ISRCS 2012

Improving Cyber-Security of Smart Grid Systems via Anomaly Detection and Linguistic Domain Knowledge

August 14th, 2012

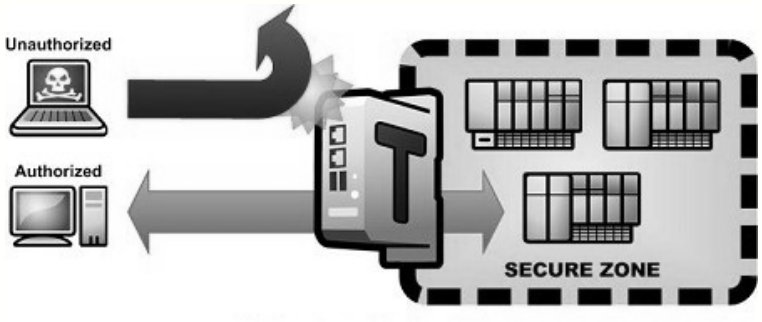
Ondrej Linda, Todd Vollmer, Milos Manic

Outline

- Motivation
  - Previous Work
- Anomaly Detection based Cyber Sensor
- Representing Domain Knowledge
  - Linguistic Fuzzy Rules
- Anomaly Detection Architecture using Linguistic Rules
- Experimental Results
- Conclusion

Cyber-Security of Critical Infrastructures

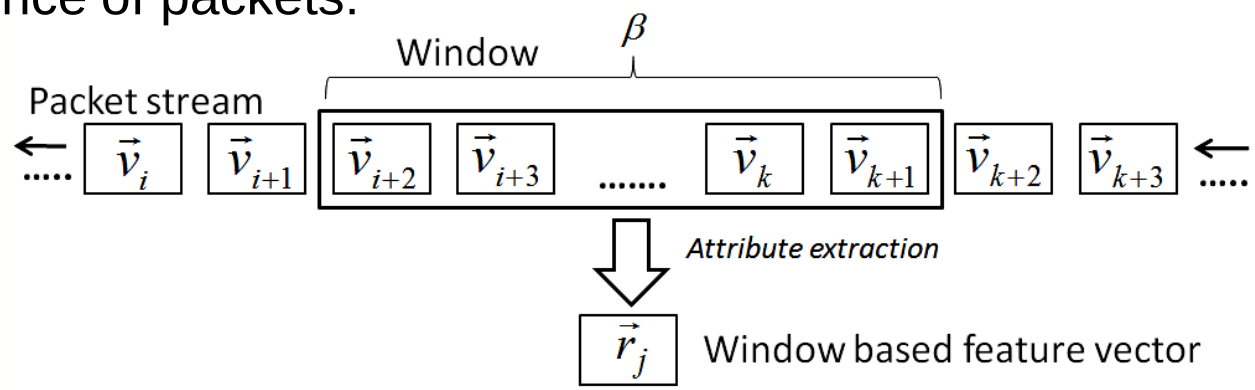
- Protection against cyber attacks and cyber terrorism
- **Critical infrastructures** (e.g. nuclear power plants, SCADA) are vulnerable
- Development of System Protection Cyber Sensor
  - Easy to deploy
  - Low Cost
  - Increased State-Awareness



- Previously adopted solution:
  - **Anomaly Detection**
  - **Cons:**
    - Builds single comprehensive normal behavior model
      - (unsuitable for overlapping communication streams)
    - Uses sensitivity threshold
      - (false positive – false negative tradeoff)

Window Based Feature Extraction

- **Previous work**: Use sliding window to compute statistical properties of a sequence of packets:



- 17 identified important attributes:

SELECTED WINDOW-BASED FEATURES

Num. of IP addresses	Num. of Flag Codes
Min. Num. of Packets / IP	Min. Num. of Packets / Flag Code
Max. Num. of Packets / IP	Max. Num. of Packets / Flag Code
Avg. Time between Packets	Num. of Packets with 0 Win. Size
Time Length of the Window	Num. of Packets with 0 Data Len.
Data Speed	Avg. Win. Size
Num. of Protocols	Avg. Data Length
Min. Num. of Packets / Protocol	Num. of Ports
Max. Num. of Packets / Protocol	

