# Security Aware Microgrids: Securing Goose Messages Against Cyberattacks

Tools and research in cybersecurity —resources for security professionals & Managers


## Professor Osama Mohammed

*mohammed@fiu.edu*

**Energy Systems Research Laboratory**
**Department of Electrical & Computer Engineering**
**Florida International University**
**Miami, Florida**


Invited Presentation at American Public Power Association and Florida Municipal Power Agency Southeast Regional Municipal Utility Cybersecurity Summit, Orlando, Florida
July 10, 2019

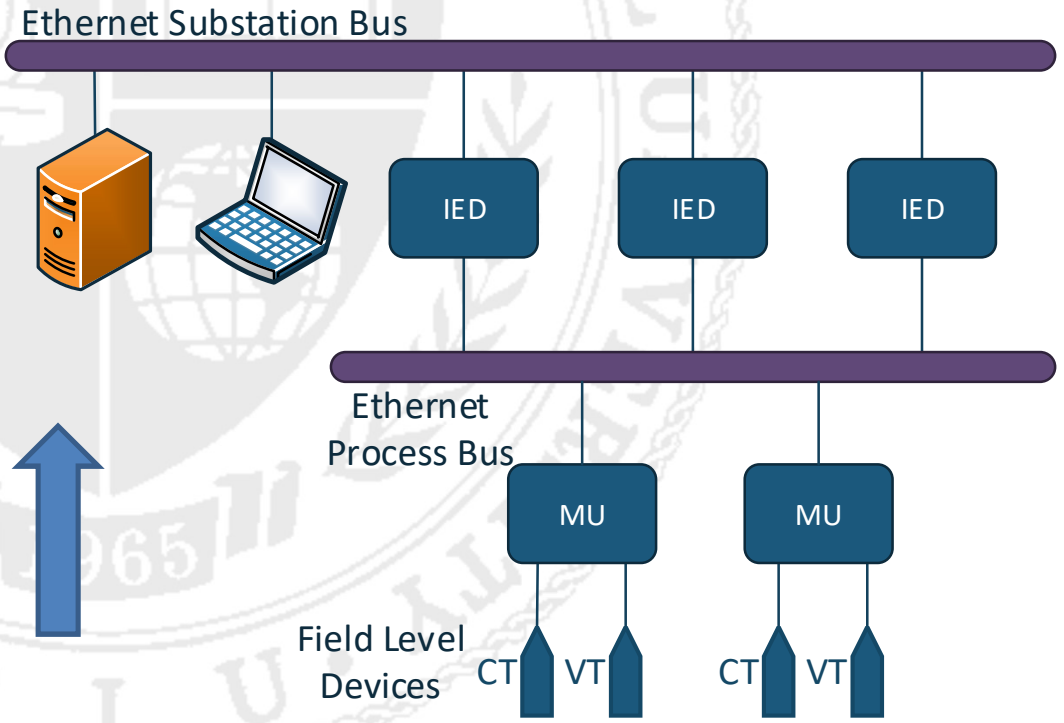
# Looking at the IEC 61850 and IEEE 802.3 Industry Standards

- IEC 61850 and IEEE 802.3 for Ethernet -based communication in electrical substations.
- Data modelling standard that ensures interoperability of devices in Substation Automation Systems (SAS) (different vendors and different types of equipment can easily communicate together)

Manufacturing Message Service (MMS):
Monitoring and high level control (configuration files …)

Generic Object Oriented Substation Event (GOOSE):
Event driven commands

Sampled Measured Values (SMV): Measurements

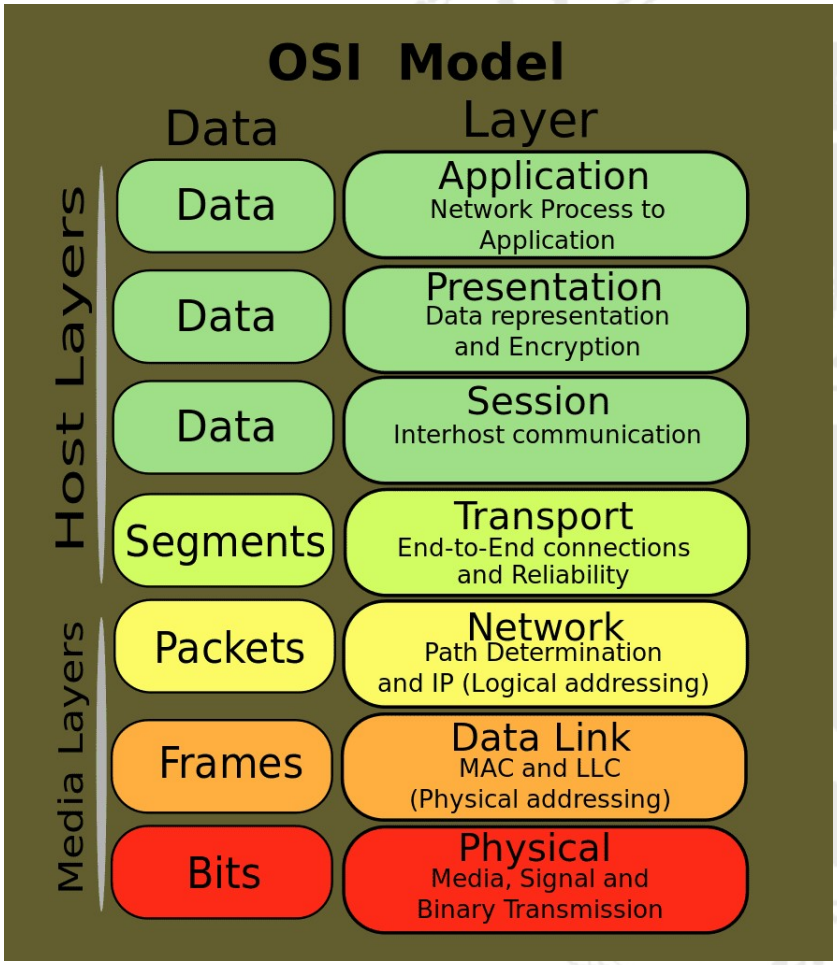


# Generic Object Oriented Substation Events (GOOSE) Messages

- GOOSE messages are used for critical events in substations and microgrids control.
- Used mainly to control opening/closing status of circuit breakers.
- Sent and broadcast Layer 2 messages of the Open System Interconnect (OSI) data model.

| Destination MAC Address | | Source MAC Address | | Priority Tagging/VLAN ID |
|---|---|---|---|---|
| Ethertype (88B8) | | APPID | | Length |
| Reserved 1 | | Reserved 2 | Tag | Length | goosePDU |
| Tag | Length | gocbRef | Tag | Length | timeAllowedtoLive |
| Tag | Length | datSet | Tag | Length | goID |
| Tag | Length | t | Tag | Length | stNum |
| Tag | Length | sqNum | Tag | Length | test |
| Tag | Length | confRev | Tag | Length | ndsCom |
| Tag | Length | numDatSetEntries | Tag | Length | allData |
| Tag | Length | Data 1 (Boolean) | Tag | Length | Data 2 (Float) |
| ●●●●●● | ●●●●●● | | Tag | Length | Data N |

# The Open System Interconnect (OSI) Data Model




**Host layers**:

7. Application: High-level APIs, including resource sharing, remote file access.

6. Presentation: Translation of data between a networking service and an application; including character encoding, data compression and encryption/decryption.

