Compensation-Aware Runtime Monitoring

Christian Colombo[1], Gordon J. Pace[1], and Patrick Abela[2]

University of Malta[1], Ixaris Ltd[2]

November 3rd, 2010

Motivation

- Monitoring induces an overhead
- Various approaches have been taken to mitigate this issue
- Sometimes even a small overhead is unacceptable

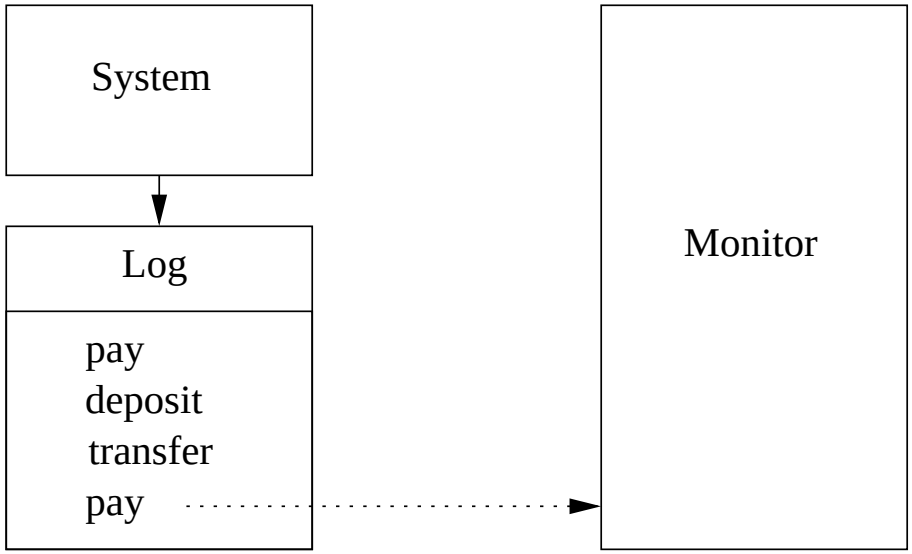
Dilemma

- Keeping system and monitor in synch
  - Slows down system
- Desynchronising the system from the monitor
  - Problems are detected late

Dilemma

- Keeping system and monitor in synch
  - Slows down system
- Desynchronising the system from the monitor
  - Problems are detected late
- Synchronise only when a problem is detected

Late Detection



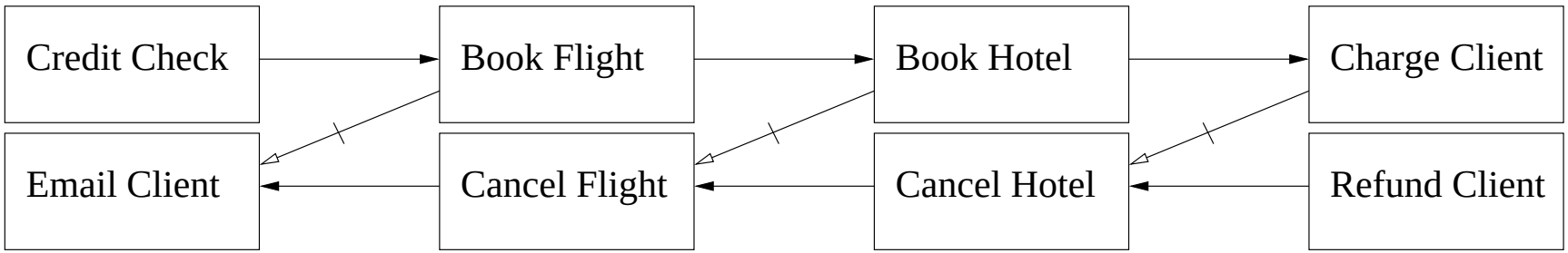
Synchronisation Technique

- In distributed games periodic synchronisation is required
- The game state of a player might have to be "reversed" to match the global state