Online Learning Algorithm

- Online network behavior patterns extraction
  - Apply **Nearest Neighbor clustering algorithm** to the incoming pre-processed stream of packets
  - Also accumulate statistical information about the patterns assigned to each cluster

- Cluster attributes:

$$P_i = \{\vec{c}_i, w_i, M_i\},\ \vec{c}_i = \{c_i^1, \ldots, c_i^n\},\ M_i = \begin{vmatrix} \overline{c}_i^1 & \cdots & \overline{c}_i^n \\ \underline{c}_i^1 & \cdots & \underline{c}_i^n \end{vmatrix}$$

- Modified cluster update rule for the Nearest Neighbor clustering:

$$\vec{c}_a = \frac{w_a \vec{c}_a + \vec{x}_i}{w_a + 1},\ w_a = w_a + 1$$

$$\overline{c}_i^j = \max(x_i^j, \overline{c}_i^j),\ \underline{c}_i^j = \min(x_i^j, \underline{c}_i^j) \quad j = 1 \ldots n$$

Fuzzy Rule Extraction

- During the testing phase, individual clusters are used to initialize fuzzy rules:

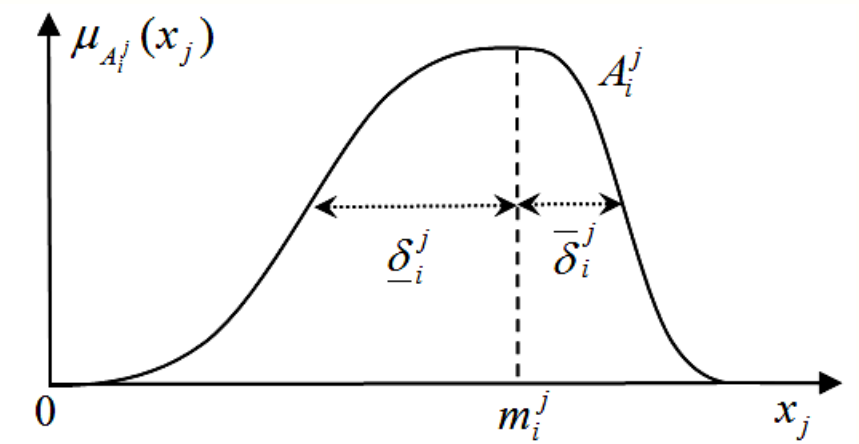
$$\text{Rule } R_k\text{: } \textbf{IF } x_1 \text{ is } A_1^k \textbf{ AND } \ldots \textbf{ AND } x_n \text{ is } A_n^k \textbf{ THEN } y_k \text{ is } B^k$$

- Gaussian fuzzy set:

$$m_i^j = c_i^j$$

$$\overline{\delta}_i^j = \alpha(\overline{c}_i^j - c_i^j)$$

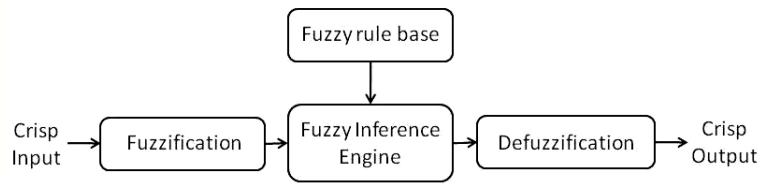
$$\underline{\delta}_i^j = \alpha(c_i^j - \underline{c}_i^j)$$



α - Fuzzines parameter

Fuzzy Rule Based Anomaly Detection

- Uses fuzzy inference with the extracted set of normal network behavior rules:



- Fuzzy Rules: Rule R_k: **IF** x_1 is A_1^k **AND** … **AND** x_n is A_n^k **THEN** y_k is B^k

