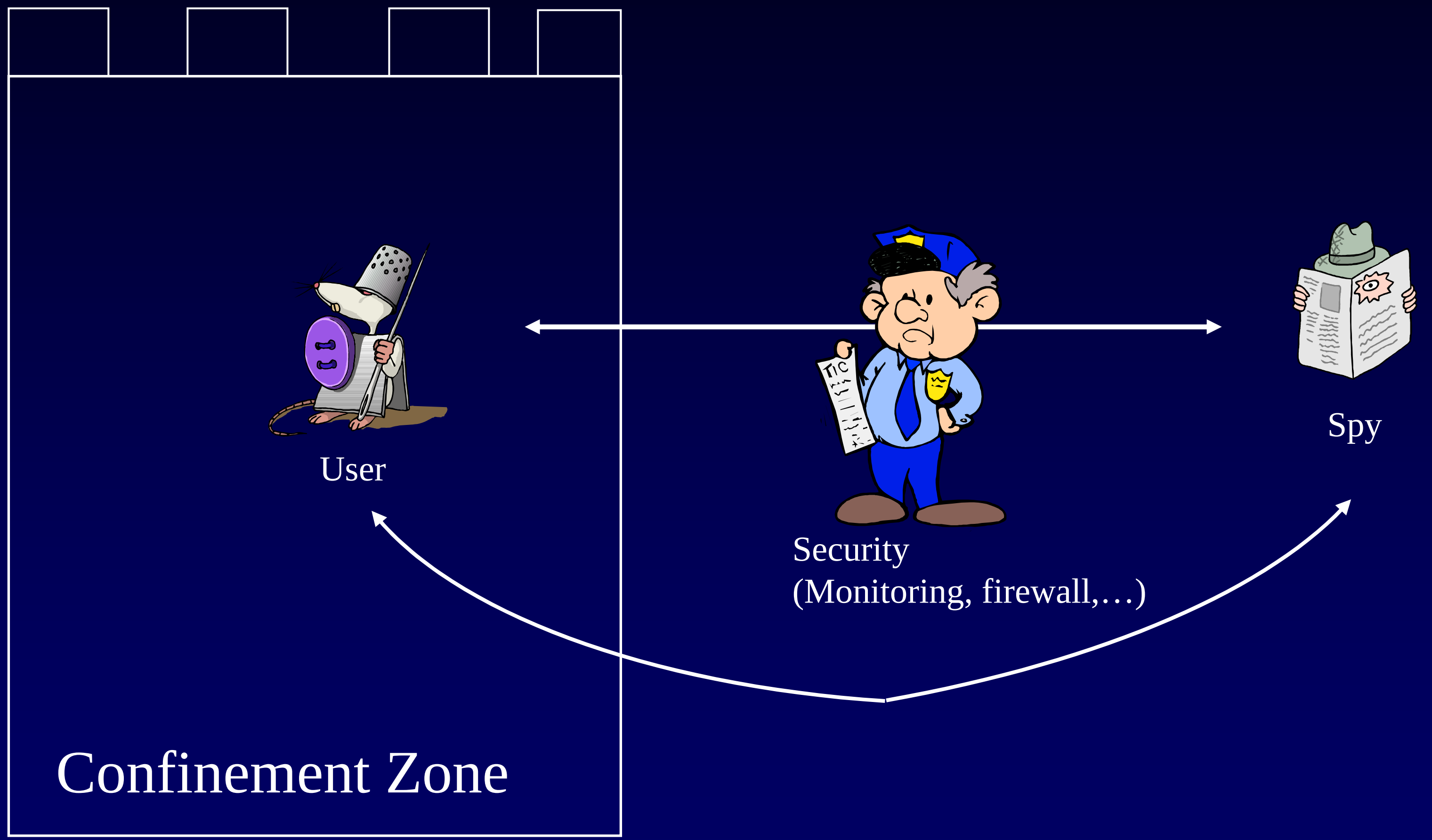
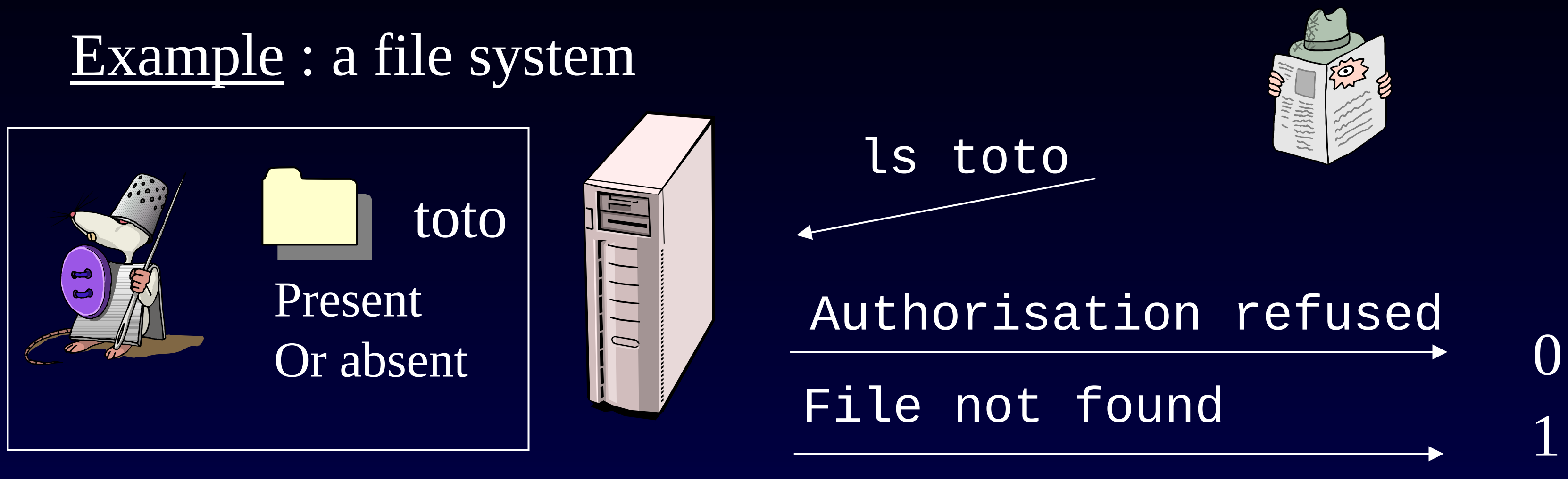
Covert channels detection : using games with scenarios