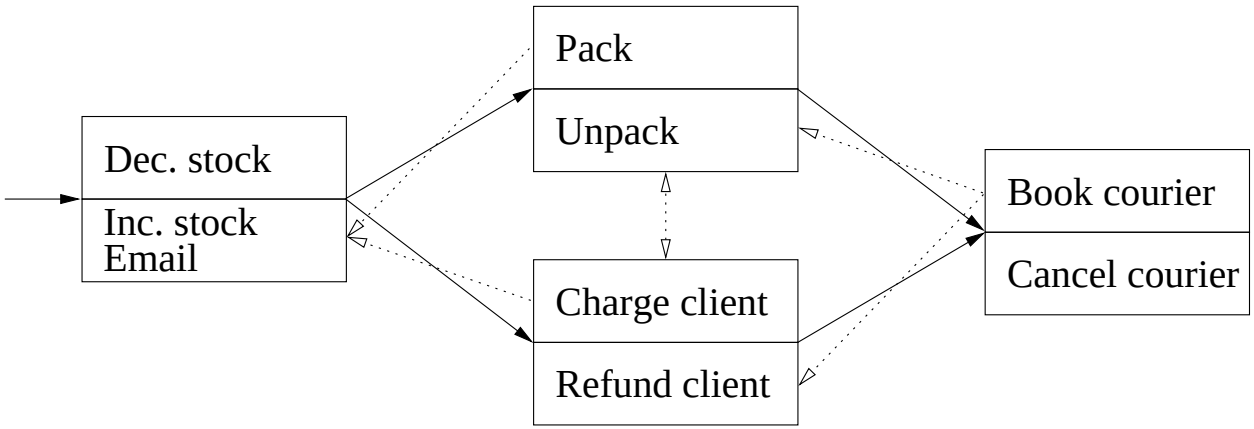
Synchronisation Technique

- In distributed games periodic synchronisation is required
- The game state of a player might have to be "reversed" to match the global state
- Compensations have been devised exactly for this purpose!

