CRITIS 2017

Timing-based anomaly detection in SCADA networks

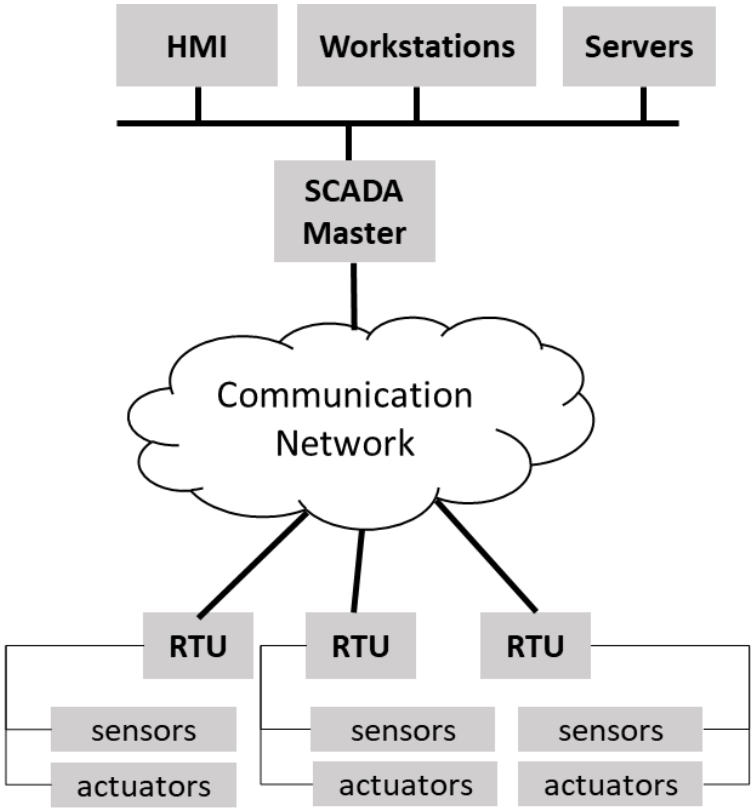
Chih-Yuan Lin, Simin Nadjm-Tehrani
and Mikael Asplund
Linköping University, Sweden

LINKÖPING UNIVERSITY

What is SCADA?

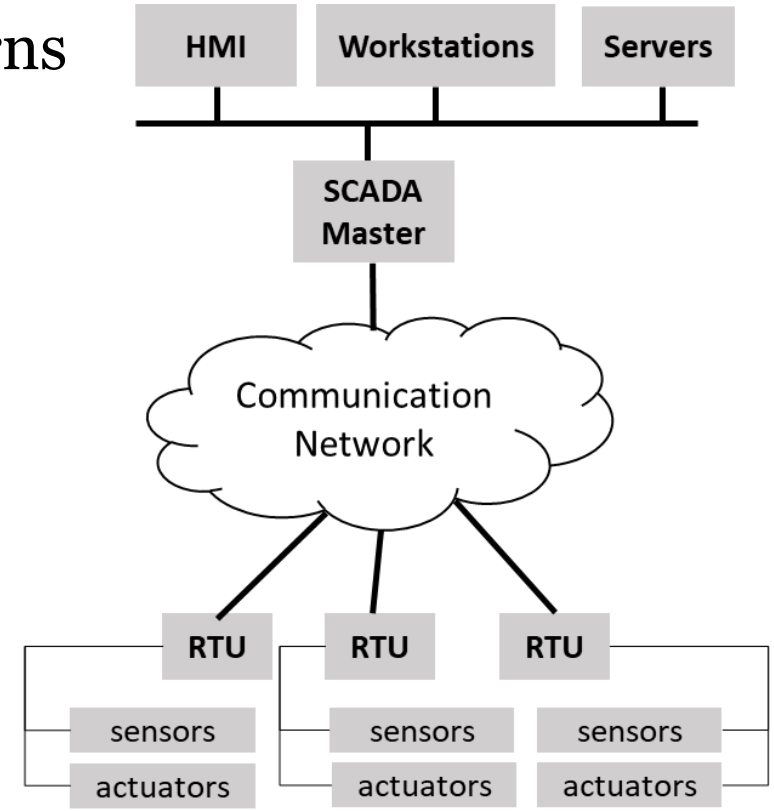
- Supervisory Control And Data Acquisition
- An Industrial automation control system running our modern industries, including *critical infrastructures*
  - Power stations
  - Transportation systems

A simple SCADA architecture



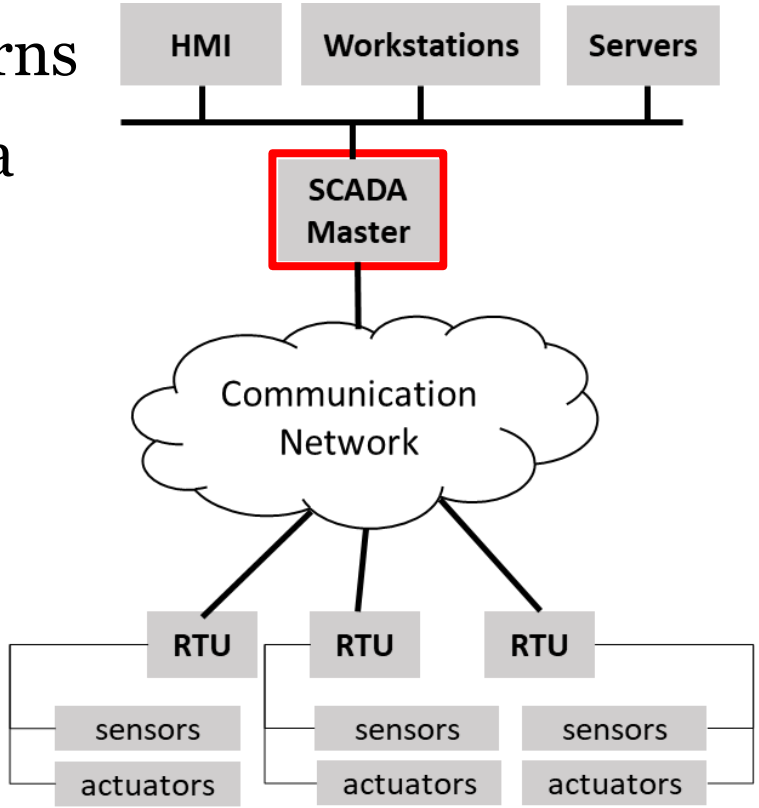
Characteristics of SCADA traffic

- Stable communication patterns



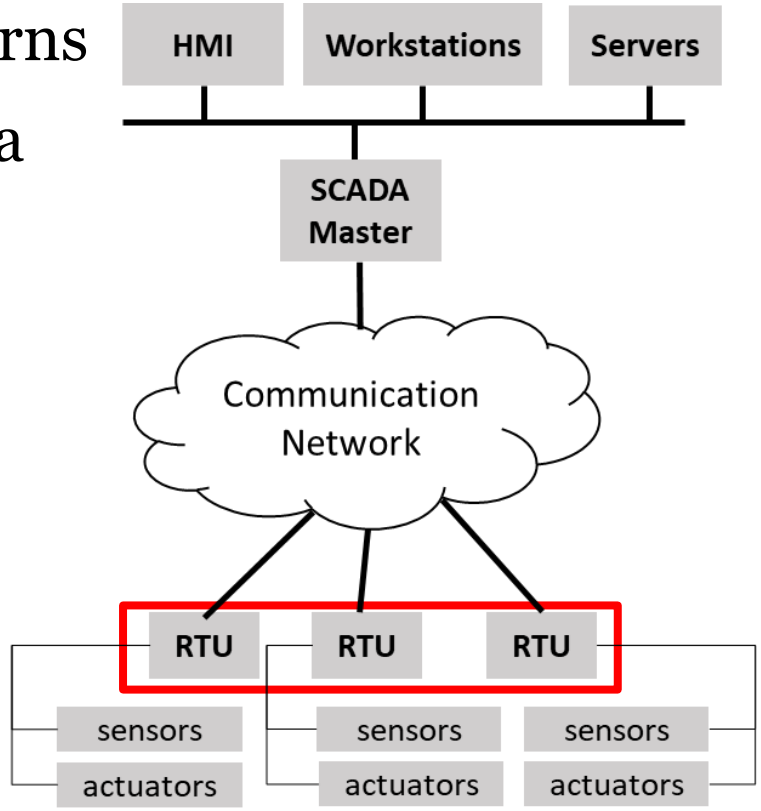
Characteristics of SCADA traffic

- Stable communication patterns
- SCADA master retrieves data from field devices by polling



