CAMNEP: Multistage Collective Network Behavior Analysis System with Hardware Accelerated NetFlow Probes

Martin Rehak, Pavel Celeda, Michal Pechoucek, Jiri Novotny

CESNET, z. s. p. o.

Gerstner Laboratory - Agent Technology Center

Department of Cybernetics, Czech Technical University

Institute of Computer Science, Masaryk University

Supported by Czech Ministry of Education grants 6383917201 (CESNET), 1M0567, 6840770038 (CTU) and CERDEC/ITC-A projects N62558-07-C-0001, W911NF-08-1-0250

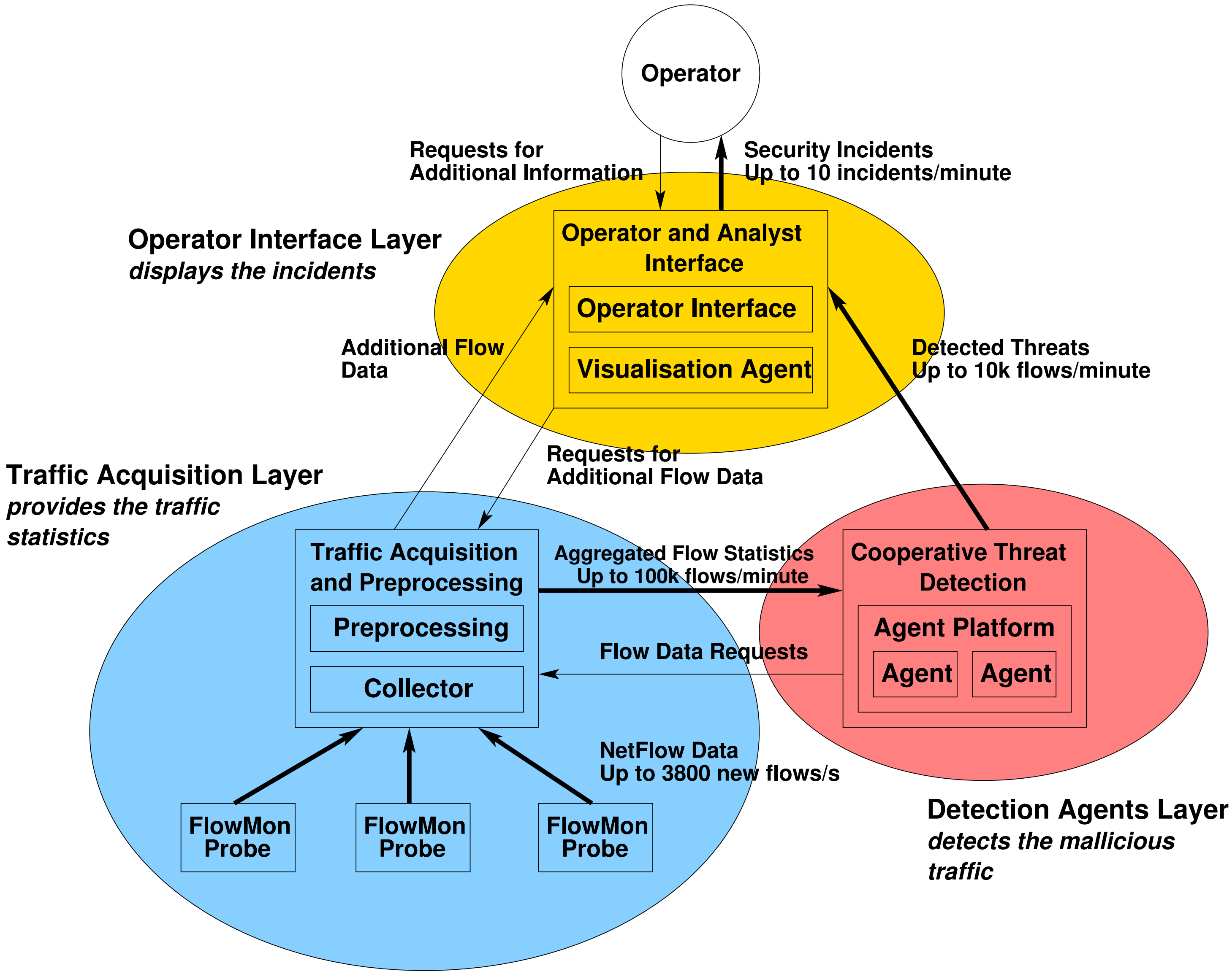
Overview

- Network Intrusion Detection Systems
- Anomaly Detection Models
- Trust-Based Anomaly Integration
- Experimental Results

Network Intrusion Detection

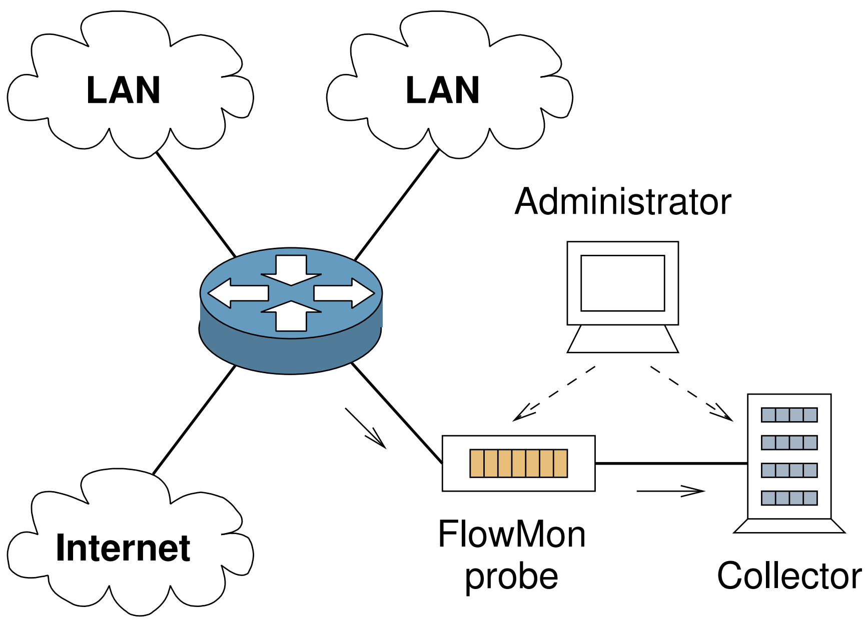
- Identification of attacks against hosts or networks from the network traffic observation
  - **Signature based** - detects patterns in packet content
  - **Stateful protocol analysis** - anomalies in TCP protocol state sequences
  - **Network Behavior Analysis (NBA)** - identifies attacks from traffic statistics
- Current Challenges
  - **False positives** - legitimate traffic labeled as malicious
  - **False negatives** - malicious traffic classified as legitimate
  - **Performance** - high network speed, near-real-time results
- **Our Contribution**: Efficient algorithm for integration of NBA methods
  - Linear with traffic
  - Improves the classification rate by multi-layer combination
  - Based on extended trust modeling

System Architecture



High-Speed Network Traffic Acquisition

- **Probes** observe the traffic at the wire speed
- Each probe generates **NetFlow** traffic statistics
- Results are stored and preprocessed in **collector** servers
- **Hardware acceleration** necessary for high-speed networks

