Prioritizing Intrusion Analysis Using Dempster-Shafer Theory

Loai Zomlot*, Sathya Chandran*, Xinming Ou*,

S. Raj Rajagopalan+

*Kansas State University, +HP Labs

PROBLEM

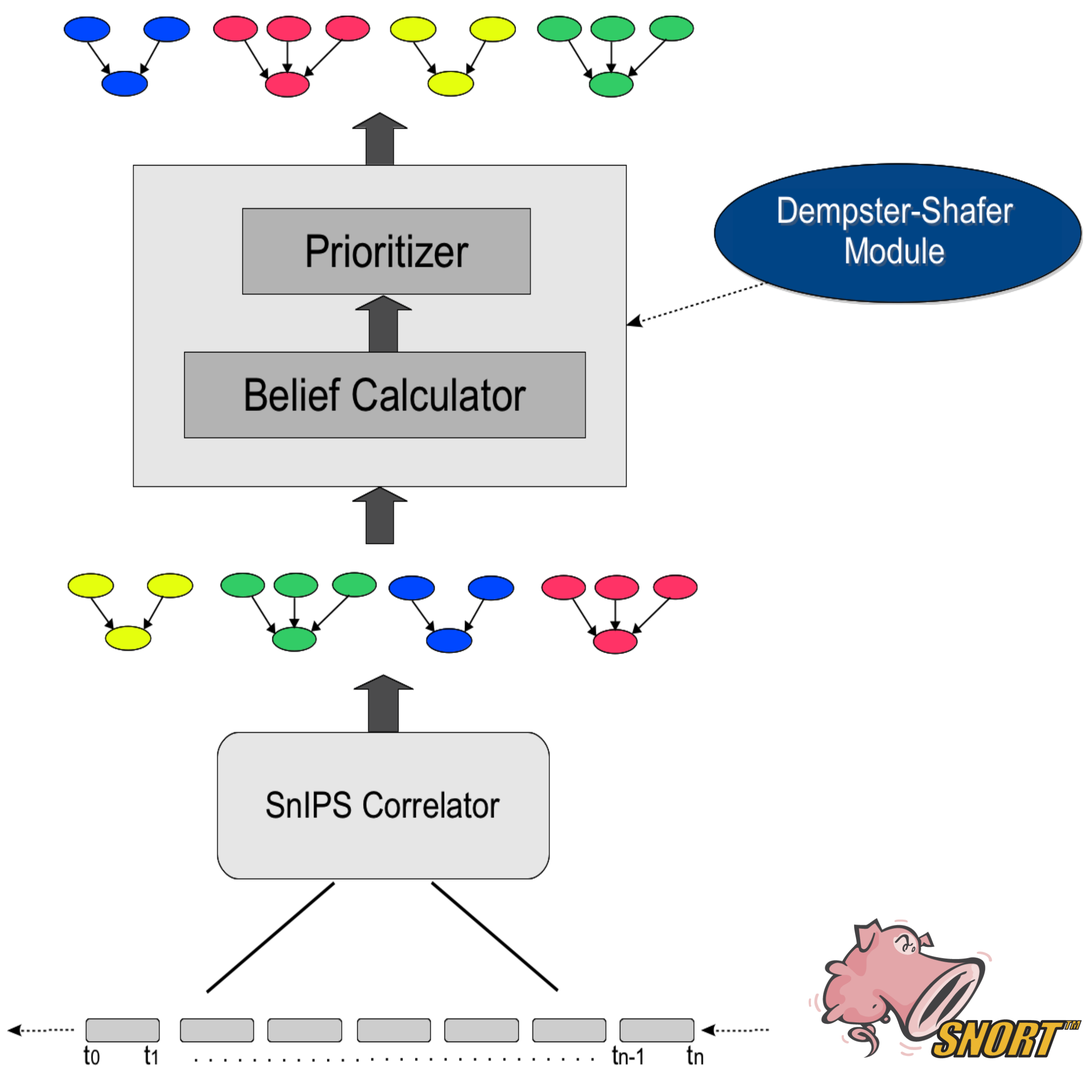
High False positive rate in IDS alerts

SOLUTION

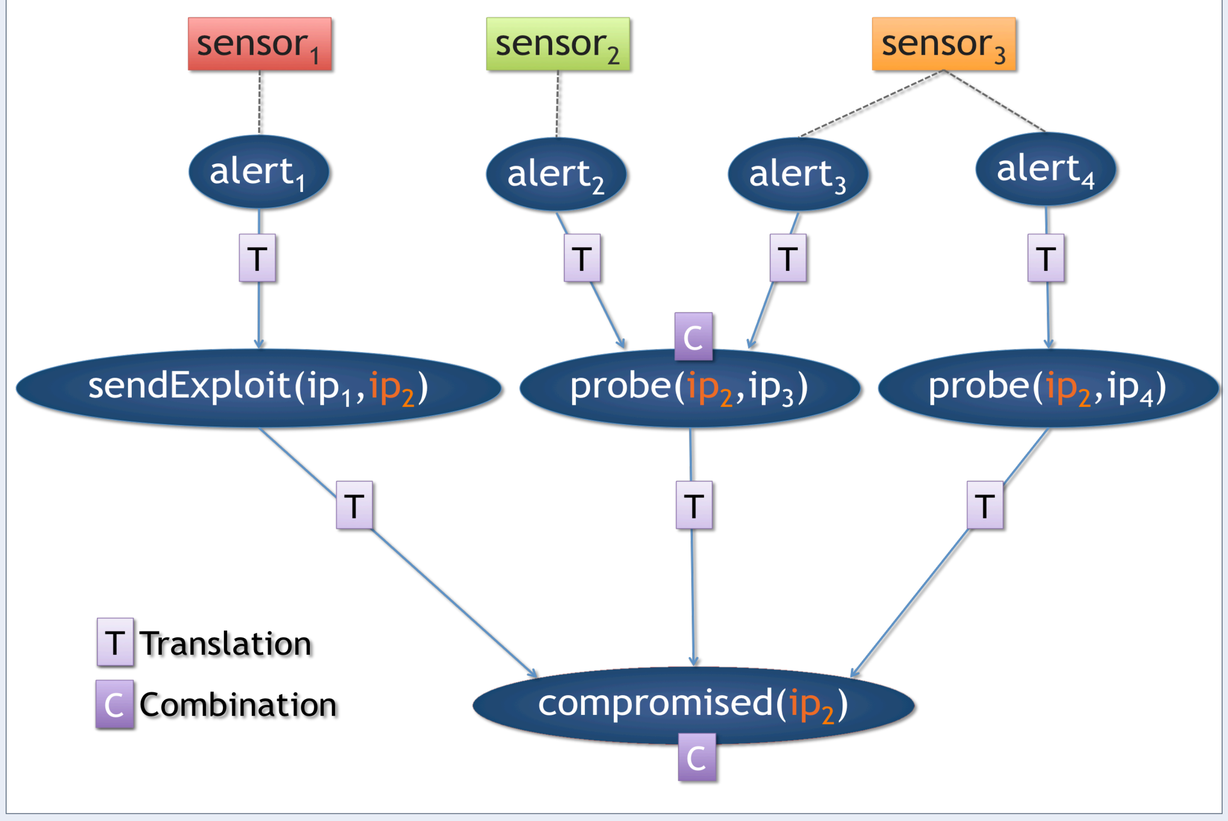
Using DS to prioritize IDS alerts

- Using unknown to capture uncertainty
- Accounting for lack of independence among alerts
- Efficient algorithm

SYSTEM ARCHITECTURE



BELIEF CALCULATION OVERVIEW



BELIEF CALCULATION METHODS

DS Translation Process

$alert_2$		maps to	$probe(ip_2,ip_3)$	
element	bpa		element	bpa
{trustworthy}	0.33	→	{true}	0.33
{non-trustworthy}	0.67	→	{true, false}	0.67

DS Combination Process

Standard

$$m_{1,2}(h) = \frac{1}{1-K} \cdot \sum_{h_1 \cap h_2 = h} m_1(h_1) \cdot m_2(h_2) \qquad K = \sum_{h_1 \cap h_2 = \{\}} m_1(h_1) \cdot m_2(h_2)$$

