Parameterized Verification of Systems with Broadcast Communication

Arnaud Sangnier

IRIF - Université Paris Diderot-Paris 7

joint work with Giorgio Delzanno & Gianluigi Zavattaro

DRV - Bertinoro - 19th May 2016
Verify network of processes of unbounded size

Why to consider such networks?

- Classical distributed algorithms (mutual exclusion, leader election, ...)
- Telecommunication protocols (routing, ...)
- Algorithms for ad-hoc networks
- Model for biological systems
- and many more applications ...
Hypothesis

All the processes have the same behavior

In [Esparza, STACS’14], such networks are called crowd

More precisely:

- Each process will follow the same protocol
- Process can communicate
- Communication way:
  - Message passing
  - Shared variable
  - Broadcast communication
  - Multi-diffusion (selective broadcast)

Question:
Is there a network with N processes which allows to reach a goal?
Outline

1. Systems with broadcast communication

2. Ad Hoc Networks

3. Conclusion
Outline

1 Systems with broadcast communication

2 Ad Hoc Networks

3 Conclusion
Parameterized Networks with Broadcast

[Esparza et al., LICS’99]

Main characteristics

- No creation/deletion of processes
- Each process executes the same finite state protocol
- Synchronization through broadcast of a message
- All the processes receive the message
A protocol $P = \langle Q, \Sigma, R, Q_0 \rangle$

Finite state system whose transitions are labeled with:

1. broadcast of messages - $!!m$
2. reception of messages - $??m$
3. internal actions - $\tau$

where $m$ belongs to the finite alphabet $\Sigma$

A protocol defines a Broadcast Network (BN)
Broadcast Networks: configurations

A configuration is a multiset $\gamma : Q \mapsto \mathbb{N}$

- Same as for Rendez-vous Networks

<table>
<thead>
<tr>
<th>Blue</th>
<th>Orange</th>
<th>Green</th>
</tr>
</thead>
</table>

- **Initial configurations**: $\gamma(q) > 0$ iff $q \in Q_0$

**Remarks:**
- The size of configurations is not bounded
- Infinite number of configurations

$\Rightarrow$ BN are infinite state systems
Broadcast Networks: semantics

Transition system $BN(P) = \langle C, \rightarrow, C_0 \rangle$ associated to $P$

- $C$: set of configurations
- $\rightarrow$: $C \times C$: transition relation
- $C_0$: initial configurations

The relation $\rightarrow$ respects the following rules during an execution:
- The number of processes in an execution does not change
- Processes can only change their state
- Two kind of transitions according to the given process
  1. **local actions** - one process performs an internal action $\tau$
  2. **broadcast** - one process emits a message with $!!m$, all the processes that can receive it with $??m$ have to receive it
Broadcast Networks: an example

Systems with broadcast communication
Broadcast Networks: an example

Systems with broadcast communication
Broadcast Networks: an example
Broadcast Networks: an example
Broadcast Networks: an example

Systems with broadcast communication
Broadcast Networks: an example
Reachability question

**Parameters:** Number of processes

### Control State Reachability (REACH)

**Input:** A protocol and a control state \( q \in Q \);

**Output:** Does there exist \( \gamma \in C_0 \) and \( \gamma' \in C \) s.t. \( \gamma \rightarrow^* \gamma' \) and \( \gamma(q) > 0 \)?

### Remarks:

- This problem considers an infinite number of possible initial configurations
- Reachability of a configuration \( \gamma' \) is easier, **the number of processes is in fact fixed**
Well Quasi Ordering (wqo)

$(X, \leq)$ is a well-quasi ordering if for all infinite sequences $s_1, s_2, \ldots$, there exists $i < j$ such that $s_i \leq s_j$.

Upward closed set

A set $Y \subseteq X$ is upward closed w.r.t $(X, \leq)$ if $y \in Y$ and $y \leq y'$ implies $y' \in Y$.

- Upward closure of $Y \subseteq X$: $Y \uparrow = \{ x \in X \mid \exists y \in Y \land y \leq x \}$

Lemma

If $(X, \leq)$ is a wqo and if $Y \subseteq X$ is upward closed w.r.t. $(X, \leq)$, then there exists a finite set $B \subseteq X$ s.t. $Y = B \uparrow$. 
Well structured transition systems everywhere

\[ \gamma \preceq \gamma' \text{ iff } \forall q \in Q, \text{ we have } \gamma(q) \leq \gamma'(q) \]

Theorem

\((C, \preceq)\) is a well-quasi-ordering.
Well structured transition systems everywhere

\[ \gamma \preceq \gamma' \text{ iff } \forall q \in Q, \text{ we have } \gamma(q) \leq \gamma'(q) \]

**Theorem**

\((C, \preceq)\) is a well-quasi-ordering.

