Timed Multiset Rewriting and the Verification of Time-Sensitive Distributed Systems

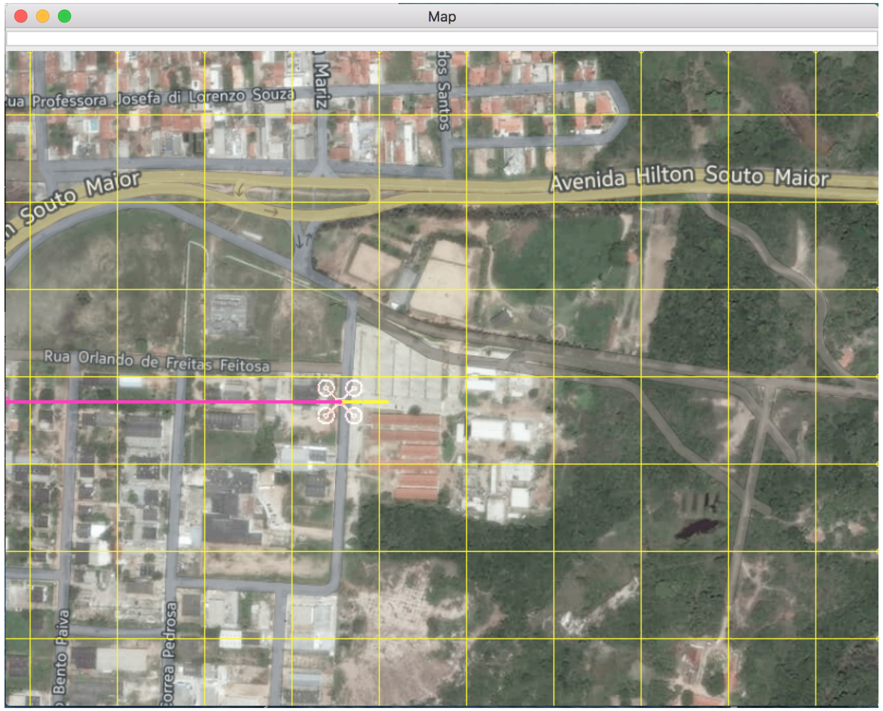
Max Kanovich[1,6], **Tajana Ban Kirigin**[2],Vivek Nigam[3], Andre Scedrov[4,6], and Carolyn Talcott[5]

[1]University College London, UK
[2]University of Rijeka, HR
[3]Federal University of Paraíba, Brazil
[4]University of Pennsylvania, USA
[5]SRI International, USA
[6]National Research University Higher School of Economics, Moscow, Russia

Problem Definition

Time-Sensitive Distributed Systems (TSDS)

Drones carrying out **the surveillance of some area must always have recent pictures**, i.e., at most M time units old, of some strategic locations.


Map
ua Professora Josefa di Lorenzo Souza
Mariz
dos Santos
n Souto Maior
Avenida Hilton Souto Maior
Rua Orlando de Freitas Feitosa
Bento Paiva
orrea Pedrosa

For example, monitoring of a sugar-cane plantation for spots with diseases.

Problem Definition

Time-Sensitive Distributed Systems (TSDS)

Drones should satisfy possibly **quantitative properties:**

- not run out of energy;
- should collectively have a set of **recent pictures of all sensitive locations**.

Moreover, the **environment may interfere**:

- presence of winds;
- GPS failure.

Problem Definition

Two types of properties:

- **Realizability:** Under some given time constraints, the specified system can achieve the assigned goal, e.g., always collect a recent picture of the sensitive locations.
- **Survivability:** For all possible outcomes (of drone actions or environment interference), the specified system can achieve the assigned goal

Contributions

Main Contributions:

- We propose a formal framework for specifying TSDS and the properties above.
- We propose the class of *progressive timed systems*;
- We investigate the complexity of realizability and survivability for progressive timed systems;
- We carry out preliminary experiments.