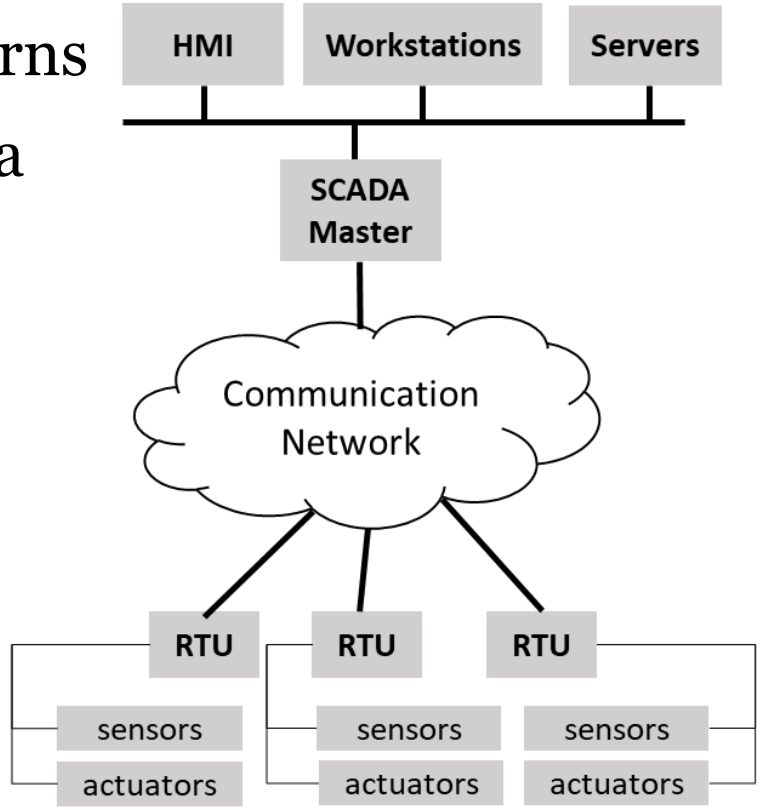
Characteristics of SCADA traffic

- Stable communication patterns
- SCADA master retrieves data from field devices by polling
- Some protocols allow asynchronous messages



Characteristics of SCADA traffic

- Stable communication patterns
- SCADA master retrieves data from field devices by polling
- Some protocols allow asynchronous messages
- SCADA-specific protocols
  - Siemens S7, Modbus and IEC-104



Threat Model

- Targeted attacks may contain only valid commands/messages
  - Flooding attack
  - Injection attack
  - TCP-sequence prediction attack

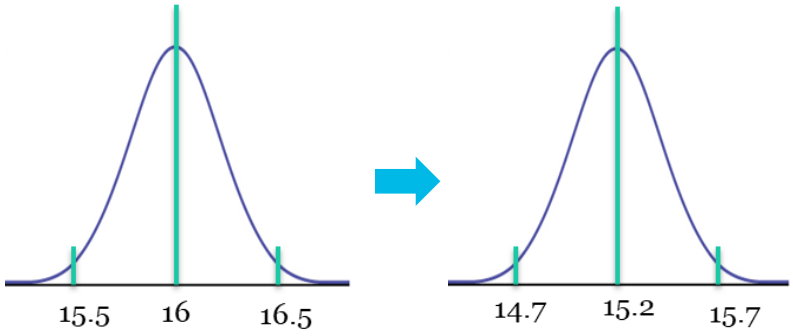
- All these attacks may cause timing anomalies

Our approach

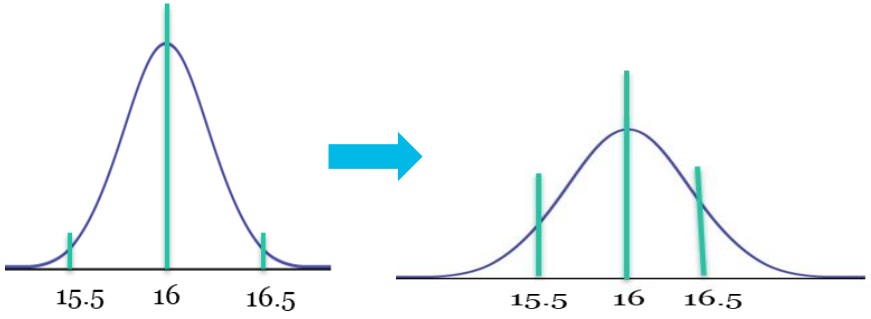
- Timing-based anomaly detection
  - Inter-arrival times of repeated messages
- Sampling distribution of
  - Sample mean
    - average of observations in a sample set
  - Sample range
    - difference of maximum and minimum observation in a sample set

Sample mean & sample range

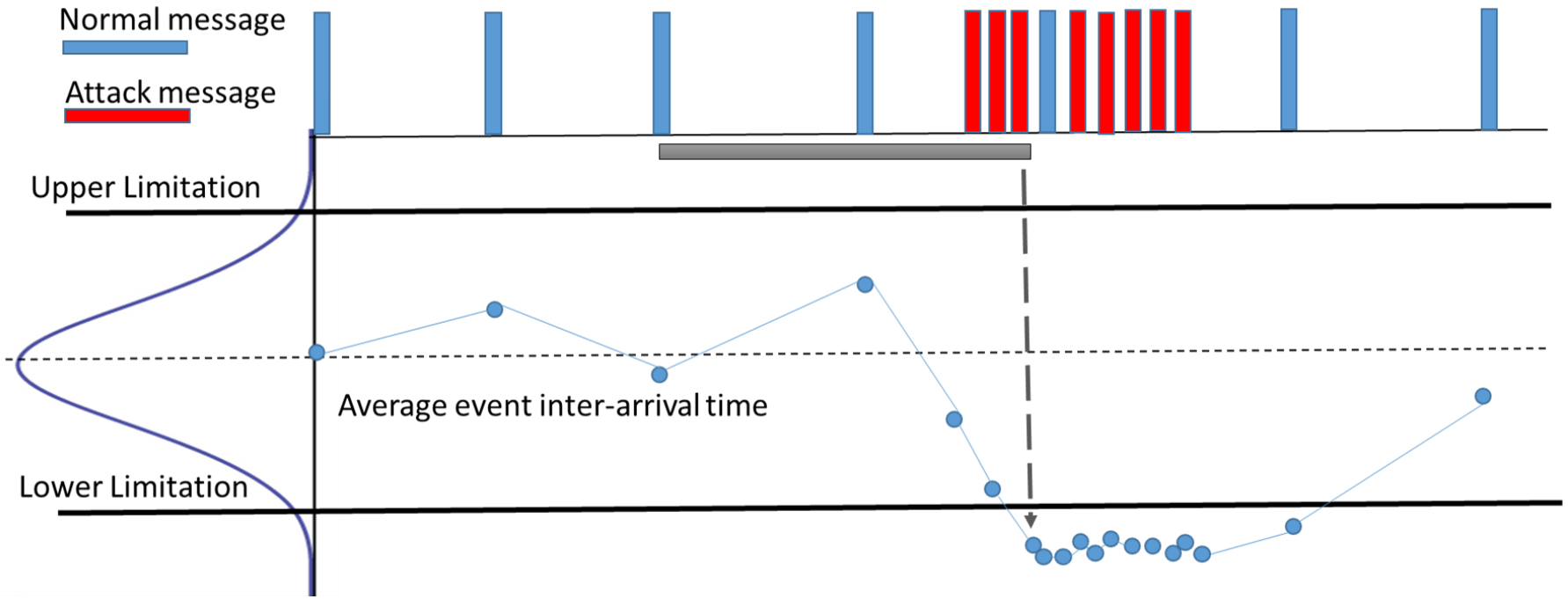
- *Sample mean*
- Can detect shift of central tendency