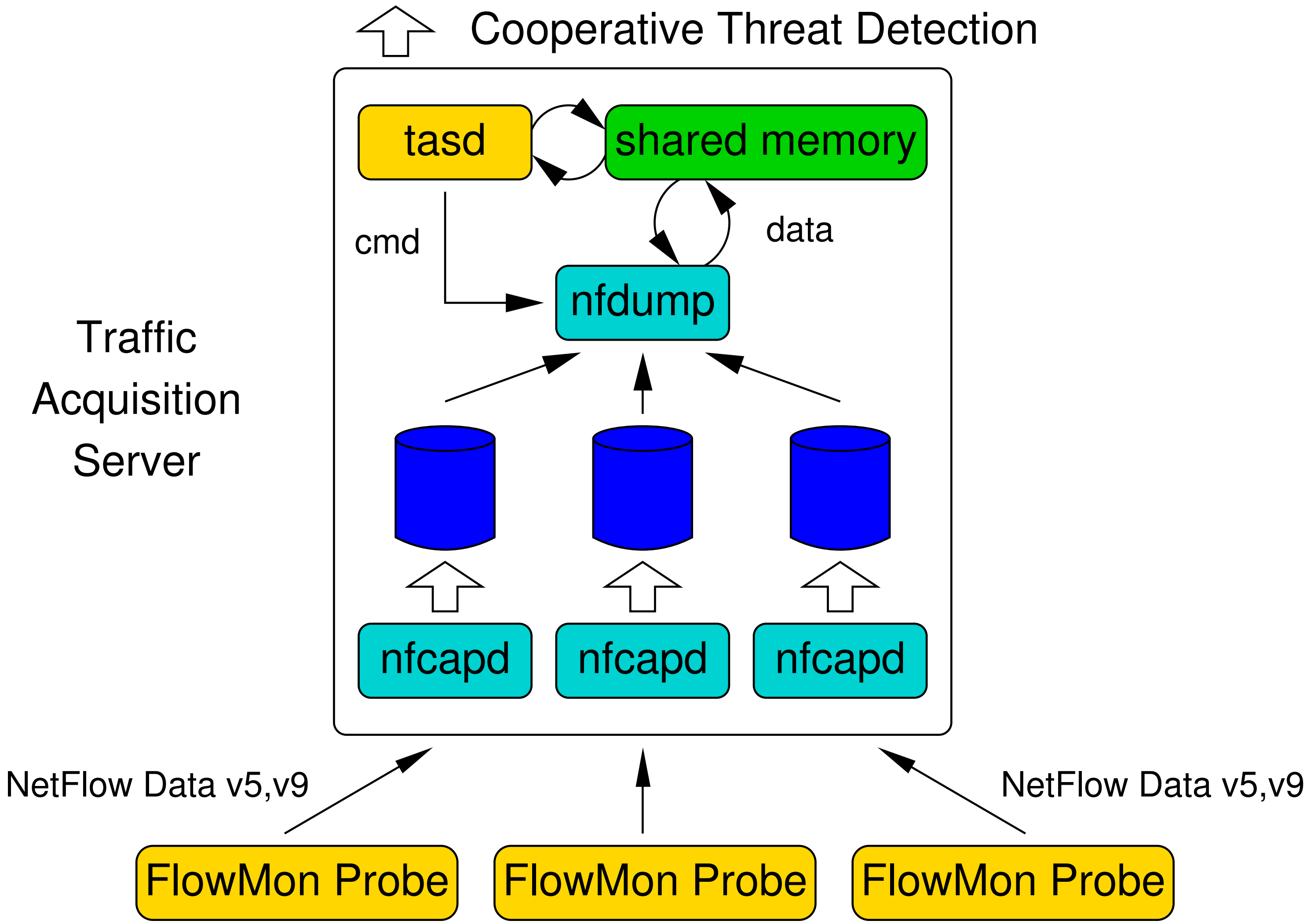


Hardware Accelerated FlowMon Probe

- **Requirements:**
  - traffic characteristics change heavily in time - network probes must **behave reliably** in all possible cases
  - capable of generating **NetFlow traffic statistics**
  - work at **wire speed** (1Gbits/sec - 10Gbits/sec)

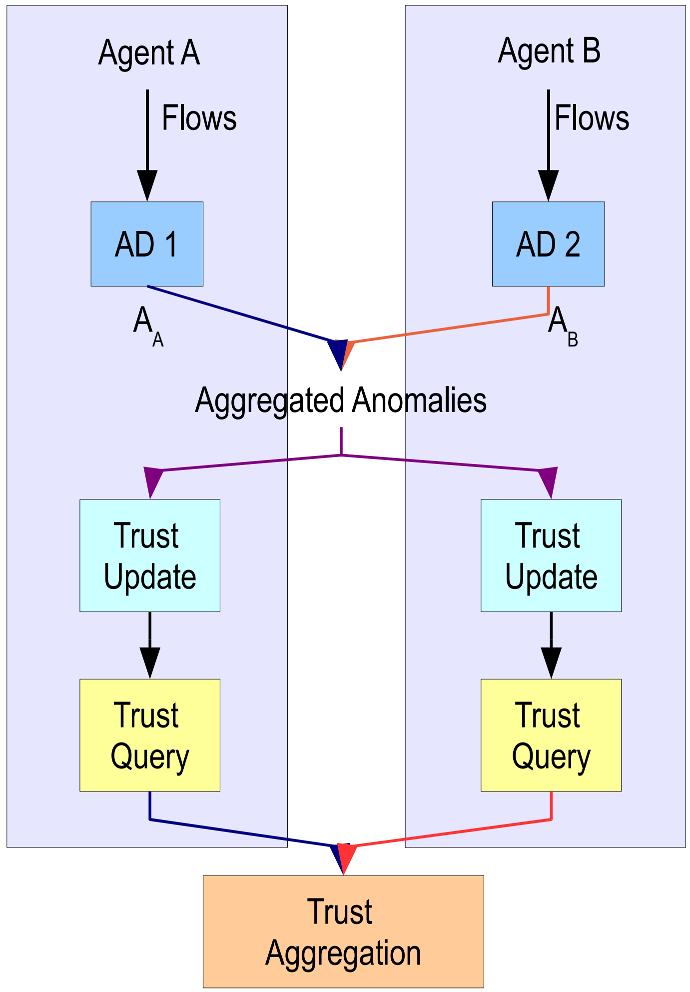
- **FlowMon Probe:**
  - developed in Liberouter project
  - hardware accelerated network card based on COMBO hardware
  - high performance and accuracy
  - handles 1Gbits/sec and 10Gbits/sec traffic at line rate
  - exports acquired NetFlow data to different collectors

Traffic Acquisition Server Architecture



Detection Process Overview

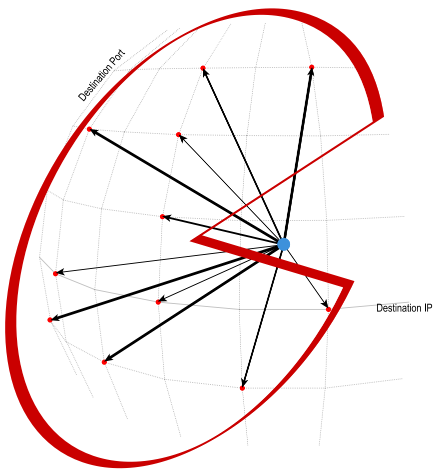
- Each agent based on one **anomaly detection** method
- **Input:** NetFlow statistics, same for all agents
- **Anomaly:** aggregated from individual agent's anomalies
- **Update:** heterogenous trust model are updated, each has a **different structure**
- **Query:** all agents evaluate all flows, and aggregate the output

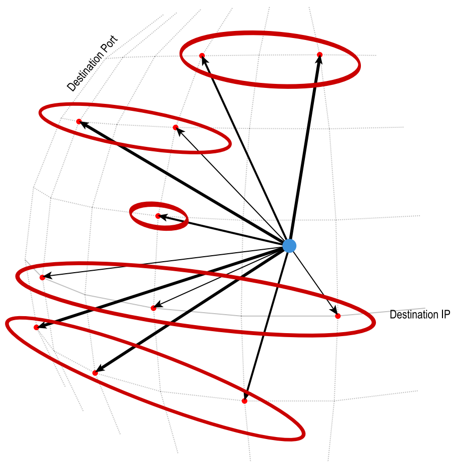


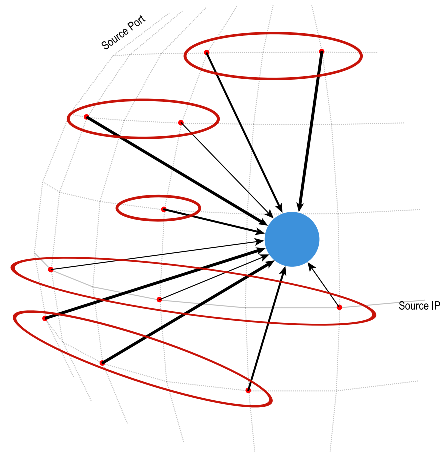
Anomaly Detection Input (simplified)