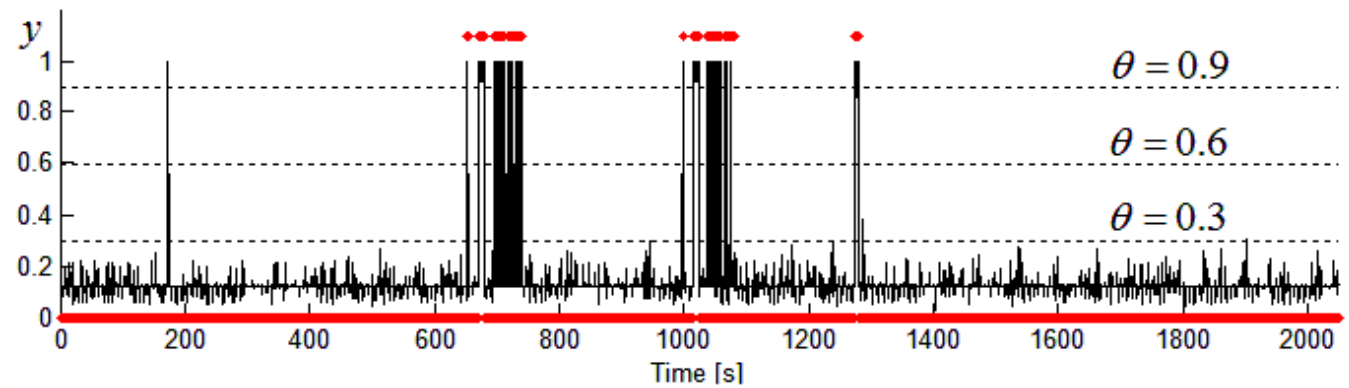
- Degree of Firing: $$\mu_{R_i}(\vec{x}) = \min_{j=1\ldots n}\{\mu_{A_i^j}(x_j)\}$$

- Aggregate rule outputs: $$y(\vec{x}) = \max_{i=1\ldots C} \mu_{R_i}(\vec{x})$$

  – Rules describe the similarity of the observed behavior and the normal behavior. Hence, the output of each rule is its own firing strength

Anomaly Detection – Case Study

- Anomaly Detection results on a single communication stream
  - Detection performance with different sensitivity threshold values



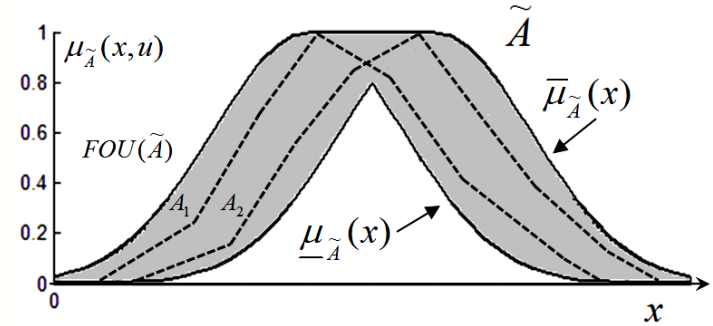
CLASSIFICATION PERFORMANCE WITH DIFFERENT SENSITIVITY THRESHOLDS

Threshold	Correct Rate	False Pos.	False Neg.
0.3	99.9037%	0.1217%	0.0275%
0.6	99.5504%	0.1082%	1.3753%
0.9	99.3799%	0.1082%	2.0079%

  - Adjusting sensitivity threshold leads to false negative – false positive tradeoff

Representing Domain Knowledge

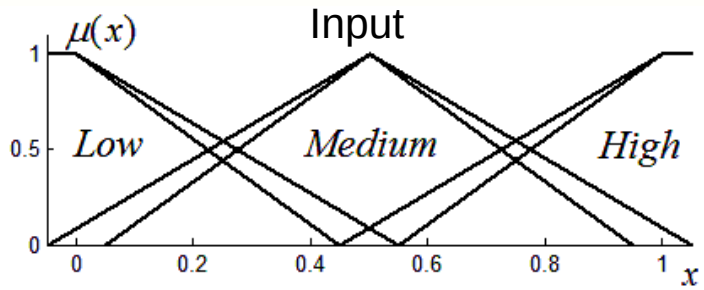
- Modeling of domain knowledge using **linguistic fuzzy rules**
  - Use Interval Type-2 Fuzzy Sets (IT2 FSs)
  - Handle **linguistic uncertainty**