5. Session: Managing communication sessions, i.e. continuous exchange of information in the form of multiple back-and-forth transmissions between two nodes.

4. Transport: Reliable transmission of data segments between points on a network, including segmentation, acknowledgement, and multiplexing.

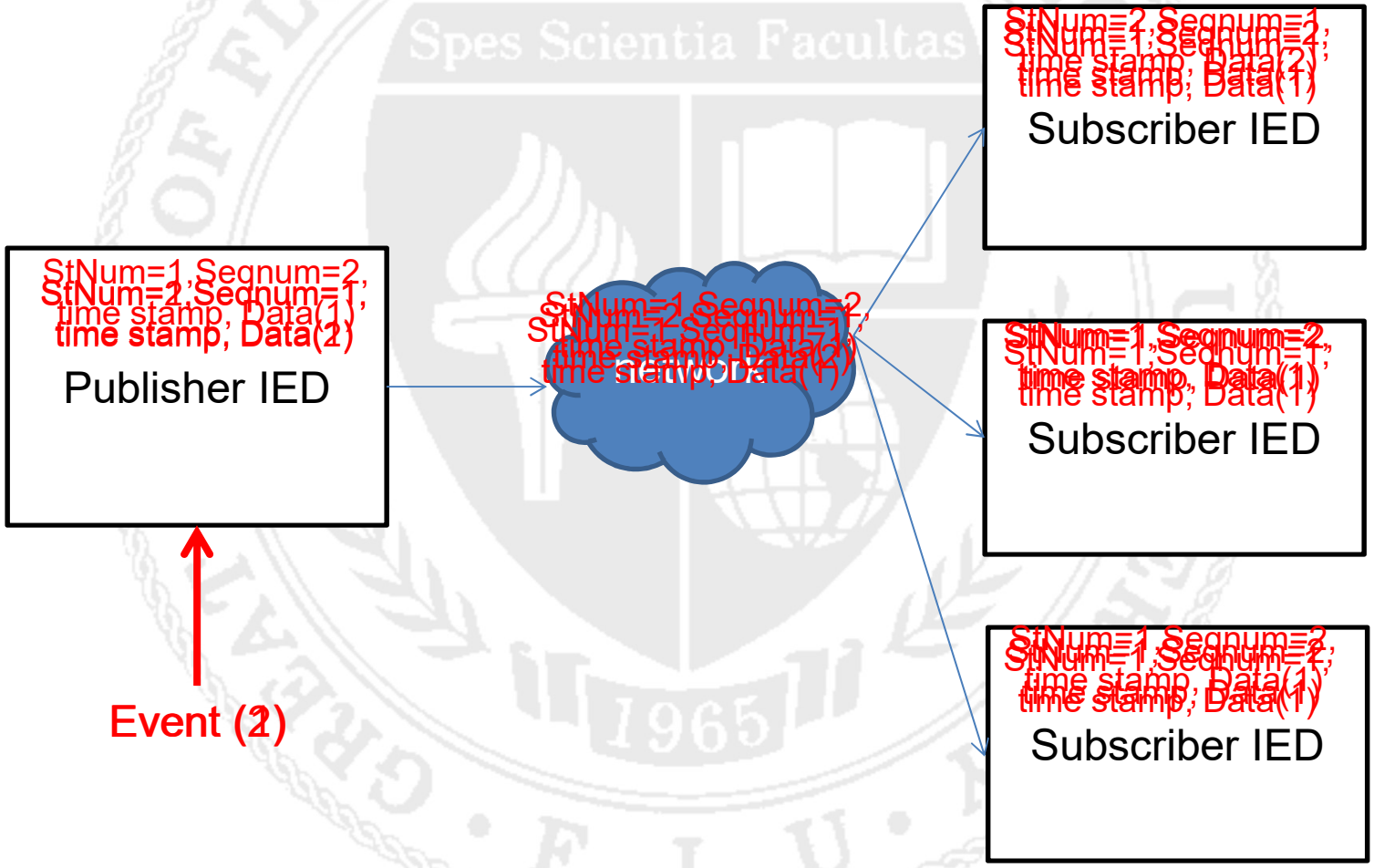
**Media layers**:

