



Communication Pattern Anomaly Detection in Process Control Systems

Sponsored by the Department of Energy National SCADA Test Bed Program
Managed by the National Energy Technology Laboratory
The views herein are the responsibility of the authors and do not necessarily
reflect those of the funding agency.

**Alfonso Valdes
Steven Cheung**

SRI International



Securing Process Control Systems



- ◆ **Digital controls are essential to modern infrastructure systems**
- ◆ **Migration from proprietary systems to commodity platforms, TCP/IP and other common standards, connection to corporate IT**
 - Significant gains in productivity, inter-operability
 - Increasing exposure to cyber attack?
- ◆ **Best practice architectures call for perimeter defenses**
 - Increasingly diffuse electronic perimeter
- ◆ **Intrusion Detection provides a necessary complementary defense**

DATES Vision



- ◆ **Future control systems with PCS aware defense perimeter**
- ◆ **IDS systems fully tuned for control system protocols and highest threat attacks**
- ◆ **Realtime event correlation system for threat identification and response**
- ◆ **Developed in partnership with leading SIEM and PCS providers**
- ◆ **Demonstrated on realistic PCS implementations**

Intrusion Monitoring as Part of Defense in Depth



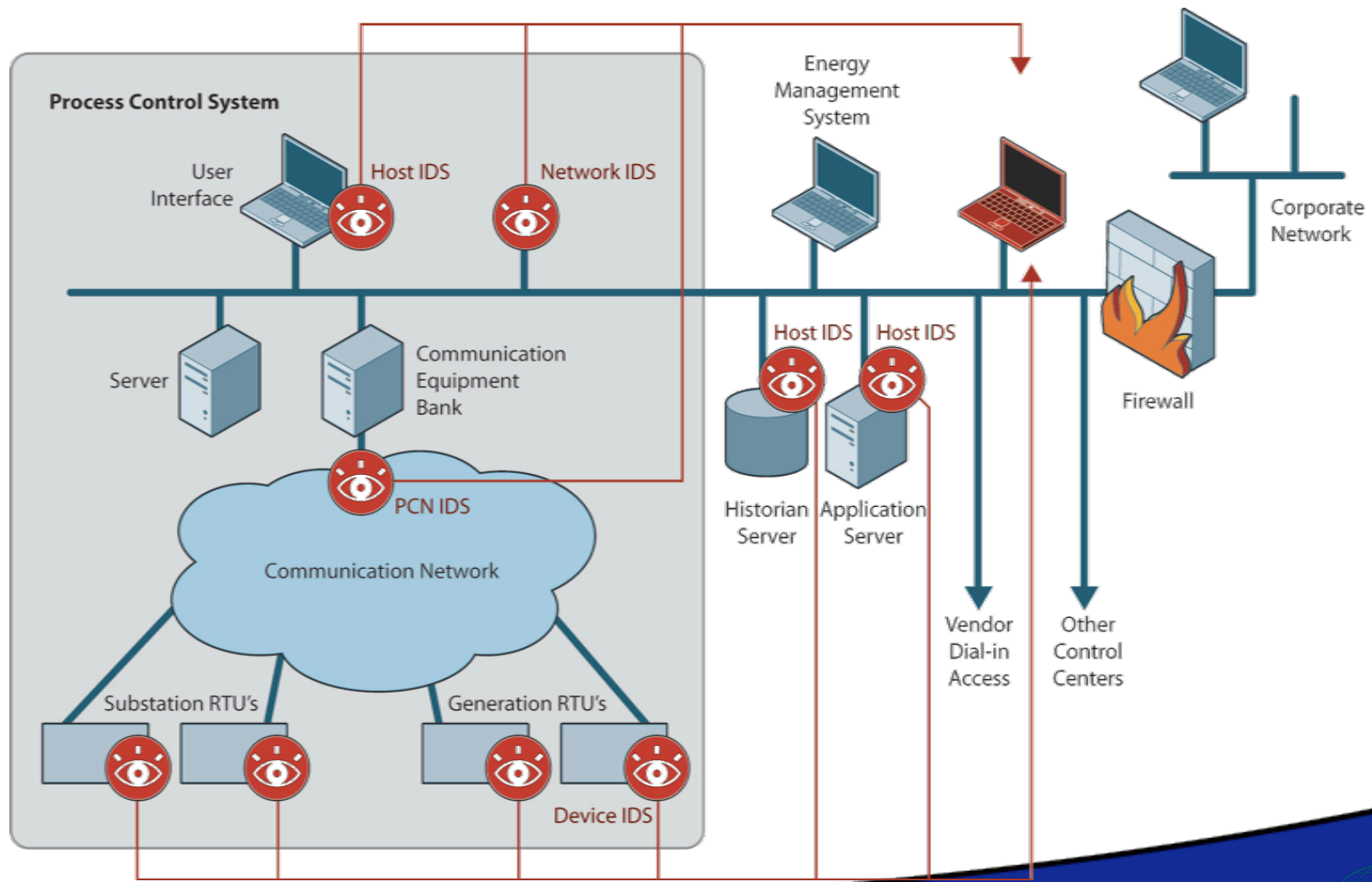
◆ Control Systems use perimeter defenses