Loïc Hélouët	INRIA Rennes
Marc Zeitoun	LIAFA
Aldric Degorre	ENS Cachan

Motivations



Example : a file system



- threat : performance, billing, security, …
- all channels can not be eliminated

Recommendations:

- Identify covert channels
- Illustrate their use through scenarios
- Compute their bandwidth

Non interference

Current trend : Covert channels defined as an interference property

- a model S of a system
- two models of processes U,V that should not communicate

show that $(U \parallel S) \parallel V \neq S \parallel V$

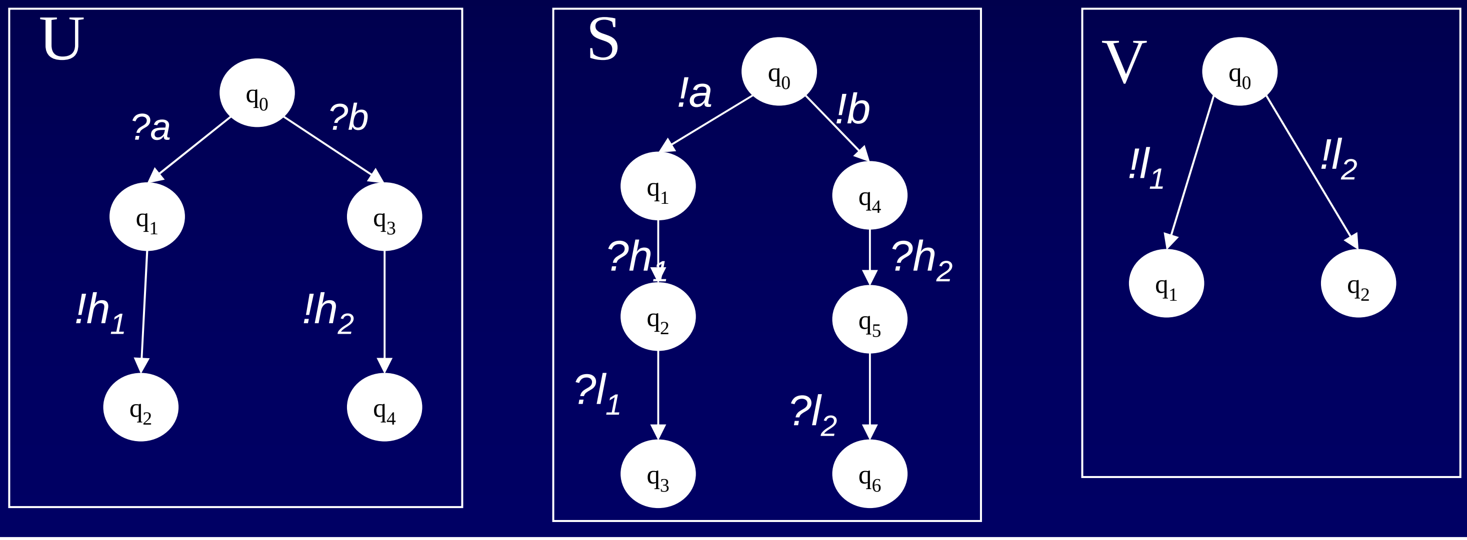
« what U does affects what V sees or can do »