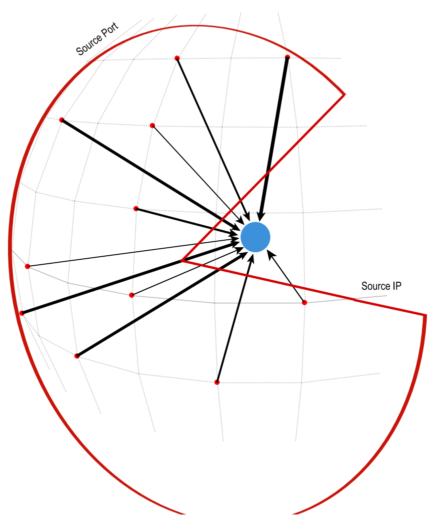
Duration	Proto	Src IP Addr:Port	Dst IP Addr:Port	Flags	Pack.	Bytes
0.000	TCP	192.168.195.164:1086	192.168.10.12:445	.A....	2	84
0.000	TCP	62.97.162.208:3417	192.168.192.83:1172	.AP...	1	42
0.577	TCP	192.168.195.132:2544	194.228.32.3:80	.A.R..	3	126
0.576	TCP	192.168.195.132:2545	194.228.32.3:80	.A.R..	3	126
0.000	UDP	192.168.60.31:4021	192.168.19.247:53	......	1	55
0.000	UDP	192.168.19.247:53	192.168.60.31:4021	......	1	149
0.000	UDP	192.168.60.31:4021	192.168.60.1:53	......	1	55
0.000	UDP	192.168.60.31:4020	192.43.244.18:123	......	1	72
30.276	TCP	192.168.192.170:61158	71.33.170.53:1358	.AP...	307	368627
0.000	UDP	24.28.89.160:63319	192.168.192.83:58359	......	1	42
0.000	TCP	63.208.197.21:443	192.168.192.106:1031	.AP...	1	73
0.093	TCP	192.168.193.58:1302	192.168.192.5:110	.AP.SF	8	356
0.093	TCP	192.168.192.5:110	192.168.193.58:1302	.AP.SF	8	440
0.000	UDP	85.160.81.10:6766	192.168.192.217:11084	......	1	45
0.000	UDP	192.168.192.217:11084	85.160.81.10:6766	......	1	45
0.000	TCP	192.168.19.247:1723	192.168.60.19:1042	.AP...	1	56

Anomaly Detection Methods: MINDS





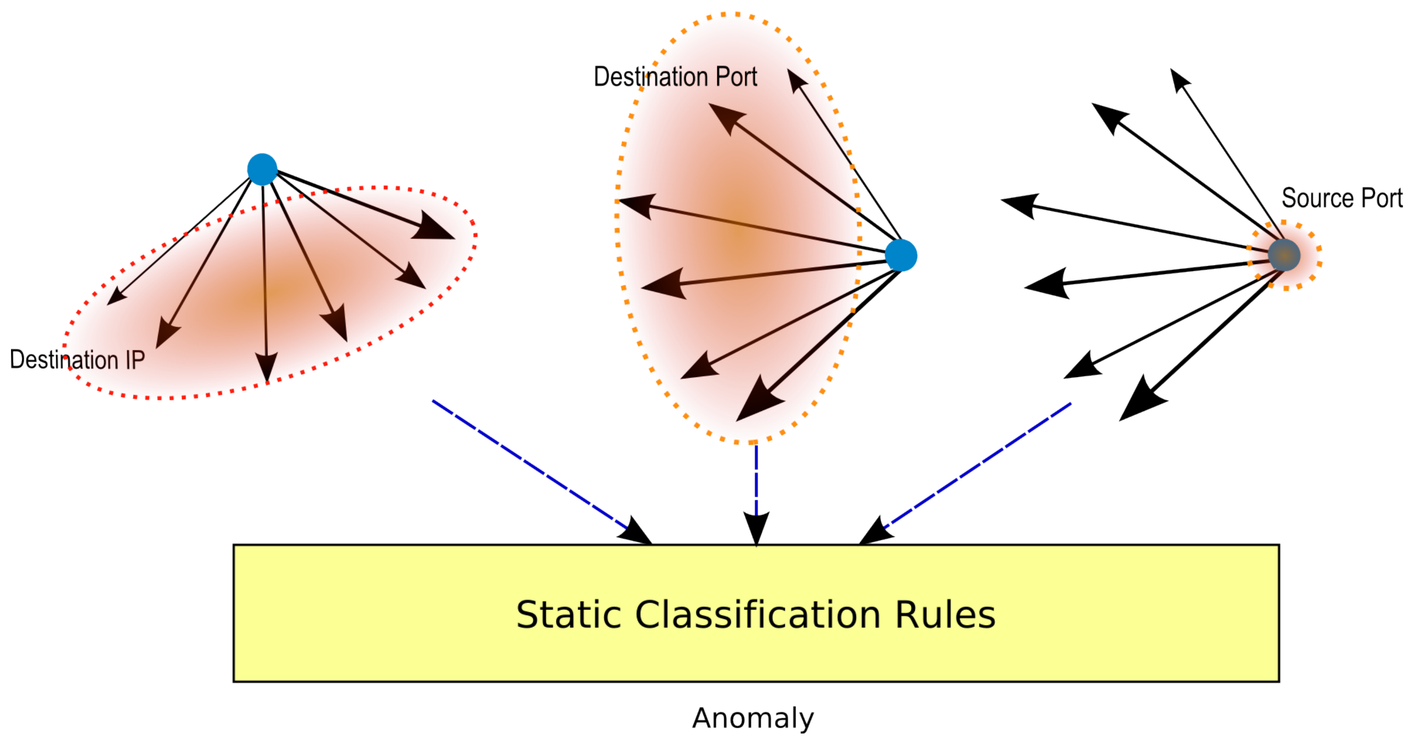




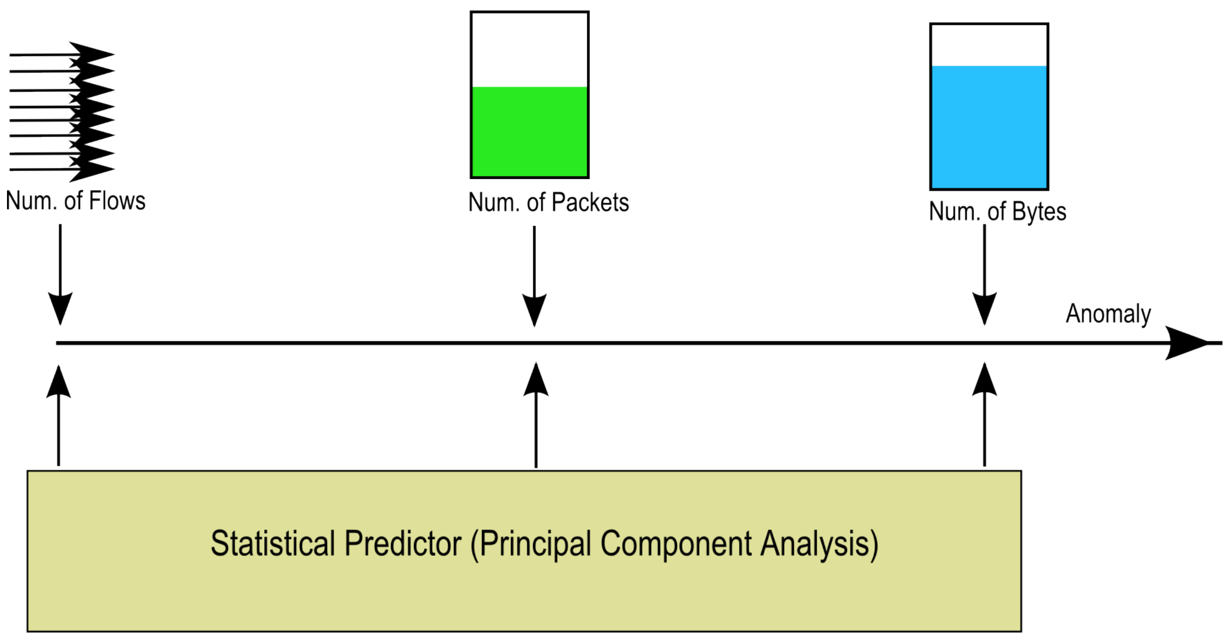
- **Features:** Flow counts from/to important IP/port combinations.
- **Classification:** Comparison with windowed average of past values, different from original MINDS.

Anomaly Detection Methods: Xu et al.

- **Features:** Determines the entropies of dstIP, dstPrt and srcPrt on the set of all flows from each source IP.
- **Classification:**Classifies the traffic with a set of static rules.
- All flows from the same source share the classification features and result.