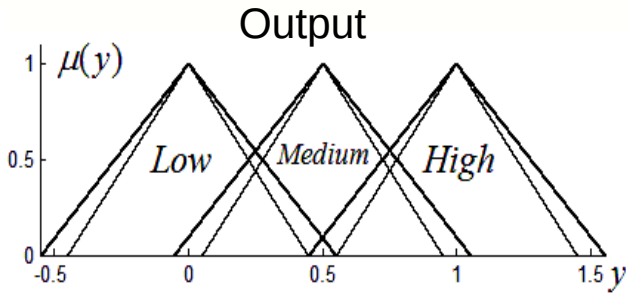


IT2 Fuzzy Rule:

Rule R_k: **IF** x_1 is $\tilde{A}_1^k$ **AND** … **AND** x_n is $\tilde{A}_n^k$ **THEN** y_k is $\tilde{B}^k$

- IT2 Fuzzy Logic System is used to compute the sensitivity threshold

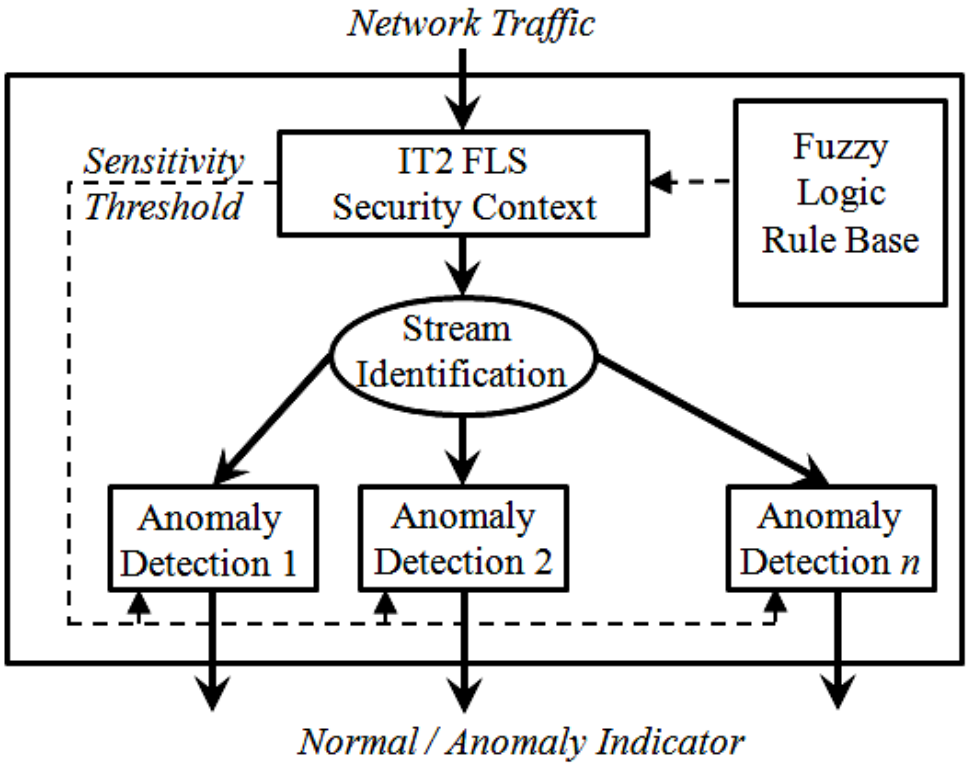




Ex. : *If number of protocols is high then sensitivity threshold is low*

Anomaly Detection System Architecture

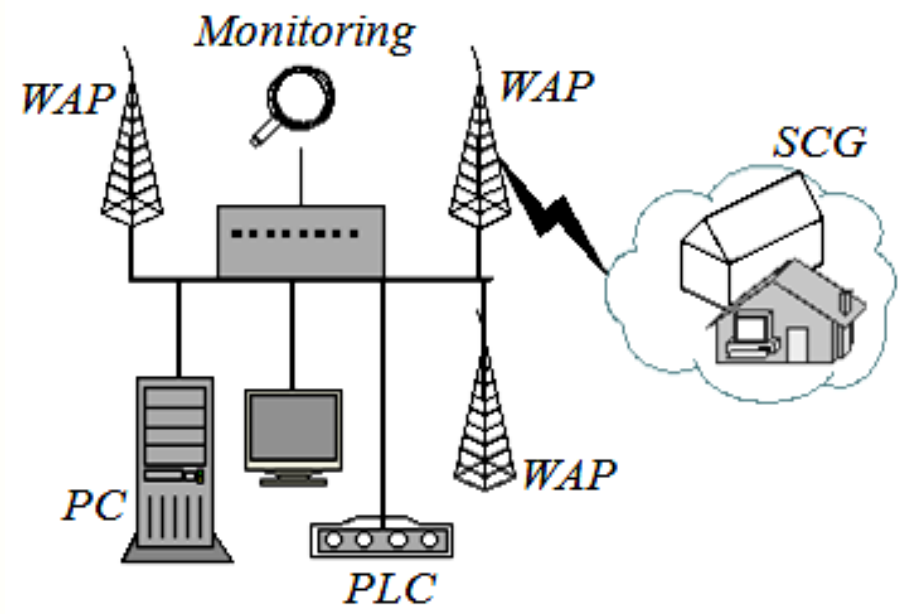
- 1) Determine Cyber-Security Context
  - Uses linguistic rules to compute the sensitivity threshold
- 2) Isolate individual communication streams
  - e.g. IP-based
- 3) Calculate the anomalous level in each communication stream
- 4) Use the computed sensitivity threshold to classify the input
  - Normal / anomaly



Assumption: Representative normal behavior was used for training