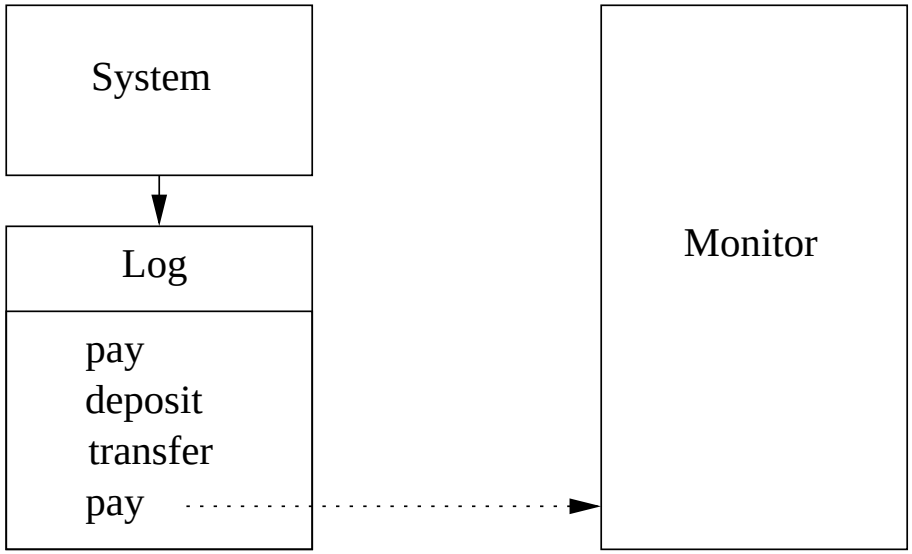
Reversing the State of a System



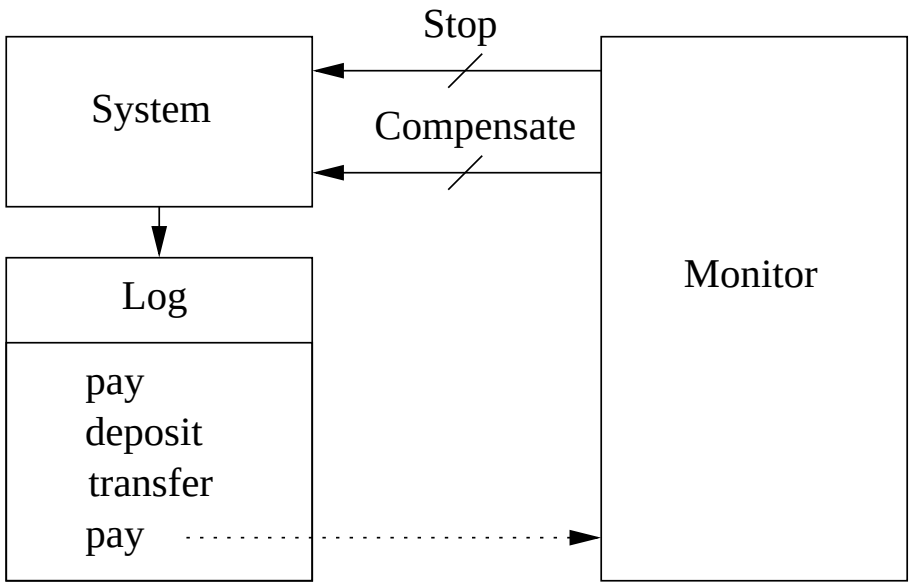
Reversing the State of a System



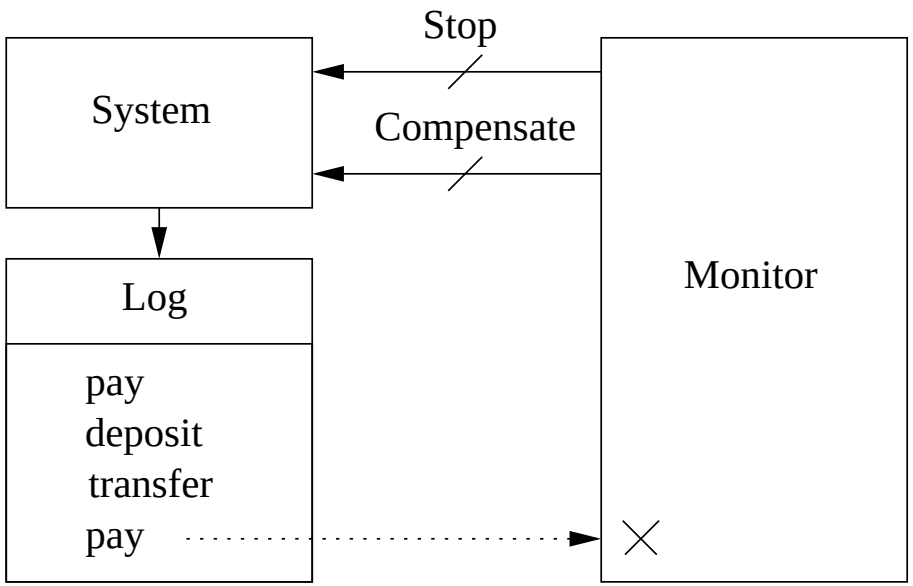
Offline Monitoring



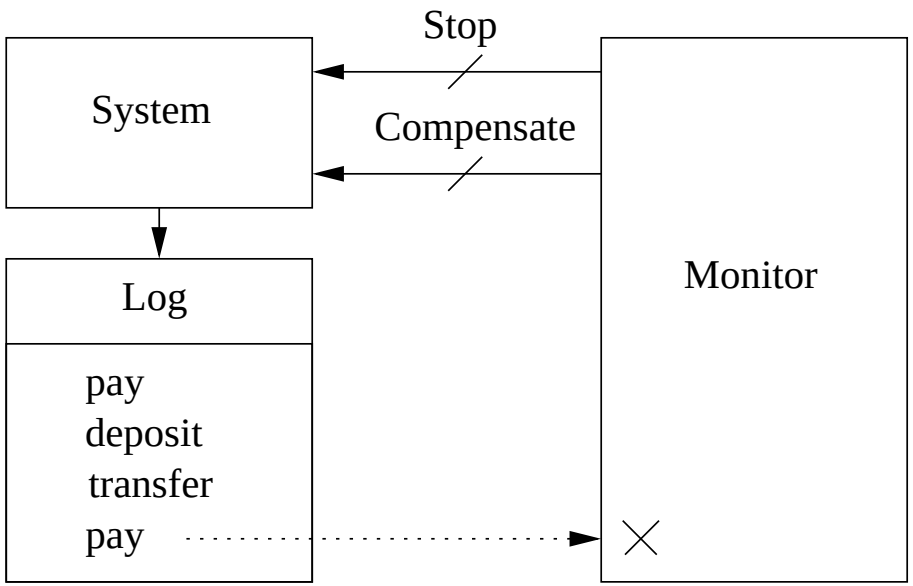
Asynchronous Monitoring with Synchronisation Capability