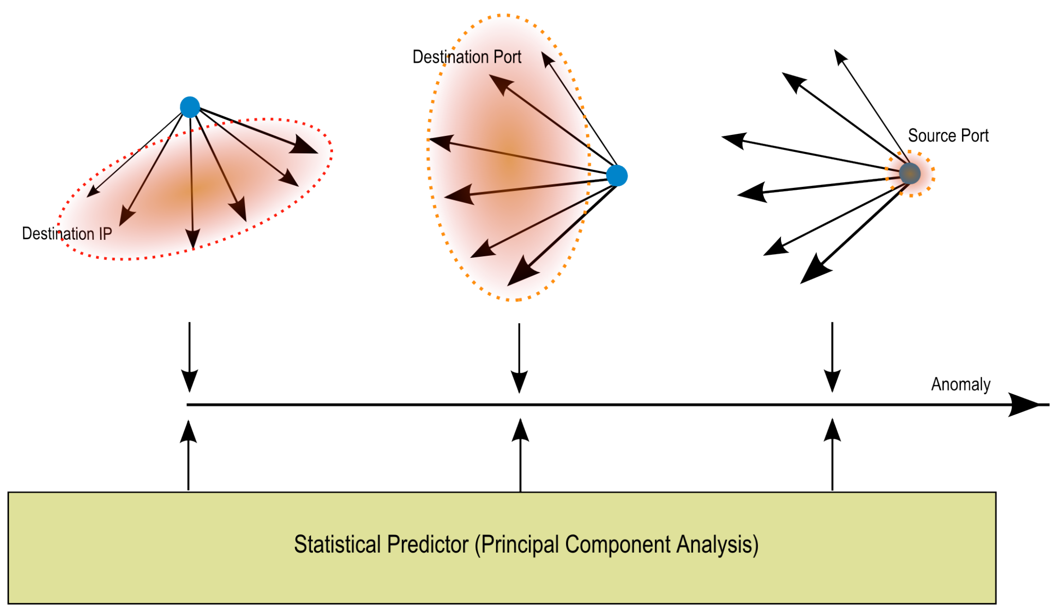


- Uses Principal Component Analysis to predict the volume of traffic from individual sources.
- **Features:** Ratio of predicted/observed numbers of bytes, packets and flows.
- **Classification:** Anomaly is derived from the ratio of prediction and observation, for all flows from the same source.



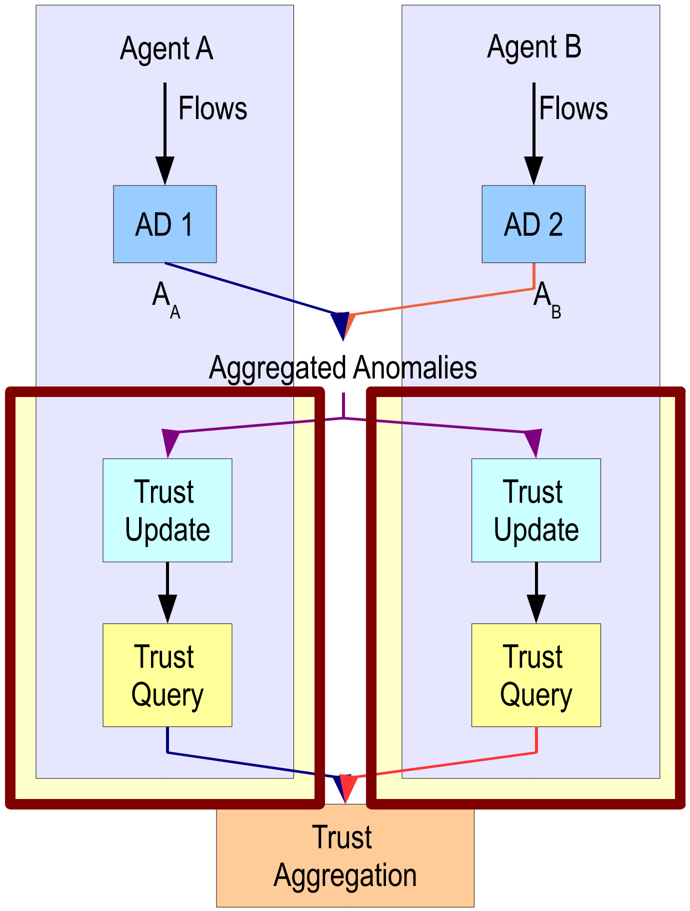
Anomaly Detection Methods: Entropy Prediction, Lakhina et al.

- Uses Principal Component Analysis to predict the entropies of features on the flows from each source IP.
- **Features:** Difference between the predicted and observed entropies of dstIP, dstPrt and srcPrt on the set of all flows from each source IP.
- **Classification:** Anomaly is derived from the difference between the prediction and observation, defined by the source only.



Extended Trust Modeling

- Agents describe each flow using its **identity** and **context**.
- Identity - defined by the features measured on the flow
- Context - uses the features from the AD model, measured on other flows
- Metric **feature space**, metrics determines similarity
- Trustfulness is determined for cluster **centroids** in the feature space



Extended Trust Modeling: Identity/Context Example

Duration	Proto	Src IP Addr:Port	Dst IP Addr:Port	Flags	Pack.	Bytes
0.000	TCP	**192.168.195.164**:1086	192.168.10.12:445	.A....	2	84
0.000	TCP	62.97.162.208:3417	192.168.192.83:1172	.AP...	1	42
0.577	TCP	**192.168.195.164**:2544	194.228.32.3:80	.A.R..	3	126
0.576	TCP	192.168.195.132:2545	194.228.32.3:80	.A.R..	3	126
0.000	UDP	192.168.60.31:4021	192.168.19.247:53	......	1	55
0.000	UDP	**192.168.195.164**:1087	192.168.60.31:445	......	1	149
0.000	UDP	192.168.60.31:4021	192.168.60.1:53	......	1	55
0.000	UDP	192.168.60.31:4020	192.43.244.18:123	......	1	72

Identity

- srcIP: 192.168.195.164
- dstIP: 192.168.10.12
- srcPrt:1086
- dstPrt: 445
- protocol: TCP
- bytes: 84
- packets: 2

Context (MINDS)

- count-srcIP: 3
- count-dstIP: 1
- count-srcIP-dstPrt:2
- count-dstIP-srcPrt:1

Extended Trust Modeling: Identity/Context Example

Duration	Proto	Src IP Addr:Port	Dst IP Addr:Port	Flags	Pack.	Bytes
0.000	TCP	**192.168.195.164**:1086	192.168.10.12:445	.A....	2	84
0.000	TCP	62.97.162.208:3417	192.168.192.83:1172	.AP...	1	42
0.577	TCP	**192.168.195.164**:2544	194.228.32.3:80	.A.R..	3	126
0.576	TCP	192.168.195.132:2545	194.228.32.3:80	.A.R..	3	126
0.000	UDP	192.168.60.31:4021	192.168.19.247:53	......	1	55
0.000	UDP	**192.168.195.164**:1087	192.168.60.31:445	......	1	149
0.000	UDP	192.168.60.31:4021	192.168.60.1:53	......	1	55
0.000	UDP	192.168.60.31:4020	192.43.244.18:123	......	1	72

Identity

- srcIP: 192.168.195.164
- dstIP: 192.168.10.12
- srcPrt:1086
- dstPrt: 445
- protocol: TCP
- bytes: 84
- packets: 2

Context (MINDS)

- count-srcIP: 3
- count-dstIP: 1
- count-srcIP-dstPrt:2
- count-dstIP-srcPrt:1

Extended Trust Modeling: Identity/Context Example

Duration	Proto	Src IP Addr:Port	Dst IP Addr:Port	Flags	Pack.	Bytes
0.000	TCP	**192.168.195.164**:1086	192.168.10.12:445	.A....	2	84
0.000	TCP	62.97.162.208:3417	192.168.192.83:1172	.AP...	1	42
0.577	TCP	**192.168.195.164**:2544	194.228.32.3:80	.A.R..	3	126
0.576	TCP	192.168.195.132:2545	194.228.32.3:80	.A.R..	3	126
0.000	UDP	192.168.60.31:4021	192.168.19.247:53	......	1	55
0.000	UDP	**192.168.195.164**:1087	192.168.60.31:445	......	1	149
0.000	UDP	192.168.60.31:4021	192.168.60.1:53	......	1	55
0.000	UDP	192.168.60.31:4020	192.43.244.18:123	......	1	72

