Encryption of Sampled Value Protocol in Substations Using One-Time Pads

By: Tolulope Olugbenga, Ashraf Ali, Kwasi Boakye-Boateng, Mohammadreza MontazeriShatoori

Outline

Introduction

Problem

Proposed Algorithm

Implementation

Results

Conclusion & Future Work

Substation Automation System

It is essential in economically maintaining the energy balance between generation and demand in the operation of electrical power

The most important functions of a SAS are:

Control

Monitoring

Alarming

Measurement

Substation Automation System

An SAS is based on a lot of dedicated software stored in pieces of hardware that belong to a set of substation secondary components.

An SAS is comprised of three levels of devices plus two Local Area Networks integrated:

Process

Bay

Station

Substation Automation System

The process level devices:

analog/digital converters (Merging Units) and actuator devices to make the transition between SAS and high voltage equipment.

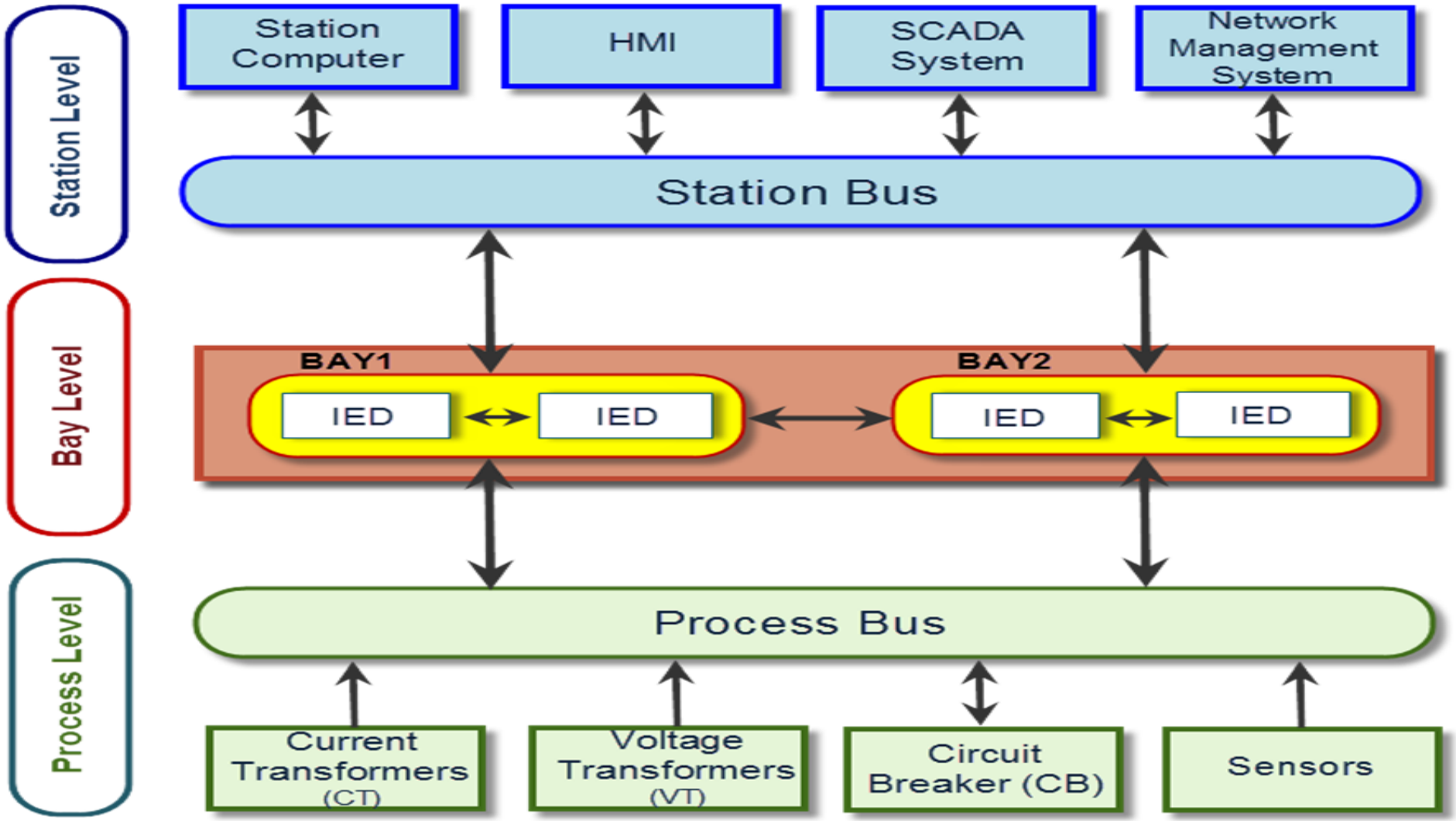
The bay level devices:

a set of Intelligent Electronic Devices (IEDs) that receive and process signals coming from high voltage equipment.

The station level devices:

all computers and other components required to run control functionalities and to communicate with internal and external subsystems (eg. SCADA and HMI).

SAS Architecture



International Electrotechnical Commission (IEC) 61850

A standard for communication and information exchange with the substation

Ethernet-based (IEEE 802.3 standard) communication

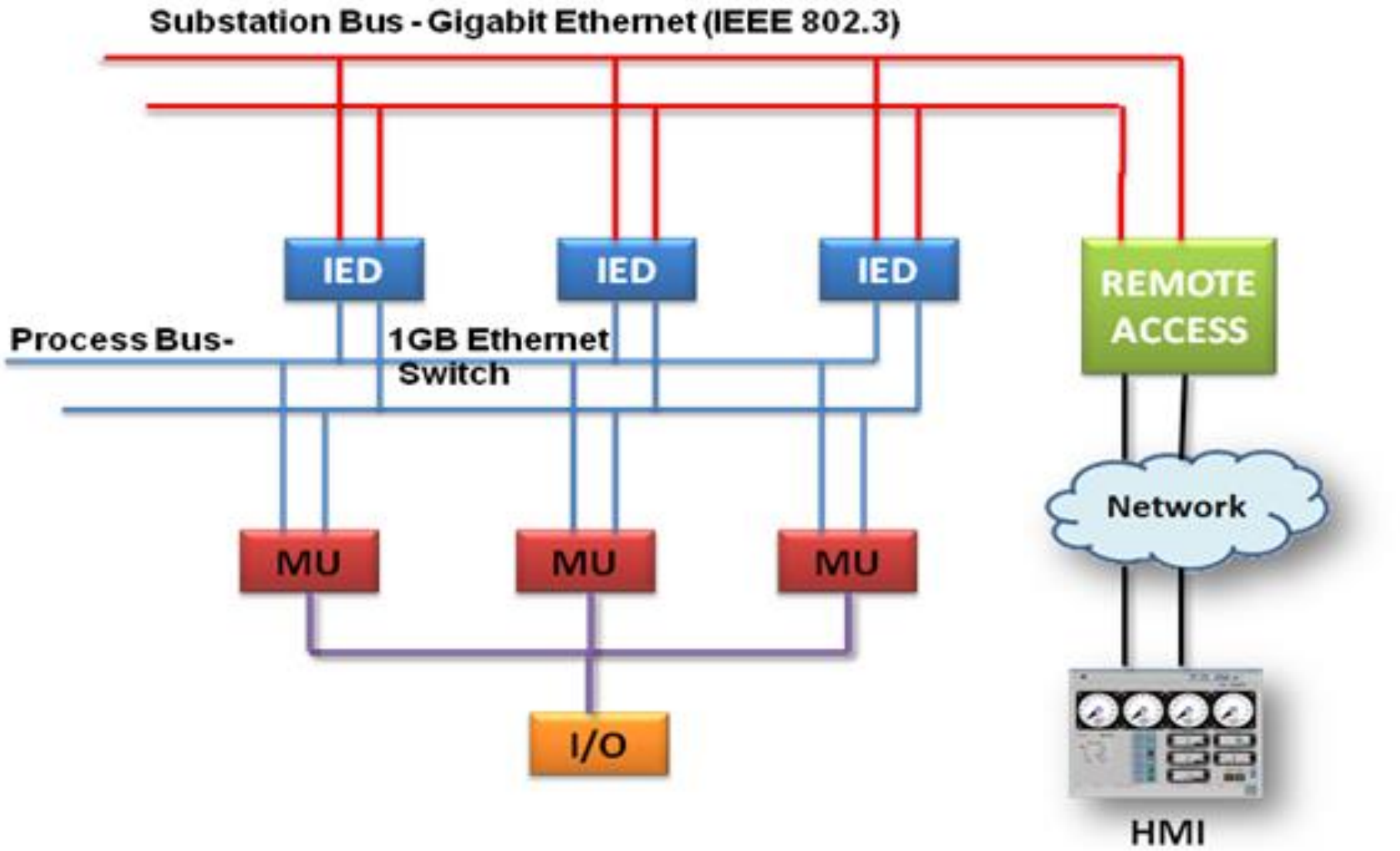
Ensures vendor interoperability among devices