Customized

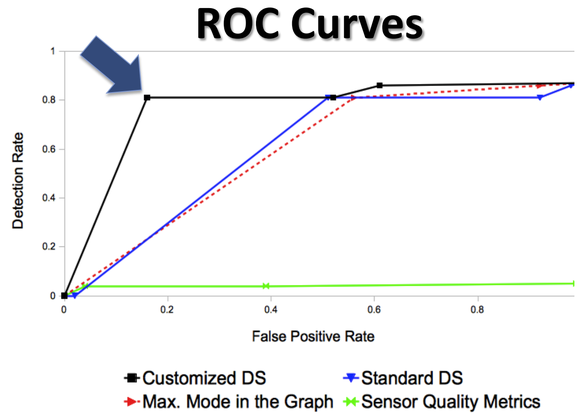
$$m_{1,2}(h) = \sum_{h_1 \cap h_2 = h} \psi[h_1, h_2]$$

$$\psi[t,t] = r_1 \cdot m_1(t) + (1-r_1) \cdot m_1(t) \cdot m_2(t)$$
$$\psi[t,\theta] = (1-r_1) \cdot m_1(t) \cdot m_2(\theta)$$
$$\psi[\theta,t] = (1-r_2) \cdot m_1(\theta) \cdot m_2(t)$$
$$\psi[\theta,\theta] = r_1 \cdot m_2(\theta) + (1-r_1) \cdot m_1(\theta) \cdot m_2(\theta)$$

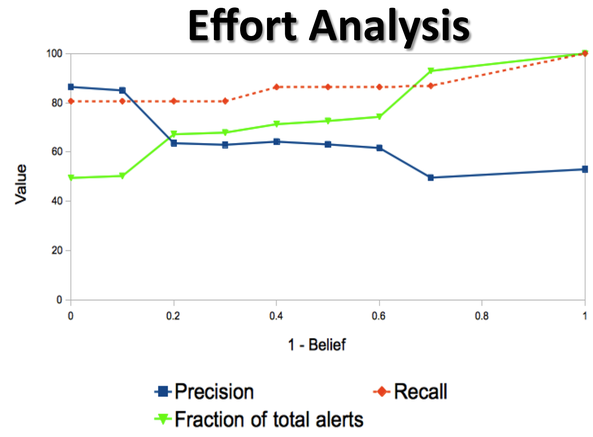
r_i : estimated overlapping factor

EVALUATION

ROC Curves

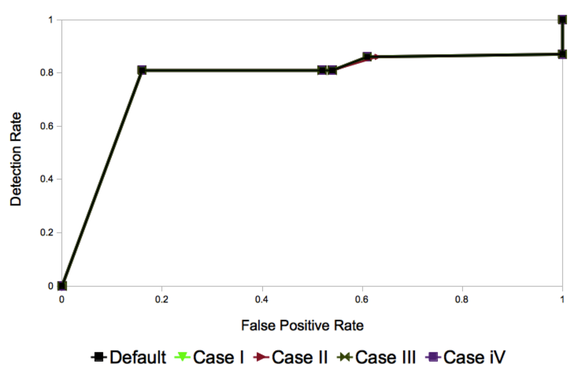


Effort Analysis



Figures are for MIT LL99 training dataset

Sensitivity Analysis



Tags	Metrics	
unlikely	0.01	10% ↓
possible	0.33	10% ↓
likely	0.66	10% ↓
probable	0.99	10%

REFERENCES

- Loai Zomlot, Sathya Chandran, Kui Luo, Xinming Ou, and S. Raj Rajagopalan. Prioritizing intrusion analysis using Dempster-Shafer theory. In the 4th ACM Workshop on Artificial Intelligence and Security (AISec), 2011.
- Sathya Chandran, Loai Zomlot, and Xinming Ou. Practical IDS alert correlation in the face of dynamic threats. In the 10th International Conference on Security and Management (SAM), 2011.
- Xinming Ou, S. Raj Rajagopalan, and Sakthiyuvaraja Sakthivelmurugan. An empirical approach to modeling uncertainty in intrusion analysis. In the 25th Annual Computer Security Applications Conference (ACSAC), 2009.

ACKNOWLEDGMENT

This research was funded by the U.S. National Science Foundation (0954138, 1018703), AFOSR (FA9550-09-1-0138) and HP Labs Innovation Research Program.