Identity

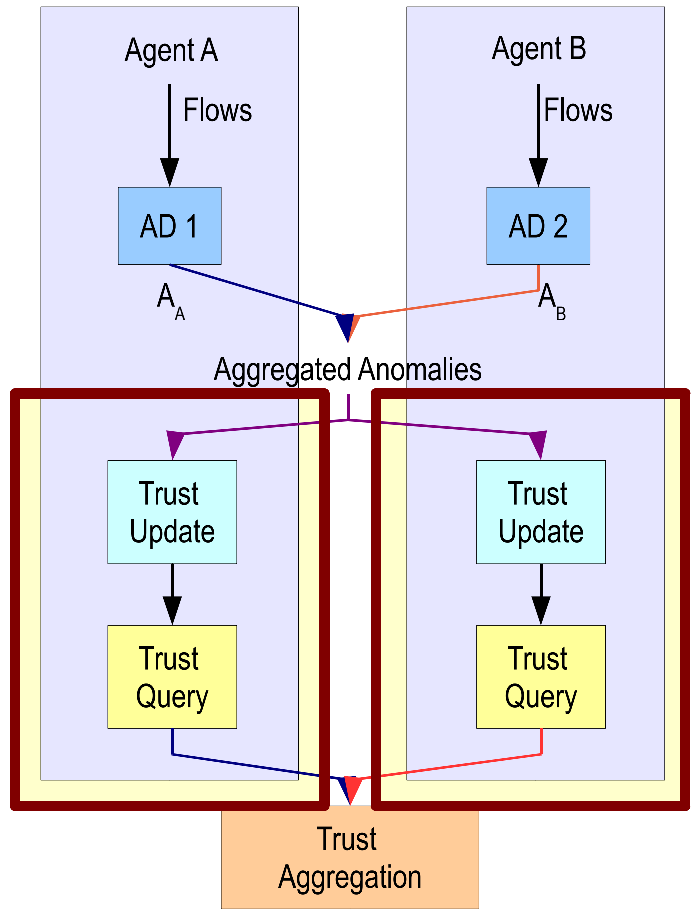
- srcIP: 192.168.195.164
- dstIP: 192.168.10.12
- srcPrt:1086
- dstPrt: 445
- protocol: TCP
- bytes: 84
- packets: 2

Context (MINDS)

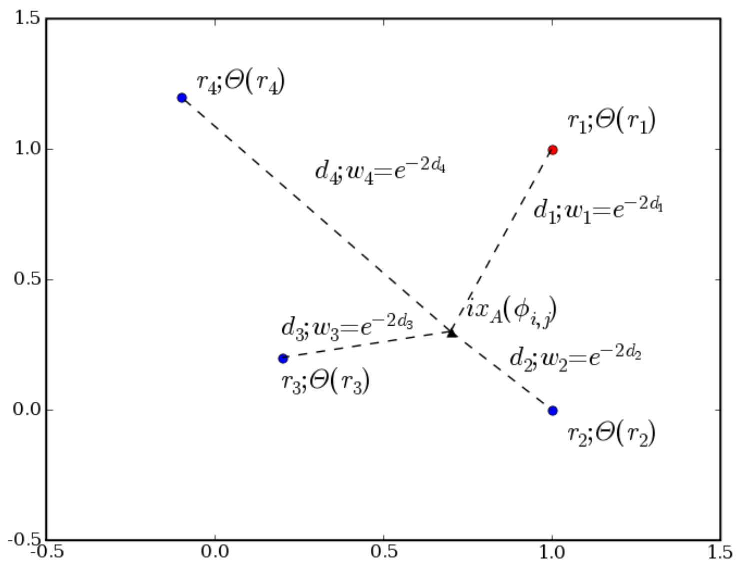
- count-srcIP: 3
- count-dstIP: 1
- count-srcIP-dstPrt:2
- count-dstIP-srcPrt:1

Extended Trust Modeling

- Agents describe each flow using its **identity** and **context**.
- **Identity** - defined by the features measured on the flow
- **Context** - uses the features from the AD model, measured on other flows
- Metric **feature space**, metrics determines similarity
- Trustfulness is determined for cluster **centroids** in the feature space

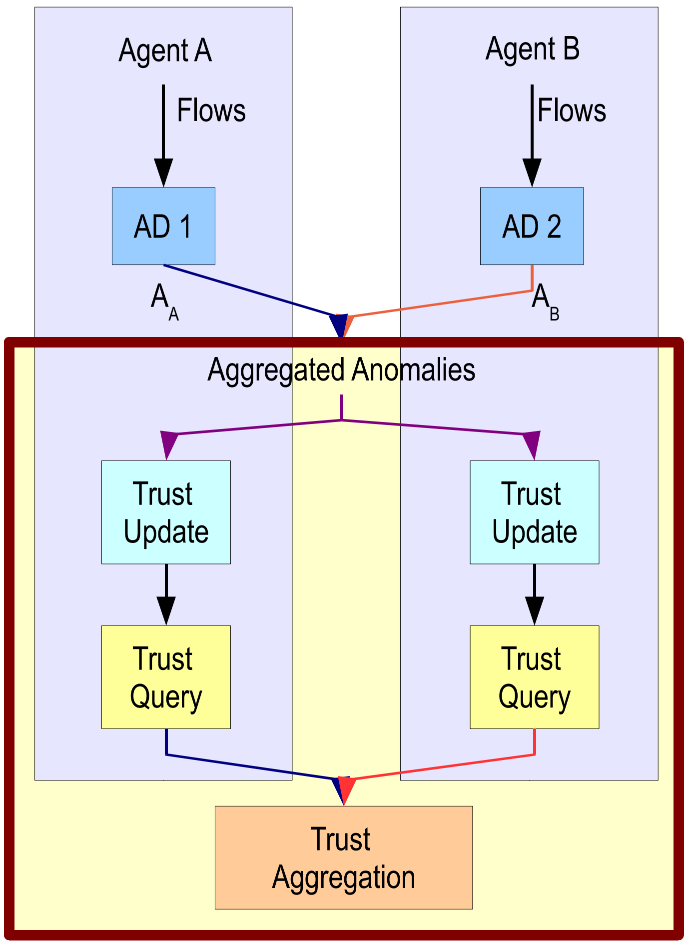


Trust Update and Query



- Trustfulness **update**:
  1. Find **relevant** centroids
  2. Determine the update **weight** for each centroid
  3. **Update** the trustfulness of centroid using a given weight
- Trustfulness **query**:
  1. Find **relevant** centroids
  2. Determine the **weight** for each centroid
  3. **Aggregate** the trustfulness from centroid, with respective weights