Abstracts data and services making them independent of any underlying protocol.

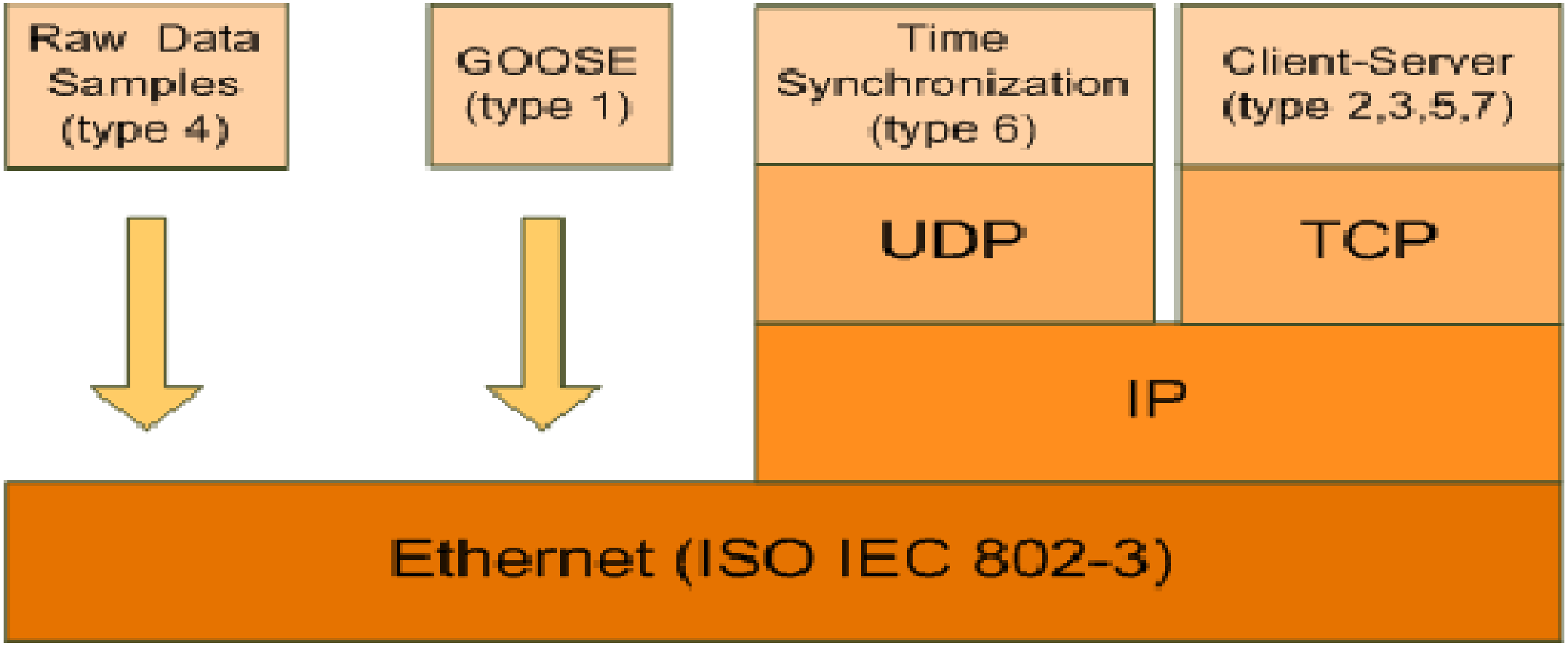
Protocol must be well-mapped to IEC 61850 data objects and services to be implemented.

