al., 2012) that GPS spoofing can cause intentional tripping of power generators and may even cause physical damage to equipment. A further work analyzing detection of GPS spoofing attacks is presented in (Yu et al., 2014).

In short, cyber vulnerabilities analysis is a hot research topic and numerous research articles are available in literature. There are also number of available surveys analyzing cyber threats relevant to smart grid in general, PMU network, and/or synchrophasor applications (Boyer and McBride, 2009), (Baumeister, 2010), (Yan et al., 2012), (Zargar et al., 2013), (Beasley et al., 2014).

Most of the research in literature addresses cyber vulnerabilities for power system in general with few have little focus on synchrophasors network. No

much work is available on analyzing cyber vulnerabilities in IEEE C37.118-2 communication standard. This paper analyzes cyber vulnerabilities in IEEE C37.118-2 standard and evaluates possible impact on the synchrophasor application. Further, this paper also recommends a security mechanism to be used with IEEE C37.118-2 standard to achieve protection against different cyber attacks. Although IEEE C37.118-2 standard is being widely used, its requirements and limitations in practical environment have never been addressed. To this aim, this paper also presents detailed performance evaluation of IEEE C37.118-2 standard.

3 OVERVIEW OF SYNCHROPHASOR MEASUREMENT SYSTEM

A synchrophasor system consists of several basic building blocks including GPS receivers, PMUs, PDCs, communication network and equipment and visualization, monitoring or control software as shown in Fig. 1. A PMU is the device that performs measurements of synchrophasor data which represent electrical quantities for current/voltage waveform at a given time instant. The measurements performed by PMU are normally time stamped to a common and highly precise time source often GPS. Thus, PMU devices are normally equipped with a GPS antenna. The PMU can be a standalone device with dedicated functionality or it may co-exist on a multi-functional device. There are two possible modes of operations of PMU; commanded and spontaneous. In commanded mode, PMU establishes bi-directional communication with its peer (local or remote PDC or application). The peer can send commands to PMU to control its operations (e.g., stop/start or control synchrophasors transmission). The communication between PMU and its peer is normally private unicast in commanded mode. In spontaneous mode, PMU operations cannot be controlled by its peer. The communication is uni-directional (from PMU to its peer) and PMU is not able to receive any commands. The communication between PMU and its peers is normally multicast in spontaneous mode of operation.

Another important element in a synchrophasor system is PDC. PDC is a device which receives synchrophasor data from more than 1 PMU and aggregates and transmits as one output stream. A PDC may be receiving data from multiple PMUs (i.e., substation PDC in Fig. 1) or multiple PDCs (i.e., Control Center PDC in Fig. 1).

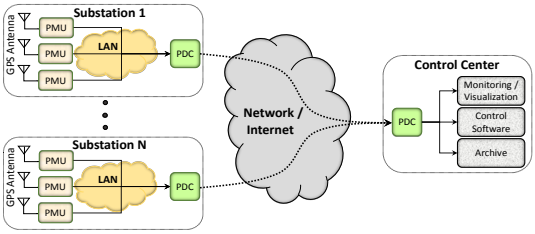


Figure 1: Generic synchrophasor communication system.

As illustrated in Fig. 1, the control center may be receiving data from more than one substation and handover to respective application. The application may be designed for simply archiving data, performing visualization/monitoring or performing protection and control functionalities. It can be observed in Fig. 1 that the synchrophasor data could be directly provided by PMUs to respective application without needing any PDC. However, such approach will result in a lot of network traffic overhead (analyzed in Section 6) and ambiguity for control application in interpreting data from each PMU. Thus, the substation PDC makes the transmission much more efficient by sending out only one stream of data instead of multiple streams.

As depicted in Fig. 1, synchrophasor measurements are transmitted in real-time over insecure public Internet. Thus, a suitable communication protocol is required that can ensure security as well as low transmission latency. IEEE C37.118-2 is most wide used communication framework for synchrophasor applications. Although it lacks security features and is vulnerable to cyber attacks. Section 4 analyzes importance of security and presents a suitable security mechanism for IEEE C37.118-2 standard.

4 IEEE C37.118-2 COMMUNICATION STANDARD

Synchrophasor applications demand real-time transmission of messages with very low latency. This section briefly addresses the IEEE C37.118-2 standard, which evolved as one of the most suitable and well tested standard for the transmission of synchrophasor measurements. IEEE C37.118-2 standard effectively addresses synchrophasor requirements, presents suitable format and structure for messages and ensures to keep communication overhead to the minimum possible level.

4.1 Overview

With the development of synchrophasor technology and its need for transmission over wide area networks, IEEE established a working group to develop a suitable communication standard. The working group developed IEEE 1344 in 1995, the first standard for transmission of synchrophasor measurements in real-time. IEEE 1344 addresses data formats, structures and time synchronization of data from multiple sources. However, it does not address measurement accuracy, support for transmission hierarchy, hardware and software requirements, process for calculating synchrophasors, security mechanism and transport protocol. These considerations are left to the users based on their needs and application requirements.

In 2005, IEEE 1344 was replaced by an improved IEEE C37.118 standard which overcomes the limitations of the previous standard and focuses on the requirements for future power systems. The most obvious improvements include the introduction of methods for evaluating measurement performance, accounting measurements from multiple PMUs and a more complete messaging system. It introduced Total Vector Error (TVE) criterion to check if the measurements are compliant with the standard. It mainly shifted focus from the measurement method to the measurement results. Thus, any algorithm or technique can be used as long as it produces acceptable results.

