Dynamic Risk Evaluation Using Hidden Markov Models

Kjetil Haslum
Centre for Quantifiable Quality of Service in Communication Systems
Norwegian University of Science and Technology
Trondheim, Norway
haslum@q2s.ntnu.no

2005-09-21

Content

- Introduction
- Monitoring and Assessment Architecture
- Risk Assessment Model
- Hidden Markov Models
- Quantitative Risk Assessment
- Example
- Future Work

Introduction

- This presentation will focus on our paper “Real-time Risk Assessment with Network Sensors and Intrusion Detection System”, accepted at the 2005 International Conference on Computational Intelligence and Security December 15-19, 2005 in Xi’an, China.
- This paper consider a real-time risk assessment method for information systems and networks based on observations from network sensors such as intrusion detection systems.
- The system risk is dynamically evaluated and provides a mechanism for handling data from sensors with different trustworthiness.
- The chosen architecture is based on sensors that collect observations and agents that preform the risk assessment.

Monitoring and Assessment Architecture

- Assets that are subject to monitoring are called objects, and may for instance be computers, routers and other networks resources.

- A sensor can be any information-gathering program or device, including network sniffers (using sampling or filtering), different types of intrusion detection systems (IDS), logging systems, virus detectors, honeypots, etc. The main task of the sensors is to gather information on the security state of objects.

- An agent is responsible for collecting and aggregating sensor data from a set of sensors that monitors a set of objects. The main task of the agent is to perform real-time risk assessment based on these data.

Risk Assessment Model

- The security states of each object is described by a Discrete Time Markov Chain (DTMC). This is a stochastic process $\{x_n, n = 1, 2, \ldots\}$ where the state transition probabilities only depend on the current state.
- States $S = \{s_1, s_2, \ldots, s_N\}$
- The state sequence $X = x_1 x_2 \cdots x_T, \quad x_t \in S$
- The state transition probability matrix $\mathbf{P} = \{p_{ij}\}$, where $p_{ij} = P(x_t = s_j | x_{t-1} = s_i)$
- The initial state distribution vector $\pi = \{\pi_i\}$, where $\pi_i = P(x_1 = s_i)$
- How can we relate observations from sensors to states?

Hidden Markov Models (HMM)

A HMM is defined by the triple $\lambda = \{\mathbf{P}, \mathbf{Q}, \pi\}$. A HMM is used to relate the observation process to a Markov model. The relation between the observation sequence and the state sequence is described by the $\mathbf{Q}$ matrix.

- Observations messages
  $V = \{v_1, v_2, \ldots, v_M\}$
- Observation sequences
  $Y = y_1 y_2 \cdots y_T, \quad y_t \in V$
- Observation probability distribution matrix
  $\mathbf{Q} = \{q_j(l)\}$ where $q_j(l) = P(y_t = v_l | x_t = s_j)$
- The state probability distribution at time t denoted $\gamma_t(i) = P(x_t = s_i)$, can be calculated with an $O(N^2)$ algorithm.

Quantitative Risk Assessment

- For each object, define a mapping $C : S \rightarrow R$ for expected cost due to loss of confidentiality, integrity and availability.

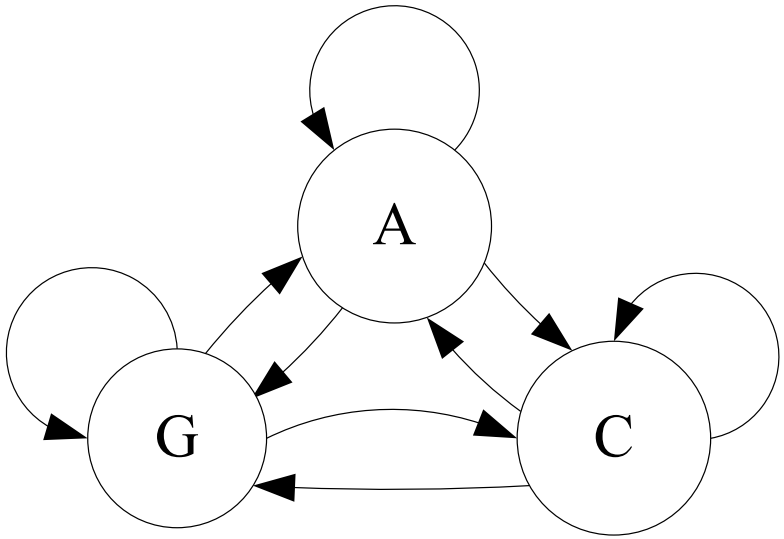
- Total risk at time t can then be calculated as

$$R_t = \sum_{i=1}^{N} \gamma_t(i) C(i)$$

Example Laptop Risk Assessment

- To illustrate the theory, we preform a real-time risk assessment for a laptop. There are two sensors: an Host Intrusion Detection System (HIDS), that processes log files and checks system integrity; and a Network Intrusion Detection System (NIDS), that is capable of monitoring traffic between the outside network and the internal host.