**Monotonicity lemma**

For \(\gamma_1, \gamma'_1, \gamma_2 \in C\), if
- \(\gamma_1 \Rightarrow \gamma'_1\) and \(\gamma_1 \preceq \gamma_2\),
then there exists \(\gamma'_2 \in C\) s.t.
- \(\gamma_2 \Rightarrow \gamma'_2\) and \(\gamma'_1 \preceq \gamma'_2\)

- BN are **Well Structured Transition Systems**
  [Abdulla et al., LICS’96; Finkel & Schnoebelen, TCS’01]
Deciding \textsc{Reach} in Broadcast Networks

\textbf{Theorem} \cite{EsperzaEtAlLICS99}

\textsc{Reach} is decidable for Broadcast Networks

\textbf{Idea of the proof}

- For $S \subseteq \mathcal{C}$, $\text{pre}(S) = \\{ \gamma \in \mathcal{C} \mid \gamma \Rightarrow \gamma' \land \gamma' \in S \}$
Deciding \textsc{Reach} in Broadcast Networks

**Theorem** [Esperza et al., LICS’99]

\textsc{Reach} is decidable for Broadcast Networks

**Idea of the proof**

- For $S \subseteq \mathcal{C}$, $\text{pre}(S) = \{ \gamma \in \mathcal{C} \mid \gamma \Rightarrow \gamma' \land \gamma' \in S \}$
- if $S$ is upward-closed, then $\text{pre}(S)$ is upward closed
Deciding **REACH** in Broadcast Networks

**Theorem** [Esperza et al., LICS’99]

**REACH** is decidable for Broadcast Networks

**Idea of the proof**

- For $S \subseteq C$, $pre(S) = \{ \gamma \in C \mid \gamma \Rightarrow \gamma' \land \gamma' \in S \}$
- if $S$ is upward-closed, then $pre(S)$ is upward closed
- let $\Gamma : C \mapsto C$ s.t. $\Gamma(S) = S \cup pre(S)$
Deciding $\text{REACH}$ in Broadcast Networks

**Theorem** [Esperza et al., LICS’99]

$\text{REACH}$ is decidable for Broadcast Networks

**Idea of the proof**

- For $S \subseteq \mathcal{C}$, $\text{pre}(S) = \{ \gamma \in \mathcal{C} \mid \gamma \Rightarrow \gamma' \land \gamma' \in S \}$
- if $S$ is upward-closed, then $\text{pre}(S)$ is upward closed
- let $\Gamma : \mathcal{C} \mapsto \mathcal{C}$ s.t. $\Gamma(S) = S \cup \text{pre}(S)$
- For $S$ upward-closed, there exists $i \in \mathbb{N}$ s.t. $\Gamma^{i+1}(S) = \Gamma^i(S)$ and given a finite basis $B$ of $S$, one can compute a finite basis $B'$ of $\Gamma^i(S)$
Deciding \texttt{REACH} in Broadcast Networks

\textbf{Theorem} \cite{Esperza99}

\texttt{REACH} is decidable for Broadcast Networks

\textbf{Idea of the proof}

- For $S \subseteq \mathcal{C}$, $\text{pre}(S) = \{\gamma \in \mathcal{C} \mid \gamma \Rightarrow \gamma' \land \gamma' \in S\}$
- if $S$ is upward-closed, then $\text{pre}(S)$ is upward closed
- let $\Gamma : \mathcal{C} \mapsto \mathcal{C}$ s.t. $\Gamma(S) = S \cup \text{pre}(S)$
- For $S$ upward-closed, there exists $i \in \mathbb{N}$ s.t. $\Gamma^{i+1}(S) = \Gamma^i(S)$ and given a finite basis $B$ of $S$, one can compute a finite basis $B'$ of $\Gamma^i(S)$
- Take for $S$ the configuration $\gamma$ such that $\gamma(q) = 1$ and $\gamma(q') = 0$ for all $q' \neq q$
Deciding \textsc{Reach} in Broadcast Networks