Agenda

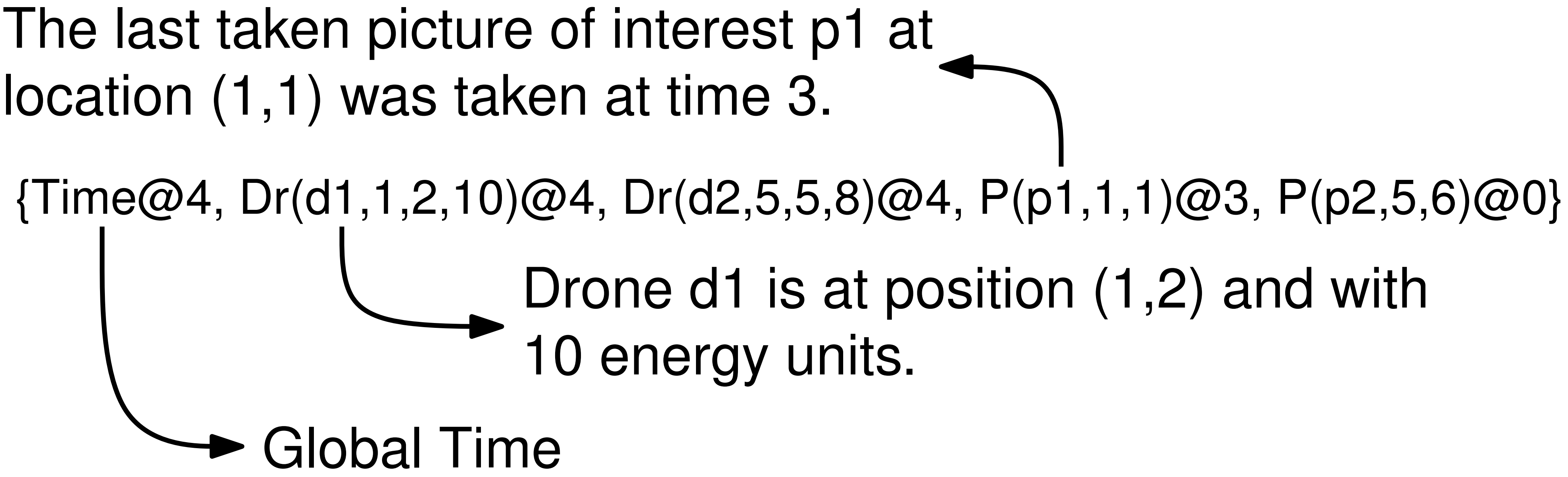
- Problem Definition

Timed Multiset Rewriting Framework

- Quantitative Temporal Properties
- Progressive Timed MSR
- Simulations
- Conclusions and Future Work

Timed Multiset Rewriting

- **Timestamped Facts:** – A Fact F with an associated real number t, written $F@t$. We use the fact **Time** to specify the global time.
- **Configuration** – A multiset of facts with **exactly one occurrence of the fact Time**.



The last taken picture of interest p1 at location (1,1) was taken at time 3.

{Time@4, Dr(d1,1,2,10)@4, Dr(d2,5,5,8)@4, P(p1,1,1)@3, P(p2,5,6)@0}

Drone d1 is at position (1,2) and with 10 energy units.

Global Time

Timed Multiset Rewriting

- **Tick Rule** – Advances Global Time.

$$Time@T \longrightarrow Time@(T+1)$$

- **Instantaneous Rules** – Changes the state, but not the global time

Time Constraints:
$T > T' \pm D$ and $T = T' \pm D$

$$Time@T, \mathcal{W}, F_1@T'_1, \ldots, F_n@T'_n \mid C \longrightarrow$$
$$Time@T, \mathcal{W}, Q_1@(T+D_1), \ldots, Q_m@(T+D_m)$$

where $D_1, \ldots, D_m$ are non-negative natural numbers.