The IEEE C37.118 standard was limited to address accuracy requirements only for steady state conditions. Over time, the IEEE realized the need to address requirements for synchrophasor measurements also under dynamic conditions. Further, IEEE C37.118 standard combined synchrophasor measurement and communication functions. To overcome the shortcomings and fix some minor errors, IEEE C37.118 split into two parts in 2011, IEEE C37.118-1 and IEEE C37.118-2. IEEE C37.118-1 addresses requirements for synchrophasor measurements under dynamic conditions which makes it very suitable for most of the applications where the phasor measurements could be severely affected by system noise and disturbances. Whereas, IEEE C37.118-2 addresses only the communication framework and requirements for transmission of synchrophasors. It is worth mentioning that IEEE C37.118-2 is an extended standard with some new features but provides full backward compatibility with original IEEE C37.118. Further, it also does not put any restriction on the choice of communication protocol, communication medium and the mode of communication.

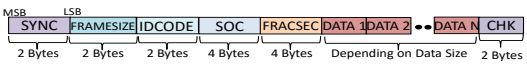


Figure 2: IEEE C37.118-2 standard message format.

4.2 Message Format and Types

IEEE C37.118-2 specified a standard format for different types of the messages as depicted in Fig. 2. Each message begins with identification and synchronization word (SYNC), followed by FRAMESIZE (total Bytes inside message), IDCODE (ID of the synchrophasor data source), SOC (Second Of Century count since epoch midnight 01.01.1970), FRACSEC (FRACtion of SECond and time quality), DATA (Depends on message type) and CHK (Cyclic Redundancy Check (CRC)). The content and structure of DATA field is different for different types of messages. IEEE C37.118-2 standard described four types of messages: data, configuration, command and header. Header message carries descriptive information in human readable format while all other types of messages are in machine readable format. Command messages are sent by the control application to data source (e.g., PMU, PDC) as instructions/orders while data, configuration and header are sent by the data source.

4.2.1 Data Message

Data messages are sent by the data source which include real-time measurements of synchrophasors. The sending device can be a PMU (containing single block of data) or PDC (containing multiple blocks of data). Each block of data contains a complete structure according to IEEE C37.118-2 (phasors in polar or rectangular format, analog and digital values, frequency deviation, rate of change of frequency etc). In the case of a PDC, data from multiple PMUs is correlated to a particular time stamp and transmitted in a single message.

4.2.2 Configuration Message

Configuration messages contain information and processing parameters (calibration factors, meta data, data types, etc) for a synchrophasor data stream. It basically provides necessary information to the receiver on how to decode data messages. IEEE C37.118-2 standard identified three types of configuration messages: CFG-1, CFG-2 and CFG-3. CFG-1 and CFG-2 were also present in the first IEEE C37.118 standard published in 2005. CFG-1 represents data source (PMU, PDC) capabilities and the data it will be reporting. CFG-2 represents measurements currently

being transmitted in data messages. CFG-3 is similar to CFG-1 and CFG-2 but includes added information and flexible framing.

4.2.3 Header Message

Header messages carry human readable descriptive information about the data source, scaling algorithms, filtering etc. It does not have a special format for the DATA field (in Fig. 2) but carries information in ASCII format.

4.2.4 Command Message

Command messages are orders received by a data source device. These orders include but are not limited to: start and stop transmission of data messages, send header message, send CFG-1, CFG-2 or CFG-3 configuration message etc.

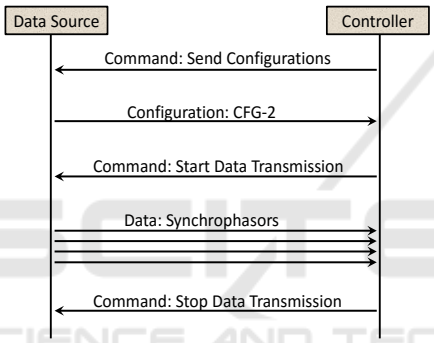


Figure 3: Generic IEEE C37.118-2 communication scenario for data source operating in commanded mode.

Fig. 3 depicts a generic communication scenario when the data source operates in commanded mode. For simplicity header message is not shown which may be requested by control application/controller using command message. Upon receiving request, data source sends a header message to the controller. When a data source operates in spontaneous mode (cannot receive commands), then communication should only contain data and configuration messages. A data source will ensure to send configuration messages whenever necessary to enable the receiver to correctly decode data messages.

4.3 Communication Modes and Protocols

IEEE C37.118-2 only specifies different types of messages and their structure, format and content. It does not put any restriction on communication mode or choice of transport protocol. Most industrial implementations targeted either RS232 serial or IP based network communication depending on the application. The possible communication modes include: client-server/unicast (one device sends data which is received by one other device), multicast (one device sends data which is received by a group of device) and broadcast (one device sends data which is received by all available device in the network). The freedom on the choice of transport protocol leads to several combination: (i) TCP for all types of messages, (ii) UDP for all types of messages, and (iii) data messages on UDP while all other messages on TCP. Each combination will have its own pros and cons which we will try to analyze in Section 6.