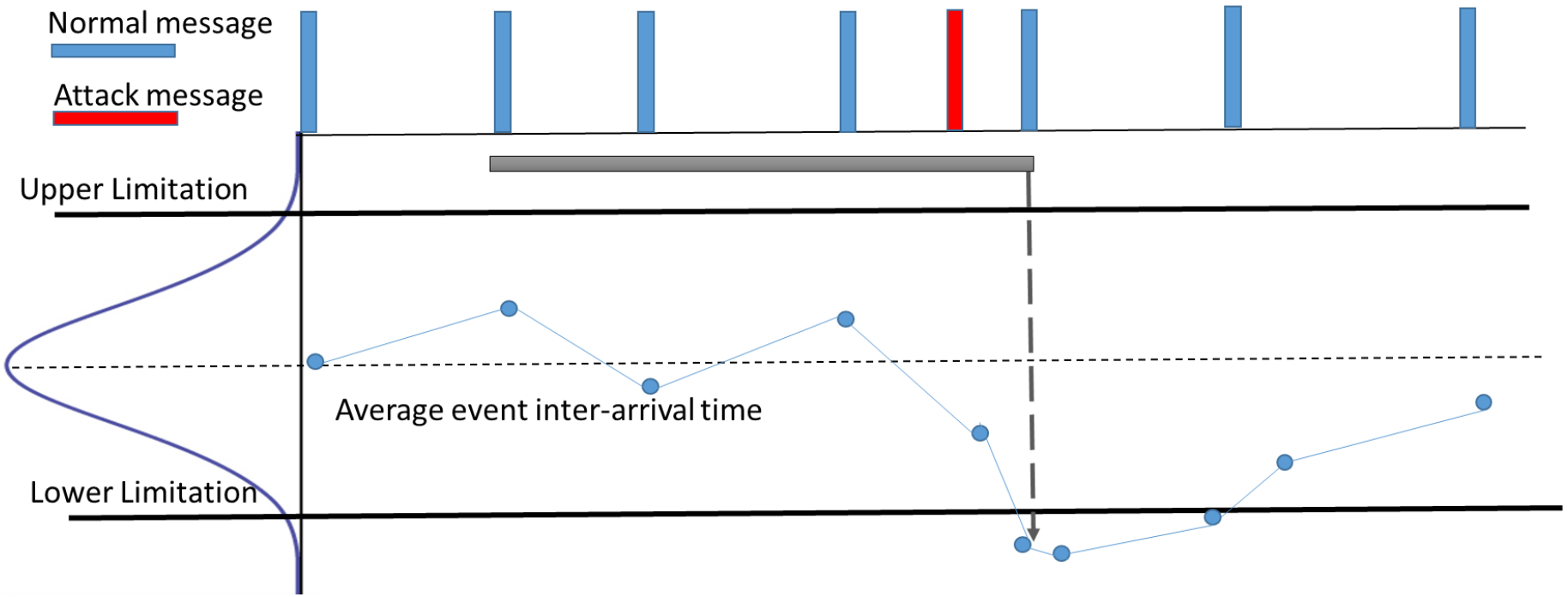
- *Sample range*
- Can detect change of dispersion