Agenda

- Problem Definition
- Timed Multiset Rewriting Framework
- **Quantitative Temporal Properties**
- Progressive Timed MSR
- Simulations
- Conclusions and Future Work

Critical Configuration Specification

Critical configuration specification is a set of pairs

$$\mathcal{CS} = \{\langle \mathcal{S}_1, \mathcal{C}_1 \rangle, \ldots, \langle \mathcal{S}_n, \mathcal{C}_n \rangle\}$$

where for each pair $\langle \mathcal{S}_j, \mathcal{C}_j \rangle$ $\mathcal{C}_j$ is a set of time constraints and $\mathcal{S}_j$ is a set of timestamped facts:

Given a **critical configuration specification**, $\mathcal{CS} = \{\langle \mathcal{S}_1, \mathcal{C}_1 \rangle, \ldots, \langle \mathcal{S}_n, \mathcal{C}_n \rangle\}$, we say that a configuration $\mathcal{S}$ is critical if for some $1 \leq i \leq n$, there is a grounding substitution, σ such that:

- $\mathcal{S}_i\sigma \subseteq \mathcal{S}$
- all constraints in $\mathcal{C}_i\sigma$ are valid.

Examples

- **A configuration is critical if a drone is out of energy:**

$$\{\langle\{Dr(Id, X, Y, 0)@T\}, \emptyset\rangle \mid Id \in \{d1, d2\}, X \in \{0, \ldots, x_{max}\}, Y \in \{0, \ldots, y_{max}\}\}$$

- **A configuration is critical if a picture of a point of interest is stale:**

$$\left\{ \begin{array}{c} \langle\{P(p_1, x_1, y_1)@T_1, Time@T\}, T > T_1 + M\rangle, \\ \ldots, \\ \langle\{P(p_n, x_n, y_n)@T_n, Time@T\}, T > T_n + M\rangle \end{array} \right\}$$

One can specify specific bounds!

Problem Definitions

- A (possibly infinite) trace $\mathcal{S}_0 \to \mathcal{S}_1 \to \cdots$ is **compliant** w.r.t. a critical configuration specification if it does not contain any critical configuration.

- A (possibly infinite) trace $\mathcal{P}$ of a timed MSR $\mathcal{A}$ uses a **lazy time sampling** if for any occurrence of the Tick rule $\mathcal{S}_i \longrightarrow_{Tick} \mathcal{S}_{i+1}$ in $\mathcal{P}$, no instance of any instantaneous rule in $\mathcal{A}$ can be applied to the configuration $\mathcal{S}_i$.

- Lazy time samping establishes a preference of instantaneous rules over the Tick Rule. **That is, we assume systems react before time passes.**

Problem Definitions

A timed MSR $\mathcal{A}$ is **realizable** with respect to the **lazy time sampling**, a critical configuration specification $\mathcal{CS}$ and an initial configuration $\mathcal{S}_0$ if there **exists a trace**, $\mathcal{P}$, that starts with $\mathcal{S}_0$ and uses the lazy time sampling such that

- $\mathcal{P}$ is compliant with respect to $\mathcal{CS}$;
- Global time tends to infinity in $\mathcal{P}$.

Problem Definitions

A timed MSR $\mathcal{A}$ satisfies **survivability** with respect to the lazy time sampling, a critical configuration specification $\mathcal{CS}$ and an initial configuration $\mathcal{S}_0$ if it is realizable and if **all infinite traces**, $\mathcal{P}$, that start with $\mathcal{S}_0$ and use the lazy time sampling are such that:

- $\mathcal{P}$ is compliant with respect to $\mathcal{CS}$;
- Global time tends to infinity in $\mathcal{P}$.

Challenge

Both realizability and survivability mention the following condition on traces:

- Global time tends to infinity in $\mathcal{P}$.

This means that we have to deal with infinite traces.

Problem Definitions

We also consider **time bounded versions** of realizability and survivability problems:

Their definition is similar to the previous ones, but where traces with exactly n instances of the Tick rule are considered for a given n.

