Quantitative Evaluation of Attack Defense Trees
using Stochastic Timed Automata

August 21, 2017

Peter Gjøl Jensen[1] Kim Guldstrand Larsen[1] Axel Legay[2]
Danny Bøgsted Poulsen[3]

Department of Computer Science, Aalborg University

INRIA - Rennes

Christian Albrechts Univertät, Kiel

Introduction

Motivation

Attack Defense Trees (ADTs) are…

- Formally well founded,
- Mathematically simple,
- Good tool in the box.

Attack Defense Trees **can not**…

- express quantitative measures (revenue, effort, ...),
- exhibit temporal behavior,
- exhibit probabilistic behavior,
- express variance.

Introduction

Motivation

Attack Defense Trees (ADTs) are...

- Formally well founded,
- Mathematically simple,
- Good tool in the box.

Attack Defense Trees **can not**...

- express quantitative measures (revenue, effort, ...),
- exhibit temporal behavior,
- exhibit probabilistic behavior,
- express variance.

Real attacks are...

- having quantitative measures (revenue, effort, ...),
- time-dependent,
- highly uncertain,
- dependent on attacker.

Introduction
Solutions?

Use non ADT formalism

- Lots of expressive power,
- Great Tool support,
- Unfamiliar to users,
- “Cannons and sparrows”.

Add semantics to ADTs

- Resonable expressiveness,
- Translate into other formalism,
- Familiar to users,
- Analytic tools for free!

Introduction
Solution!

Extend ADTs

- Add time, probabilities and measures,
- Translate into Timed Automata,
- Analyze via UPPAAL – and other high-level techniques,
- Automatize via Python.

ANalysis Of VAriance (ANOVA)

Check for a family of attackers the variance of the effectiveness of defenses.

Introduction
Restriction

Type System of Aslanyan

We consider only well-formed ADTs – trees in which the attacker does not actively harm himself.

Introduction

Let us model a small shop

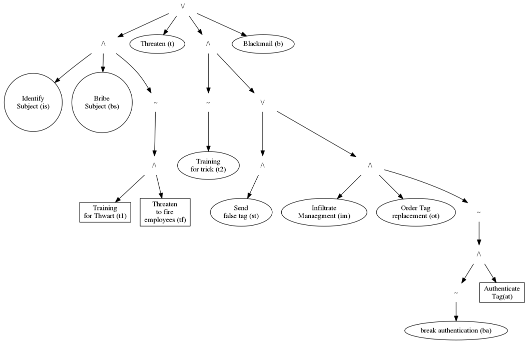
What would it take to substitute some RFID-tag in the shop?

Introduction
By example

$$p \in \mathtt{A}_d \cup \mathtt{A}_a$$

$$t ::= p \mid t \wedge t \mid t \vee t \mid \sim t$$

$$(is \wedge bs \wedge \neg(t1 \wedge tf)) \vee (t) \vee ((\neg t2) \wedge (st \vee (im \wedge ot \wedge \neg((\neg ba) \wedge at)))) \vee (b)$$



Introduction

Attacker Question

Given a set of defensive actions $D \subseteq \mathtt{A}_d$, can we select a set of attacks $A \subseteq \mathtt{A}_a$ s.t. the attack succeeds?

Defender Question

Can we select a set of defensive actions $D \subseteq \mathtt{A}_d$ s.t. for all the attacker choices $A \subseteq \mathtt{A}_a$ no attack succeeds?

Introduction
Existing Work

We are not the first

- Hermanns et al. recently introduced Attack-Defense-Diagrams,
  - Non-trivial extension/mutation of ADTs,
  - non-parameterized.
- Gadyatskaya et. al. extend ADTs with temporal and stochastic semantics,
  - Close to ADTs,
  - basis of current work,
  - non-parameterized.
- ...both use translation to Timed Automata.

Temporal Semantics

- Security is a game,
- Attacker choices are done in sequence,
- Defender chooses up front.

ADT – Tree-Graph

- Defines LTS,
- Rephrase previous questions as model-checking-questions,
- Reasoning on runs,
- Attacker is still a subset of attacker actions.

Run

$(v^0, D)(v_1, \alpha_1)(v_2, \alpha_2)\dots(v_n, \dagger)v_n$
where $v^0 = (\emptyset, \emptyset)$ and $v_1, \dots, v_n \in 2^{\mathtt{A}_a} \times 2^{\mathtt{A}_d}$

Timed Temporal Semantics

Duration Function

$\Delta : \mathtt{A}_a \rightarrow \mathcal{B}(\mathbb{R})$ - where $\mathcal{B}(\mathbb{R})$ denotes all possible intervals over $\mathbb{R}$

Timed Attacker

A timed attacker is thus a tuple $\mathtt{Att}^{\tau} = (\mathtt{Att}, \Delta)$ where $\mathtt{Att}$ is an attacker and Δ is defined as above.