- Firewalls, switches
- Network segmentation
- DMZ between control and business networks

◆ Why monitor?

- Ensure perimeter defenses are still effective (Configuration Drift)
- Ensure perimeter defenses are not bypassed (Out of band connections, dual ported devices—What's on YOUR Field LAN?)
- Ensure perimeter defenses are not compromised (Attack on the firewall itself)
- Be aware of unsuccessful attempts to penetrate

High Level Monitoring Architecture



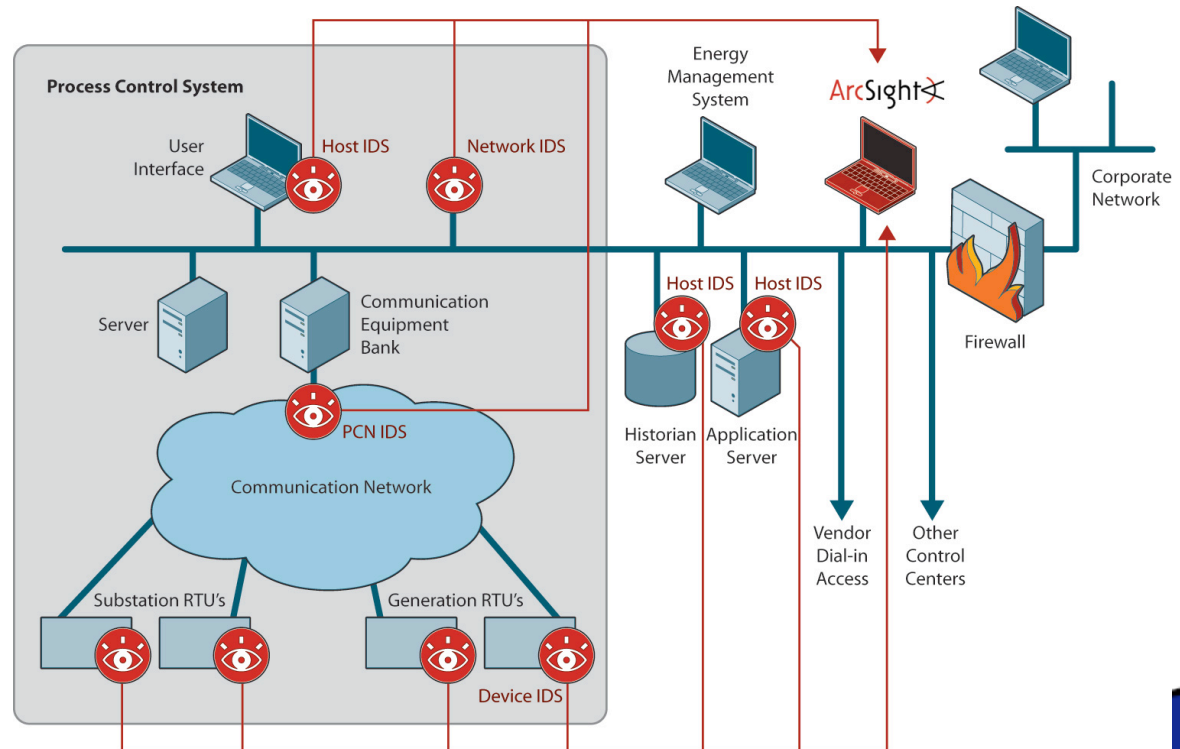
Detection and Event Management



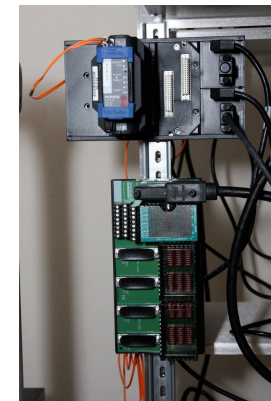
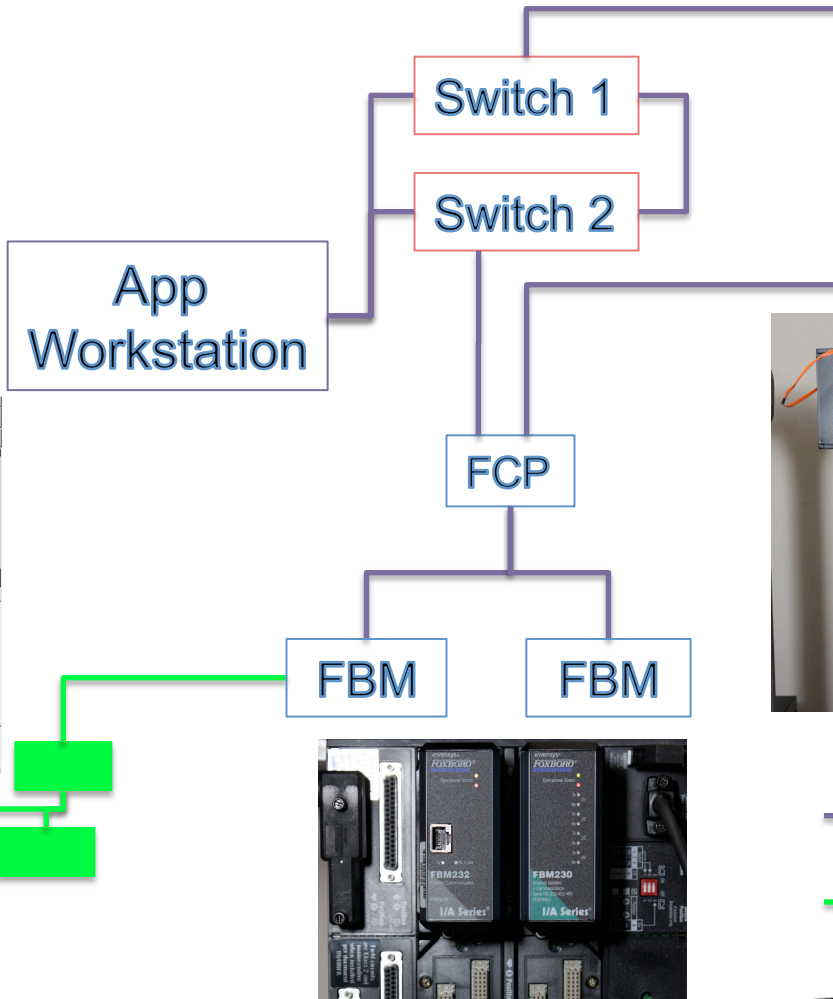
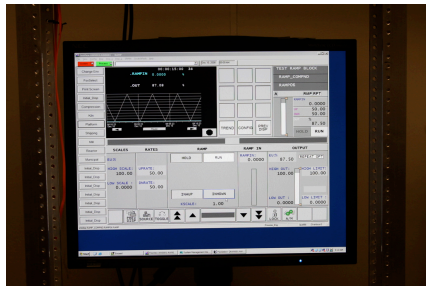
- ◆ Control System aware IDS at the Device, Control LAN, and Host
- ◆ Event Correlation integrates new detection data sources into ArcSight