- n-time-bounded realizable;
- n-time-bounded survivability.

These problems are still interesting because one has to deal with the non-determinism of system specifications. In fact, without suitable restrictions, these problems are undecidable [Kanovich et al. RTA 12].

Agenda

- Problem Definition
- Timed Multiset Rewriting Framework
- Quantitative Temporal Properties
- **Progressive Timed MSR**
- Simulations
- Conclusions and Future Work

Progressive Timed MSR

A **Timed MSR** is a set of rules containing only instantaneous rules and the tick rule.

A **Progressive Timed MSR** is a Timed MSR such that:

- **All Rules are Balanced:** Creates the same number of facts as it consumes:

consumes n facts

$$Time@T, \mathcal{W}, F_1@T'_1, \ldots, F_n@T'_n \mid C \longrightarrow$$
$$Time@T, \mathcal{W}, Q_1@(T + D_1), \ldots, Q_n@(T + D_n)$$

creates n facts

Progressive Timed MSR

A **Timed MSR** is a set of rules containing only instantaneous rules and the tick rule.

A **Progressive Timed MSR** is a Timed MSR such that:

- **All Rules are Balanced:** Creates the same number of facts as it consumes:
- **Advancing Time:** Creates at least one fact in the future:

$$Time@T, \mathcal{W}, F_1@T'_1, \ldots, F_n@T'_n \mid C \longrightarrow$$
$$Time@T, \mathcal{W}, Q_1@(T + D_1), \ldots, Q_n@(T + D_n)$$

For some $1 \leq i \leq n$, $D_i > 0$

Progressive Timed MSR

A **Timed MSR** is a set of rules containing only instantaneous rules and the tick rule.

A **Progressive Timed MSR** is a Timed MSR such that:

- **All Rules are Balanced:** Creates the same number of facts as it consumes:
- **Advancing Time:** Creates at least one fact in the future:
- **No facts in the future consumed:** All facts consumed are either at the same time as global time or in the past:

contains the constraint $T'_i \leq T$,
for all $1 \leq i \leq n$

$$Time@T, \mathcal{W}, F_1@T'_1, \ldots, F_n@T'_n \mid C \longrightarrow$$
$$Time@T, \mathcal{W}, Q_1@(T + D_1), \ldots, Q_n@(T + D_n)$$

Progressive Timed MSR

Proposition: Let $\mathcal{A}$ be a PTS, $\mathcal{S}_0$ an initial configuration and m the number of facts in $\mathcal{S}_0$. For all traces $\mathcal{P}$ of $\mathcal{A}$ starting from $\mathcal{S}_0$, let

$$\mathcal{S}_i \longrightarrow_{Tick} \longrightarrow \mathcal{S}_{i+1} \longrightarrow \cdots \longrightarrow \mathcal{S}_j \longrightarrow_{Tick} \longrightarrow \mathcal{S}_{j+1}$$

be any sub-sequence of $\mathcal{P}$ with exactly two instances of the Tick rule, one at the beginning and the other at the end. Then $j - i < m$.

Proposition: Let $\mathcal{A}$ be a PTS. In all infinite traces of $\mathcal{A}$ the global time tends to infinity.

Previous Complexity Results

Reachability Problem – Finite Plans		
Balanced Actions	Untimed System	**PSPACE-complete** [Kanovich et al., IC'14]
	System with discrete time	**PSPACE-complete** [Kanovich et al., RTA'12]
	System with continuous time	**PSPACE-complete** [Kanovich et al., POST'15]
Actions not necessarily balanced		**Undecidable**

Main Complexity Results

Realizability		
Progressive MSR	n-bounded	**NP-complete** **new**
	time tending to infinite	**PSPACE-complete** **new**
Not Necessary Progressive		**Undecidable** [Kanovich et al. RTA 12]

This is a non-trivial result as the decision problem is over the set of infinite traces. In fact, we are on the verge of undecidability: relaxing **conditions leads to undecidability.**

Main Complexity Results

Class containing the classes NP and co-NP.