5 SECURITY ANALYSIS & RECOMMENDATIONS

IEEE C37.118-2 does not specify any kind of cryptographic signature. Thus, packets are vulnerable to spoofing, being modified in the network during transmission or being transmitted by un-authorized peers. This section first analyzes how vulnerabilities in IEEE C37.118-2 based communication system could be exploited in the form of different possible attacks. To overcome the vulnerabilities, a security mechanism based on Group Domain of Interpretation (GDOI) is recommended that could be efficiently integrated in IEEE C37.118-2 communication systems (Weis et al., 2011). Finally, this section also analyzes the effectiveness of the recommended security system.

5.1 Cyber Vulnerabilities Analysis

Cyber vulnerabilities in IEEE C37.118-2 could be exploited by unauthorized entities/attackers to extract, modify or insert messages in the network. With the knowledge of vulnerabilities, different types of attacks could be launched which may impair the communication and cause physical damage to the synchrophasor system. The attacks described here are based on the generic synchrophasor system depicted in Fig. 1.

5.1.1 Reconnaissance Attack

In a reconnaissance attack, an adversary first tries to discover vulnerabilities in the network which could be exploited for the actual attack. It is the unauthorized learning process of the network devices or communication system to discover available services, open ports, identify network stack daemons or the operating system, etc. Reconnaissance itself is not normally a harmful action but provides necessary information

for the adversary to plan and launch more severe attacks such as Denial of Service (DoS) attack, access attack etc.

Reconnaissance attack could be launched either on the physical device or on the communication network. The main focus here is the communication network. Through eavesdropping on network traffic of IEEE C37.118-2, attackers could learn about the substation name, names and locations of different physical components (e.g., PMU, breakers) and configurations of the device sending packets. Such information is normally carried by IEEE C37.118-2 configuration messages. The attacker may be interested in controlling the PMU operations (or the whole substation depending on synchrophasor application) through eavesdropping on command messages. Eavesdropping on data messages will enable an attacker to know the current physical state of the substation. The level of risk through eavesdropping on header messages might be low or high depending on the synchrophasor application. In short, eavesdropping on different types of IEEE C37.118-2 messages can enable an attacker to launch high impact attacks on the substation.

5.1.2 Authentication/Access Attack

Authentication is an access control mechanism which ensures that only authorized users can get access to a system or resources. It is the process in which credentials provided by the client devices are checked and compared to the information on file/database and access is granted only if the credentials match. Unauthorized access to a device or information is sometimes also referred to as access attack.

IEEE C37.118-2 does not specify any form of authentication between communicating devices. Thus, it is possible that the control application or the PDC interprets messages being received from genuine PMUs but it may not be the case. The messages may be received from non-intended PMUs or from attackers through packet injection or replay attacks.

Not only on the network traffic, access attacks may also take place on the physical device e.g., PMU/PDC or control center. Once attacker has control on the physical device, he can easily alter packets being transmitted or injects packets on its own.

5.1.3 Man In The Middle Attack

In a Man In The Middle (MITM) attack, the attacker impersonates two communicating devices and makes them believe that they are directly communicating with each other. Instead, the attacker lies in the middle and is able to intercept each and every packet exchanged between the two communicating devices. The MITM attack may also involve connection/session hijacking. The attacker capabilities in a successful MITM attack include hijacking packets, altering or dropping them and injecting new packets.

The MITM attack can target any message type in an IEEE C37.118-2 synchrophasor communication system. However, its impact could be much more severe on command, configuration and data messages compared to header messages. Targeting configuration messages will enable an attacker to severely disrupt the synchrophasor application. The attacker can easily leave a receiver (applications at the control center) unable to decode/understand data messages. This makes attack on configuration messages the most attractive choice for an attacker. Command messages control the whole communication and an attacker may intentionally disrupt or start/stop the transmission of data messages. Attacks on data messages may alter/modify the synchrophasor measurements and make the receiver believe that the data is genuine. This will leave receiver unintentionally performing decisions based on incorrect data. The impact of MITM attack on header messages is application dependent.

5.1.4 Replay or Reflection Attack

Replay attacks rely on MITM attack to record communication between two devices and replay it to hide real system information. The replay packets might lead to incorrect decisions by the receiving device. Further, this attack does not require detailed knowledge of the underlying system. The impact of replay attacks on different types of IEEE C37.118-2 messages is similar to a MITM attack. Replaying data messages may cause the receiver to carry out incorrect actions. If configurations change, replaying old configuration messages could prevent the receiver from decoding upcoming data messages.

5.1.5 Denial of Service Attack

The DoS attack is different from previous attacks as it does not require unauthorized access to network traffic or the communicating devices but simply attempts to disrupt or block communication between the communicating devices. The DoS attacks overwhelm the target device with high data rate bulk packets so that it becomes irresponsive due to lack of available resources (bandwidth, CPU, memory etc) or buffer overflow. Referring to Fig. 1, the DoS attack can be on the communication link between PMUs and substation PDC, substation PDC and control center PDC or control center PDC and the control applications.