Theoretically a protocol could be created specifically for IEC61850 albeit complex

IEC 61850 SAS Implementation



IEC 61850 OSI Architecture



IEC 61850 Performance Requirements

Message Type	Delay Constraint(ms)
1A - Fast messages, trip	≤ 3
1B - Fast messages, others	≤ 20
2 - Medium speed messages	≤ 100
3 - Low speed Messages	≤ 500
4 - Raw Data Messages	≤ 3, ≤ 10
5 - File Transfer Functions	≤ 1000
6 - Time synchronization messages	N/A
7 - Command Message With Access control	N/A

Sampled Measured Values (SMV or SV)

Used for communication between IEDs

Reliable, fast and real-time (Type 4)

SV messages embed numerical samples of current and voltage signals

Uses **publish-subscribe** model of communication

Publish-Subscribe Model

Comprises an IED (the publisher) creates a message that is delivered to a group of destination IEDs (the subscribers) simultaneously in a single transmission from the source.

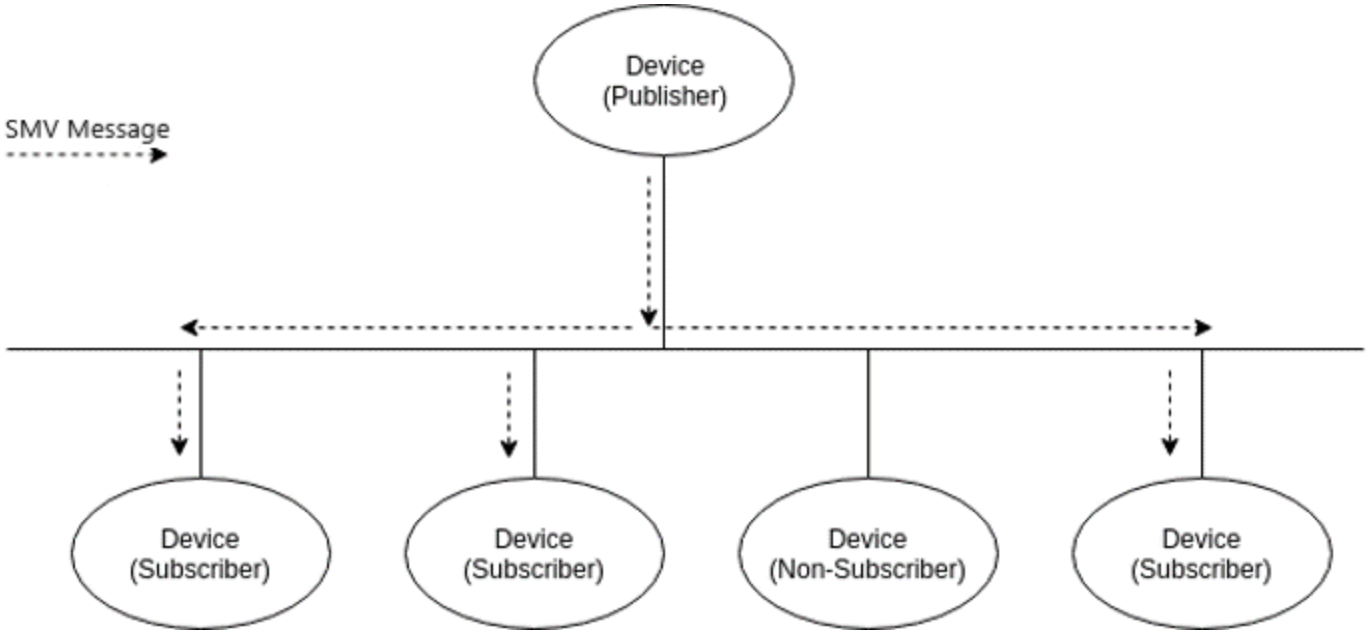
Multicast messages

Repetition strategy against packet loss

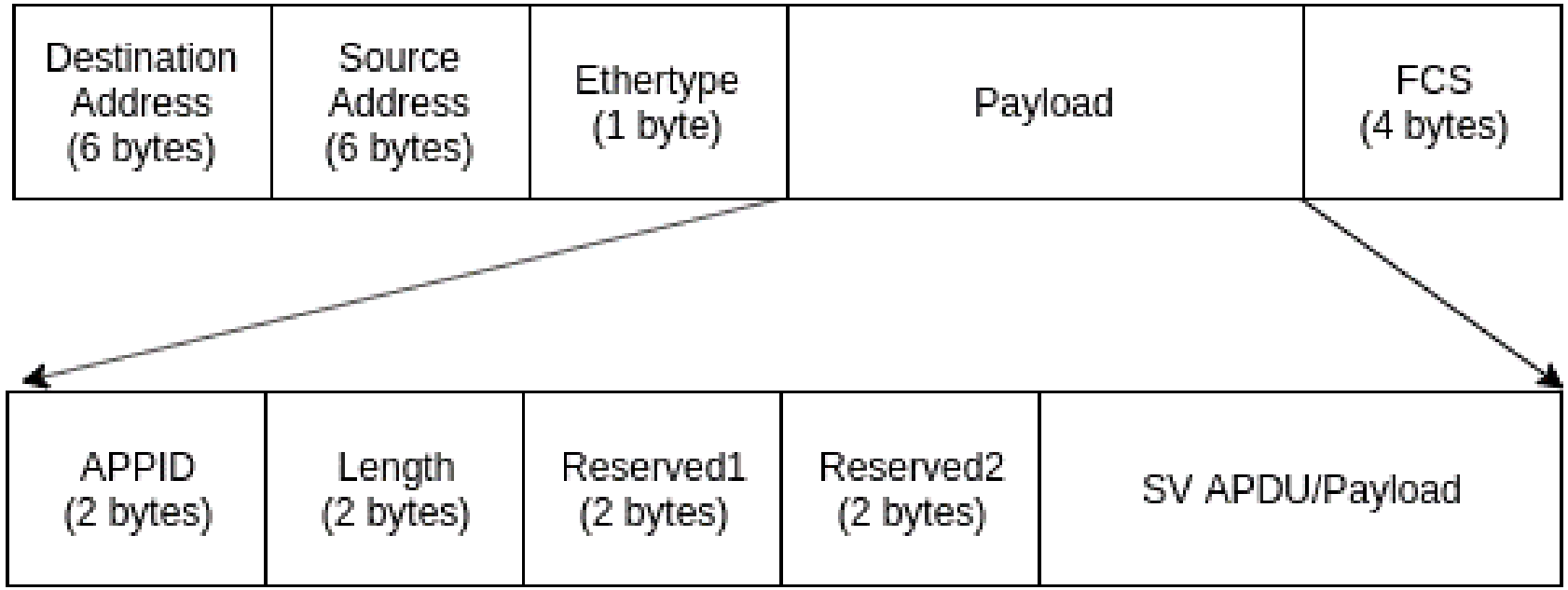
Unconfirmed communication

Event driven timing

ASN.1 encoded payload



SV Packet Structure



SV Packet Structure

The SV datagram has twelve fields that define the Protocol Data Unit (PDU)

destination (multicast) address and **source** address are Ethernet MAC addresses (recommended format **01-0C-CD-04-YY-YY)**

Ethertype of a SV message is 88-BA.

Application ID and **length** (m + 8 bytes).

The **Reserved1** and **Reserved2** fields (set to 0, reserved for future use)

Application PDU (APDU) and **Field Control Sequence** (FCS).