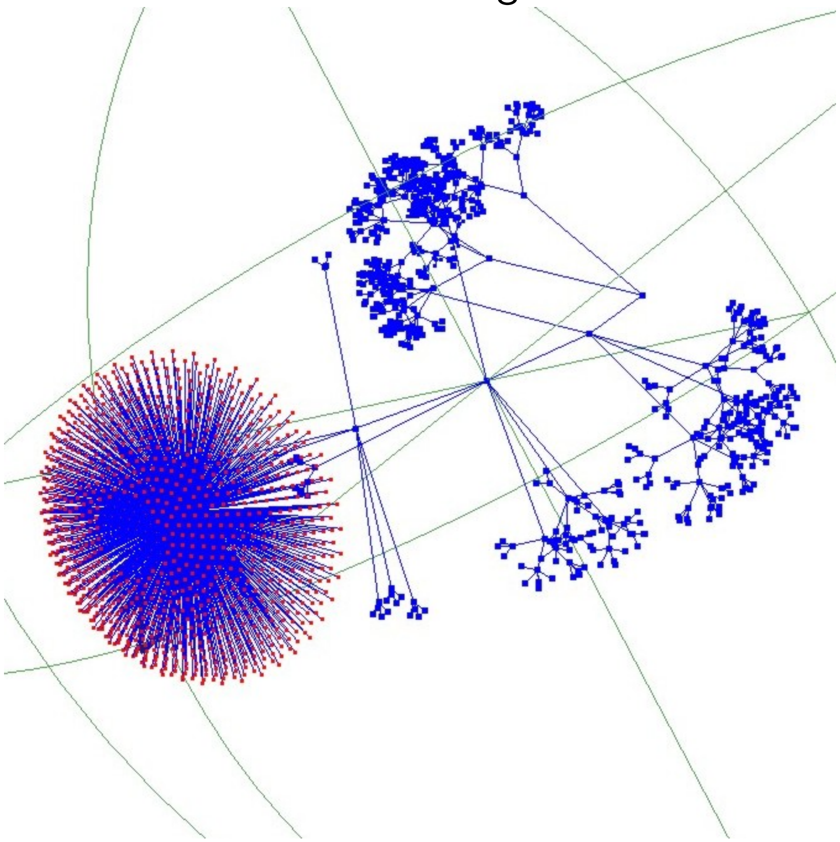
Multi-Source Trustfulness Integration



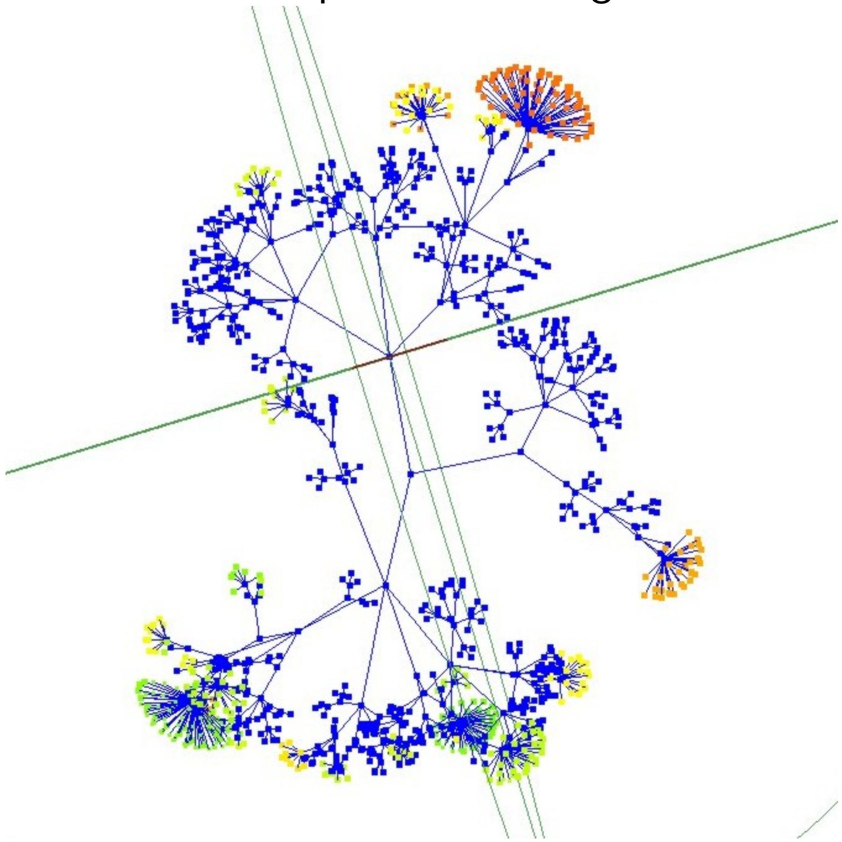
- Effectiveness improved by:
- **Aggregated anomaly value** reduces the effect of singular anomaly peaks
- Similarity between flows varies between the agents e.g. trustfulness is based on anomaly aggregated over the **agent-specific clusters**
- Normalized individual **trustfulness** is **re-aggregated** into the common value

Agent Specific Clusters

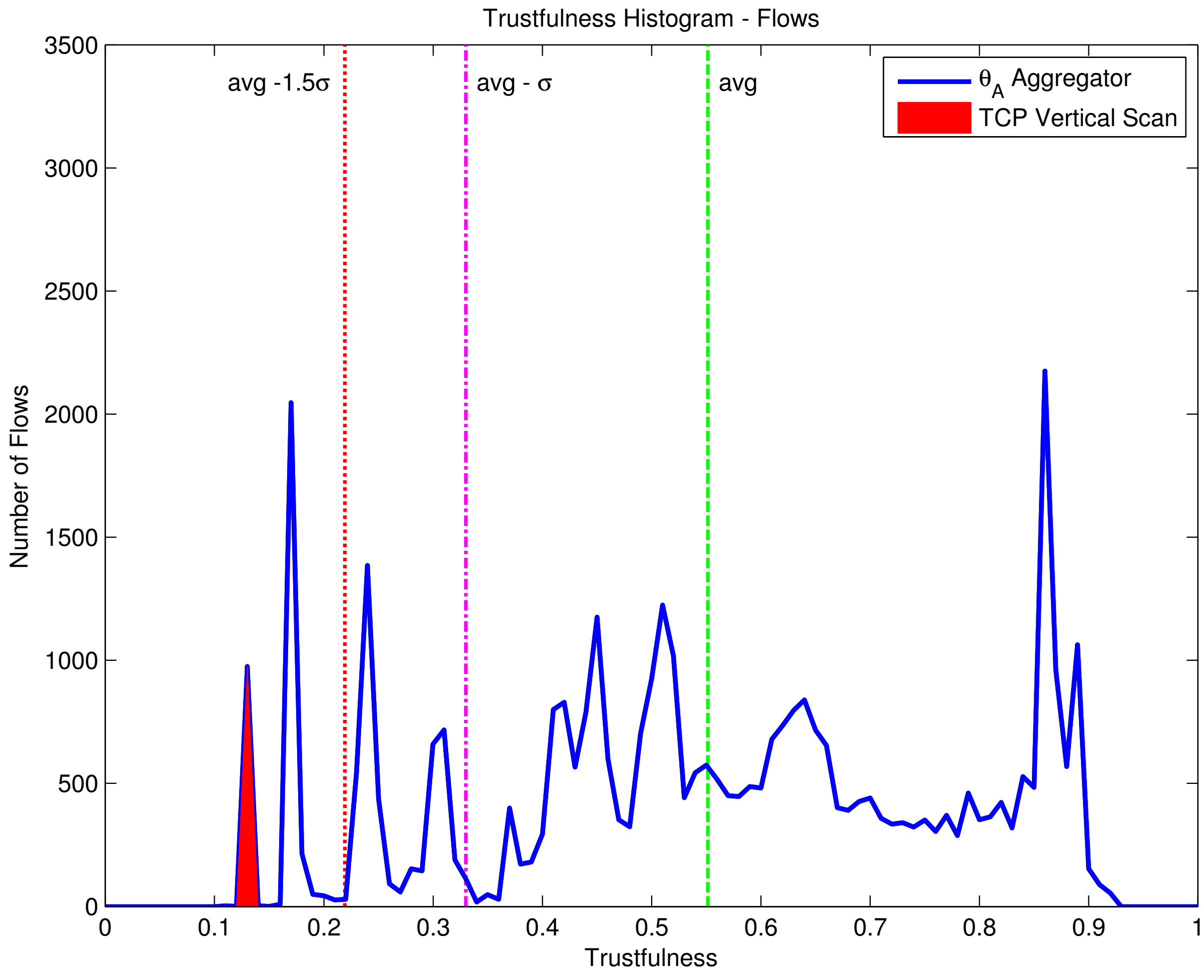
Attack data (as identified by other agent) are concentrated in a single centroid.



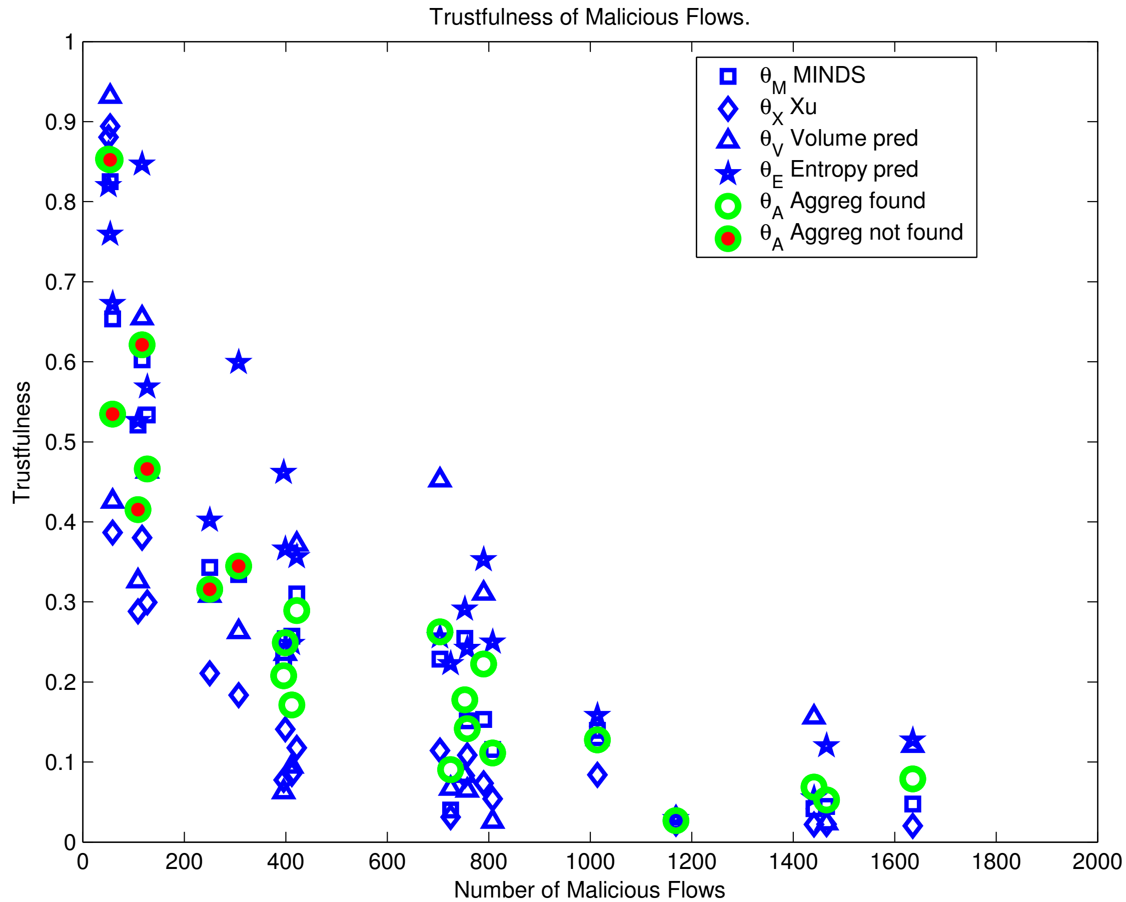
False positive data are spread across the whole feature space of other agent.