Reachability problem

No liveness …

Models

- Automata or algebras
- Synchronous communications
- Does not consider causality

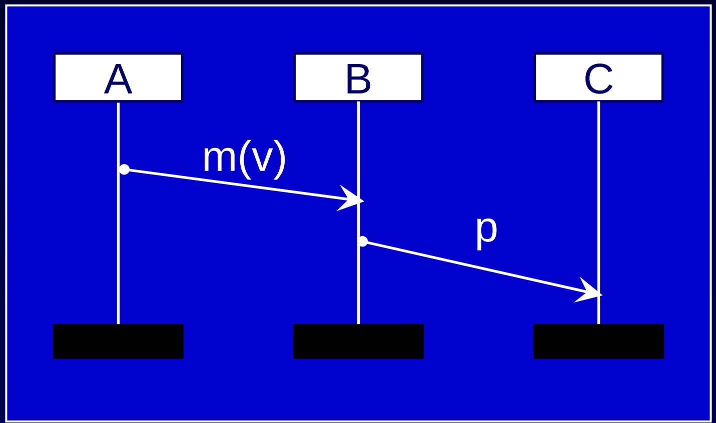


PLAN

- Message Sequence Charts
- Games
- Covert Channels as a game ?
- Conclusions & perspectives

Message Sequence Charts

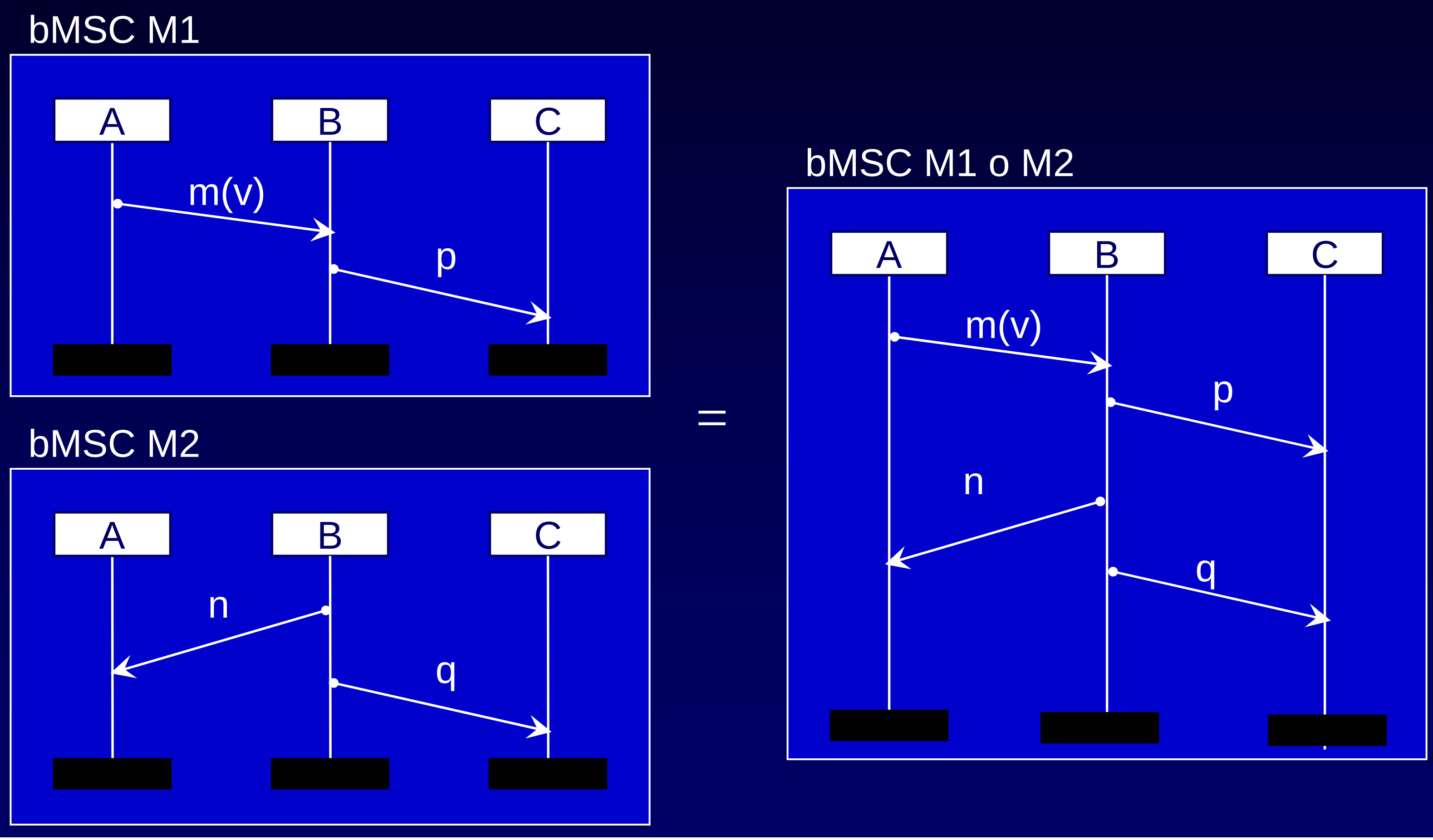
bMSC M



$M = < E, \leq, Act, P, \alpha , \varphi , m >$

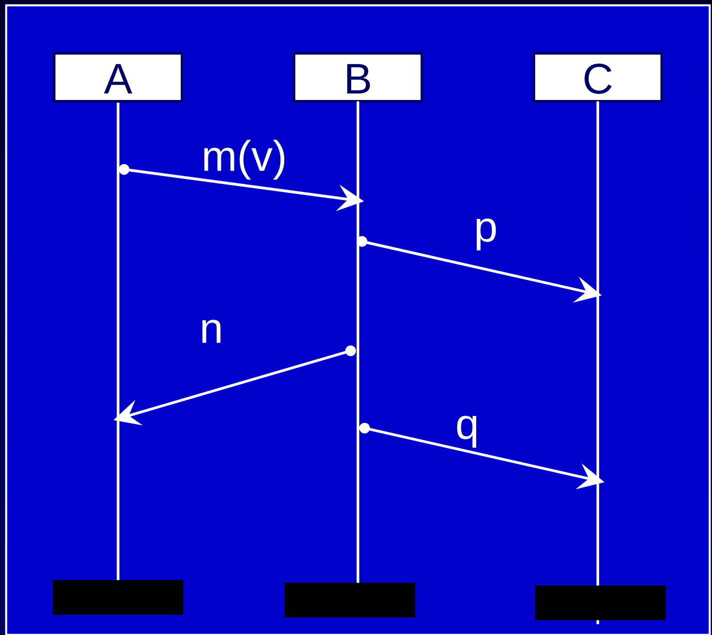
- E : events
- $\leq \subseteq E \times E$: causal order
- Act : action names
- P : Instances
- $\varphi : E \rightarrow P$: locality
- $\alpha : E \rightarrow Act$: labeling
- $m \subseteq E \times E$: messages