◆ Result:

- Correlate attack steps
- Follow an attack across LAN segments



Test System Diagram (SRI/Invensys)



No.	Time	Source	Destination	Protocol	Info
217	11:14:20.1203	192.168.1.2	192.168.1.2	UDP	www-app-gpnet: www-app-gpnet: 192.168.1.2:11111
218	11:14:20.1204	192.168.1.2	192.168.1.2	UDP	www-app-gpnet: www-app-gpnet: 192.168.1.2:11111
219	11:14:20.1205	192.168.1.2	192.168.1.2	UDP	www-app-gpnet: www-app-gpnet: 192.168.1.2:11111
220	11:14:20.1206	192.168.1.2	192.168.1.2	UDP	www-app-gpnet: www-app-gpnet: 192.168.1.2:11111
221	11:14:20.1207	192.168.1.2	192.168.1.2	UDP	www-app-gpnet: www-app-gpnet: 192.168.1.2:11111
222	11:14:20.1208	192.168.1.2	192.168.1.2	UDP	www-app-gpnet: www-app-gpnet: 192.168.1.2:11111
223	11:14:20.1209	192.168.1.2	192.168.1.2	UDP	www-app-gpnet: www-app-gpnet: 192.168.1.2:11111
224	11:14:20.1210	192.168.1.2	192.168.1.2	UDP	www-app-gpnet: www-app-gpnet: 192.168.1.2:11111
225	11:14:20.1211	192.168.1.2	192.168.1.2	UDP	www-app-gpnet: www-app-gpnet: 192.168.1.2:11111
226	11:14:20.1212	192.168.1.2	192.168.1.2	UDP	www-app-gpnet: www-app-gpnet: 192.168.1.2:11111
227	11:14:20.1213	192.168.1.2	192.168.1.2	UDP	www-app-gpnet: www-app-gpnet: 192.168.1.2:11111
228	11:14:20.1214	192.168.1.2	192.168.1.2	UDP	www-app-gpnet: www-app-gpnet: 192.168.1.2:11111
229	11:14:20.1215	192.168.1.2	192.168.1.2	UDP	www-app-gpnet: www-app-gpnet: 192.168.1.2:11111
230	11:14:20.1216	192.168.1.2	192.168.1.2	UDP	www-app-gpnet: www-app-gpnet: 192.168.1.2:11111
231	11:14:20.1217	192.168.1.2	192.168.1.2	UDP	www-app-gpnet: www-app-gpnet: 192.168.1.2:11111
232	11:14:20.1218	192.168.1.2	192.168.1.2	UDP	www-app-gpnet: www-app-gpnet: 192.168.1.2:11111
233	11:14:20.1219	192.168.1.2	192.168.1.2	UDP	www-app-gpnet: www-app-gpnet: 192.168.1.2:11111
234	11:14:20.1220	192.168.1.2	192.168.1.2	UDP	www-app-gpnet: www-app-gpnet: 192.168.1.2:11111
235	11:14:20.1221	192.168.1.2	192.168.1.2	UDP	www-app-gpnet: www-app-gpnet: 192.168.1.2:11111
236	11:14:20.1222	192.168.1.2	192.168.1.2	UDP	www-app-gpnet: www-app-gpnet: 192.168.1.2:11111
237	11:14:20.1223	192.168.1.2	192.168.1.2	UDP	www-app-gpnet: www-app-gpnet: 192.168.1.2:11111
238	11:14:20.1224	192.168.1.2	192.168.1.2	UDP	www-app-gpnet: www-app-gpnet: 192.168.1.2:11111
239	11:14:20.1225	192.168.1.2	192.168.1.2	UDP	www-app-gpnet: www-app-gpnet: 192.168.1.2:11111
240	11:14:20.1226	192.168.1.2	192.168.1.2	UDP	www-app-gpnet: www-app-gpnet: 192.168.1.2:11111
241	11:14:20.1227	192.168.1.2	192.168.1.2	UDP	www-app-gpnet: www-app-gpnet: 192.168.1.2:11111
242	11:14:20.1228	192.168.1.2	192.168.1.2	UDP	www-app-gpnet: www-app-gpnet: 192.168.1.2:11111
243	11:14:20.1229	192.168.1.2	192.168.1.2	UDP	www-app-gpnet: www-app-gpnet: 192.168.1.2:11111
244	11:14:20.1230	192.168.1.2	192.168.1.2	UDP	www-app-gpnet: www-app-gpnet: 192.168.1.2:11111
245	11:14:20.1231	192.168.1.2	192.168.1.2	UDP	www-app-gpnet: www-app-gpnet: 192.168.1.2:11111
246	11:14:20.1232	192.168.1.2	192.168.1.2	UDP	www-app-gpnet: www-app-gpnet: 192.168.1.2:11111
247	11:14:20.1233	192.168.1.2	192.168.1.2	UDP	www-app-gpnet: www-app-gpnet: 192.168.1.2:11111
248	11:14:20.1234	192.168.1.2	192.168.1.2	UDP	www-app-gpnet: www-app-gpnet: 192.168.1.2:11111
249	11:14:20.1235	192.168.1.2	192.168.1.2	UDP	www-app-gpnet: www-app-gpnet: 192.168.1.2:11111
250	11:14:20.1236	192.168.1.2	192.168.1.2	UDP	www-app-gpnet: www-app-gpnet: 192.168.1.2:11111