Timed Run

$(v^0, D)(v_1, d_1, \alpha_1)(v_2, d_2, \alpha_2) \ldots (v_n, \dagger)v_n$
for all $1 \leq i < n$, $d_i \in \Delta(c(\alpha_i))$ where $c(a) = c(\neg a) = a$.

Timed Temporal Semantics

Attacker Question

Given a set of defensive actions $D \subseteq \mathtt{A}_d$, does there exists and attacker s.t. the attack succeeds within τ units of time?

Defender Question

Can we select a set of defensive actions $D \subseteq \mathtt{A}_d$ s.t. for all possible attackers, no attack succeeds withing τ units of time?

Techniques

Use standard symbolic/polyhedra-based model-checking techniques deployed by UPPAAL.

Stochastic Semantics

Uncertainties

- Defensive measure not garuanteed to be “in place” (metal detector),
- Attacker action relies on uncertain information etc (knowledge of vulnerability, skill).
- Exact duration is infeasible.

Both attacker and defender actions can fail

Stochastic Semantics

Attackers/Defenders

General idea; add probability masses.

Defender

Measures are selected according to a probability mass function $\gamma_{\mathtt{Def}} : 2^{\mathtt{A}_d} \rightarrow [0, 1]$.
A stochastic defender is thus a tuple $\mathtt{Def}^{\mathcal{S}} = (\mathtt{Def}, \gamma_{\mathtt{Def}})$.

Attacker

$\mathtt{Att}^{\mathcal{S}} = (\mathtt{Att}^{\mathcal{T}}, \gamma_{\mathtt{Att}}, \delta)$ where $\mathtt{Att}^{\mathcal{T}} = (\mathtt{Att}, \Delta)$ is a timed attacker,
$\gamma_{\mathtt{Att}} : \mathcal{V} \rightarrow \mathtt{A}_a \cup \{\dagger\} \rightarrow \mathbb{R}$ assigns a probability mass function to each state for selecting the action to perform and
$\delta : \mathtt{A}_a \rightarrow \mathbb{R} \rightarrow \mathbb{R}$ assigns a probability density to the possible execution times of each action

Stochastic Semantics
Requirements

- Non-zero probabilities for selected actions,
- Zero-probabilities for non-selected actions.
- Respect timing intervals.

Defender

$\gamma_{\texttt{Def}}(D) \neq 0 \implies D \in \texttt{Def}(v^{t^0})$

Attacker

1. if $\gamma_{\texttt{Att}}(v^t)(a) \neq 0$ then $a \in \texttt{Att}(v^t)$ and
2. if $\delta(a)(r) \neq 0$ then $r \in \Delta(a)$.

Stochastic Semantics
Environment

Models outside influence (success-rate in bribing etc.)

$$\mathtt{Env}_a : \{a, \neg a\} \rightarrow]0, 1[$$

Stochastic Semantics
Over Runs

Interval I, successors-state v' and action α, the probability of attacker choices

$$G_v^{\mathtt{Att}^{\mathcal{S}}|\mathtt{Def}^{\mathcal{S}}|\mathtt{Env}}(\pi) = (v_0 = v) \cdot \gamma_{\mathtt{Att}}(v)(c(\alpha)) \cdot \left(\int_{I_0} (\delta(c(\alpha))(\tau))\, \mathrm{d}\tau \right) \cdot \mathtt{Env}_{c(\alpha)}(\alpha) \cdot G_{v'}^{\mathtt{Att}^{\mathcal{S}}|\mathtt{Def}^{\mathcal{S}}|\mathtt{Env}}(\pi^1),$$

The probability of defender choices D, where $\Pi = (v^0, D)\pi$

$$F_{v^0}^{\mathtt{Att}^{\mathcal{S}}|\mathtt{Def}^{\mathcal{S}}|\mathtt{Env}}(\Pi) = \gamma_{\mathtt{Def}}(D) \cdot G_v^{\mathtt{Att}^{\mathcal{S}}|\mathtt{Def}^{\mathcal{S}}|\mathtt{Env}}(\pi)$$

Stochastic Semantics

Environment

let $\omega = (v^0, D)(v_1, d_1, \alpha_1)(v_2, d_2, \alpha_2)\ldots(v_n, \dagger)v_n$ be a timed run over the timed ADT ψ.
We give a time-bound indicator function for timebound τ;

$$1_{\psi,\tau}(\omega) = \begin{cases} 1 & \text{if } [\![\psi]\!] v_n \text{ and } \sum_{i=1}^{n-1} d_i \leq \tau \\ 0 & \text{otherwise} \end{cases}.$$

And can then define the probability measure of success as

$$\mathbb{P}^{\mathtt{Att}^{\mathcal{S}}}(\psi, \tau) = \int_{\omega \in \Omega^{\tau}(\psi)} 1_{\psi,\tau}(\omega) \mathrm{d}F^{\mathtt{Att}^{\mathcal{S}}|\mathtt{Def}^{\mathcal{S}}}$$

Stochastic Semantics

Stochastic Question

Given an AD-tree, a stochastic attacker, a stochastic defender and time bound τ; what is the probability of a successful attack.