Problem – Attack Taxonomy Relating To SV

Attack	Security Requirement Violated	Effects	IEC 62351 Recommendation
Detection of control devices	Confidentiality	Number of devices and message contents are exposed to the adversary	No comprehensive countermeasures provided
Replay, alteration and spoofing attacks	Integrity	Modified messages can cause high voltage devices to malfunction leading to cascading effects	RSA signatures suggested but they affect real-time performance of SV
DoS/DDoS Attacks	Availability	Real-time operations of IEDs will fail which can possibly leading to cascading failures within the substation	No sufficient solutions provided

Problem – Existing Research Securing SV

Protocol	Latency(ms)	Problem
CLPKC [25]	$\approx$ 1.409	Theoretical, hardware-based and difficult to be replicated practically
NTRU [22]	$>$ 50	High latency, even though implemented on Raspberry Pi
Hybrid DES-RSA [24]	$<$ 2	Requires high performance computing

Problem – Existing Research Securing SV

	Type of Attack			
Protocol	**Detection of devices**	**Replay**	**Alteration and spoofing**	**DoS/DDoS**
CLPLK	Attacker can monitor messages.	Replayed packets will be accepted by devices because there is no check for freshness.	No known drawbacks due to authentication and signature fields.	Flooding of devices with unmodified replay packets will be accepted by devices.
NTRU	No known drawbacks. Attacker is unable to monitor encrypted packets.	Replayed packets will be accepted by devices because there is no check for freshness.	No known drawbacks due to authentication and signature fields.	Flooding of devices with unmodified replay packets will be accepted by devices.
Hybrid RSA and DES	No known drawbacks. Attacker is unable to monitor encrypted packets.	Replayed packets will be accepted by devices because there is no check for freshness.	No known drawbacks due to authentication and signature fields.	Flooding of devices with unmodified replay packets will be accepted by devices.

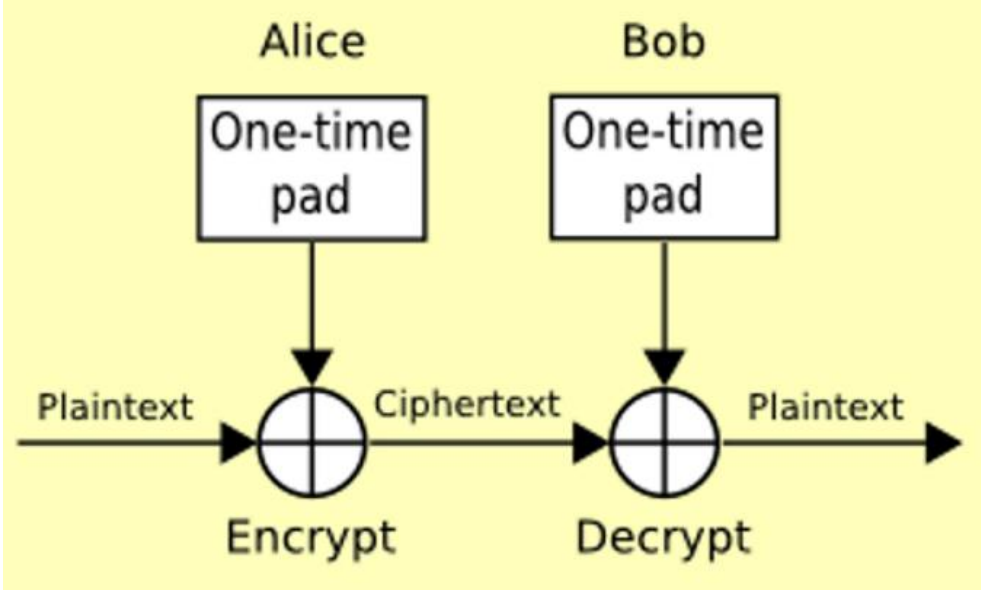
Motivation

Encrypt SV Packets with One-Time Pads (OTP)