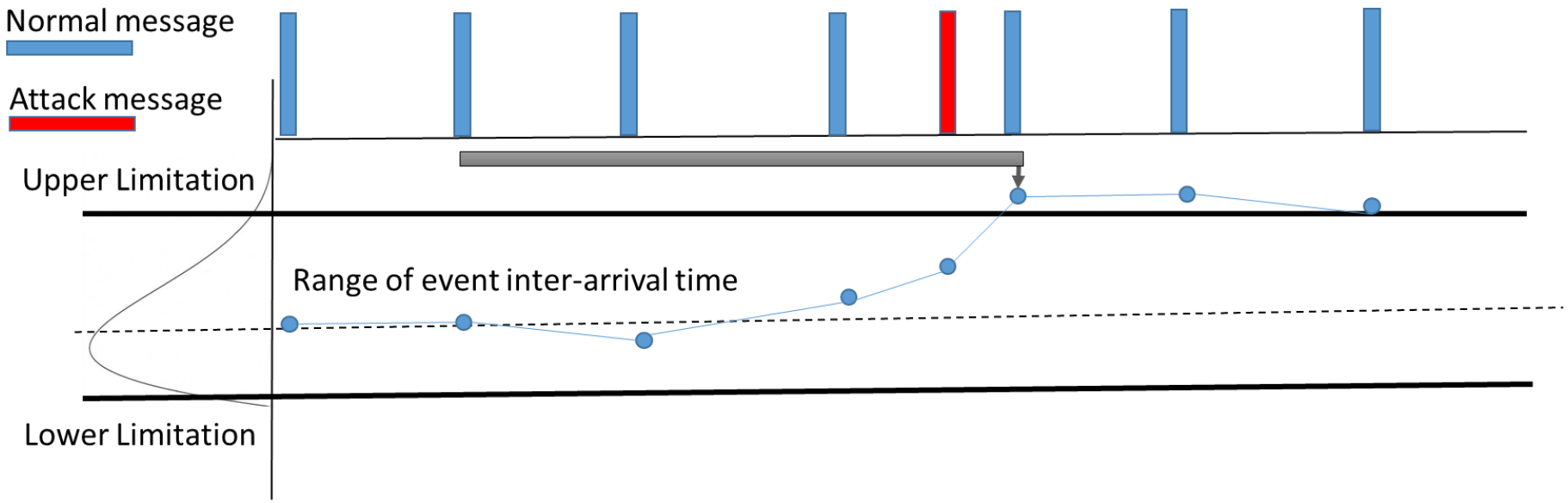
Flooding attack & mean model



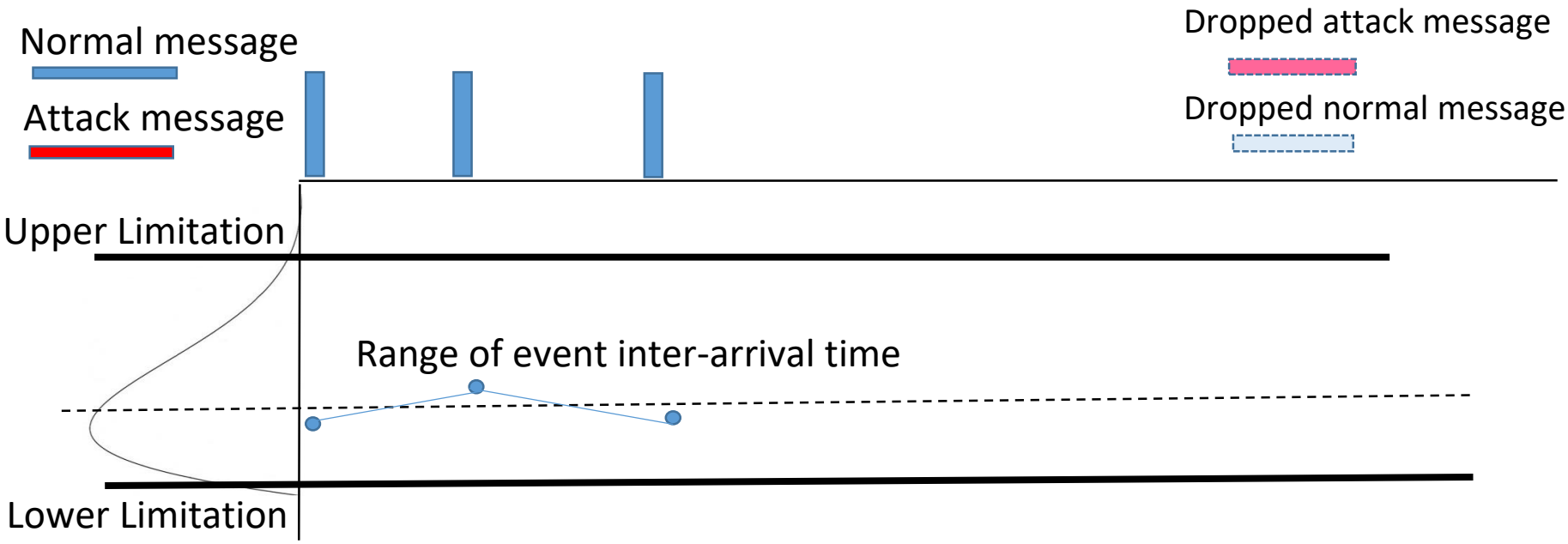
Injection attack & mean model



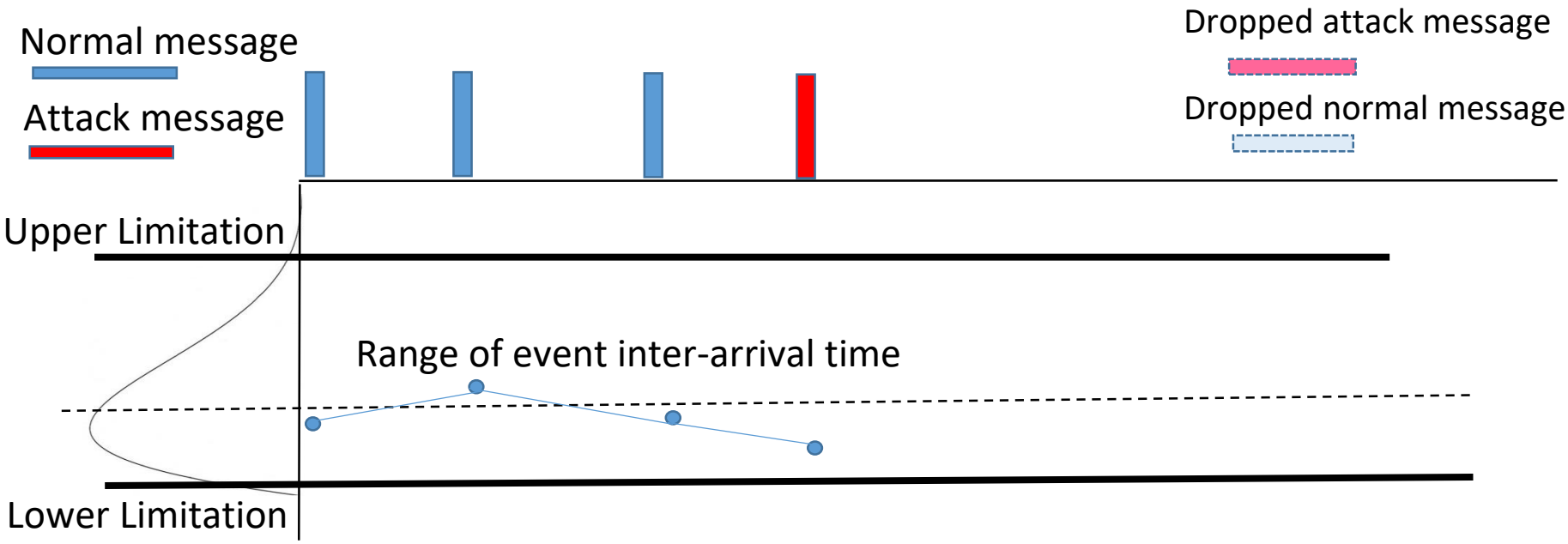
Injection attack & range model



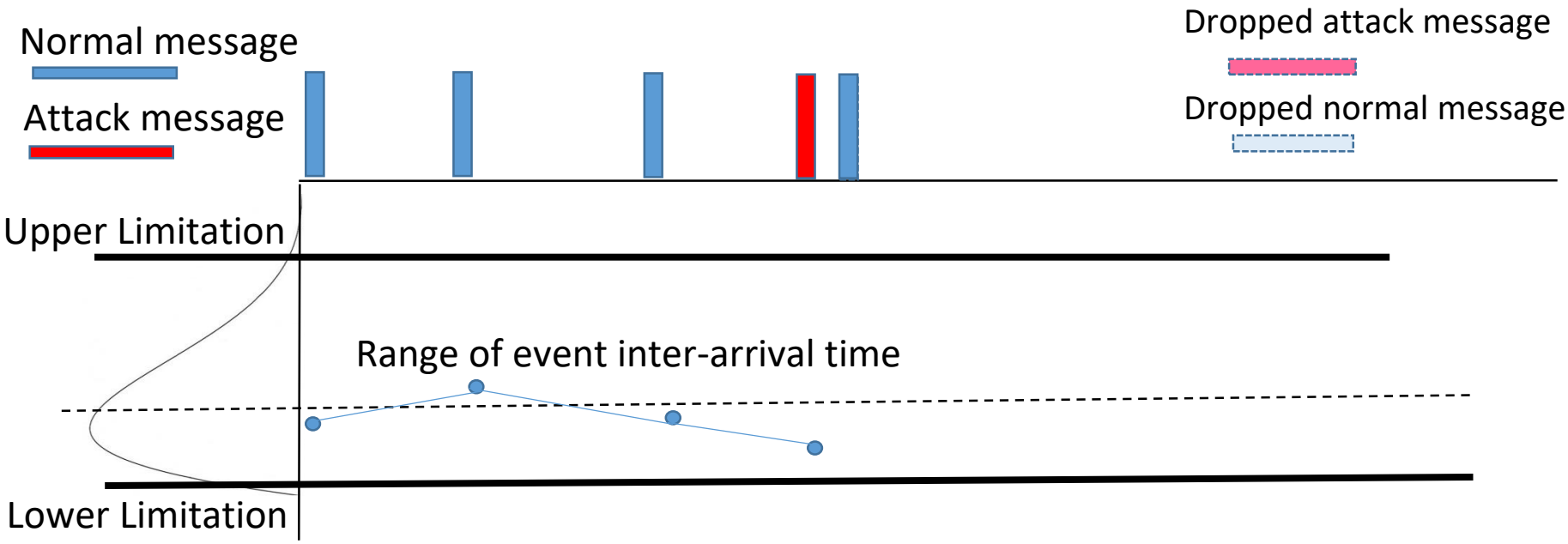
Prediction attack & range model



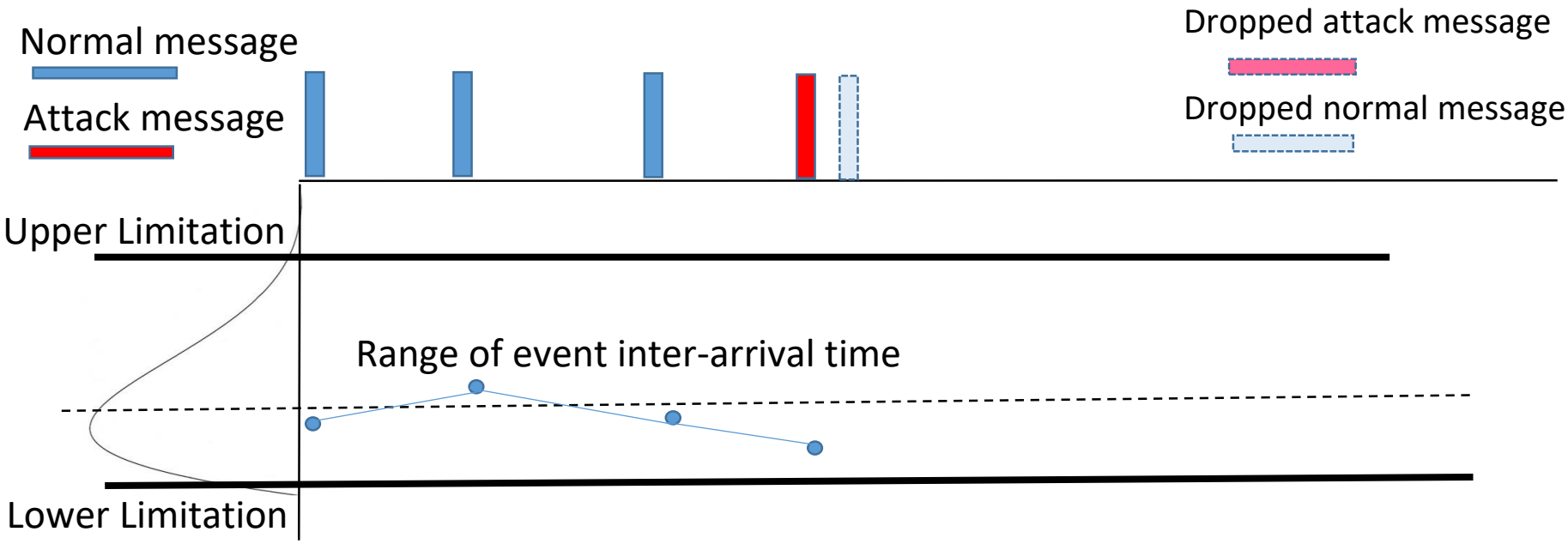
Prediction attack & range model



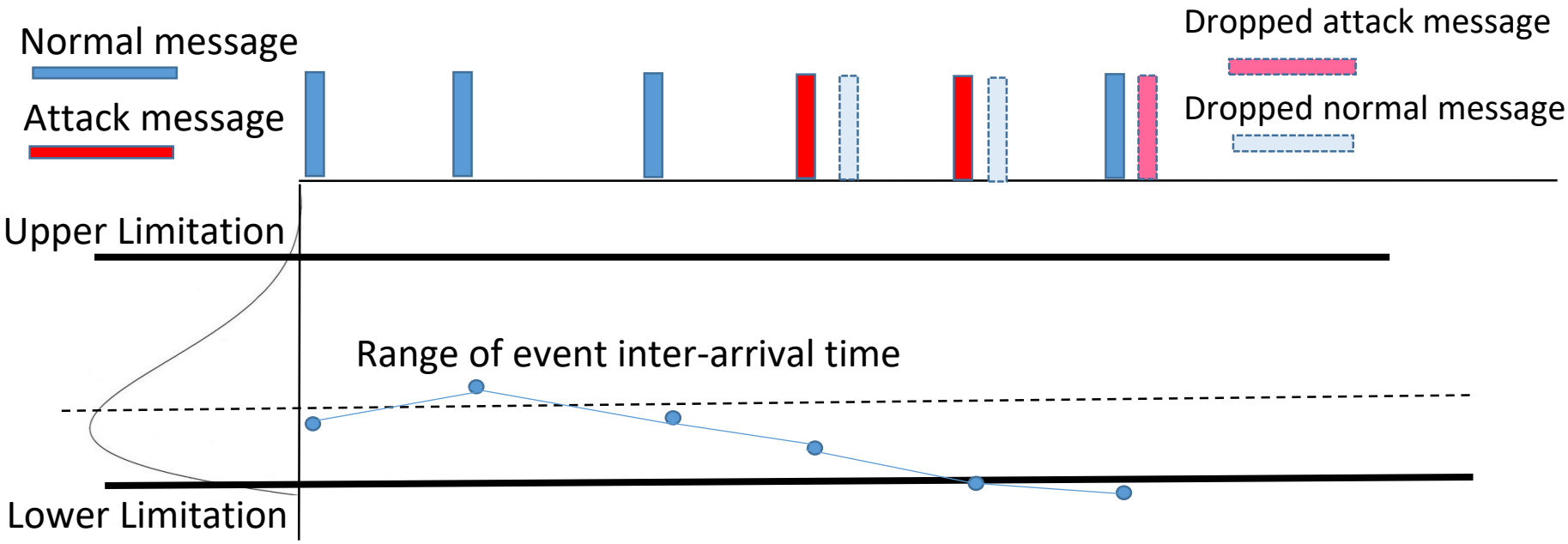
Prediction attack & range model