Theorem [Esperza et al., LICS’99]
\textsc{Reach} is decidable for Broadcast Networks

Idea of the proof
- For $S \subseteq C$, $pre(S) = \{ \gamma \in C \mid \gamma \Rightarrow \gamma' \land \gamma' \in S \}$
- if $S$ is upward-closed, then $pre(S)$ is upward closed
- let $\Gamma : C \mapsto C$ s.t. $\Gamma(S) = S \cup pre(S)$
- For $S$ upward-closed, there exists $i \in \mathbb{N}$ s.t. $\Gamma^{i+1}(S) = \Gamma^i(S)$ and given a finite basis $B$ of $S$, one can compute a finite basis $B'$ of $\Gamma^i(S)$
- Take for $S$ the configuration $\gamma$ such that $\gamma(q) = 1$ and $\gamma(q') = 0$ for all $q' \neq q$

Theorem [Schmitz & Schnoebelen, CONCUR’13]
\textsc{Reach} for Broadcast Networks is Ackermann-complete.
Outline

1. Systems with broadcast communication
2. Ad Hoc Networks
3. Conclusion
Main characteristics of Ad Hoc Networks

- Nodes can be mobile
- Topology is not known a priori
- Messages are broadcasted to the neighbours
- Problems linked to communication (collision, loss of messages, etc.)
Defining a model for Ad Hoc Networks

<table>
<thead>
<tr>
<th>Main characteristics</th>
<th>[Delzanno et al., CONCUR’10]</th>
</tr>
</thead>
<tbody>
<tr>
<td>No creation/deletion of nodes</td>
<td></td>
</tr>
<tr>
<td>Each node executes the same finite state process</td>
<td></td>
</tr>
<tr>
<td>Model based on the $\omega$-calculus</td>
<td></td>
</tr>
<tr>
<td>Broadcast of the messages to the neighbors</td>
<td></td>
</tr>
<tr>
<td>Static topology represented by a connectivity graph</td>
<td></td>
</tr>
</tbody>
</table>
Ad Hoc Networks: syntax

A protocol $P = \langle Q, \Sigma, R, Q_0 \rangle$

Finite state system whose transitions are labeled with:

1. broadcast of messages - $!!m$
2. reception of messages - $??m$
3. internal actions - $\tau$

where $m$ belongs to the finite alphabet $\Sigma$

A protocol defines an Ad Hoc Network (AHN)
A configuration is a graph $\gamma = \langle V, E, L \rangle$

- $V$: finite set of vertices
- $E$: $V \times V$: finite set of edges
- $L$: $V \rightarrow Q$: labeling function

**Initial configurations**: all vertices are labeled with initial states

**Notation**: $L(\gamma)$ all the labels present in $\gamma$

**Remarks**:
- The size of the considered graphs is not bounded
- Infinite number of configurations

$\Rightarrow$ BN are infinite state systems
Ad Hoc Networks: semantics

Transition system $BN(P) = \langle C, \rightarrow, C_0 \rangle$ associated to $P$

- $C$ : set of configurations
- $\rightarrow$: $C \times C$ : transition relation
- $C_0$ : initial configurations

The relation $\rightarrow$ respects the following rules during an execution:

- The topology remains static
  - The number of vertices does not change
  - The edges do not change
  - Only the labels of the vertices can evolve

- Two kind of transitions according to the given protocol
  1. local actions - one process performs an internal action $\tau$
  2. broadcast - one process emits a message with $!!m$, all its neighbors that can receive it with $??m$ have to receive it
Ad Hoc Networks: an example

![Diagram of Ad Hoc Networks example]
Ad Hoc Networks: an example

Ad Hoc Networks
Ad Hoc Networks: an example
Ad Hoc Networks: an example
Ad Hoc Networks: an example
Ad Hoc Networks: an example
Ad Hoc Networks: an example

![Diagram of ad hoc networks example]
Ensuring the form of a topology

The Req/Ack/Ok-protocol

Properties
Ensuring the form of a topology

The Req/Ack/Ok-protocol

Properties

Ad Hoc Networks
Ensuring the form of a topology

The Req/Ack/Ok-protocol

Properties
Ensuring the form of a topology

The Req/Ack/Ok-protocol

Properties
Ensuring the form of a topology

The Req/Ack/Ok-protocol

Properties
Ensuring the form of a topology

The Req/Ack/Ok-protocol

Properties
Ensuring the form of a topology

The Req/Ack/Ok-protocol

Properties
Ensuring the form of a topology

The Req/Ack/Ok-protocol

Properties
## Undecidability result

<table>
<thead>
<tr>
<th>Theorem</th>
<th>[Delzanno et al, CONCUR’10]</th>
</tr>
</thead>
<tbody>
<tr>
<td>REACH for Ad Hoc Networks is undecidable.</td>
<td></td>
</tr>
</tbody>
</table>
Undecidability result

Theorem [Delzanno et al, CONCUR’10]

REACH for Ad Hoc Networks is undecidable.