3. Network: Structuring and managing a multi-node network, including addressing, routing and traffic control.

2. Data link: Reliable transmission of data frames between two nodes connected by a physical layer.

1. Physical: Transmission and reception of raw bit streams over a physical medium.

# GOOSE Messages Transmission Mechanism



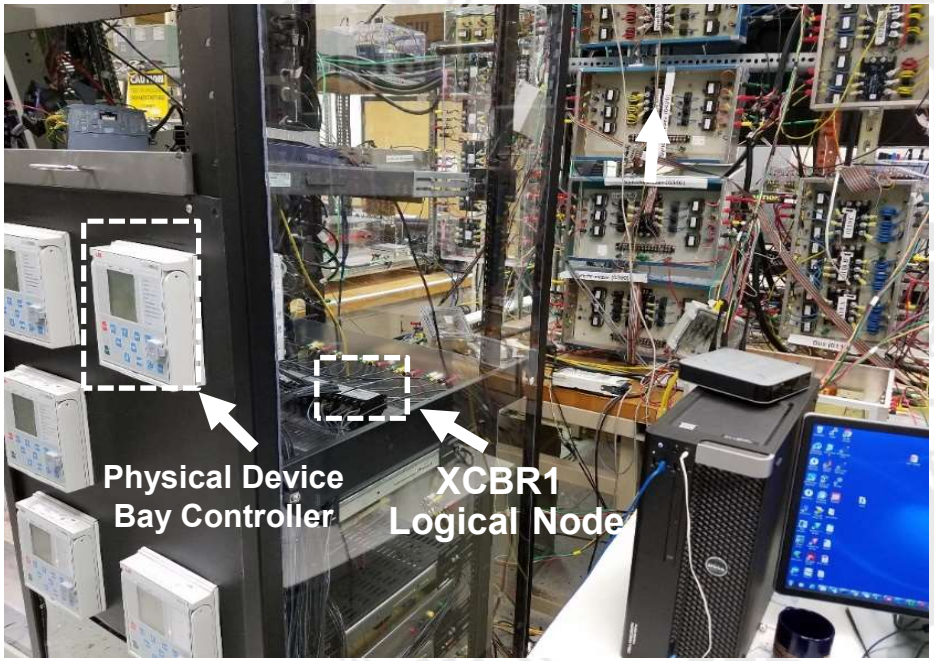
# Security threats

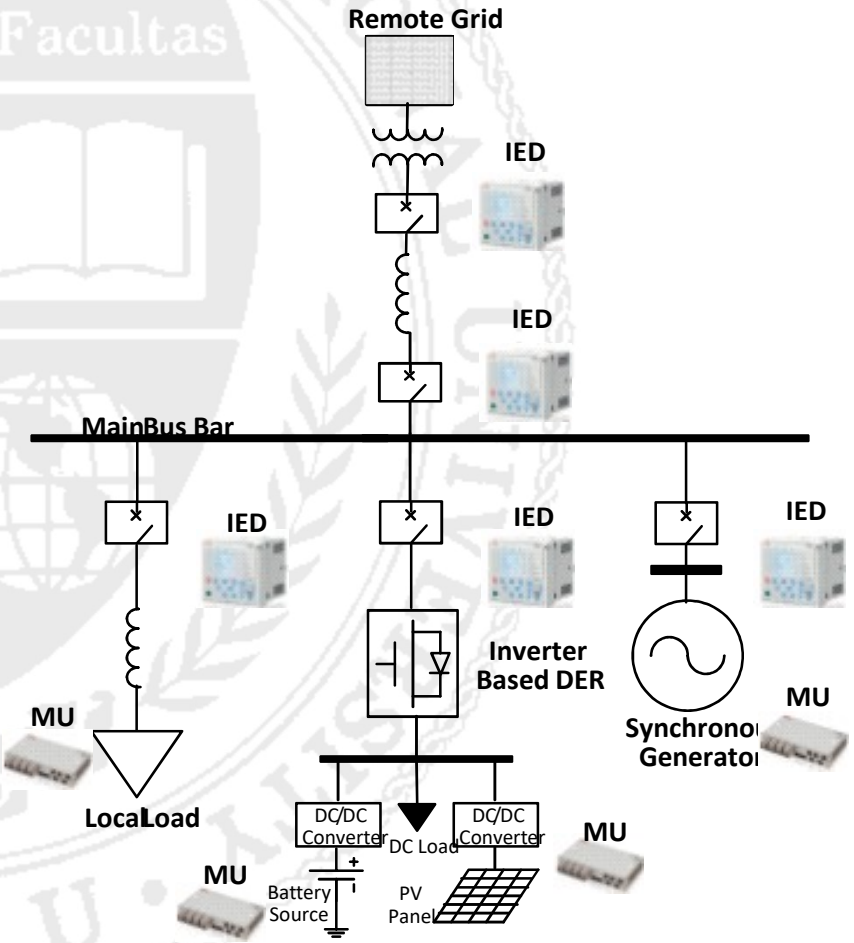
- Original IEC 61850 standard doesn't define any security measure.
- In order to address the security issue in IEC 61850 and other automation protocols such as DNP3, IEC TC 57 WG 10 issued IEC 62351 security standard.
- **"for applications using GOOSE and IEC 61850-9-2 (SMV) and requiring 4 ms response times, multicast configurations and low CPU overhead, encryption is not recommended" .**