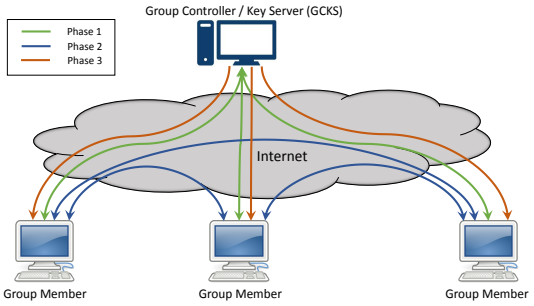


Figure 4: Generic GDOI-based communication scenario.

The most feasible choice for most of the attackers will be targeting communication link between substation PDC and control center PDC. This will lead to loss of substations visibility for the control center.

Normally, DoS attacks will prevent all types of IEEE C37.118-2 messages being processed by the receiver. However, if the DoS attack is weak, it may result in less number of messages being lost at the receiver. Depending on the type of message (that is lost), the impact of DoS attack could be different. Loss of configuration message will leave receiver unable to decode upcoming data messages. Loss of few data messages will make difficult for the receiver to take decisions due to not having enough information about the synchrophasor system dynamics. Loss of command message will prevent receiver from controlling data source. While the impact of DoS attack on header message is application dependent.

5.2 Enabling Security based on GDOI

To secure the IEEE C37.118-2 based communication system against attacks, its inherent vulnerabilities should be addressed. Further, a mechanism should be introduced that can make attacker activities visible to the user. To this aim, this paper suggests the use of GDOI to ensure secure communication of synchrophasors using IEEE C37.118-2. GDOI is a group key management protocol published by Cisco Systems & MIT (Weis et al., 2011). Since publication, GDOI is getting increasing popularity. It has already been adopted in IEC 61850-90-5, a real time communication system for the smart grid applications. GDOI ensures that the communication remains highly secure by constantly changing group Security Associations (SAs).

The generic GDOI-based communication scenario is depicted in Fig. 4. The GDOI group key management model consists of two types of devices: Group Controller/Key Server (GCKS) and Group Member (GM). GCKS is responsible to maintain group security policy and generation of keys. As shown in Fig. 4, the GDOI mechanism consists of three phases:

- **Phase 1:** The group members authenticate and register with the GCKS in order to get IPsec SAs which are necessary to secure communication between the group members. The registration phase is secured through encryption using Pairwise key. It is possible that GCKS manages more than one group and each group has different SAs. To request security policies and keys, group members need to provide group ID to GCKS. After the group ID is verified, GCKS sends group security policy to the group member. The group member checks if it can handle the policy and acknowledges to the GCKS in order to download the Key Encryption Key (KEK). The KEK is used to encrypt the message in which GCKS provides Traffic Encryption Key (TEK) to the group member.
- **Phase 2:** The group member uses TEK as an IPsec SA to encrypt messages it exchanges with other group members. In synchrophasor applications, TEK will be used to encrypt different types of IEEE C37.118-2 messages.
- **Phase 3:** Remember, GCKS assigns both KEK and TEK keys with certain validity period. The keys should be refreshed periodically and provided to group members before the expiry of previous keys to enable uninterrupted secure communication between group members. This keys update mechanism can be unicast to a single group member or multicast to all group members. Multicast update messages have no delivery acknowledgment and are transmitted multiple times to account for any packet loss.

The GDOI protocol is based on Internet Security Association and Key Management Protocol (ISAKMP) to protect the group members authentication and registration in Phase 1. All the group members and GCKS must have the same ISAKMP policy acquired via an out of band method. The ISAKMP policy should be strong enough as the whole GDOI mechanism security depends on it. Two new ISAKMP exchanges are defined in GDOI: GROUPKEY-PULL and GROUPKEY-PUSH. GROUPKEY-PULL exchange is used in Phase 1 as explained above. GROUPKEY-PULL exchange allows group members to request group policy and keying material (KEK, TEK) from GCKS. GROUPKEY-PUSH exchange is Phase 3 in which GCKS distributes the updated group policy and keying material to all authorized group members before the expiry of the previous keying material.

It is important that GCKS is explicitly a trusted entity by all group members. If no authentication is

performed, MITM attack between GCKS and group member could be possible for a rogue GDOI participant. It is also important that GCKS explicitly authenticates/authorizes each group member before sending them group policy and keying material. The GCKS should implement a method for authenticating members (e.g., by maintaining an up to date authorization list).

5.3 Benefits of GDOI based Security

All the different types of attacks described in Section 5.1 could be mitigated if the devices and IEEE C37.118-2 communication are appropriately secured. As explained before, the reconnaissance attack could either take place on the network devices or the communication network. The main focus here is only on the communication network. If IEEE C37.118-2 messages are encrypted, eavesdropping on network traffic would not benefit the attacker. Although IEEE C37.118-2 does not include authentication, still the authentication or access attacks could be prevented. It is due to the fact that unauthorized users could not acquire security policy and keying material from GCKS. Without having valid TEK, devices are not be able to communicate. Similarly to eavesdropping on network traffic, MITM attack could be easily prevented due to encrypted messages.

The replay attacks replay the recorded communication between two devices. These attacks could also be prevented due to periodic security policy and keying material refreshment mechanism used in GDOI. The replayed messages might be based on old keying material which is no longer valid. This obviously depends on the validity period of keys assigned by GCKS. A shorter key validity period could effectively prevent IEEE C37.118-2 based communication from replay attacks. The DoS attacks overwhelm the target device with high traffic. The impact of DoS attacks can be mitigated to a degree if the receiver simply discard messages without processing them. This is only possible if the receive knows that messages are received from unauthorized device. The GDOI mechanism prevents any unauthorized device being able to communication with authorized devices.