Sequential composition

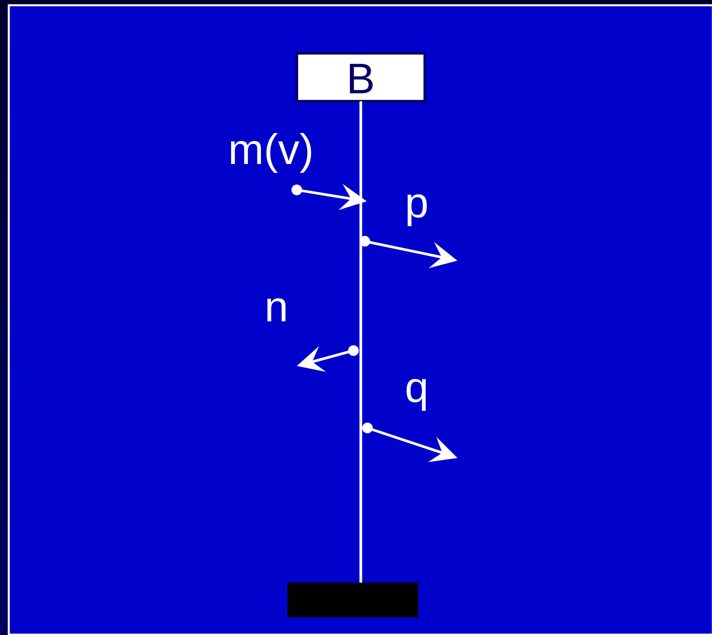


Projection

bMSC M

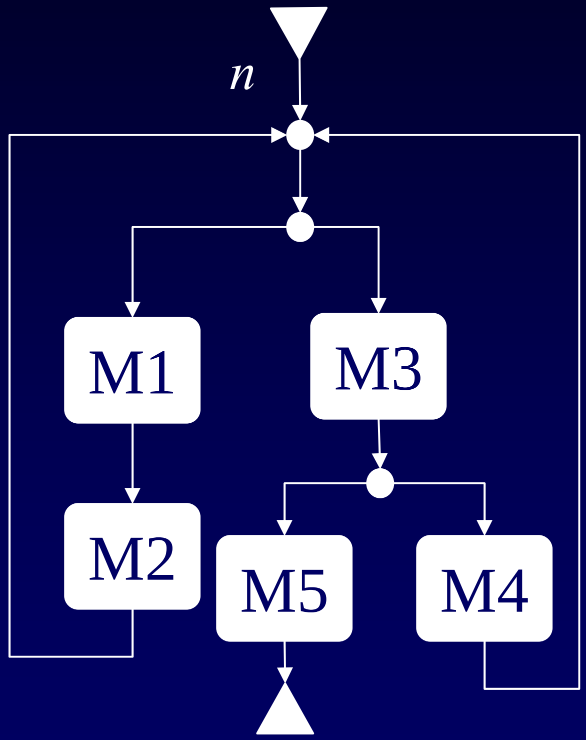


bMSC $\pi_B(M)$



$$\pi_B(M) = \{\ ?m(v)\ .\ !p\ .\ !n\ .\ !q\ \}$$

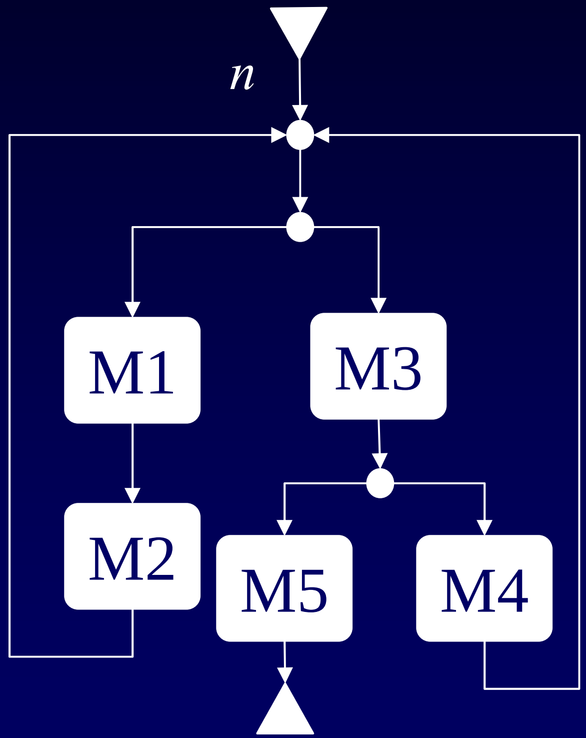
HMSC



$$H = (N, \rightarrow, \mathcal{M}, n_0)$$

- N : nodes
- $\rightarrow \subseteq N \times \mathcal{M} \times N$: transitions
- $\mathcal{M}$: bMSCs
- n_0 : initial node

HMSC



<u>Paths :</u>

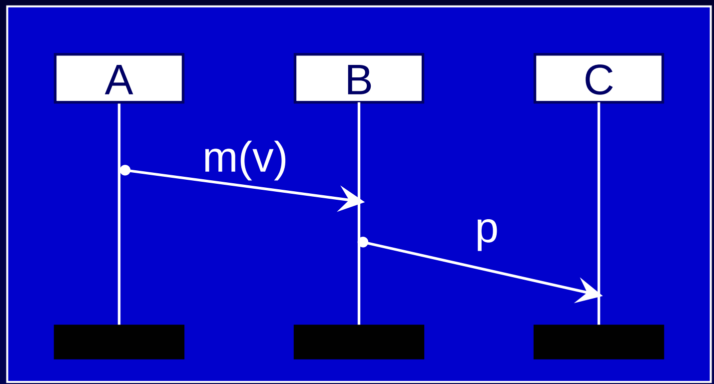
$p=(n_1,M_1,n_2).\ (n_2,M_2,n_3)\ \ldots\ (n_k,M_k,n_{k+1})$

Associated orders :

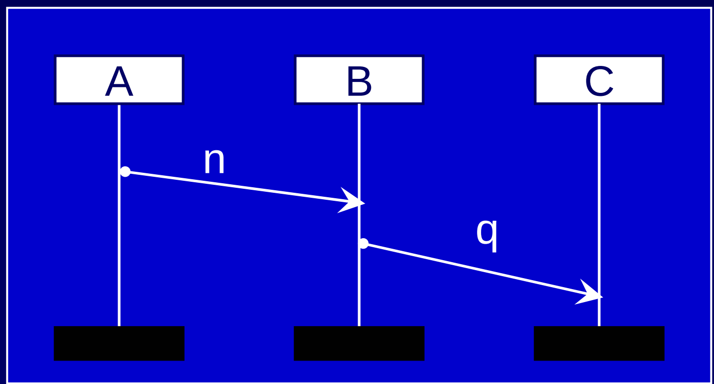
$O_p= M_1 \text{ o } M_2 \text{ o } \ldots \text{ o } M_k$