**Lack of Encryption → Message Understanding and Modification**

# Attack Scenario:
# GOOSE Manipulation on Commercial IEDS

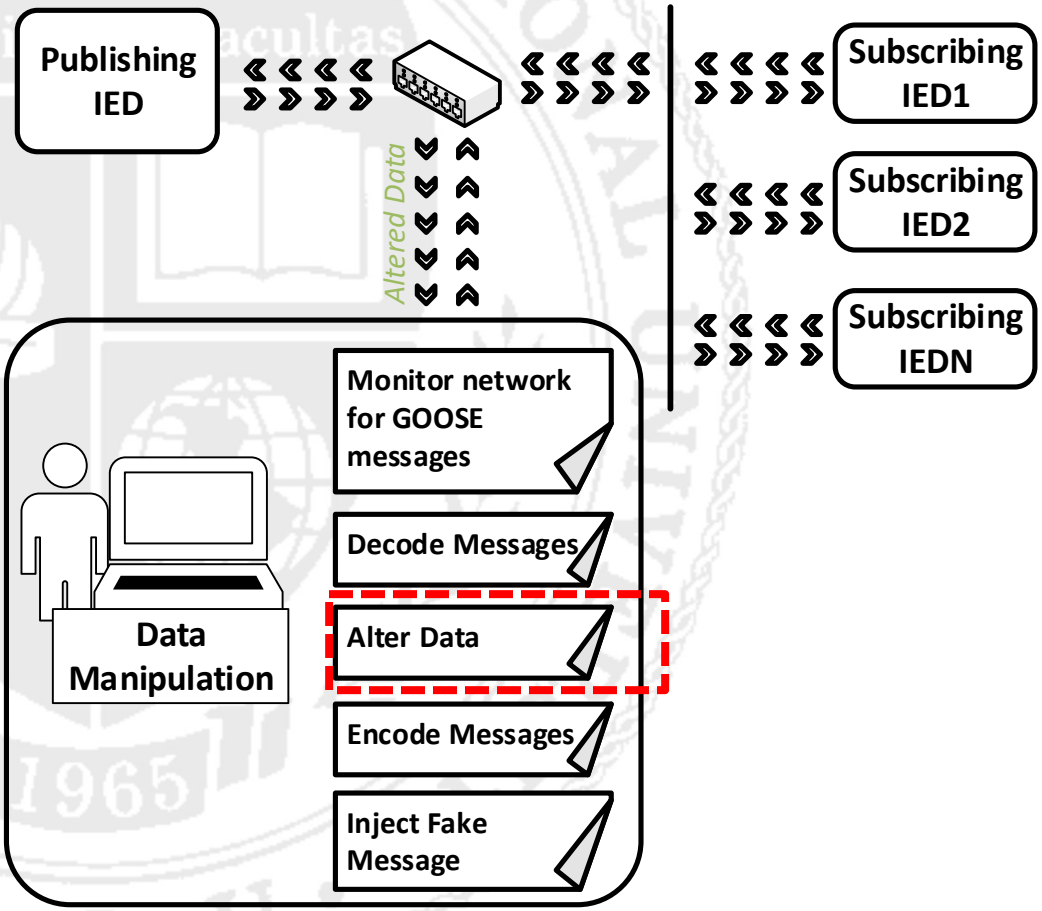
Commercial IEDs at FIU Testbed



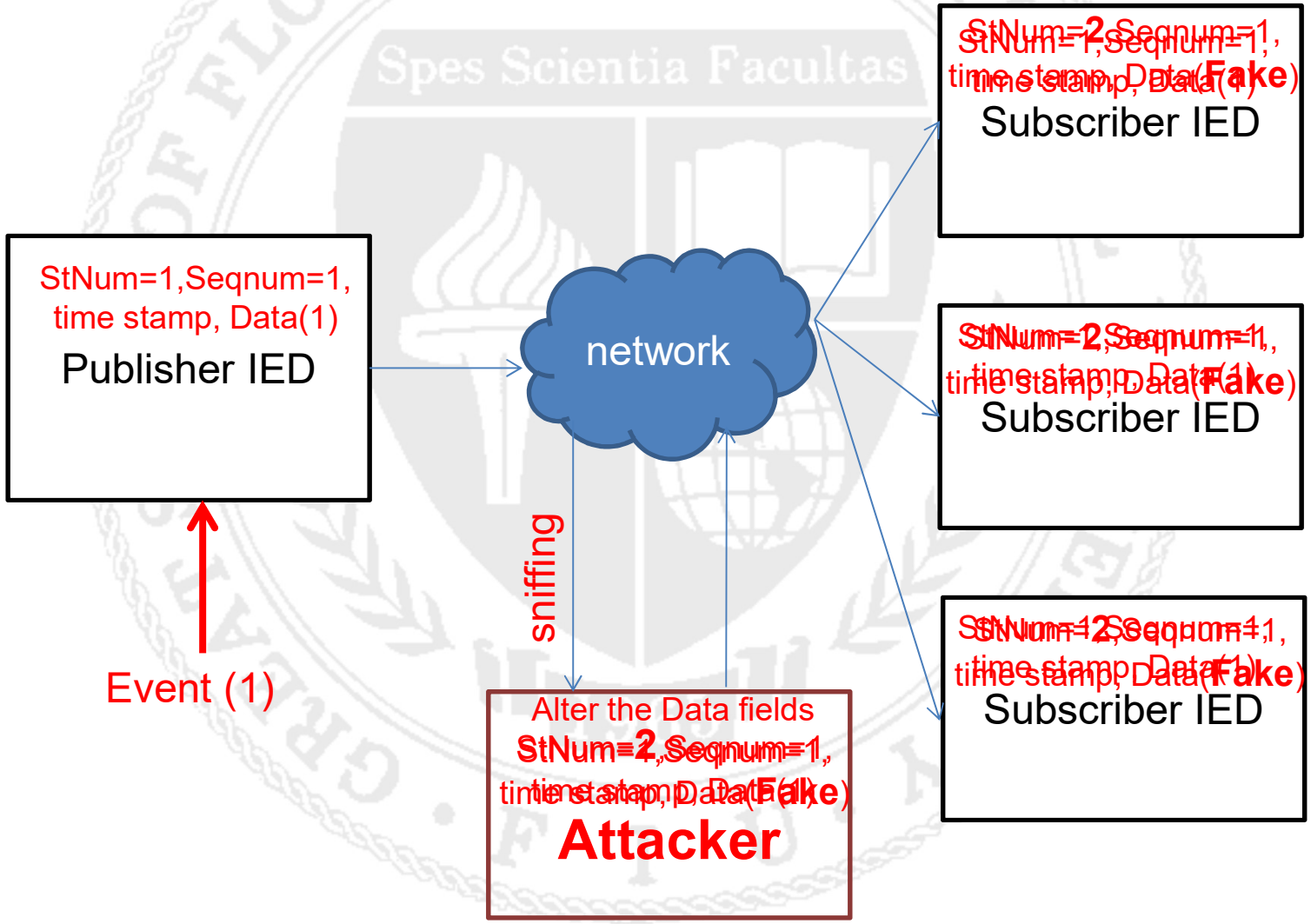



# Attack Scenario:
# GOOSE Manipulation on Commercial IEDS

Automated script using Python in conjunction with packet crafting libraries from Scapy.