Thus, different types of attacks could be prevented as long as key distribution mechanism is not compromised. GDOI assumes that the network is insecure and could be exploited by attackers. However, it assumes that GCKS and group members are all trusted and secure. Any compromised group member may enable attacker to reveal group policy and keying material necessary to eavesdrop on network traffic. Therefore, group members must have proper security in place preventing unauthorized access to them.

GDOI consists of three different phases as described in Section 5.2. From a security point of view, attackers will most probably look for vulnerabilities in Phase 1 ISAKMP authentication, GROUPKEY-PULL and GROUPKEY-PUSH exchanges of secret keying material. The effectiveness of these exchanges is briefly described in the following.

5.3.1 Phase 1 ISAKMP Authentication

The authentication in Phase 1 is achieved via pre-shared keys assuming secure GCKS and group members. Any connection hijacking or MITM attack will foil the authentication of one or more communicating peers during key establishment. An attacker may launch replay or reflection attack between GCKS and a group member and replays captured messages to a group member. The replay of previous key management messages could be detected as GDOI relies on hash based message authentication along with Phase 1 nonce mechanism. Further, GDOI provides prevention against DoS attacks by identifying spurious messages through a Phase 1 cookie mechanism prior to processing cryptographic hash.

5.3.2 GROUPKEY-PULL Exchange

GROUPKEY-PULL exchange is used by group members to request security policy and keying material from GCKS. It is assumed that GCKS and group members are secure and properly authenticated in Phase 1. The GROUPKEY-PULL exchange is protected against connection hijacking and MITM attacks as the authentication involves a secret known only to GCKS and group members when constructing HASH payload. Thus, the attacker could not alter a message that goes undetected by GCKS or group members. GCKS also keeps track of previously processed GROUPKEY-PULL messages (e.g., message HASH) and directly rejects messages previously processed in order to not overload the computational resources. This contributes to preventing against replay and DoS attacks.

5.3.3 GROUPKEY-PUSH Exchange

GROUPKEY-PUSH exchange is used by GCKS to update group members about new security policy and keying material prior to the expiry of previous SAs. The message is encrypted by KEK which is only known to group members and distributed in previous GROUPKEY-PUSH exchange or GROUPKEY-PULL exchange. The KEK is only known to GCKS and group members (both are assumed secure) and

this provides protection against connection hijacking and MITM attacks. The GROUPKEY-PUSH messages carry an increasing sequence number which provides protection against reflection/replay attacks. A group member will simply discard a GROUPKEY-PUSH message if it contains sequence number the same or lower than a previously received message. Further, cookies provide protection against DoS attacks for GROUPKEY-PUSH message.

6 PERFORMANCE EVALUATION

The implementation of the IEEE C37.118-2 library was carried out in Linux OS using Python programming language. A number of experiments were performed to analyze the requirements, effectiveness and limitations of IEEE C37.118-2 using different transport protocols. Currently, research focuses on the efficient design of PMUs/PDCs on compact hardware. To this aim, all the experimental results reported in this section were performed on a low power pocket PC i.e., Raspberry Pi v2 (CPU: ARMv6 700 MHz, Memory 512 MB, Power consumption: 3.6 W (idle) & 3.8 W (full load)).

It is worth noting that any synchrophasor application based on IEEE C37.118-2 will have its own resource requirements and performance metrics based on its size, complexity and capabilities. The reported results in this section are performance metrics only ascribable to IEEE C37.118-2 library in any developed application. For all the reported results, it is assumed that the PMU/PDC sends data messages each carrying 2 phasors, 2 analog values and 1 digital word, all expressed in integer format except frequency deviation (FREQ) and rate of change of frequency (DFREQ) in floating point format. The same settings are also reflected in Configuration (Config) messages.

6.1 Communication Overhead

The communication overhead is a significant performance metric for any protocol. It indirectly reflects the maximum size of data that can be included inside any packet. Further, it is also a factor affecting channel bandwidth requirements for transmission of messages. Normally, synchrophasor systems involve high data transmission rates. This in turn requires more channel bandwidth especially if the protocols communication overhead is high.

The overhead for IEEE C37.118-2 is reported in Table 1 considering different types of messages sent over UDP or TCP. It can be observed that the communication overhead is significantly low for Data and Config messages; the two most frequently exchanged messages in IEEE C37.118-2 based communication systems. Compared to UDP, TCP has quite high communication overhead due to exchange of several additional packets during connection establishment and termination.

Table 1: Size of real information and message formatting as percentage of overall communication overhead (including headers and protocol scemantics).

	Using UDP		Using TCP	
	RealInfo	Formatting	RealInfo	Formatting
Data	26.83 %	21.95 %	3.77 %	3.08 %
Config	86.70 %	3.67 %	40.30 %	1.71 %
Command	3.33 %	26.67 %	0.36 %	2.85 %
Header	21.62 %	21.62 %	2.78 %	2.78 %

Fig. 5 depicts how the communication overhead is affecting with the increasing size of data messages. The size of real information inside the packet increases when a PDC aggregates data from multiple PMUs which in turn results in lower communication overhead. The number of PMUs data inside a PDC depends on its location. A local/substation PDC may aggregate data from 10 PMUs whereas regional control center or super PDC may carry data from up to 1000 PMUs (Grigsby, 2012). Fig. 5 illustrates that UDP is the most favorable choice to transmit small size packets. Choosing a low communication overhead option (i.e., UDP) could significantly reduce channel bandwidth requirement. However, UDP is a non-reliable protocol. The TCP could be a suitable choice for transmission of large size packets (when its overhead is not significantly high compared to UDP) to achieve reliability and other benefits offered by TCP in general.