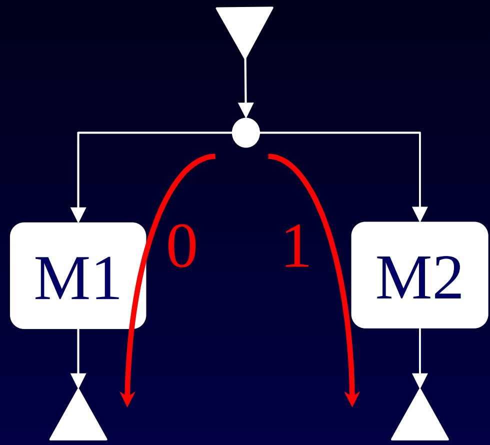
Choices

bMSC M1



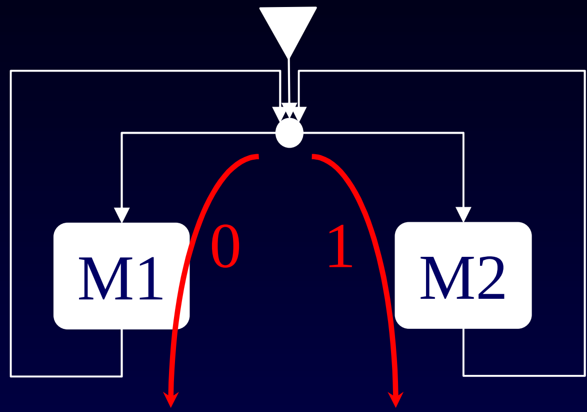
bMSC M2



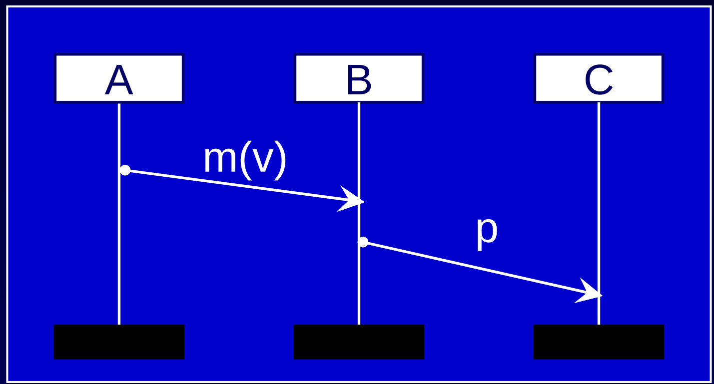


Events observed on instance C		events executed on instance A
?p	=>	!m(v)
?q	=>	!n