— Control LAN
 — Field LAN



Detection Strategies



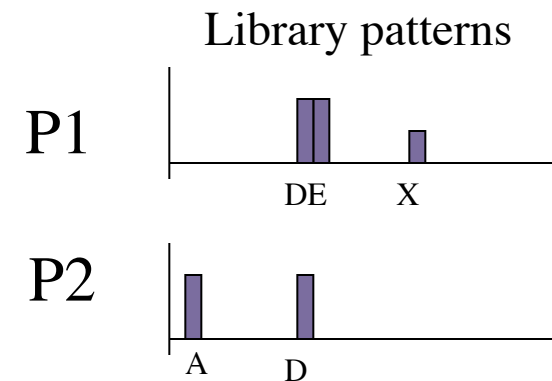
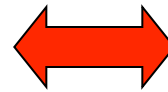
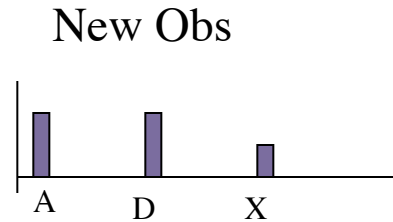
- ◆ **Signature: Look for known misuse**
- ◆ **Model Based**
 - Note regularities in PCS traffic
 - From configuration to rules
 - Machine learning of comm patterns, master/slave, temporal dynamics
 - Encode a model of expected behavior
 - Alert on exceptions
- ◆ **Specification**
 - Based on formal analysis of a protocol, or a particular implementation of a protocol
- ◆ **Deep process awareness**

Anomaly Detection Based on Learning

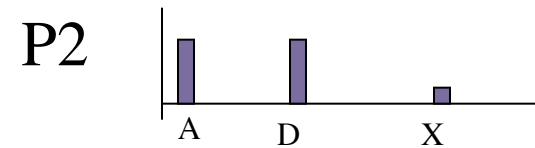


- ◆ **Observe the traffic of interest**
- ◆ **Learn patterns of normal behavior**
 - Requirement for attack-free training data?
- ◆ **After learning, alert on traffic that is extremely unusual**
 - Is the unusual malicious?
 - Is the malicious unusual by the particular statistical characterization
- ◆ **Plus: Defense against novel attacks**
- ◆ **Minus: High False Positive (FP) rate in practice**