Asynchronous Monitoring with Synchronisation Capability



Asynchronous Monitoring with Synchronisation Capability



Upon error detection:

- Stop system
- Compensate for transfer, deposit, pay

Synchronous Monitoring

- System transition system: $\sigma \xrightarrow{a}_{sys} \sigma'$
- Monitor transition system: $m \xrightarrow{a}_{mon} m'$

Synchronous Monitoring

- System transition system: $\sigma \xrightarrow{a}_{sys} \sigma'$
- Monitor transition system: $m \xrightarrow{a}_{mon} m'$
- Stopped system state: $\odot$
- Broken monitor state: $\otimes$

Synchronous Monitoring

- System transition system: $\sigma \xrightarrow{a}_{sys} \sigma'$
- Monitor transition system: $m \xrightarrow{a}_{mon} m'$
- Stopped system state: $\odot$
- Broken monitor state: $\otimes$

$$\textsc{Sync}\ \frac{\sigma \xrightarrow{a}_{sys} \sigma',\ m \xrightarrow{a}_{mon} m'}{(\sigma, m) \xrightarrow{a}_{\|} (\sigma', m')}\ m \neq \otimes$$

$$\textsc{SyncErr}\ \frac{\sigma \xrightarrow{a}_{sys} \sigma',\ m \xrightarrow{a}_{mon} \otimes}{(\sigma, m) \xrightarrow{a}_{\|} (\odot, \otimes)}$$

Asynchronous Monitoring

$$\textsc{Async}_S \ \frac{\sigma \xrightarrow{a}_{sys} \sigma'}{(\sigma, w, m) \xrightarrow{a}_{|||} (\sigma', wa, m)}$$

$$\textsc{Async}_M \ \frac{m \xrightarrow{a}_{mon} m'}{(\sigma, aw, m) \xrightarrow{\tau}_{|||} (\sigma, w, m')}$$

$$\textsc{AsyncErr} \ \frac{}{(\sigma, w, \otimes) \xrightarrow{\tau}_{|||} (\odot, w, \otimes)} \ \sigma \neq \odot$$

Asynchronous Monitoring

$$\textsc{AsyncS}\ \frac{\sigma \xrightarrow{a}_{sys} \sigma'}{(\sigma, w, m) \xrightarrow{a}_{|||} (\sigma', wa, m)}$$

$$\textsc{AsyncM}\ \frac{m \xrightarrow{a}_{mon} m'}{(\sigma, aw, m) \xrightarrow{\tau}_{|||} (\sigma, w, m')}$$

$$\textsc{AsyncErr}\ \frac{}{(\sigma, w, \otimes) \xrightarrow{\tau}_{|||} (\odot, w, \otimes)}\ \sigma \neq \odot$$

$$\textsc{Comp}\ \frac{}{(\odot, wa, \otimes) \xrightarrow{\overline{a}}_{C} (\odot, w, \otimes)}$$

Soundness of Compensation-Based Approach

- The system and the monitor running asynchronously with compensations for synchronisation

exhibits the same behaviour as

- The system running in synch with the monitor

Soundness of Compensation-Based Approach

- The system and the monitor running asynchronously with compensations for synchronisation

exhibits the same behaviour as

- The system running in synch with the monitor

- $a\ b\ c\ d\ e\ f\ x\ h\ i\ j\ \bar{j}\ \bar{i}\ \bar{h}$

is the same as

- $a\ b\ c\ d\ e\ f\ x$

Soundness of Compensation-Based Approach

- The system and the monitor running asynchronously with compensations for synchronisation