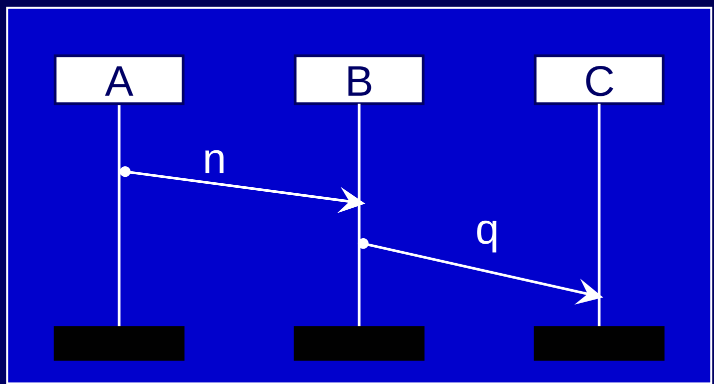
A simple way to pass info …



bMSC M1

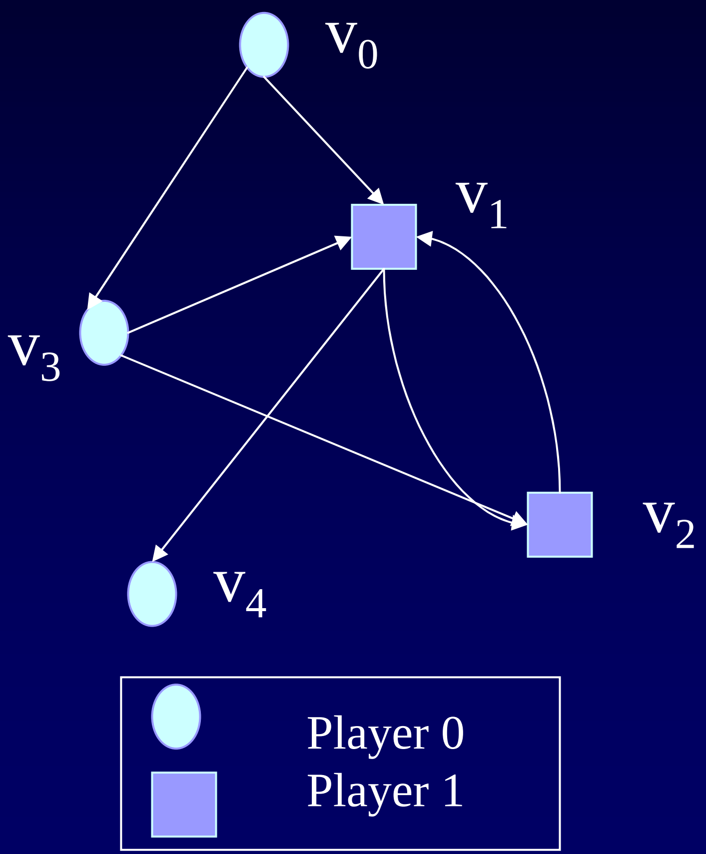


bMSC M2



More elaborated encoding strategies ?

Games



<u>Arena</u> :

Vertices V

Edges E

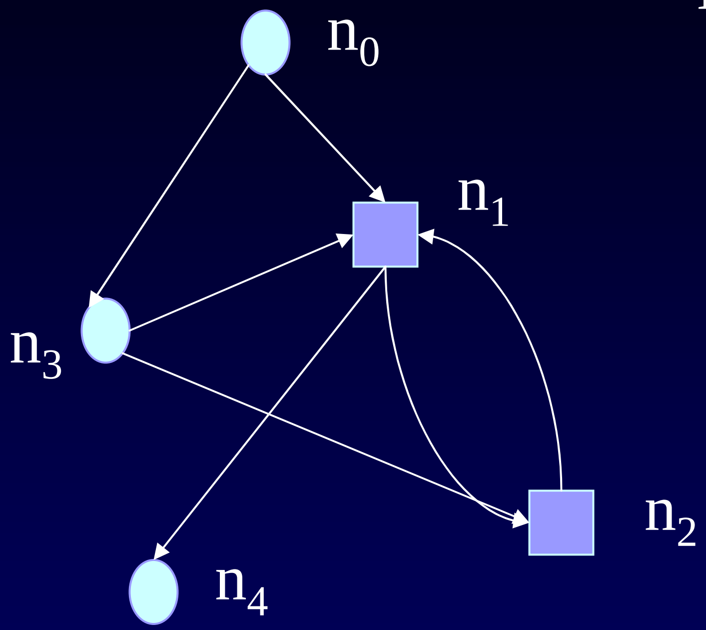
2 players : $\sigma = \{ 0,1 \}$

<u>Winning conditions</u> :

$Win \in \mathcal{P}(V)$ *(Buchi Game)*