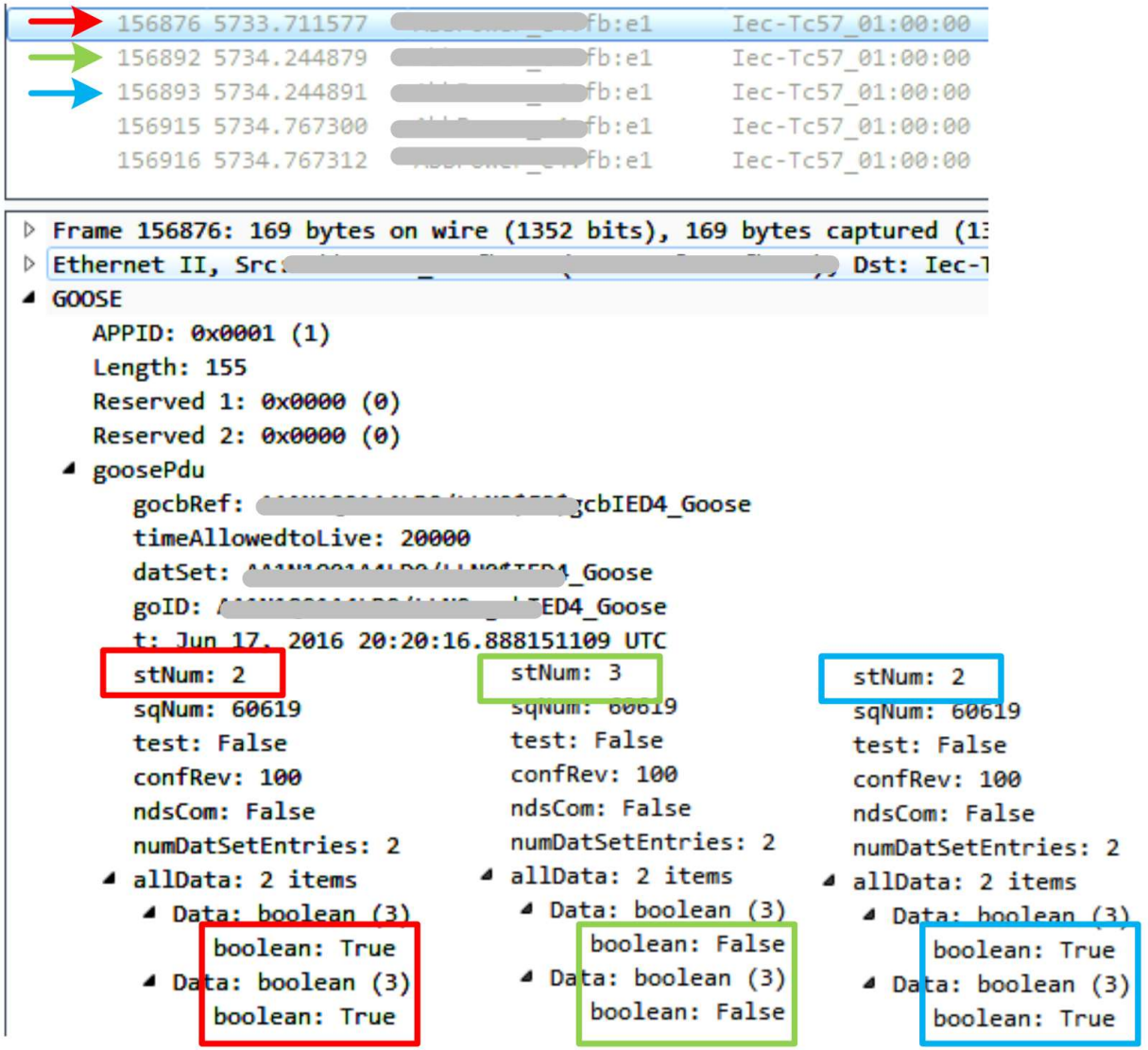
# GOOSE Poisoning Attack



# Attack on Commercial IED

- Aside from targeti
  attacks is emphasi
  conventional netw
- **The modified contr
  before being transr**

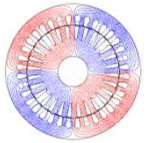
## GOOSE Manipulation Example



# Encryption and Authentication Challenges

- IEC 62351 standard requires Transport Layer Security (TLS) handshake and message encryption for Manufacturing Message Specification (MMS) protocol messages.
- IEC 62351 recommends not to use any encryption on GOOSE messages due to time restriction <4msec.
- IEC 62351 recommends the use of **RSA (**Rivest–Shamir–Adleman) encryption for **message Authentication**.
- Latest available hardware fails to sign the GOOSE without violating the time restriction.





# Encryption and Authentication Challenges

## RSA Signing and Verification Execution Time on Several Processors

| RSA Operation (key length) | iPAQ Pocket PC (400 MHz) | Jornada Handheld PC (206 MHz) | HP Com-paq laptop (1.7 GHz) |
|---|---|---|---|
| Sign (512-bit) | 0.0260 s | 0.0460 s | 0.0016 s |
| Verify (512-bit) | 0.0010 s | 0.0020 s | 0.0002 s |
| Sign (1024-bit) | 0.0560 s | 0.1070 s | 0.0089 s |
| Verify (1024-bit) | 0.0030 s | 0.0060 s | 0.0005 s |
| Sign (2048-bit) | 0.2950 s | 0.5670 s | 0.0564 s |
| Verify (2048-bit) | 0.0090 s | 0.0170 s | 0.0016 s |
| Sign (4096-bit) | 1.8490 s | 3.5500 s | 0.3756 s |
| Verify (4096-bit) | 0.0300 s | 0.0580 s | 0.0056 s |

*D Berbecaru, 'On Measuring SSL-based Secure Data Transfer with Handheld Devices', Politecnico di Torino, Dip. di Automatica e Informatica*

# Sequence Hopping Algorithm for Securing GOOSE Messages


New filed will be added to the message HseqNum.

The HseqNum will be a random value generated by pseudo random number generator.

New HseqNum will be generated by the publisher @ every event.

Each subscriber will generate random sequence synchronized with the publisher

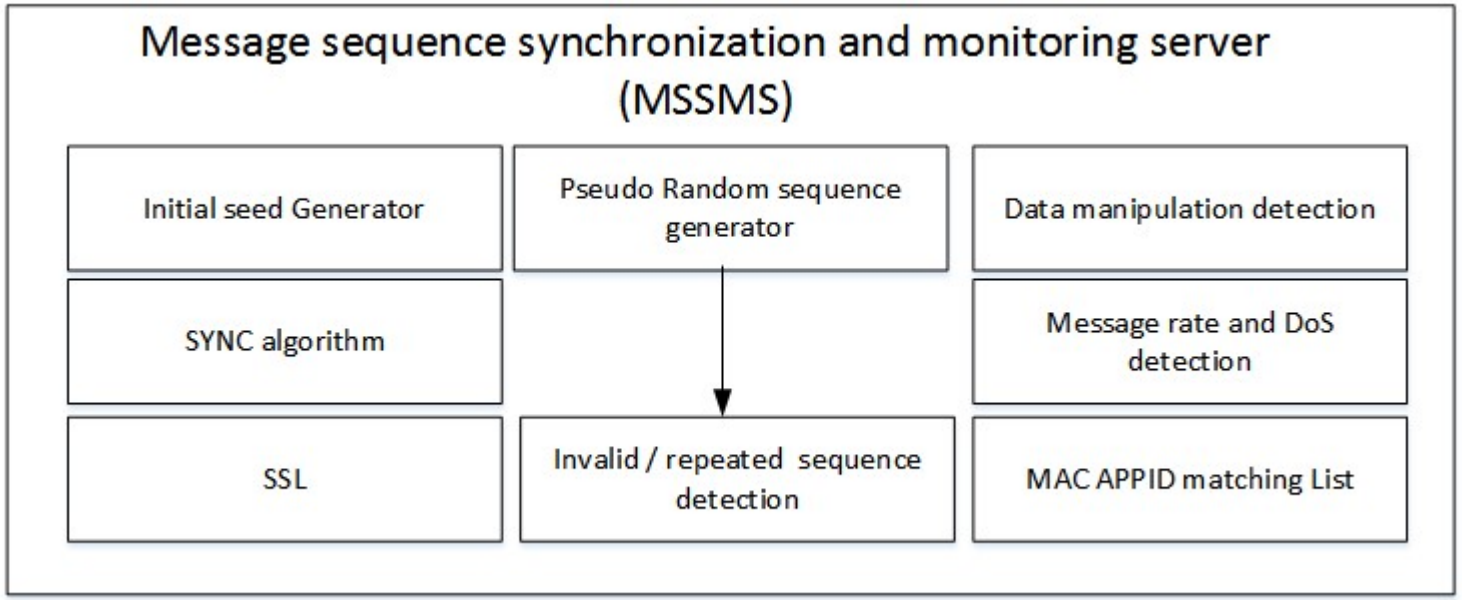
subscriber will accept only the message with matching HseqNum.