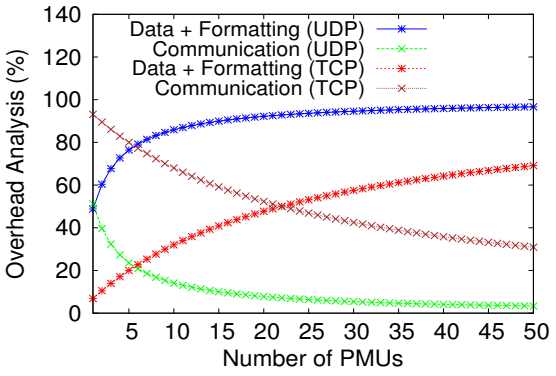


Figure 5: Overhead analysis when PDC aggregates data from multiple PMUs.

6.2 Impact of Latencies

Latency is the critical factor that can impair the performance of real-time applications in three ways: (i) application latency which is ascribable to encoding and decoding of different types of messages, (ii) network latency which is time taken by packets to traverse the network, and (iii) transport latency which is time taken by transport protocol e.g., TCP to acknowledge or retransmit data. Network and transport latencies are linked with available bandwidth (low latencies are observed on high bandwidth channels and vice versa) whereas application latency depends on the processing power of a given device. Table 2 presents the sum of all three latencies for different types of IEEE C37.118-2 messages averaged over 100 transmissions. To avoid clock synchronization issues between sender and receiver, latency measurements were calculated from two-way time measurements. The observed latencies are comparatively low for UDP than TCP but the difference is not too significant. It is due to the fact that most of the latency is ascribable to encoding and decoding of messages on a low power device i.e., Raspberry Pi. Based on the values reported in Table 2, there should be ideally no packet loss if messages are transmitted at appropriate rate (roughly 90 and 97 data messages per second for TCP and UDP, respectively). Practically, high data rates can be easily supported (especially for UDP) using parallel processing and large size socket buffer.

It can be observed in Table 2 that latencies are different for different types of messages. This is due to different message size, format and structure. The latencies are expected to increase with increase in message size and complexity. Which will in turn affect the maximum possible data transmission rate. Fig. 6 divides latencies into two parts: (i) time required to encode the message and send it to receiver device, and (ii) time required to receive a message, analyze/decode it and extract data. It is apparent from Fig. 6 that encoding latencies are quite low compared to decoding latencies. It is due to the fact that PDC simply aggregates data from multiple PMUs during the encoding process whereas control application in decoding process performs deep inspection of received packet to separate data of each PMU and analyze each and every bit according to Config. message. This obviously depends on the processing power of the devices performing PDC and control application functionalities (Raspberry Pi in this case).

Compared to UDP, TCP provides several benefits such as flow and error control, reliability and guaranteed delivery of data. However, TCP is normally not suggested for high rate real-time transmission of messages. To analyze the suitability of TCP for real-time transmissions, Fig. 7 reports packet loss with increasing data rate. For each data rate, 10,000 packets were transmitted and number of lost packets were counted. It can be observed in Fig. 7 that the packet loss increases rapidly with increase in the data transmission rate. This is due to the fact that each lost packet causes an interval of packets loss. If TCP waits for the recovery of lost packets, data transmission rate will be affected leaving worst effects on the performance of real-time applications as well as throughput. Another limitation of TCP is its incapability to support multicast instead of establishing 1-1 connection which also increases the network bandwidth requirements.

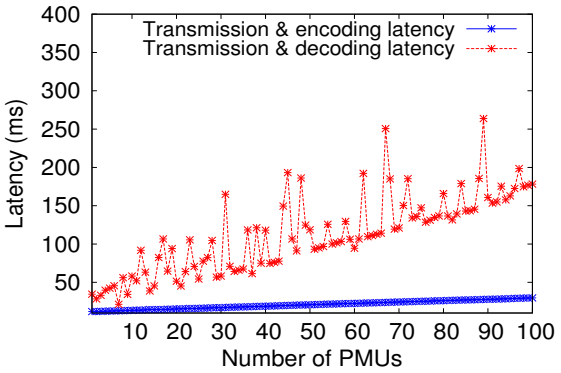


Figure 6: Transmission & encoding/decoding latencies when PDC aggregates data from multiple PMUs.

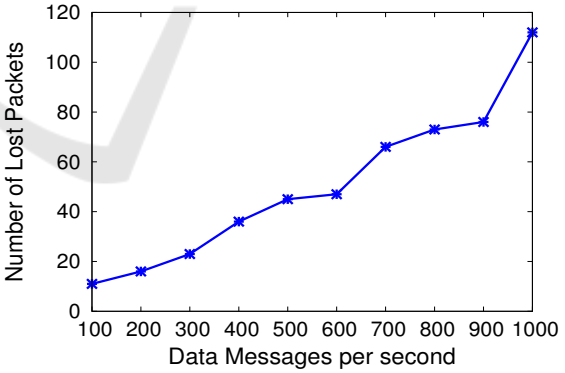


Figure 7: Packet loss with increase in data transmission rate using TCP as transport protocol.