Survivability		
Progressive MSR	n-bounded	Δ_2^p **of the polynomial hierarchy new**
	time tending to infinite	**PSPACE-complete new**
Not Necessary Progressive		**Undecidable** [Kanovich et al. RTA 12]

Agenda

- Problem Definition
- Timed Multiset Rewriting Framework
- Quantitative Temporal Properties
- Progressive Timed MSR
- **Simulations**
- Conclusions and Future Work

Symbolic Simulations in Maude

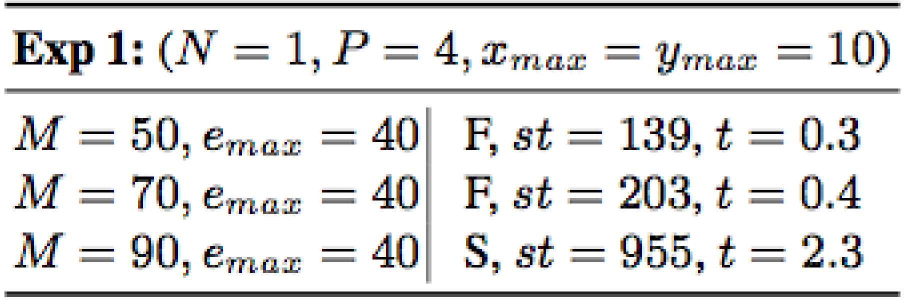
We obtained promising results in our simulations of our main example on taking photos of some points of interest. We used the following parameters:

- N – Number of Drones;
- P – the number of points of interest
- $x_{max} \times y_{max}$ – the size of the grid
- e_{max} – the maximum energy capacity of each drone
- M – the max stale time of photos

The base station where drones can recharge is at the point: $(\lceil x_{max}/2 \rceil, \lceil y_{max}/2 \rceil)$.

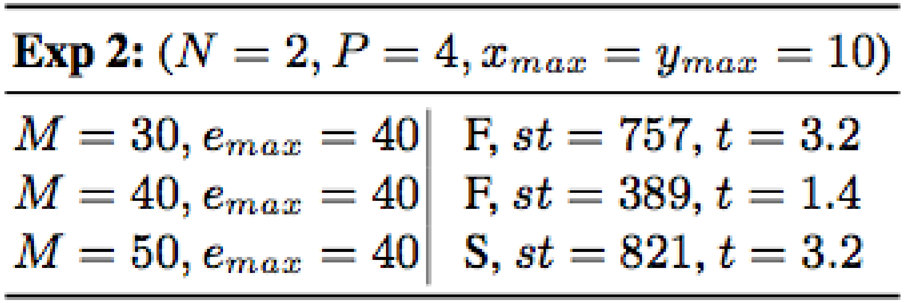
We carried out bounded simulations until time $4 \times M$.

Symbolic Simulations in Maude



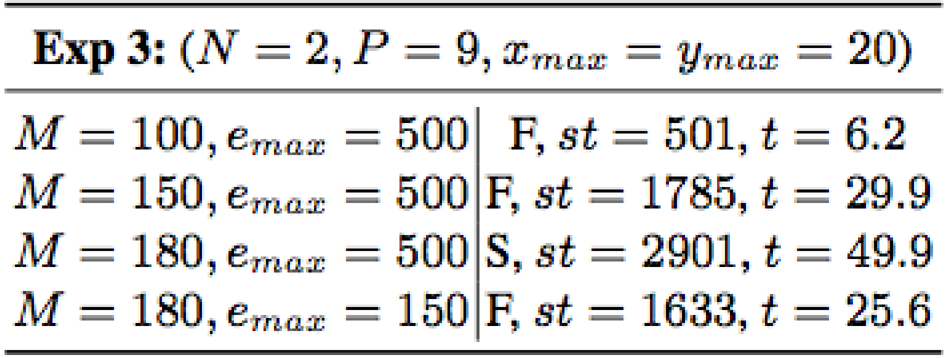
Exp 1: $(N = 1, P = 4, x_{max} = y_{max} = 10)$