System Output



Known Attacks, Regardless of Type

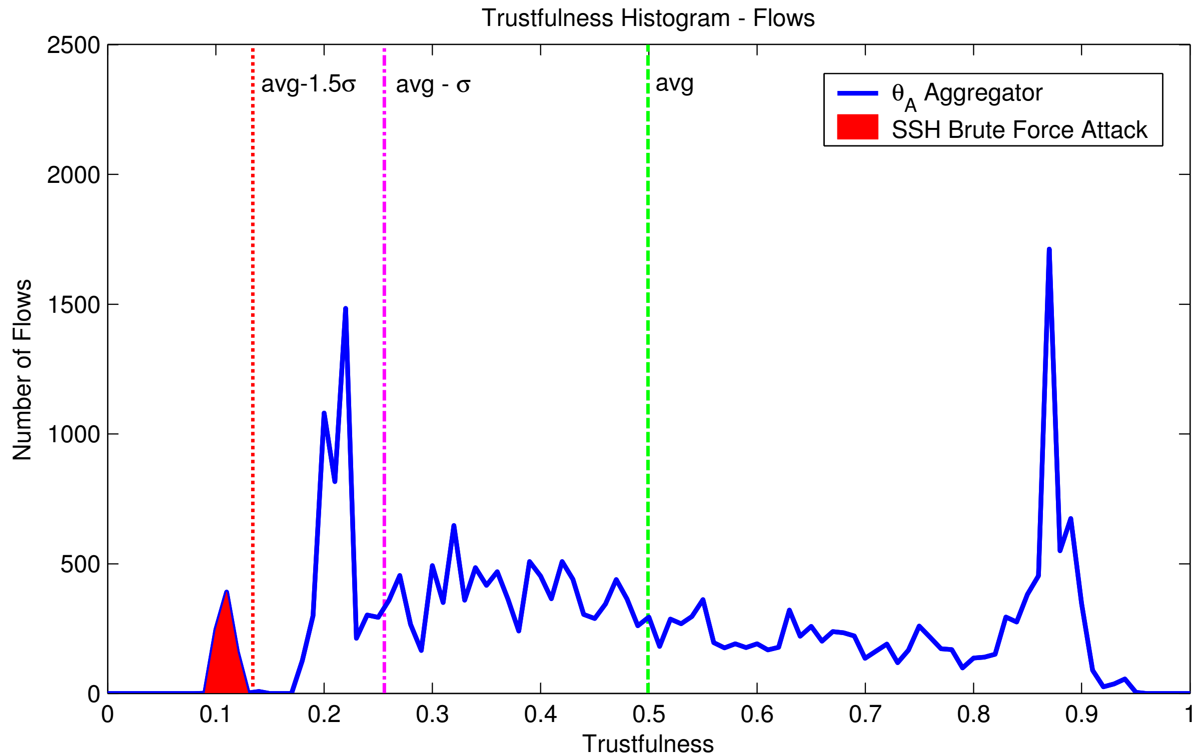


Third Party Attacks Results

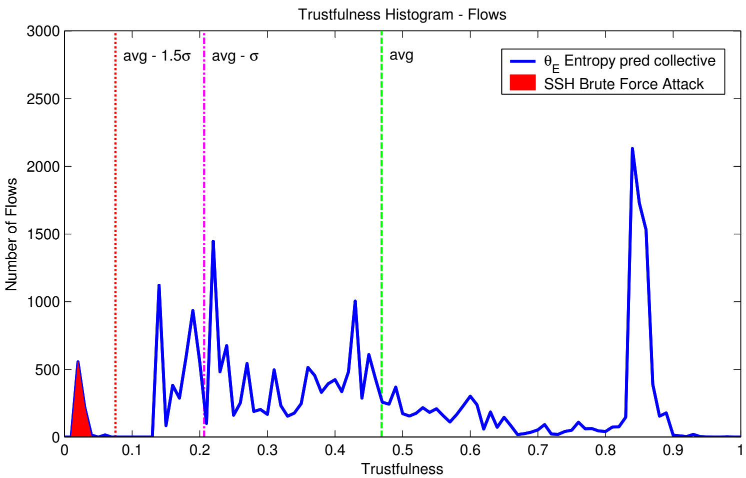
Anomalous		$A_{\mathcal{M}}$	$A_{\mathcal{X}}$	$A_{\mathcal{E}}$	$A_{\mathcal{V}}$	$A_{\mathbb{M}}$
# flows	detected	6653	3246	13541	12375	**9911**
	TP	35	168	5841	5868	**4709**
	FP	6618	3078	7700	6507	**5202**
	FP[%] all traffic	15.9 %	7.4 %	18.5 %	15.6 %	**12.5 %**
# srcIP	detected	72.5	322.3	17.2	16.7	**12.5**
	TP	1.7	0.2	2.5	2.7	**2.3**
	FP	70.8	322.1	14.7	14.0	**10.2**
	FP[%] all traffic	1.52 %	6.94 %	0.31 %	0.30 %	**0.22 %**

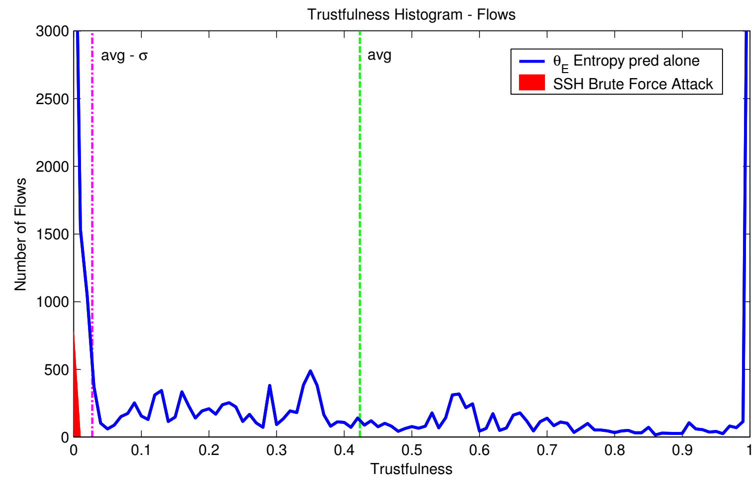
Untrusted		Θ_M	Θ_X	Θ_E	Θ_V	Θ
# flows	detected	9149	9975	10704	9518	**9741**
	TP	5242	5712	5833	5864	**5769**
	FP	3907	4263	4872	3654	**3972**
	FP[%] all traffic	9.4 %	10.2 %	11.7 %	8.8 %	**9.5 %**
# srcIP	detected	7.8	11.3	13.5	10.8	**6.7**
	TP	2.7	2.7	2.3	2.7	**2.7**
	FP	5.1	8.6	11.2	8.1	**4.0**
	FP[%] all traffic	0.11 %	0.19 %	0.24 %	0.18 %	**0.09 %**