$Win \subseteq \mathcal{P}(V)$ *(Muller Game)*

…



Play :

<u>finite :</u>

$v = v_{i1}.v_{i2} \ldots v_{ik}$ where v_{ik} sink node

<u>infinite :</u>

$w = v_{j1}.v_{j2} \ldots \in V^\omega$

$\color{red}{Inf(w)}$ $=\{v \mid \} \forall i, \exists j > i , v_j=v\}$

Player *0* wins a play *v* iff

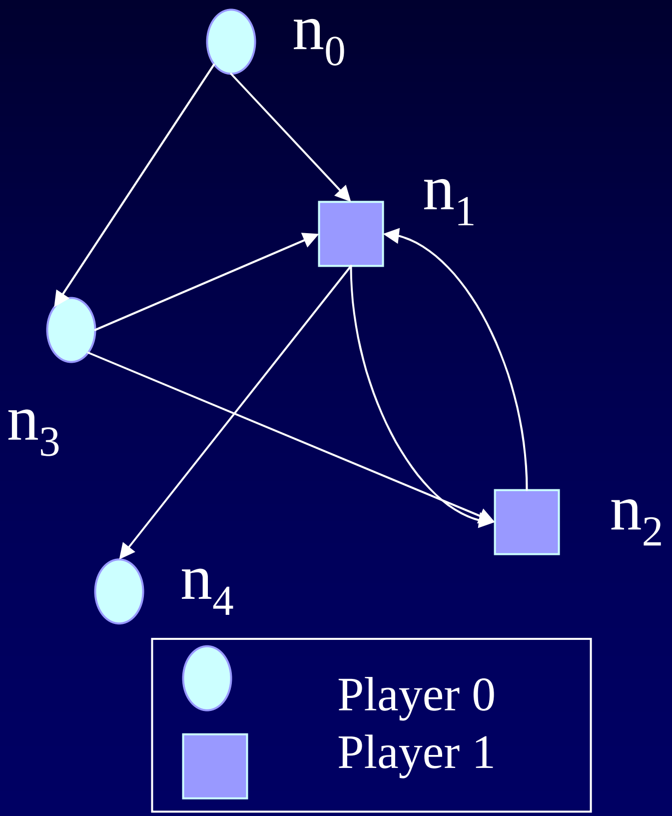
$v = n_{i1}.n_{i1} \ldots n_{ik}$ finite and P_1's turn