Pattern Learning Through SOM



- Observation matches P1 in D and X, P2 in A and D, but X has a low hit count
 - \Rightarrow P2 is a better match
- Observation is assigned the label of P2
- Depending on whether P2 is rare or previously labeled malicious, generate an alert
- New P2 has a little “X”
- Does not require attack-free training data



Flow Anomaly Detection



- ◆ **Observe flows between various nodes in field and control LANs**
- ◆ **Build statistical profile of expected flow frequencies in a given time interval**
- ◆ **Alert when observe new flow or unusual behavior in a known flow**
- ◆ **Alert on the absence of an expected flow**
- ◆ **FP Rate based on estimated flow statistics**

Experiments



- ◆ **Learn normal communication patterns**
 - Master/slave relationships
 - Normal and abnormal startup/shutdown
- ◆ **Scan the field and control LANs**
- ◆ **Rogue Master on the field LAN**

MODBUS (Normal Pattern)



Slot0

	dataSelection	dimension	addrByteShift	addrHashShift	addrScrunch	addrNumScrunch	remap	portBits	dataTracking
x	DestAddress	16	1	0	1	32	none	4	global dynamic hash
y	DestAddressPort	16	1	0	1	32	none	4	global dynamic hash

Reset Filter

FrameDecay	MaxFrames	FrameSkip	FramesByMillisec	FramesByCount
0.0	0	0	60000	0

DestAddressPort

SrcAddress

DestAddress

DestAddress

InvertImage LogData RowRemoval InvertXChart LogXChart InvertYChart LogYChart

Frame 39 records 968 starts Fri Mar 27 15:05:16 PDT 2009 ends Fri Mar 27 15:06:16 PDT 2009

Unzoom

play stop next previous last first

millisecPerFrame 1000

loop chartLog

MODBUS (Nessus Scan)



Slot0 dataSelection dimension addrByteShift addrHashShift addrScrunch addrNumScrunch remap portBits dataTracking

x DestAddress 16 1 0 1 32 none 4 global dynamic hash

Reset y DestAddressPort 16 1 0 1 32 none 4 global dynamic hash

Filter FrameDecay MaxFrames FrameSkip FramesByMillisec FramesByCount

0.0 0 0 60000 0

DestAddressPort

DestAddress

SrcAddress

DestAddress

InvertImage LogData RowRemoval InvertImage LogData RowRemoval

InvertXChart LogXChart InvertXChart LogXChart

InvertYChart LogYChart InvertYChart LogYChart

Unzoom Unzoom

Frame 44
records 16208
starts Fri Mar 27 15:10:16 PDT 2009
ends Fri Mar 27 15:11:16 PDT 2009

Frame 44
records 16300
starts Fri Mar 27 15:10:16 PDT 2009
ends Fri Mar 27 15:11:16 PDT 2009

play stop next previous last first

millisecPerFrame 1000 loop chartLog

Experimental Results



◆ No FP in lab setting

- Normal operation
- Non-malicious faults
- Learned patterns are reasonable

◆ Scans

- Detected as both anomalous flow and novel pattern
- Loud scans sometimes trigger events visible at AW

◆ Rogue devices

- Detected as both anomalous flows and novel pattern

◆ MITM (Future)

Partnership Between R&D and Industry



- ◆ **SRI (Overall Lead): Intrusion Detection, Protocol Analysis, Event Aggregation**
- ◆ **Sandia National Laboratories: Architectural Vulnerability Analysis, Attack Scenarios, Red Team**
- ◆ **ArcSight: Security Incident Event Management, Situational Awareness Dashboards**
- ◆ **Invensys: Demonstration System, real-world protocol implementations**