exhibits the same behaviour as

- The system running in synch with the monitor

- $a\ b\ c\ d\ e\ f\ x\ h\ i\ \bar{i}\ \bar{h}$

is the same as

- $a\ b\ c\ d\ e\ f\ x$

Soundness of Compensation-Based Approach

- The system and the monitor running asynchronously with compensations for synchronisation

exhibits the same behaviour as

- The system running in synch with the monitor

- $a\, b\, c\, d\, e\, f\, x\, h\, \bar{h}$

is the same as

- $a\, b\, c\, d\, e\, f\, x$

Soundness of Compensation-Based Approach

- The system and the monitor running asynchronously with compensations for synchronisation

exhibits the same behaviour as

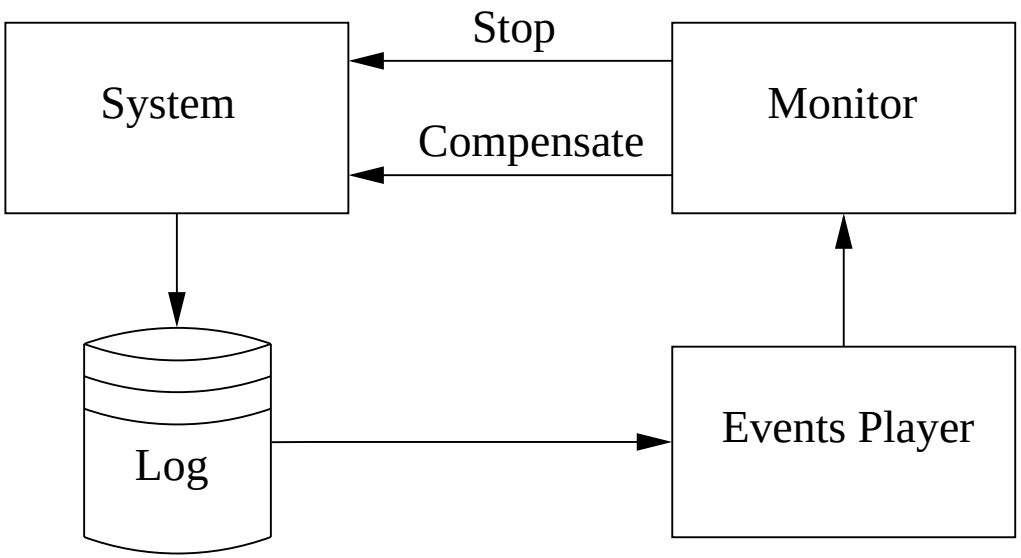
- The system running in synch with the monitor