Experimental Test-bed

- Small campus grid (SCG) and sensor network
  - Center for Advanced Energy Studies (CASE), Idaho Falls, ID
  - Smart Grid test platform
  - Heterogeneous mixture of devices
    - Wireless sensors, wind and solar power resources,
  - Wireless AMI
    - WAP gateways
  - Control systems:
    - Rockwell automation PLC
    - National Instruments PLC



Experimental Data Sets

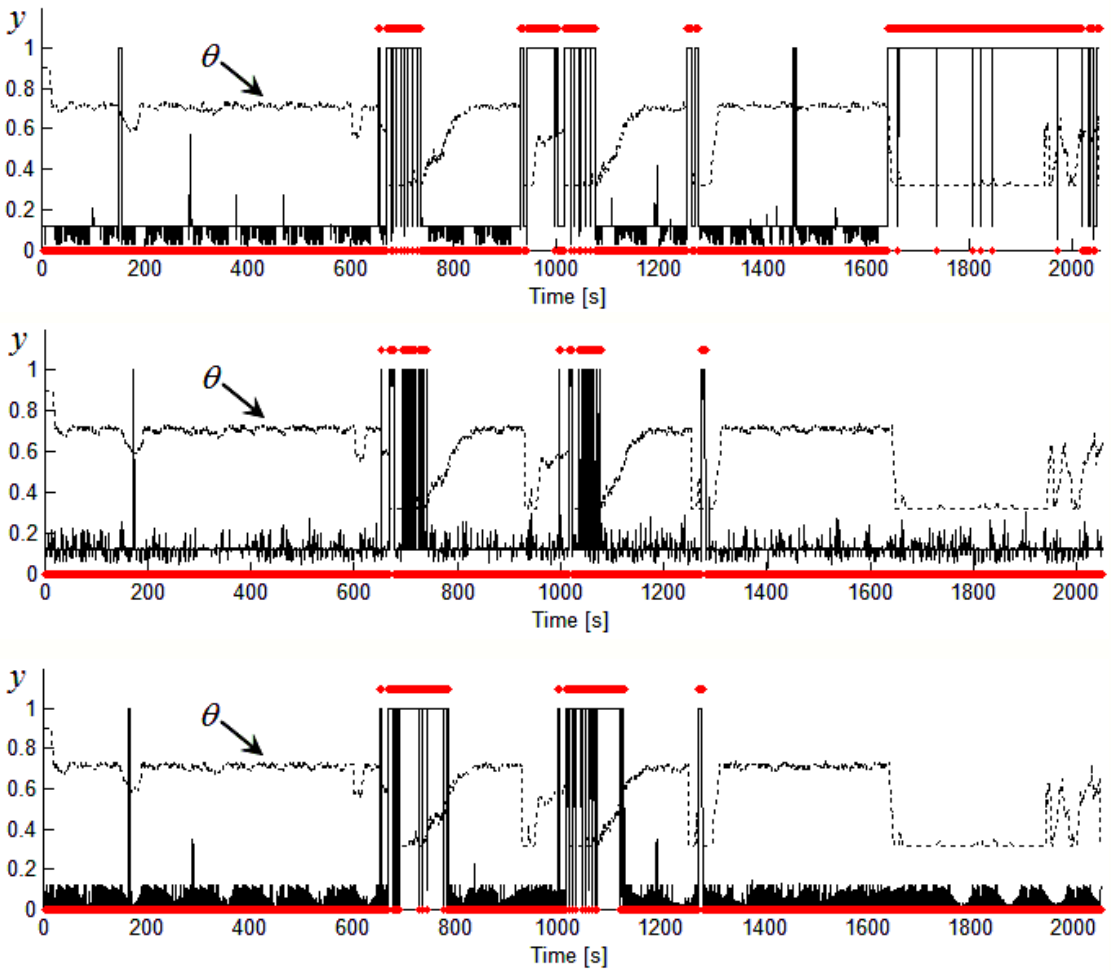
- Normal **Training Data**
  - 100,000 packets during normal operation
  - Only used during training
- **Testing Data**
  - 200,000 packets with simulated abnormal behavior
    - Nmap, Nessus (Network scanning and auditing)
    - ARP pings, SYN stealth scans, port scanning, open port identification, …
- Linguistic Domain Knowledge:

CYBER-SECURITY LINGUISTIC DOMAIN KNOWLEDGE

R_1:	If **Time of Window** is *Low* then **Sensitivity Threshold** is *Low*
R_2:	If **Time of Window** is *Medium* then **Sensitivity Threshold** is *Low*
R_3:	If **Time of Window** is *High* then **Sensitivity Threshold** is *High*
R_4:	If **Number of Protocols** is *Low* then **Sensitivity Threshold** is *High*
R_5:	If **Number of Protocols** is *Medium* then **Sensitivity Threshold** is *High*
R_6:	If **Number of Protocols** is *High* then **Sensitivity Threshold** is *Low*

Experimental Results

- Applied to 3 communication streams
  - Sensitivity threshold is automatically adjusted
  - Accurate domain knowledge lowers sensitivity when suspicious activity is observed



Experimental Results

- Provides improved tradeoff between false negatives and false positives
  - False negative on stream 2 is low
  - False positives on stream 1, 2, 3 are kept low as well

CLASSIFICATION PERFORMANCE FOR STREAM 1

Threshold	Correct Rate	False Pos.	False Neg.
0.3	99.8539%	0.1461%	0.0000%
0.6	99.8705%	0.1295%	0.0000%
0.9	99.8788%	0.1212%	0.0000%
IT2 FLS	99.8722%	0.1278%	0.0000%

CLASSIFICATION PERFORMANCE FOR STREAM 2

Threshold	Correct Rate	False Pos.	False Neg.
0.3	99.9037%	0.1217%	0.0275%
0.6	99.5504%	0.1082%	1.3753%
0.9	99.3799%	0.1082%	2.0079%
IT2 FLS	99.9111%	0.1116%	0.0275%

CLASSIFICATION PERFORMANCE FOR STREAM 3

Threshold	Correct Rate	False Pos.	False Neg.
0.3	99.8643%	0.2953%	0.0000%
0.6	99.8960%	0.2265%	0.0000%
0.9	99.8960%	0.2265%	0.0000%
IT2 FLS	99.8960%	0.2265%	0.0000%

Conclusion

- Presented novel complex anomaly detection architecture for critical control systems
  - Utilized previously designed anomaly detection system
  - Applied anomaly detection algorithms to individual communication streams
  - Used IT2 Fuzzy Logic Systems to model linguistic domain knowledge

- Tested on smart-grid experimental test bed
  - Demonstrated learning of normal behavior on individual streams
  - Available domain knowledge can lead to performance improvements
    - Balancing the false negative / positive tradeoff