DATES Summary



- ◆ **IDS is a necessary complement to perimeter in PCS**
- ◆ **DATES is developing novel approaches beyond signature detection**
- ◆ **Industry partnerships ensure real world relevance**



Backup

Similarity Function



- Generalizes $N(\text{Intersection})/ N(\text{Union})$
- “Intersection” is the sum of the min probabilities where the patterns intersect
- “Union” is the maximal probability where either pattern is non-zero

$$X = \begin{bmatrix} \frac{1}{3} & \frac{1}{3} & 0 & 0 & 0 & \frac{1}{3} \end{bmatrix}$$

$$Y = \begin{bmatrix} \frac{1}{5} & \frac{1}{5} & \frac{1}{5} & \frac{1}{5} & \frac{1}{5} & 0 \end{bmatrix}$$

Patterns overlap in the first two entries.

Y is minimum probability.

$$\Rightarrow \text{Numerator} = \frac{2}{5}$$

X is maximal probability in the first, second, and sixth entries.

Y is maximal elsewhere.

$$\Rightarrow \text{Denominator} = \frac{3}{3} + \frac{3}{5} = \frac{8}{5}$$

$$\text{Sim}(X,Y) = \frac{\frac{2}{5}}{\frac{8}{5}} = \frac{1}{4}$$

Picking the Winner



- Library patterns “compete” for new pattern
- Winner is most similar as long as similarity is over a set threshold
- Winner is slightly modified to include a little of the new pattern.

Algorithm to pick winner :

Find K s.t.

$$Sim(X, E_K) \geq Sim(X, E_k) \forall k$$

X = observed pattern

E_k = k th pattern exemplar in library

If $Sim(X, E_K) \geq T_{match}$, E_K is the winner

Else insert X into the library of pattern exemplars

T_{match} = Minimum match threshold

$$E_K \leftarrow \frac{1}{n_K + 1} (n_K E_K + X)$$

n_K = Historical (possibly aged) count of observances of E_K

Determining “Rare”



- If large number of patterns is learned, many may be rare
- Alert on tail probability
- Technique does not work for large number of patterns, but tail prob approach does no harm

$\Pr(E_K)$ = Historical probability of pattern K

$$= \frac{n_K}{\sum_k n_k}$$

$Tail_Pr(E_K)$ = Historical tail probability of pattern K

$$= \sum_{\Pr(E_k) \geq \Pr(E_j)} \Pr(E_j)$$

If $Tail_Pr(E_K) \leq T_{alert}$, generate alert

T_{alert} = alert threshold

Protocol Model: Individual fields



- ◆ **MODBUS function codes are one byte**
 - 256 possible values, but
 - MSB is used by servers to indicate exception
 - 0 is not valid, so valid range in 1-127
- ◆ **Range is partitioned into public, user-defined, and reserved**
 - With no further knowledge, can construct a “weak specification”
- ◆ **Many actual devices support a much more limited set of codes**
 - Permits definition of a stronger, more tailored specification

Protocol Model: Dependent Fields



- ◆ **Encode acceptable values of a field given the value of another field**
 - Example dependent fields include length, subfunction codes, and arguments
 - For example, “read coils” function implies the length field is 6
 - For other function codes, length varies but a range can be specified
- ◆ **Specifications for multiple ADUs: future work**

Detecting Unusual Communication Patterns



- **Specification of network access policies**
 - Comms between CZ and DMZ are restricted to corporate historian client and DMZ historian server
 - Comms between DMZ and PCZ are restricted to PCZ SCADA historian and DMZ historian server
 - SCADA server may communicate with the flow computer and the PLC using MODBUS
 - SCADA server may communicate to SCADA historian
 - SCADA HMI may communicate with SCADA server and engineering station
- **Detection of exceptions is via SNORT rules**
- **More complex networks (more devices) can be accommodated via IP address assignment with appropriate subnet masks**