Techniques

Use classical statistical methods, considering the outcome of each run as a Bernoulli experiment.
Off-the-shelve with UPPAAL SMC.

Costs

Action Cost

$$C_c : \mathtt{A}_a \rightarrow \mathcal{R}_{\geq 0}$$

Run Cost

$$\mathtt{C}(\omega) = \sum_{i=1}^{n-1} C_c(\alpha_i) \cdot d_i$$

Estimated Cost

$$\mathbb{E}^{\mathtt{Att}^{\mathcal{S}}|\mathtt{Def}^{\mathcal{S}}|\mathtt{Env}}(\psi, \tau) = \int_{\omega \in \Omega^{\tau}(\psi)} \mathtt{C}^{\tau}(\omega)\, \mathrm{d}F^{\mathtt{Att}^{\mathcal{S}}|\mathtt{Def}^{\mathcal{S}}|\mathtt{Env}}$$

Cost

Estimation Question

Given an AD-tree ψ, a stochastic attacker $\mathtt{Att}^{\mathcal{S}}$, a stochastic defender $\mathtt{Def}^{\mathcal{S}}$ and a time bound τ, what is the expected cost of an attack? i.e. calculate $\mathbb{E}^{\mathtt{Att}^{\mathcal{S}}|\mathtt{Def}^{\mathcal{S}}}(\psi, \tau)$.

Bounded

Can the attack be done within a cost-budget of *B*?

Techniques

Use classical statistical methods, measure expected value.
Off-the-shelve with UPPAAL SMC.

Encoding

- a boolean flag for each action,
- a defender component,
- an attacker component,
- an environment component for each (attacker) action.

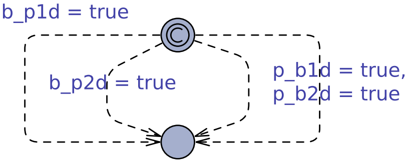
Composition

Parallel composition is well defined for Stochastic Timed Automata.

Assumption

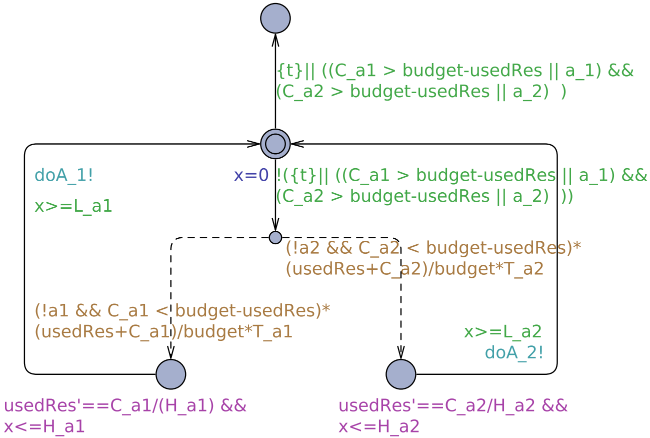
Attacker is cost-preserving.

Encoding
Defender



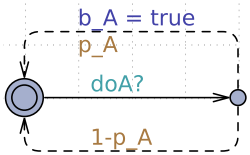
The Defender Automaton for $D = \{p1d, p2d\}$ with $\mathtt{A}_d = \{p1d, p2d, p3d\}$

Encoding
Attacker



The Attacker Automaton for $\mathtt{A}_a = \{a1, a2\}$ - - we assume a cost-preserving attacker.

Encoding
Environment



The Environment Automaton for a generic action *A*

Parameterized Attacker

Profiles

Cost, probability and duration of attacker may be influenced by

- Geographical location,
- Resources,
- Time Constraint,
- Technology,
- ...

We want to model, capture and analyze this!

Parameterized Attacker
ANOVA

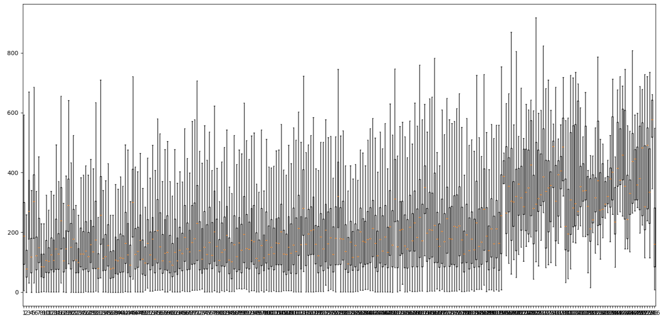
ANalysis Of VAriance (ANOVA)

- Test if one or more parameters significantly influence continuous observation
- Based on finite set of experiments,
- can in combination with Tukeys Test compute optimal parameter sets.

Parameters

- Probabilities,
- Cost,
- Duration,
- ...

Experiment



Conclusion

- Used off-the-shelve tools and methods,
- Demonstrated parametric-analysis and optimization.

Further Work

- Temporal action-dependencies,
- Interactive defender.