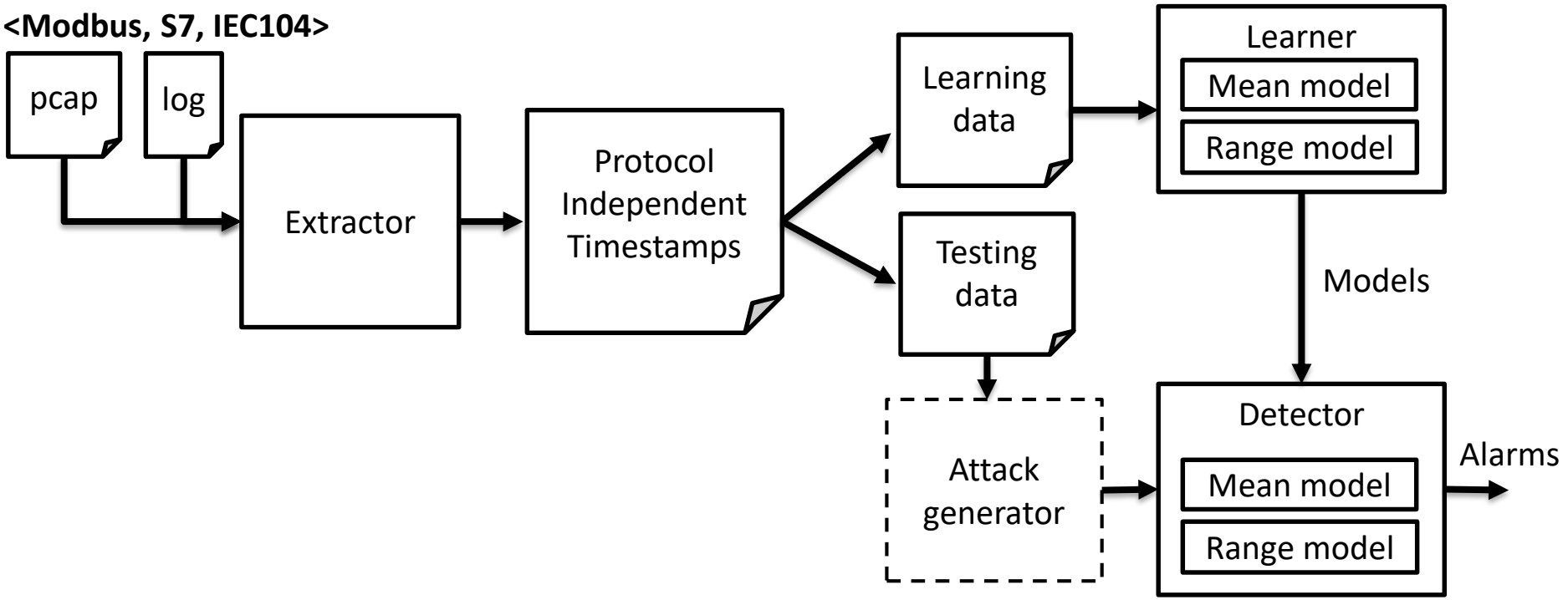
Prediction attack & range model



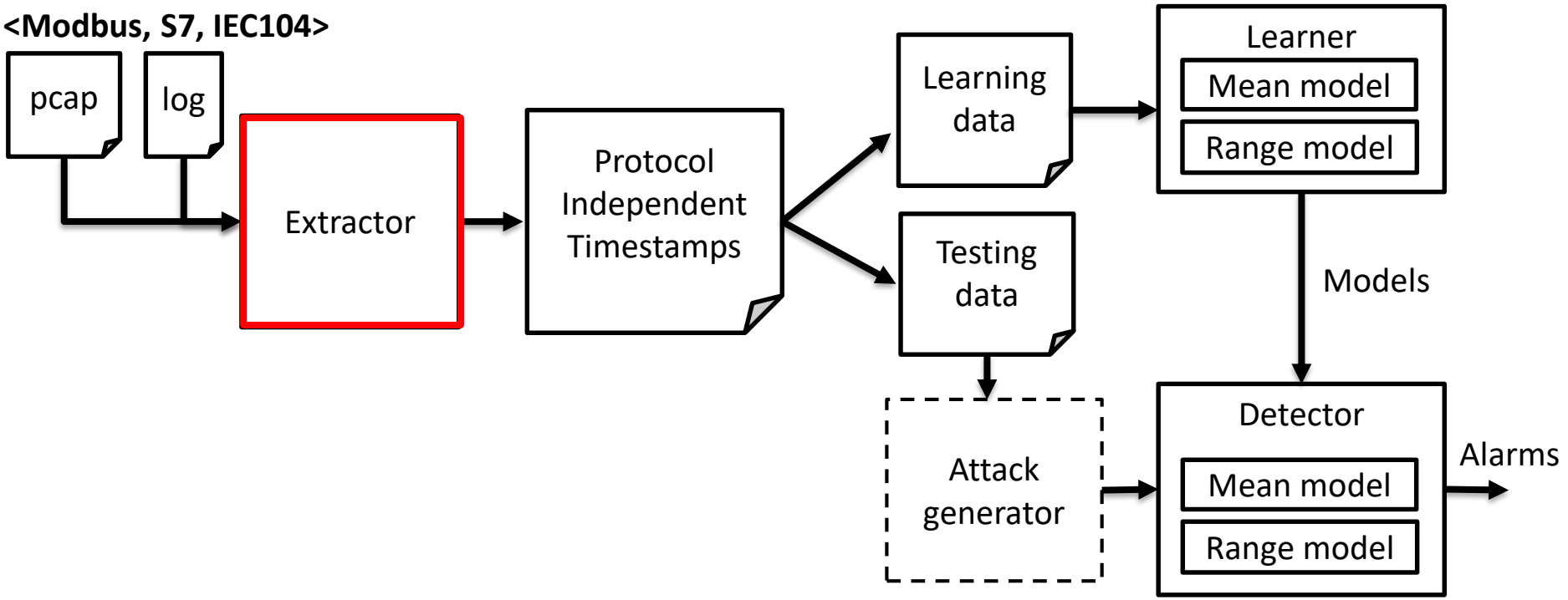
Prediction attack & range model



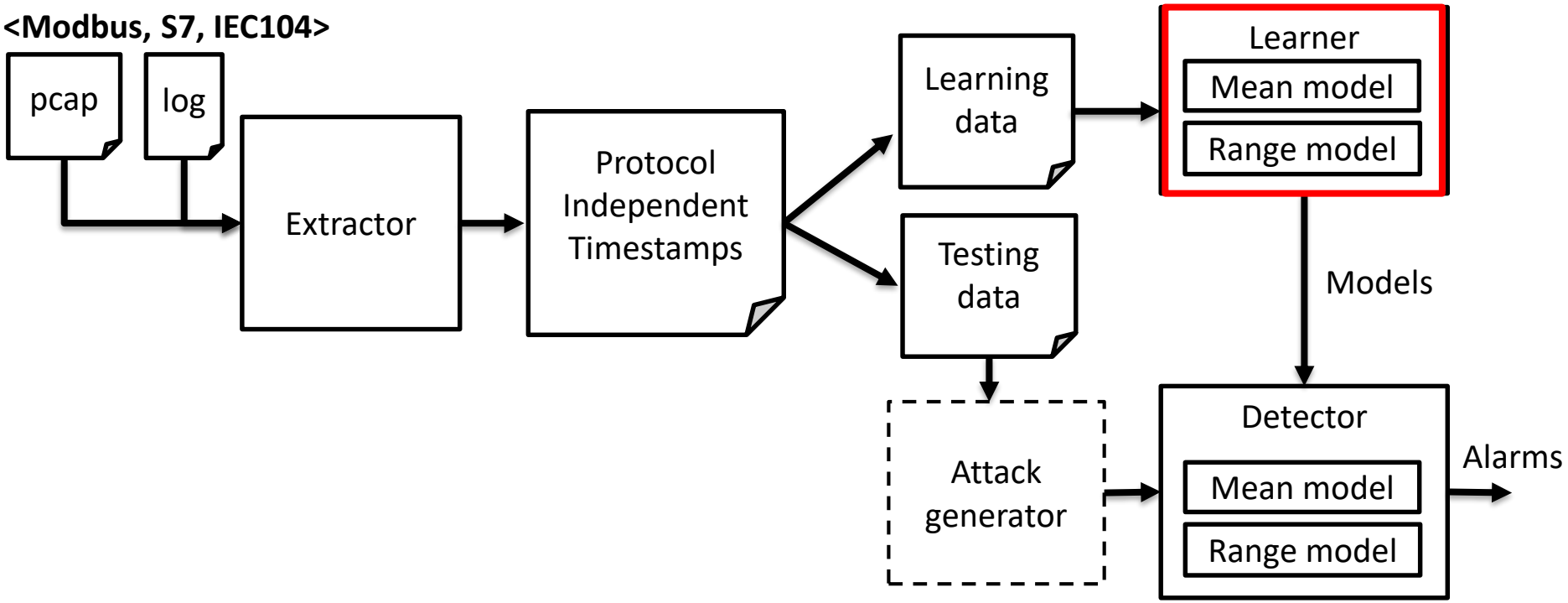
Anomaly detection workflow



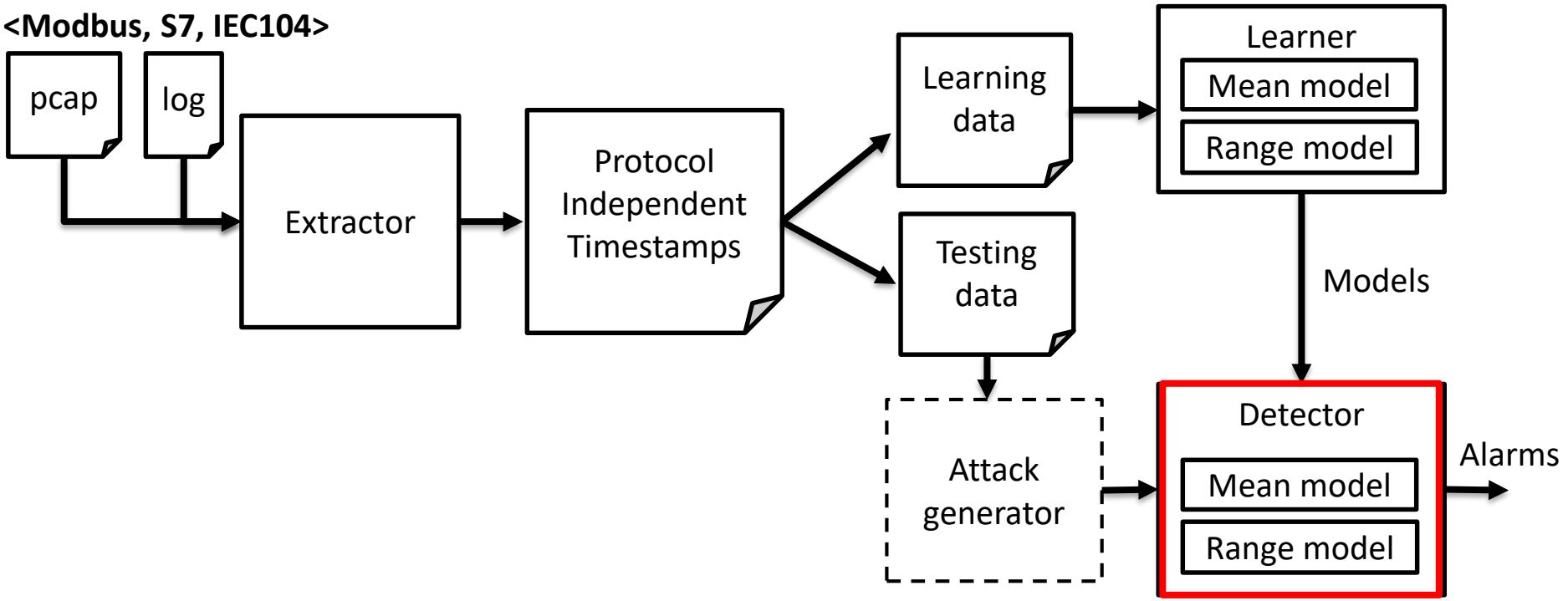
Anomaly detection workflow



Anomaly detection workflow



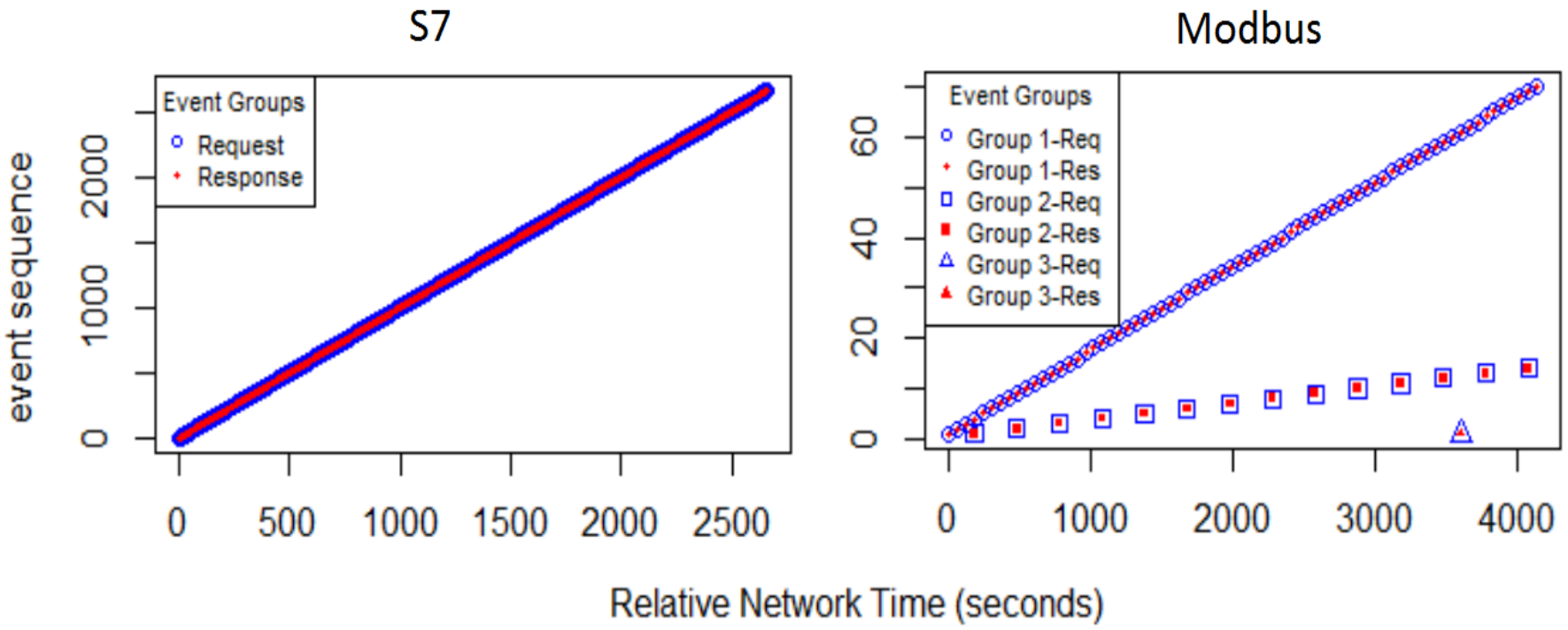
Anomaly detection workflow



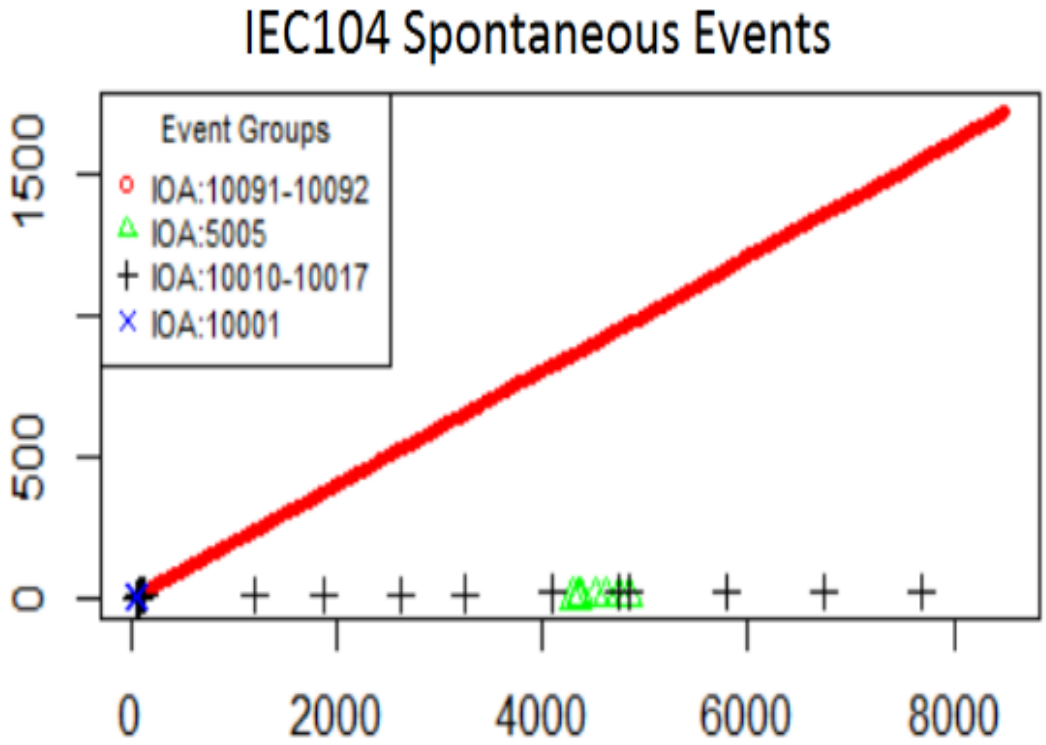
Datasets

- Modbus RTU- from actual building ventilation system
  - Synchronous request-response communication mode
- Siemens S7-simulated in 4SICSLab
  - with real Siemens devices
  - Synchronous & asynchronous messages
- IEC 60870-5-104 (IEC-104)- from our emulated testbed
  - Synchronous & asynchronous messages

Periodicity of request-response events



IEC-104 events



Overview of Selected Events

Name	Duration	Avg. period (sec)	Sd. of period (sec)	Number of events
Modbus1-req/res	5 days	59.9	2.8	5984
Modbus2-req/res	5 days	297.9	25.1	1197
S7-req/res	14 hrs	1.0	0.014	53189
IEC104-spont	24 hrs	4.9	2.9	16831

Overview of Selected Events

Name	Duration	Avg. period (sec)	Sd. of period (sec)	Number of events
Modbus1-req/res	5 days	59.9	2.8	5984
Modbus2-req/res	5 days	297.9	25.1	1197
S7-req/res	14 hrs	1.0	0.014	53189
IEC104-spont	24 hrs	4.9	2.9	16831