$M = 50, e_{max} = 40$	F, $st = 139, t = 0.3$
$M = 70, e_{max} = 40$	F, $st = 203, t = 0.4$
$M = 90, e_{max} = 40$	S, $st = 955, t = 2.3$



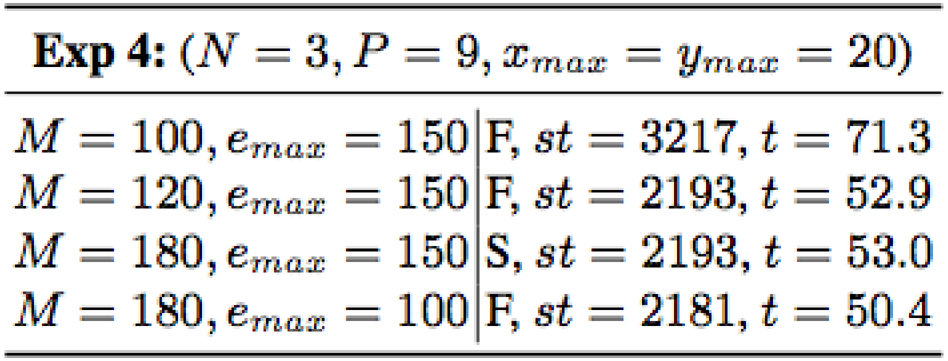
Exp 2: $(N = 2, P = 4, x_{max} = y_{max} = 10)$

$M = 30, e_{max} = 40$	F, $st = 757, t = 3.2$
$M = 40, e_{max} = 40$	F, $st = 389, t = 1.4$
$M = 50, e_{max} = 40$	S, $st = 821, t = 3.2$



Exp 3: $(N = 2, P = 9, x_{max} = y_{max} = 20)$

$M = 100, e_{max} = 500$	F, $st = 501, t = 6.2$
$M = 150, e_{max} = 500$	F, $st = 1785, t = 29.9$
$M = 180, e_{max} = 500$	S, $st = 2901, t = 49.9$
$M = 180, e_{max} = 150$	F, $st = 1633, t = 25.6$



Exp 4: $(N = 3, P = 9, x_{max} = y_{max} = 20)$

$M = 100, e_{max} = 150$	F, $st = 3217, t = 71.3$
$M = 120, e_{max} = 150$	F, $st = 2193, t = 52.9$
$M = 180, e_{max} = 150$	S, $st = 2193, t = 53.0$
$M = 180, e_{max} = 100$	F, $st = 2181, t = 50.4$

Agenda

- Problem Definition
- Timed Multiset Rewriting Framework
- Quantitative Temporal Properties
- Progressive Timed MSR
- **Simulations**

Conclusions and Future Work

Conclusions and Future Work

We proposed a framework for the specification of Timed Systems and Quantitative Temporal Properties.

We proposed the problems of **Realizability** and **Survivability** (and their time bounded versions).

We shown that for the class of Progressive MSR these problems are both decidable (PSPACE-Complete) although they are over **infinite traces**.

Finally, we carried out a number of simulations showing that it is feasible to use our framework in concrete applications.

Conclusions and Future Work

As future work, we are investigating similar problems for Cyber-Physical Systems but in the presence of malicious intruders.

Moreover, we are investigating intruder models and how to automate the verification of systems.

We also believe that the results in this work can be extended to dense times by using the machinery in our previous work [Kanovich et al. POST 2015].

Finally, we are improving our implementations by using more realistic models of drones by integrating our Maude machinery to existing drone simulators (SITL). Moreover we are investigating how to model uncertainty and the use of Statistical Model Checking in our verification.