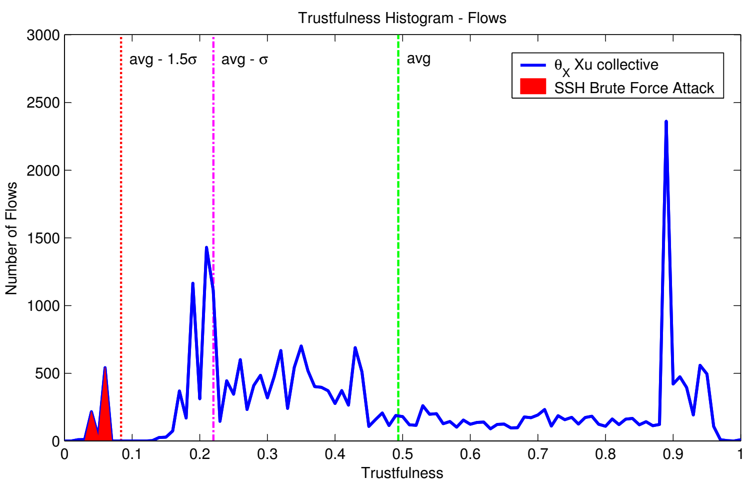
Impact of Collaboration 1

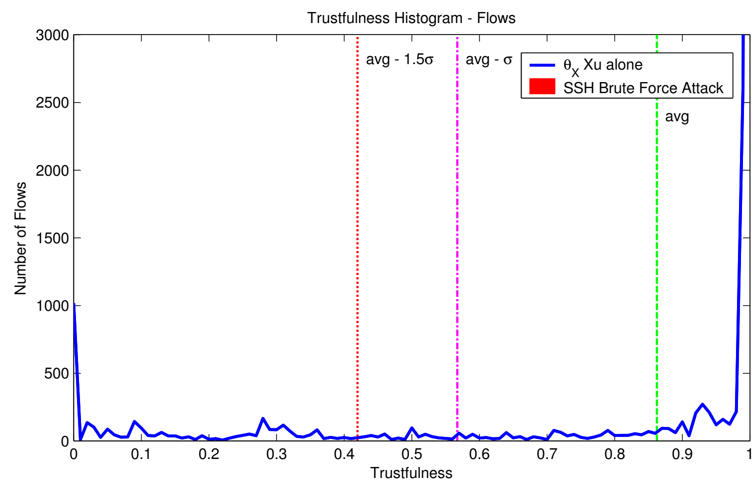


Impact of Collaboration 2

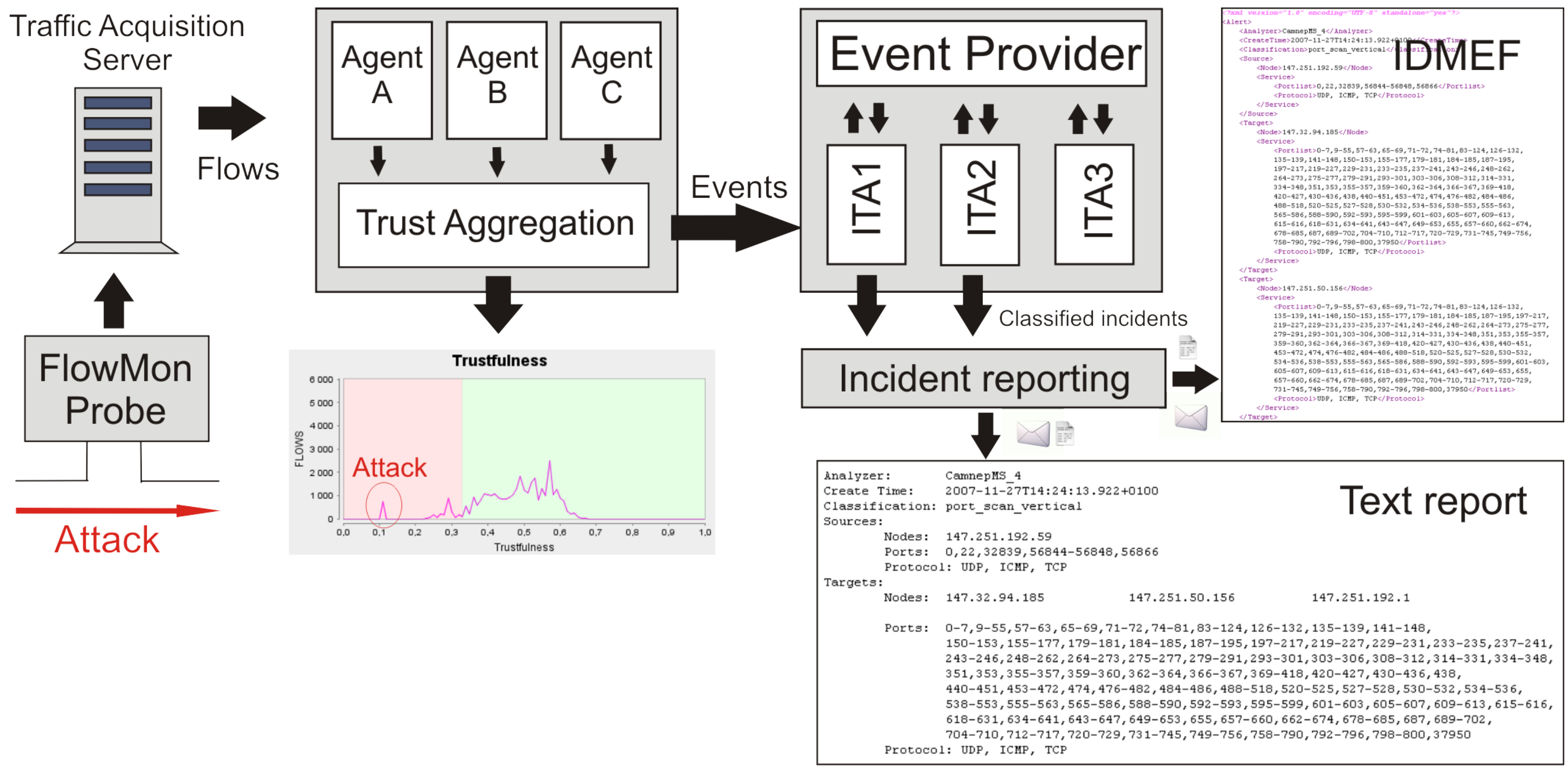








Reporting


Traffic Acquisition Server
Flows
FlowMon Probe
Attack
Agent A
Agent B
Agent C
Trust Aggregation
Trustfulness
FLOWS
Attack
Trustfulness
Events
Event Provider
ITA1
ITA2
ITA3
Classified incidents
Incident reporting
IDMEF
Text report
Analyzer: CamnepMS_4
Create Time: 2007-11-27T14:24:13.922+0100
Classification: port_scan_vertical
Sources:
Nodes: 147.251.192.59
Ports: 0,22,32839,56844-56848,56866
Protocol: UDP, ICMP, TCP
Targets:
Nodes: 147.32.94.185 147.251.50.156 147.251.192.1
Ports: 0-7,9-55,57-63,65-69,71-72,74-81,83-124,126-132,135-139,141-148,
150-153,155-177,179-181,184-185,187-195,197-217,219-227,229-231,233-235,237-241,
243-246,248-262,264-273,275-277,279-291,293-301,303-306,308-312,314-331,334-348,
351,353,355-357,359-360,362-364,366-367,369-418,420-427,430-436,438,
440-451,453-472,474,476-482,484-486,488-518,520-525,527-528,530-532,534-536,
538-553,555-563,565-586,588-590,592-593,595-599,601-603,605-607,609-613,615-616,
618-631,634-641,643-647,649-653,655,657-660,662-674,678-685,687,689-702,
704-710,712-717,720-729,731-745,749-756,758-790,792-796,798-800,37950
Protocol: UDP, ICMP, TCP

Conclusions

- Collaborative trust mechanism **reduces the error rate** of existing anomaly detection approaches.
- The error rate reduction is achieved by:
  - **Aggregation** of **anomaly** values
  - **Specific trust models** of individual agents, each providing different insight into the flow data
  - Trustfulness aggregation **re-integrates** the opinions from the various trust models, each using **different perspective**
- Agent-based trust techniques can be used under **high-performance** constraints.
- A-Globe multi-agent platform has negligible computational overhead, architecture naturally **scales** to multiprocessor environments.

Thank You For Your Attention