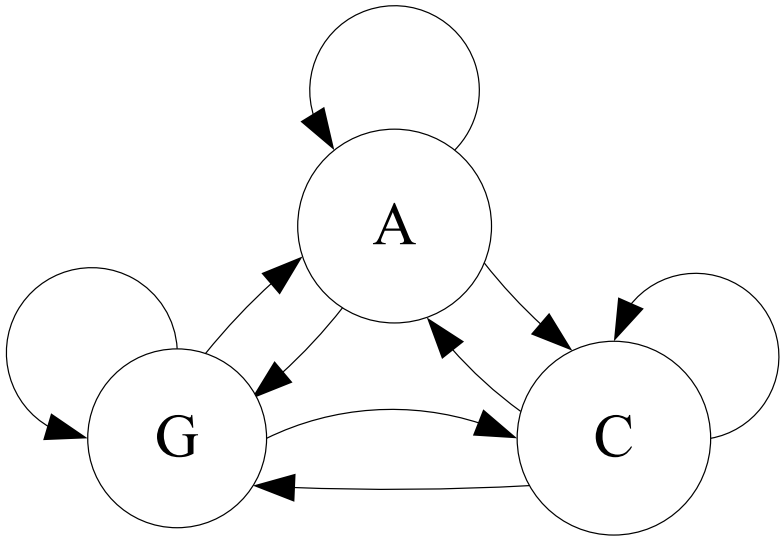
- The laptop can be in one of the following states Good, Attacked or Compromiced $S = \{G, A, C\}$ and possible observations are $V = \{g, a, c\}$.



Example Laptop Risk Assessment

- The initial state distribution $\pi = (\pi_G, \pi_A, \pi_C) = (0.8, 0.1, 0.1)$
- Expected cost $C = (C(G), C(A), C(C)) = (0, 10, 5)$
- The state transition probabilities matrix

$$P = \begin{pmatrix} p_{GG} & p_{GA} & p_{GC} \\ p_{AG} & p_{AA} & p_{AC} \\ p_{CG} & p_{CA} & p_{CC} \end{pmatrix} = \begin{pmatrix} 0.995 & 0.004 & 0.001 \\ 0.060 & 0.900 & 0.040 \\ 0.008 & 0.002 & 0.990 \end{pmatrix}$$



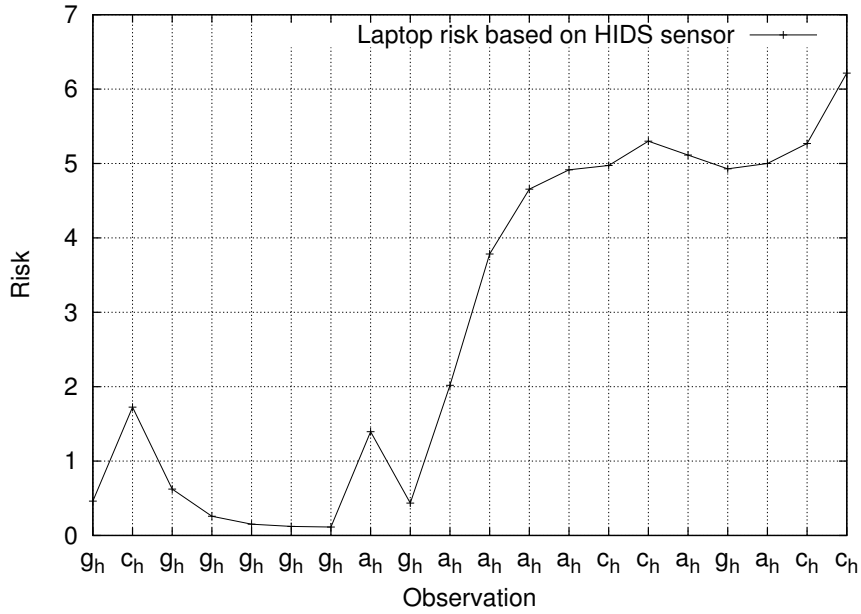
Laptop Risk Assessment by HIDS Observations

- The observation sequence from the HIDS is

$$Y_{HIDS-L} = g_h c_h g_h g_h g_h g_h g_h a_h g_h a_h a_h a_h a_h c_h c_h a_h g_h a_h c_h c_h$$