Any message with repeated or unmatched HseqNum will be rejected.

The attacker will not be able to send any message without knowing the correct HseqNum.

Any manipulated message will be rejected since it will have repeated HseqNum.

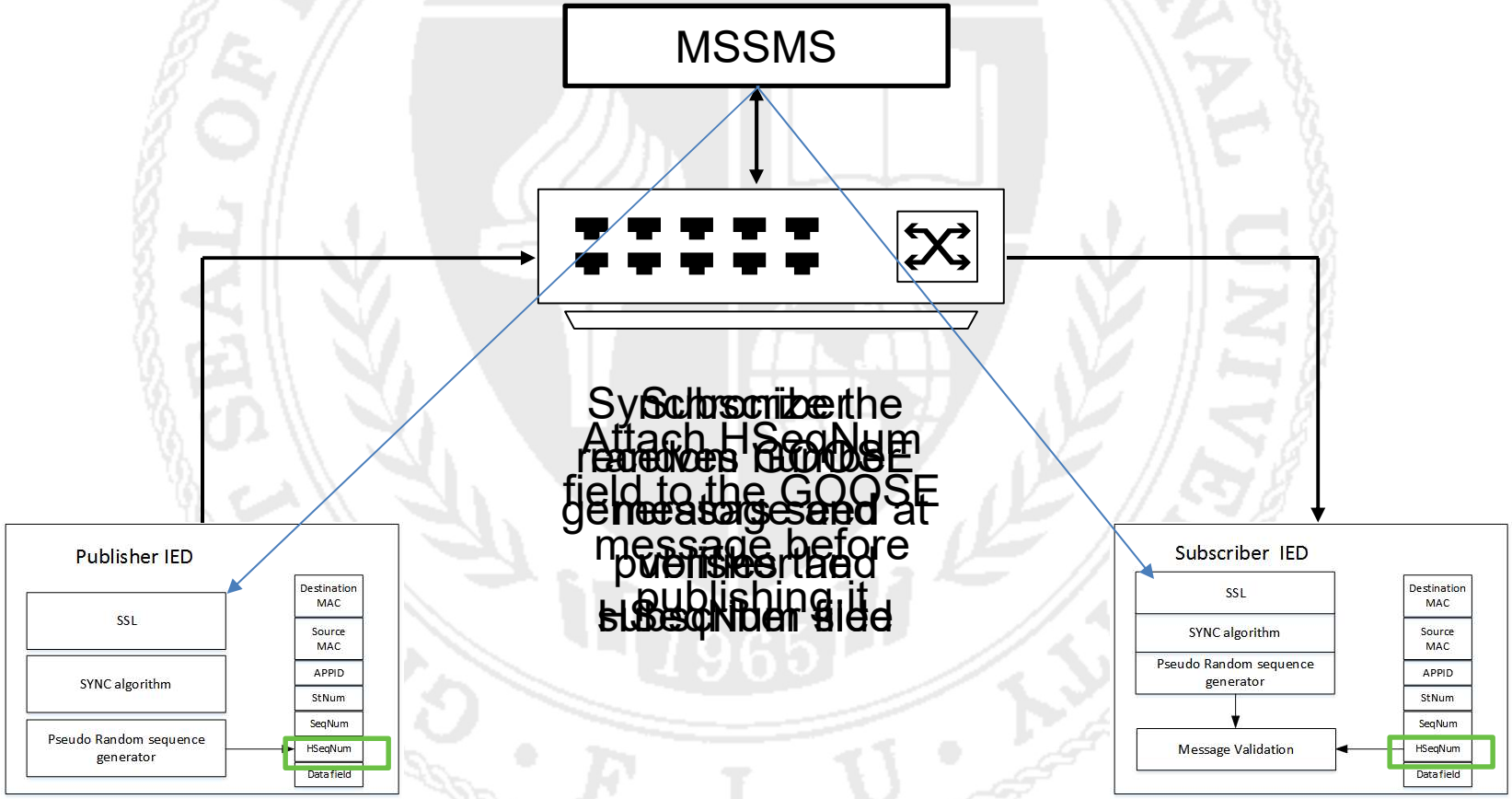
# Sequence Hopping Algorithm for Securing GOOSE Messages




- Message sequence synchronization and monitoring server (MSSMS) will be responsible about syncing all pseudo random number generators.
- The MSSMS will use encrypted connection for synchronization and exchanging initial seeds.
- The MSSMS will monitor all GOOSE broadcasted message for attack detection

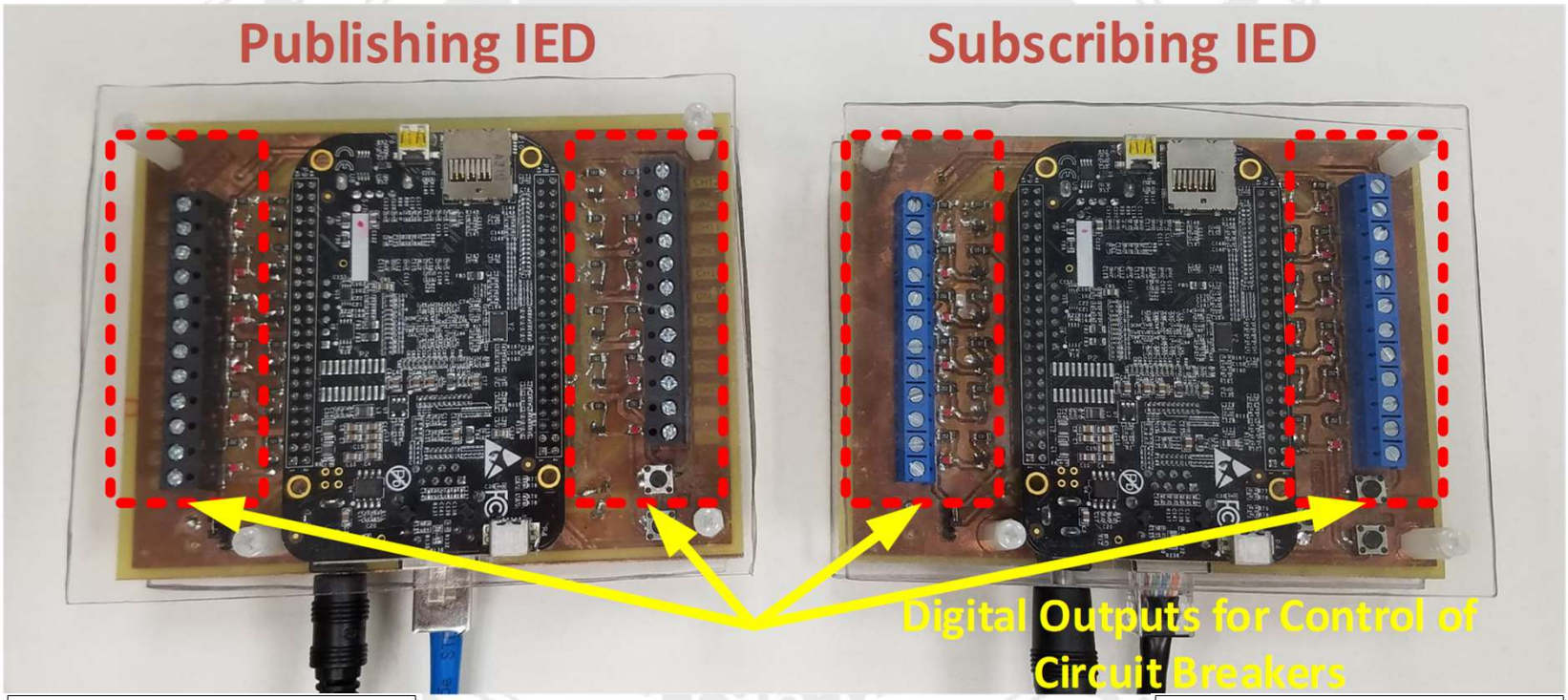
# Sequence Hopping Algorithm for Securing GOOSE Messages