OTP encryption involves a modulo addition between the key and the plaintext

The key is used once, hence the name One-Time Pad

OTP has same length as plaintext



Proposed Algorithms

Algorithm 1 Encryption Algorithm

Generate K_{srcMac}
$srcMac \leftarrow srcMac \oplus K_{srcMac}$
Generate $K_{destMac}$
$destMac \leftarrow destMac \oplus K_{destMac}$
Generate K_{APPID}
$APPID \leftarrow APPID \oplus K_{APPID}$
for $i = 0 \&\& i < l_{svPDU}$ **do**
    Generate $K_{svPDUByte}$
    $svPDU[i] \leftarrow svPDU[i] \oplus K_{svPDUByte}$
end for
Generate K_{svFCS}
$svFCS \leftarrow svFCS \oplus K_{svFCS}$
Transmit P_{sv}

Algorithm 2 Decryption Algorithm

Generate K_{srcMac}
$srcMac \leftarrow srcMac \oplus K_{srcMac}$
Generate $K_{destMac}$
$destMac \leftarrow destMac \oplus K_{destMac}$
Generate K_{APPID}
$APPID \leftarrow APPID \oplus K_{APPID}$
for $i = 0 \ \&\& \ i < l_{svPDU}$ **do**
    Generate $K_{svPDUByte}$
    $svPDU[i] \leftarrow svPDU[i] \oplus K_{svPDUByte}$
end for
Generate K_{svFCS}
$svFCS \leftarrow svFCS \oplus K_{svFCS}$
if $(destMac \neq multiMac) \ \&\& \ (srcMac \notin srcMacList)$ **then**
    Drop P_{SV}
else
    Accept P_{SV}
end if

Predicted Results – Comparisions Against Attack Taxonomy

	Type of Attack			
Protocol	**Detection of devices**	**Replay**	**Alteration and spoofing**	**DoS/DDoS**
CLPLK	Attacker can monitor messages.	Replayed packets will be accepted by devices because there is no check for freshness.	No known drawbacks due to authentication and signature fields.	Flooding of devices with unmodified replay packets will be accepted by devices.
NTRU	No known drawbacks. Attacker is unable to monitor encrypted packets.	Replayed packets will be accepted by devices because there is no check for freshness.	No known drawbacks due to authentication and signature fields.	Flooding of devices with unmodified replay packets will be accepted by devices.
Hybrid RSA and DES	No known drawbacks. Attacker is unable to monitor encrypted packets.	Replayed packets will be accepted by devices because there is no check for freshness.	No known drawbacks due to authentication and signature fields.	Flooding of devices with unmodified replay packets will be accepted by devices.
OTP	No known drawbacks. Attacker is unable to monitor encrypted packets.	No known drawbacks. Packets will be dropped because of mismatched keys.	No known drawbacks. Tampering will be detected from the FCS field after decryption.	No known drawbacks. Packets will be dropped because of mismatched keys and integrity errors detected from the FCS field.

Conclusion

Encryption/Decryption of SV packets using OTP is possible

A better environment is required to properly measure its efficiency

Key Generation, Key Exchange and Refreshment regarded as future work

Effectiveness against network congestion also regarded as future work

References

1. B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C. New York: Wiley, 1996.

2. J. Hoyos, M. Dehus, and T. X. Brown, "Exploiting the GOOSE protocol: A practical attack on cyber-infrastructure," in 2012 IEEE Globecom Workshops. IEEE, dec 2012, pp. 1508–1513.[Online]. Available:http://ieeexplore.ieee.org/document/6477809/

3. W. Fangfang, W. Huazhong, C. Dongqing, and P. Yong, "Substation Communication Security Research Based on Hybrid Encryption of DES and RSA," in 2013 Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing. IEEE, oct 2013, pp. 437–441. [Online]. Available: http://ieeexplore.ieee.org/document/6846671/

4. J. ZHANG, L. Jun'e, C. Xiong, N. Ming, W. Ting, and L. Jianbo, "A security scheme for intelligent substation communications considering real-time performance," Journal of Modern Power Systems and Clean Energy, pp. 1–14, 2019.

5. A. P. Premnath, J.-Y. Jo, and Y. Kim, "Application of NTRU Cryptographic Algorithm for SCADA Security," in 2014. 11th International Conference on Information Technology: New Generations. IEEE, apr 2014, pp. 341–346. [Online]. Available: http://ieeexplore.ieee.org/document/6822221/

6. "Scapy." [Online]. Available: https://scapy.net/

Thank you