One way to regain decidability: restrict the considered graphs
Considered order on graphs

- Given \( \gamma \in \mathcal{C} \), \( G(\gamma) \) is the associated graph

### Induced subgraph relation

Given \( \gamma_1, \gamma_2 \in \mathcal{C} \), \( \gamma_1 \preceq \gamma_2 \) if there exists a label preserving injection \( h \) from nodes of \( G(\gamma_1) \) to nodes of \( G(\gamma_2) \) s.t.:

- \((n, n')\) is an edge in \( G(\gamma_1) \) if and only if \((h(n), h(n'))\) is an edge in \( G(\gamma_2) \)

![Diagram](a-b-c-d.png)
Bounded path configurations

- $\mathcal{P}^K$: set of configurations $\gamma \in \mathcal{C}$ s.t. the length of the longest simple path in $G(\gamma)$ is smaller than $K$

---

**Theorem** [Ding, J. of Graph Theory’92]

For all $K \in \mathbb{N}$, $(\mathcal{P}^K, \preceq)$ is a well-quasi-ordering
Well structured transition systems everywhere

Monotonicity lemma

For \( \gamma_1, \gamma_1', \gamma_2 \in \mathcal{P}^K \), if

- \( \gamma_1 \Rightarrow \gamma_1' \) and \( \gamma_1 \preceq \gamma_2 \)

then there exists \( \gamma_2' \in \mathcal{P}^K \) s.t.

- \( \gamma_2 \Rightarrow \gamma_2' \) and \( \gamma_1' \preceq \gamma_2' \)

- AHN restricted to \( K \)-bounded path configurations are **Well Structured Transition Systems**

**Remark:**

- This is true with induced subgraph but not with subgraph (Node c broadcast a message received by node a and b)
Monotonicity lemma

For $\gamma_1, \gamma_1', \gamma_2 \in P^K$, if
- $\gamma_1 \Rightarrow \gamma_1'$ and $\gamma_1 \preceq \gamma_2$

then there exists $\gamma_2' \in P^K$ s.t.
- $\gamma_2 \Rightarrow \gamma_2'$ and $\gamma_1' \preceq \gamma_2'$

- AHN restricted to $K$-bounded path configurations are **Well Structured Transition Systems**

**Remark:**
- This is true with induced subgraph but not with subgraph (Node $c$ broadcast a message received by node $a$ and $b$)
Decidability result

**Theorem** [Delzanno et al., CONCUR’10]

$\text{REACH}$ is decidable for AHN restricted to $K$-bounded path configurations

**Idea of the proof**

- For $S \subseteq P^K$, $\text{pre}_K(S) = \{\gamma \in P^K \mid \gamma \Rightarrow \gamma' \land \gamma' \in S\}$
- if $S$ is upward-closed, then $\text{pre}_K(S)$ is upward closed
- let $\Gamma : P^K \mapsto P^K$ s.t. $\Gamma(S) = S \cup \text{pre}_K(S)$
- For $S$ upward-closed, there exists $i \in \mathbb{N}$ s.t. $\Gamma^{i+1}(S) = \Gamma^i(S)$ and given a finite basis $B$ of $S$, one can compute a finite basis $B'$ of $\Gamma^i(S)$
- Take for $S$ the graph with a single node labelled with $q$
Outline

1. Systems with broadcast communication
2. Ad Hoc Networks
3. Conclusion
## Conclusion

### Complexity result for \textsc{Reach} in parameterized networks

<table>
<thead>
<tr>
<th>Communication</th>
<th>Complexity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Broadcast</td>
<td>Ackermann-complete</td>
</tr>
<tr>
<td>Ad Hoc</td>
<td>Undecidable</td>
</tr>
<tr>
<td>Ad Hoc over $K$-bounded path configurations</td>
<td>Decidable</td>
</tr>
</tbody>
</table>