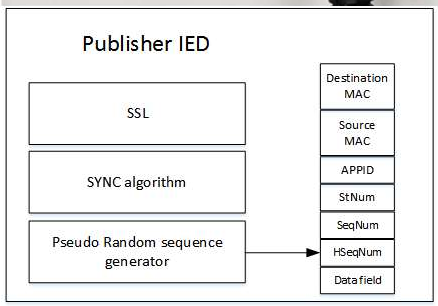
## Experimental Validation: Setup 1

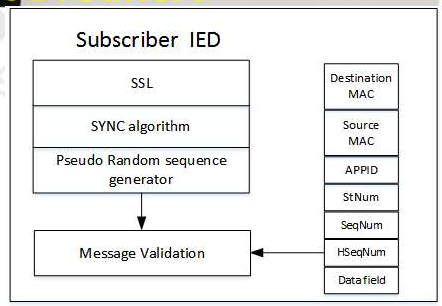


# Sequence Hopping Algorithm for Securing GOOSE Messages

## Experimental Validation

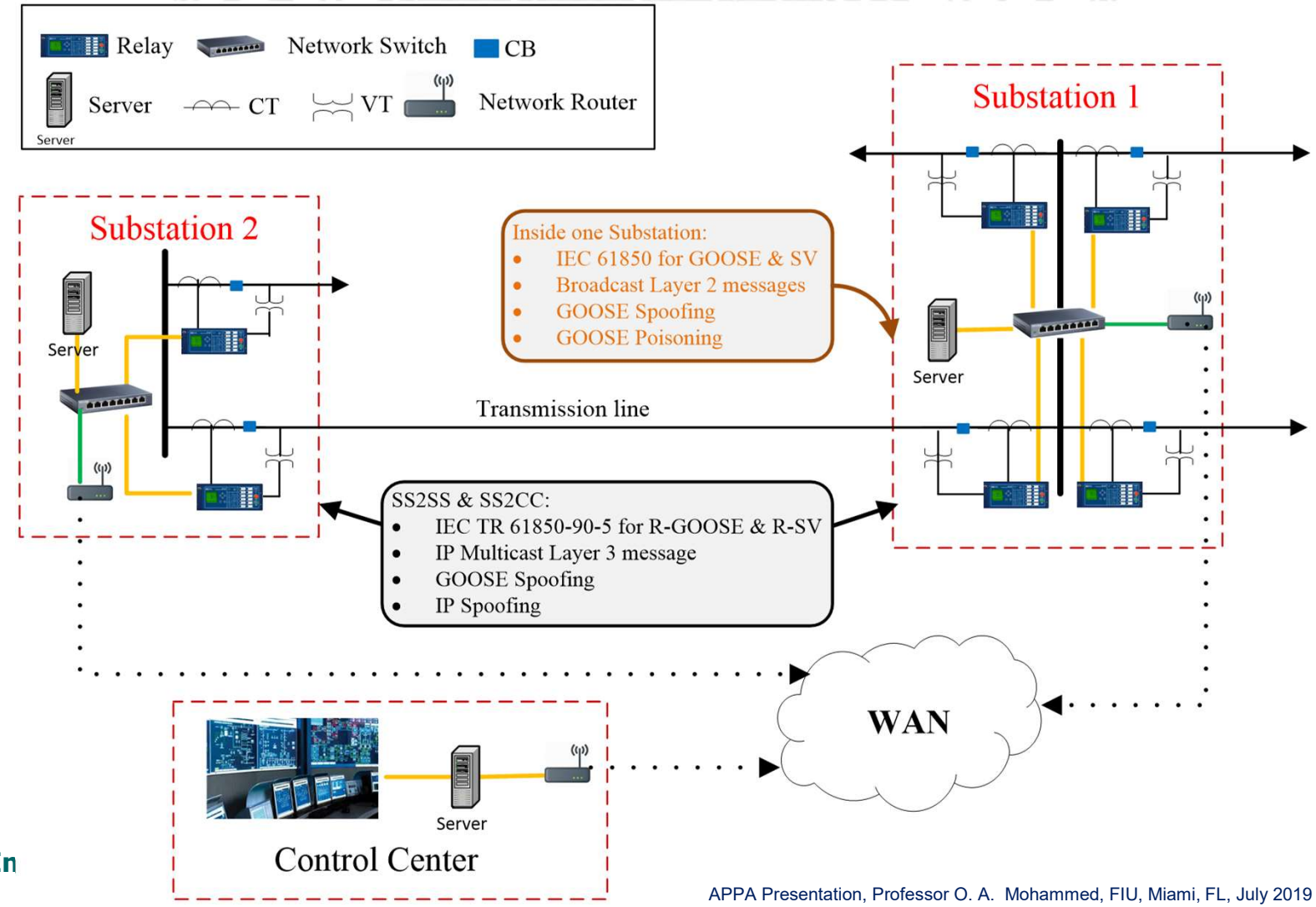


# Substation to Substation and Substation to Control Center

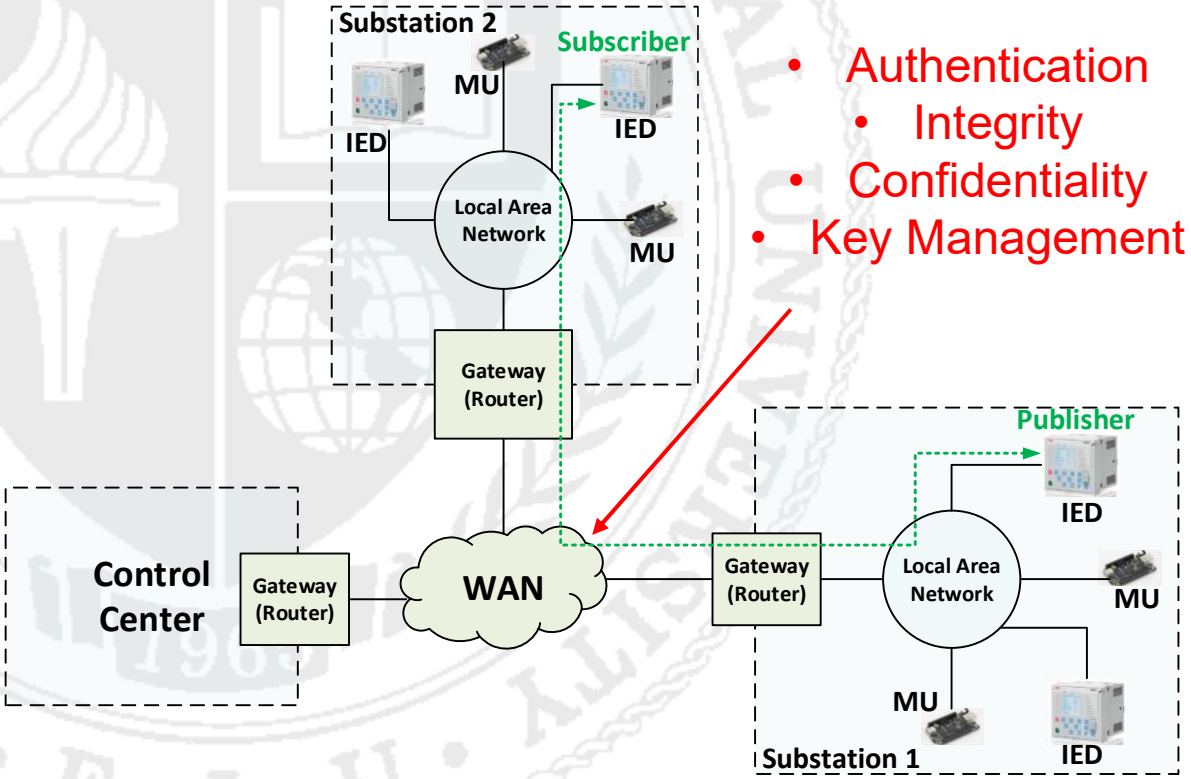
For Substation to substation (SS2SS) and substation to control center (SS2CC) communication



# Substation to Substation and Substation to Control Center

What does that requires?

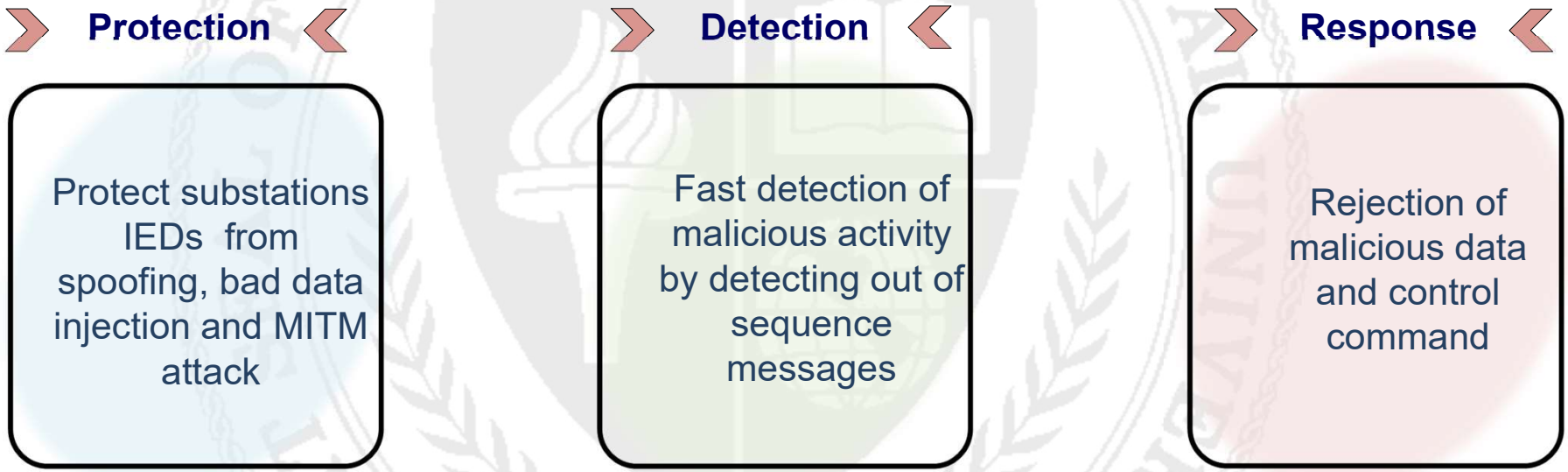
Sequence Hopping Algorithm to protect, detect, and respond to attacks on IEC 61850 R-GOOSE messages between substations (SS2SS) and between a substation and a control center (SS2CS).




- Authentication
- Integrity
- Confidentiality
- Key Management

# Need and Industry Value

- What does this solution address?
  - The proposed security algorithm falls under the categories of:




- Why is this valuable to industry?
  - Addressing the security of critical IEC 61850 GOOSE messages (IEC 61850 is the most widely industry accepted standard which lacks security).
  - We are Working on a solution for key management for Multicast IP situations.

# Conclusions

- The Sequence Hopping Algorithm exploits the Layer 2 broadcasting message characteristic, since the attacker can't block the broadcast message and the only way to manipulate the data is resending the message.
- Since any pseudo random pattern can be detected if the attacker sniffs enough samples of the sequence number the synchronization server will change seeds before generating enough numbers for correlation.
- The algorithm needs minimal computation resources (will not conflict with 4 ms time restriction).
- The server has a physical-model-checking functionality to add additional layer of security.