- $a\ b\ c\ d\ e\ f\ x$

is the same as

- $a\ b\ c\ d\ e\ f\ x$

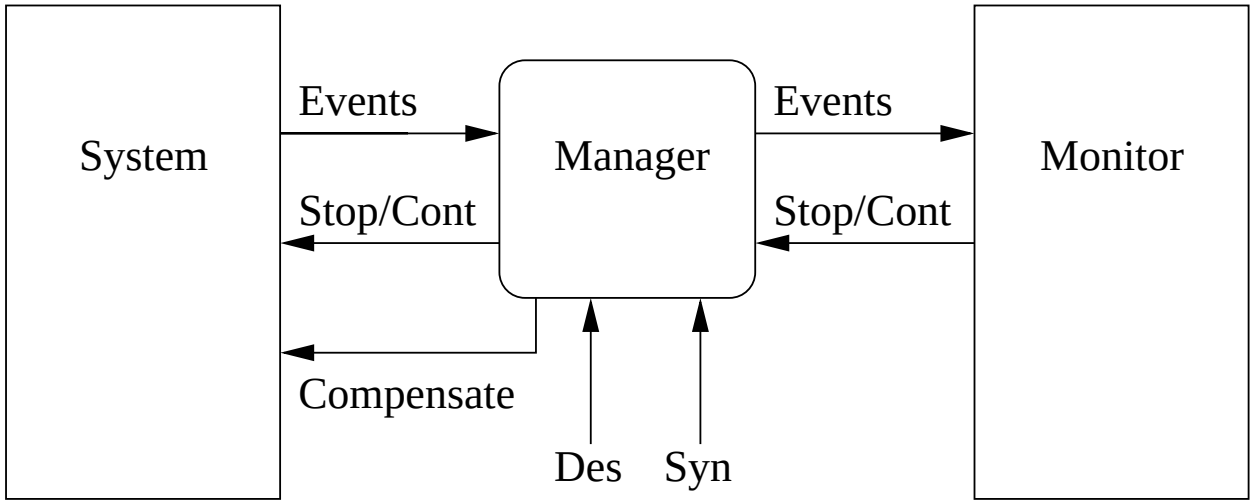
Architecture 1



Architecture 2

```
c = ok                          ;set default control to ok
while (c != stop)
  if (synch_mode)
    e = in_event()              ;read event from system
    c = out_event(e)            ;forward to monitor and get its resulting state
    out_control(c)              ;relay control to system
  else
    par                         ;parallel execution
      e1 = in_event()           ;read from system
      addToBuffer(e1)           ;store in buffer
      out_control(c)            ;return control to system
    with
      e2 = readFromBuffer()     ;read from buffer
      c = out_event(e2)         ;forward to monitor and get its resulting state
end
```

Architecture 3

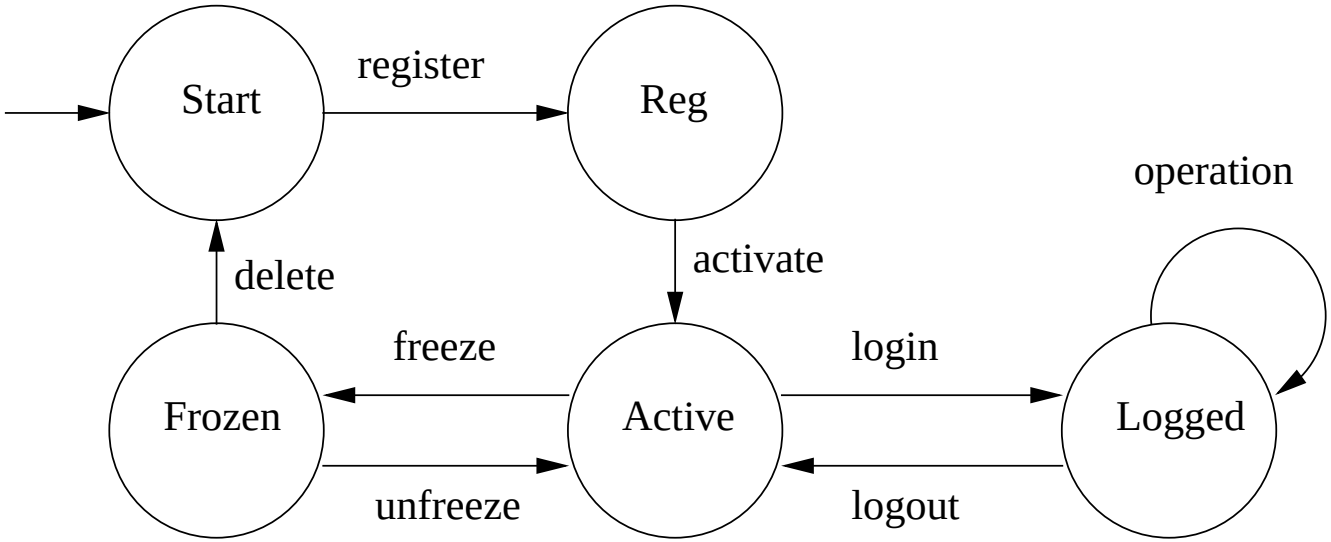


Case Study

- Life cycle properties
- Real-time properties
- Rights
- Amounts

Case Study

- Life cycle properties
- Real-time properties
- Rights
- Amounts



Conclusions

- The use of compensations to synchronise a system with its monitor
- A theory showing that monitoring asynchronously with compensation synchronisation produces the same observed behaviour as synchronous monitoring
- An architecture supporting monitor desynchronisation and resynchronisation
- The application of the architecture to an industrial case study

Future Directions

- Heuristics for deciding when to desynchronise and resynchronise
- Support a more sophisticated structure of compensations rather than the simplistic approach of having a compensation for each action

Questions