- The observation symbol probability for the Host IDS

$$Q_{HIDS-L} = \begin{pmatrix} q_G(g) & q_G(a) & q_G(c) \\ q_A(g) & q_A(a) & q_A(c) \\ q_C(g) & q_C(a) & q_C(c) \end{pmatrix} = \begin{pmatrix} 0.70 & 0.15 & 0.15 \\ 0.15 & 0.70 & 0.15 \\ 0.20 & 0.20 & 0.60 \end{pmatrix}$$



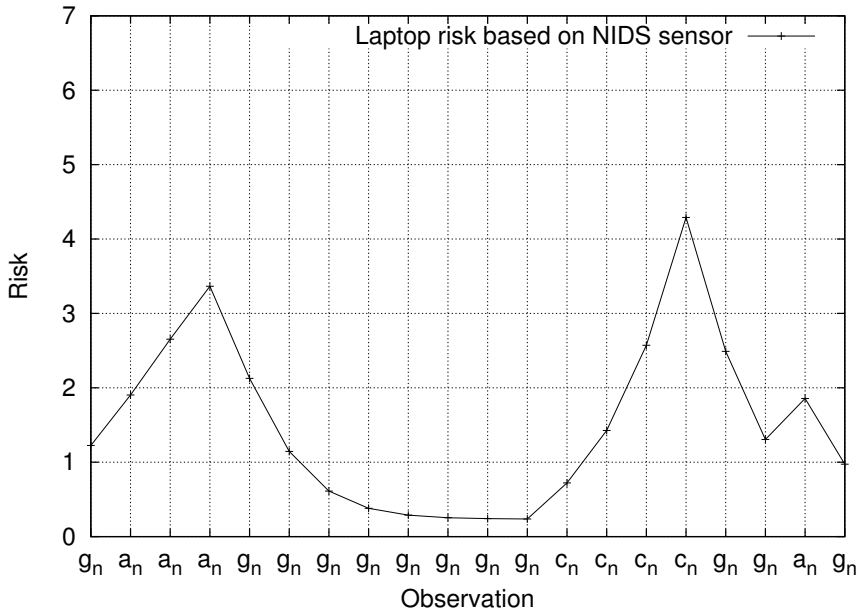
Laptop Risk Assessment by NIDS Observations

- The observation sequence from the NIDS

$$Y_{NIDS-L} = g_n a_n a_n a_n g_n g_n g_n g_n g_n g_n g_n g_n c_n c_n c_n c_n g_n g_n a_n g_n$$

- The observation symbol probability for the Network IDS

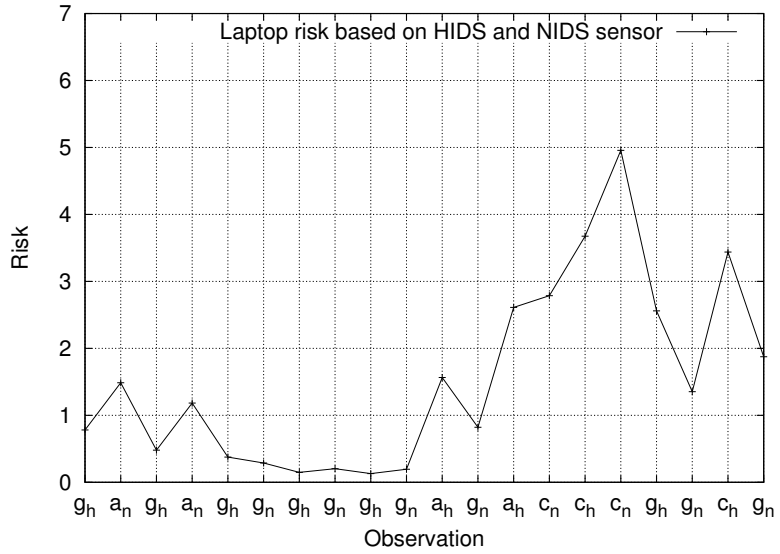
$$Q_{NIDS-L} = \begin{pmatrix} q_G(g) & q_G(a) & q_G(c) \\ q_A(g) & q_A(a) & q_A(c) \\ q_C(g) & q_C(a) & q_C(c) \end{pmatrix} = \begin{pmatrix} 0.5 & 0.3 & 0.2 \\ 0.2 & 0.6 & 0.2 \\ 0.2 & 0.2 & 0.6 \end{pmatrix}$$



Aggregating HIDS and NIDS Observations

The agent now aggregates the observations from the HIDS and NIDS sensors by sampling from the observation sequences Y_{HIDS-L} and Y_{NIDS-L} in a round-robin fashion.

- The aggregated observation sequence
  $Y = g_h a_n g_h a_n g_h g_n g_h g_n g_h g_n a_h g_n a_h c_n c_h c_n g_h g_n c_h g_n$



Future Work

- Multiple sensors
- Parameter estimation
- Better models
- Continuous models and Kalman filtering
- Response networks

Questions?