6.3 Resource Requirements

This section analyzes the resource requirements in terms of CPU and bandwidth. For applications to perform well, the minimum required processing power and bandwidth should be available. Fig. 8 presents the minimum required resources with increase in data transmission rate. It can be observed in Fig. 8(a)

Table 2: Latencies for different types of messages.

	Using UDP				Using TCP			
	Min	Average	Max	Std. Dev.	Min	Average	Max	Std. Dev.
Data	4.83 ms	10.28 ms	19.71 ms	1.96 ms	9.62 ms	11.07 ms	15.03 ms	1.13 ms
Config	7 ms	8.74 ms	17.26 ms	1.42 ms	7.82 ms	9.57 ms	13.57 ms	1.19 ms
Command	4.07 ms	5.89 ms	9.75 ms	1.39 ms	4.79 ms	6.44 ms	11 ms	1.21 ms
Header	4.17 ms	6.28 ms	13.83 ms	1.54 ms	5.98 ms	7.03 ms	11.89 ms	1.34 ms

that CPU usage of the application increases with increase in data transmission rate. Fig. 8(a) depicts results obtained on Raspberry Pi and will be different for other types of devices depending on the available CPU power. The device processing power also affects the message encoding/decoding latencies as reported in Section 6.3.

The bandwidth requirement is the most critical factor for any communication protocol. High data rate on low bandwidth links can cause traffic congestion which will in turn result in packet loss. In computing, bandwidth is the bit rate or maximum throughput that can be supported by a given communication medium. It can be observed in Fig. 8(b) and Fig. 8(c) that bandwidth requirement increases linearly with increase in data transmission rate. Further, the bandwidth requirement depends on the message size. Large size messages (e.g, including more phasors) have significant high bandwidth requirement especially at high data transmission rates. Further, the bandwidth requirement also has strong connection with the communication overhead. TCP communication overhead is higher than UDP resulting in 3-4 times increase in bandwidth requirement at a given data rate. With TCP, IEEE C37.118-2 based communication requires roughly 500 kbps at 100 data messages per second transmission rate which is lower than the maximum bandwidth of most Internet access technologies except the dialup (dialup/modem: 56 kbps, ADSL lite: 1.5 Mbps, ADSL1: 8 Mbps, ADSL2+: 24 Mbps, wireless 802.11b: 11 Mbps, wireless 802.11g: 54 Mbps, wireless 802.11n: 600 Mbps, Gigabit Ethernet: 1 Gbps, etc). Some Internet access technologies may not provide enough bandwidth for high synchrophasor data transmission rates (especially for PDC that aggregates data from multiple PMUs).

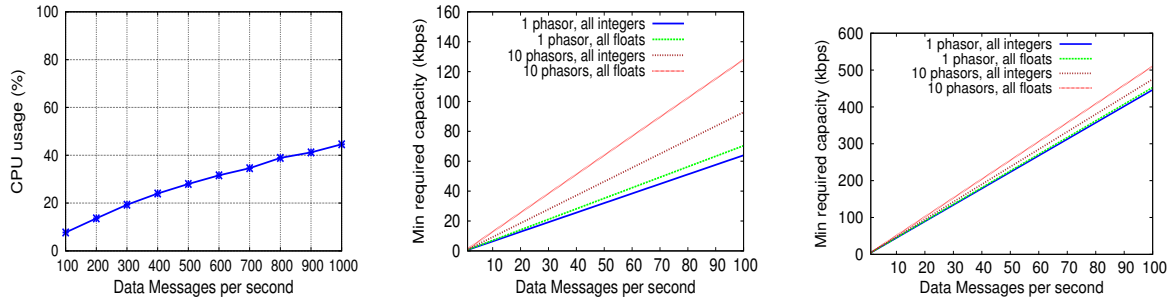
6.4 Remarks

Based on the latencies, observed packet loss and bandwidth requirement, TCP is an ideal choice only for low data rate reliable transmissions. Its performance gets worse under high data rates and low available channel bandwidth. On the other hand, UDP has low bandwidth requirements, has low communication overhead and does not cause incremental latency in case of packet loss. This makes it suitable for high data rate and real-time transmissions. However, it is unreliable and does not guarantee the delivery of data. Due to pros and cons of each transport protocol, the mixed approach will be ideal choice for IEEE C37.118-2 based communication system. The mixed approach will use reliable TCP for infrequent messages (Config, Command, Header) and non-reliable UDP for frequent Data messages. The benefits of mixed approach include reliable transmission of critical information (e.g., Config message is very important for receiver to understand how to decode received Data messages, Command messages which control whole communication between two peers, etc) and minimum latency and low packet loss for real-time streaming (Data messages). Another advantage of mixed approach is its suitability for both client-server as well as multicast mode of transmission.