Evaluation

- $\text{FPR} = \dfrac{\text{number of false alarms}}{\text{number of windows without attacks}}$ (%)
- $\text{TPR} = \dfrac{\text{number of true alarms}}{\text{number of windows with attacks}}$ (%)
- $\text{ODR} = \dfrac{\text{number of detected attack events}}{\text{number of attack events}}$ (%)

Detection Accuracy

	Flooding					Injection					Prediction				
	Mean		Range			Mean		Range			Mean		Range		
	TPR	FPR	TPR	FPR	ODR	TPR	FPR	TPR	FPR	ODR	TPR	FPR	TPR	FPR	ODR
S7-req	99.96	0.01	59.15	0.84	100	96.25	0.01	100	0.89	100	0.12	0	90.6	0.89	99.81
S7-res	99.95	0.21	56.41	1.13	100	96.66	0.2	99.58	1.16	100	0.23	0.2	91.09	1.15	99.51
Modbus1-req	99.84	0	99.69	1.13	100	83.33	0	83.33	1.16	100	0	0	92.86	1.36	99.19
Modbus1-res	99.83	0	99.68	1.15	100	83.33	0	83.33	1.2	100	0	0	91.93	1.4	99.19
Modbus2-req	99.83	0	100	0	100	83.12	0	100	0	100	4.95	0	100	0	100
Modbus2-res	99.83	0	100	0.38	100	83.12	0	100	0.38	100	4.95	0	100	0.32	100
104-spont	98.88	0.42	98.14	1.14	100	2.47	0.42	3.7	1.16	13.33	2.8	0.4	72.44	1.11	92.89

Detection Accuracy

	Flooding					Injection					Prediction				
	Mean		Range			Mean		Range			Mean		Range		
	TPR	FPR	TPR	FPR	ODR	TPR	FPR	TPR	FPR	ODR	TPR	FPR	TPR	FPR	ODR
S7-req	99.96	0.01	59.15	0.84	100	96.25	0.01	100	0.89	100	0.12	0	90.6	0.89	99.81
S7-res	99.95	0.21	56.41	1.13	100	96.66	0.2	99.58	1.16	100	0.23	0.2	91.09	1.15	99.51
Modbus1-req	99.84	0	99.69	1.13	100	83.33	0	83.33	1.16	100	0	0	92.86	1.36	99.19
Modbus1-res	99.83	0	99.68	1.15	100	83.33	0	83.33	1.2	100	0	0	91.93	1.4	99.19
Modbus2-req	99.83	0	100	0	100	83.12	0	100	0	100	4.95	0	100	0	100
Modbus2-res	99.83	0	100	0.38	100	83.12	0	100	0.38	100	4.95	0	100	0.32	100
104-spont	98.88	0.42	98.14	1.14	100	2.47	0.42	3.7	1.16	13.33	2.8	0.4	72.44	1.11	92.89

Detection Accuracy

	Flooding					Injection					Prediction				
	Mean		Range			Mean		Range			Mean		Range		
	TPR	FPR	TPR	FPR	ODR	TPR	FPR	TPR	FPR	ODR	TPR	FPR	TPR	FPR	ODR
S7-req	99.96	0.01	59.15	0.84	100	96.25	0.01	100	0.89	100	0.12	0	90.6	0.89	99.81
S7-res	99.95	0.21	56.41	1.13	100	96.66	0.2	99.58	1.16	100	0.23	0.2	91.09	1.15	99.51
Modbus1-req	99.84	0	99.69	1.13	100	83.33	0	83.33	1.16	100	0	0	92.86	1.36	99.19
Modbus1-res	99.83	0	99.68	1.15	100	83.33	0	83.33	1.2	100	0	0	91.93	1.4	99.19
Modbus2-req	99.83	0	100	0	100	83.12	0	100	0	100	4.95	0	100	0	100
Modbus2-res	99.83	0	100	0.38	100	83.12	0	100	0.38	100	4.95	0	100	0.32	100
104-spont	98.88	0.42	98.14	1.14	100	2.47	0.42	3.7	1.16	13.33	2.8	0.4	72.44	1.11	92.89

Detection Accuracy

	Flooding					Injection					Prediction				
	Mean		Range			Mean		Range			Mean		Range		
	TPR	FPR	TPR	FPR	ODR	TPR	FPR	TPR	FPR	ODR	TPR	FPR	TPR	FPR	ODR
S7-req	99.96	0.01	59.15	0.84	100	96.25	0.01	100	0.89	100	0.12	0	90.6	0.89	99.81
S7-res	99.95	0.21	56.41	1.13	100	96.66	0.2	99.58	1.16	100	0.23	0.2	91.09	1.15	99.51
Modbus1-req	99.84	0	99.69	1.13	100	83.33	0	83.33	1.16	100	0	0	92.86	1.36	99.19
Modbus1-res	99.83	0	99.68	1.15	100	83.33	0	83.33	1.2	100	0	0	91.93	1.4	99.19
Modbus2-req	99.83	0	100	0	100	83.12	0	100	0	100	4.95	0	100	0	100
Modbus2-res	99.83	0	100	0.38	100	83.12	0	100	0.38	100	4.95	0	100	0.32	100
104-spont	98.88	0.42	98.14	1.14	100	2.47	0.42	3.7	1.16	13.33	2.8	0.4	72.44	1.11	92.89

Detection Accuracy

	Flooding					Injection					Prediction				
	Mean		Range			Mean		Range			Mean		Range		
	TPR	FPR	TPR	FPR	ODR	TPR	FPR	TPR	FPR	ODR	TPR	FPR	TPR	FPR	ODR
S7-req	99.96	0.01	59.15	0.84	100	96.25	0.01	100	0.89	100	0.12	0	90.6	0.89	99.81
S7-res	99.95	0.21	56.41	1.13	100	96.66	0.2	99.58	1.16	100	0.23	0.2	91.09	1.15	99.51
Modbus1-req	99.84	0	99.69	1.13	100	83.33	0	83.33	1.16	100	0	0	92.86	1.36	99.19
Modbus1-res	99.83	0	99.68	1.15	100	83.33	0	83.33	1.2	100	0	0	91.93	1.4	99.19
Modbus2-req	99.83	0	100	0	100	83.12	0	100	0	100	4.95	0	100	0	100
Modbus2-res	99.83	0	100	0.38	100	83.12	0	100	0.38	100	4.95	0	100	0.32	100
104-spont	98.88	0.42	98.14	1.14	100	2.47	0.42	3.7	1.16	13.33	2.8	0.4	72.44	1.11	92.89

Detection Accuracy

	Flooding					Injection					Prediction				
	Mean		Range			Mean		Range			Mean		Range		
	TPR	FPR	TPR	FPR	ODR	TPR	FPR	TPR	FPR	ODR	TPR	FPR	TPR	FPR	ODR
S7-req	99.96	0.01	59.15	0.84	100	96.25	0.01	100	0.89	100	0.12	0	90.6	0.89	99.81
S7-res	99.95	0.21	56.41	1.13	100	96.66	0.2	99.58	1.16	100	0.23	0.2	91.09	1.15	99.51
Modbus1-req	99.84	0	99.69	1.13	100	83.33	0	83.33	1.16	100	0	0	92.86	1.36	99.19
Modbus1-res	99.83	0	99.68	1.15	100	83.33	0	83.33	1.2	100	0	0	91.93	1.4	99.19
Modbus2-req	99.83	0	100	0	100	83.12	0	100	0	100	4.95	0	100	0	100
Modbus2-res	99.83	0	100	0.38	100	83.12	0	100	0.38	100	4.95	0	100	0.32	100
104-spont	98.88	0.42	98.14	1.14	100	2.47	0.42	3.7	1.16	13.33	2.8	0.4	72.44	1.11	92.89

Conclusions

- Timing-based anomaly detection shown to be promising
- Identified the need for more complicated timing models for modern protocols such as IEC-104

Questions?

Paper 37

chih-yuan.lin@liu.se

www.rics.se

LINKÖPING UNIVERSITY

RICS

MSB Myndigheten för samhällsskydd och beredskap