7 CONCLUSIONS

Synchrophasors have become an integral part of the modern power system and their applications are continuously evolving. Many synchrophasor applications involve transmission of messages over the Internet. IEEE C37.118-2 is the well tested and most widely used communication standard for transmission of synchrophasors data. This paper presented an overview of IEEE C37.118-2 standard highlighting its main features and capabilities. IEEE C37.118-2 standard does not have any embedded security mechanism which makes it highly vulnerable to cyber attacks. This paper analyzed how different types of cyber attacks can exploit vulnerabilities and impact the operations of any synchrophasor application based on IEEE C37.118-2.

To overcome IEEE C37.118-2 vulnerabilities, this paper recommended a GDOI based security mechanism and addressed its effectiveness. GDOI provides enhanced security and protection against man-in-the-middle, connection hijacking, replay, reflection and denial-of-service attacks. Finally, the paper presented detailed performance evaluation of IEEE C37.118-2 and analyzed network overhead, resource requirements (e.g., bandwidth, CPU), communication



(a) CPU usage (b) Bandwidth (using UDP) (c) Bandwidth (using TCP)

Figure 8: Resource requirements with increase in data transmission rate.

latencies and their impact on the data transmission rate. The reported results provide enough information about the required resources and network characteristics before designing any synchrophasor application based on IEEE C37.118-2 standard.

ACKNOWLEDGEMENTS

This work was funded by the EPSRC CAPRICA project (EP/M002837/1).

REFERENCES

Allgood, G., Bass, L., Brown, B., Brown, K., Griffin, S., Ivers, J., Kuruganti, T., Lake, J., Lipson, H., Nutaro, J., Searle, J., and Smith, B. (2011). Security profile for wide-area monitoring, protection, and control. In *The UCAIug SG Security Working Group*.

Baumeister, T. (2010). Literature review on smart grid cyber security. In *University of Hawaii, Technical Report*.

Beasley, C., Zhong, X., Deng, J., Brooks, R., and Venayagamoorthy, G. K. (2014). A survey of electric power synchrophasor network cyber security. In *5th IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe)*. IEEE.

Boyer, W. F. and McBride, S. A. (2009). Study of security attributes of smart grid systemscurrent cyber security issues. In *INL, USDOE, Battelle Energy Alliance LLC., Rep INL/EXT-09-15500*.

Coppolino, L., DAntonio, S., and Romano, L. (2014). Exposing vulnerabilities in electric power grids: An experimental approach. In *International Journal of Critical Infrastructure Protection vol:7(1), pp:51-60*. ELSEVIER.

D'Antonio, S., Coppolino, L., Elia, I., and Formicola, V. (2011). Security issues of a phasor data concentrator for smart grid infrastructure. In *13th European Workshop on Dependable Computing*. ACM.

Grigsby, L. L. (2012). Wide-area monitoring and situational awareness. In *Power System Stability and Control - Third Edition, Volume 5*. CRC Press.

Martin, K. E., Hamai, D., Adamiak, M. G., Anderson, S., Begovic, M., Benmouyal, G., Brunello, G., Burger, J., Cai, J. Y., Dickerson, B., Gharpure, V., Kennedy, B., Karlsson, D., Phadke, A. G., Salj, J., Skendzic, V., Sperr, J., Song, Y., Huntley, C., Kasztenny, B., and Price, E. (2008). Exploring the ieee standard c37.1182005 synchrophasors for power systems. In *IEEE TRANSACTIONS ON POWER DELIVERY, VOL. 23, NO. 4*. IEEE.

Morris, T., Pan, S., Lewis, J., Moorhead, J., Younan, N., King, R., Freund, M., and Madani, V. (2011). Cyber security risk testing of substation phasor measurement units and phasor data concentrators. In *Seventh Annual Workshop on Cyber Security and Information Intelligence Research (CSIIRW '11)*. ACM.

Schweitzer, E., Gong, Y., and Donolo, M. (2008). Advanced real-time synchrophasor applications. In *35th Annual Western Protective Relay Conference*.

Shepard, D., Humphreys, T., and Fansler, A. (2012). Evaluation of the vulnerability of phasor measurement units to gps spoofing attacks. In *International Journal of Critical Infrastructure Protection*.

Sikdar, B. and Chow, J. (2011). Defending synchrophasor data networks against traffic analysis attacks. In *IEEE Transactions on Smart Grid, Vol:2, Issue: 4*. IEEE.

Stewart, J., Maufer, T., Smith, R., Anderson, C., and Ersonmez, E. (2011). Synchrophasor security practices. In *14th Annual Georgia Tech Fault and Disturbance Analysis Conference*.

Weis, B., Rowles, S., and Hardjono, T. (Oct. 2011). The group domain of interpretation. In *Internet Engineering Task Force (IETF) Request For Comments (RFC): 6407*.

Yan, Y., Qian, Y., Sharif, H., and Tipper, D. (2012). A survey on cyber security for smart grid communications. In *Communications Surveys and Tutorials, vol.14, no.4, pp.998-1010*. IEEE.

Yu, D.-Y., Ranganathan, A., Locher, T., Capkun, S., and Basin, D. (2014). Short paper: detection of gps spoofing attacks in power grids. In *Int. conference on Security and privacy in wireless & mobile networks*. ACM.

Zargar, S., Joshi, J., and Tipper, D. (2013). A survey of defense mechanisms against distributed denial of service (ddos) flooding attacks. In *Communications Surveys and Tutorials, vol. 15, no. 4, pp. 2046-2069*. IEEE.