or $w = n_{j1}.n_{j2} \ldots \in V^\omega$

and $Inf(w) \cap Win \neq \emptyset$ *(Büchi)*

$Inf(w) \in Win$ *(Muller)*

Strategy



Function $f : V' \subseteq V \rightarrow \mathcal{P}(E)$

Win = $\{n_{1,} n_2\}$

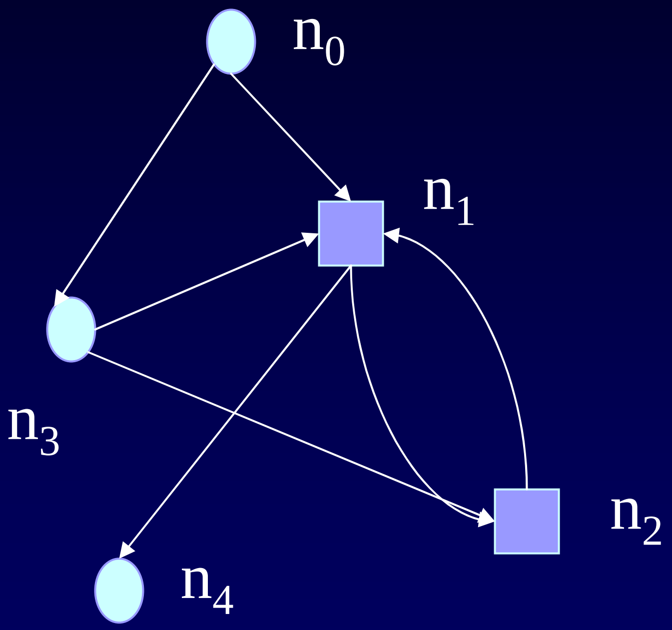
Strategy for P_1 :

$n_1 \rightarrow \{ (n_{1,} n_2) \}$

$n_2 \rightarrow \{ (n_{2,} n_1) \}$

Winning subset for P_σ:

subset for which a strategy for P_σ exists



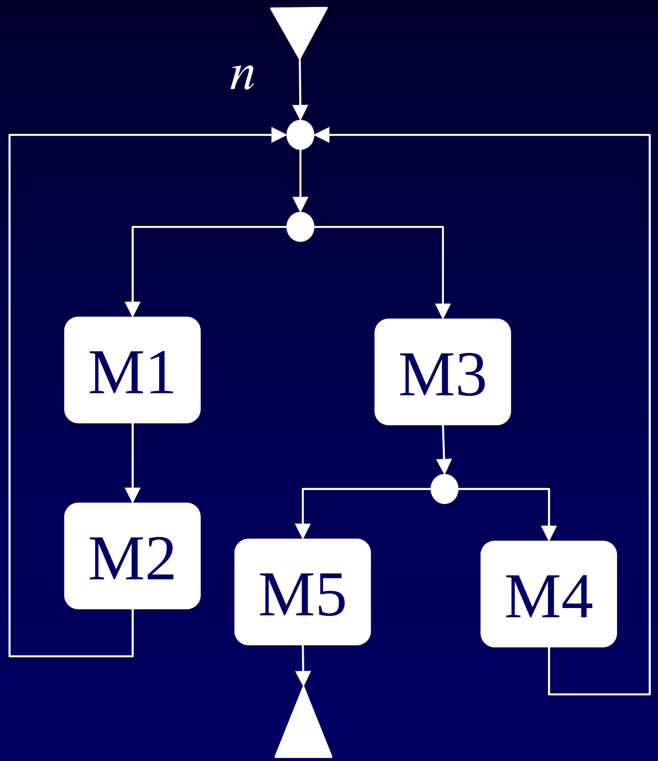
Games :

- Several problems resume to the Existence of a strategy for a given game

- Existing algorithms

- Solutions with complexity

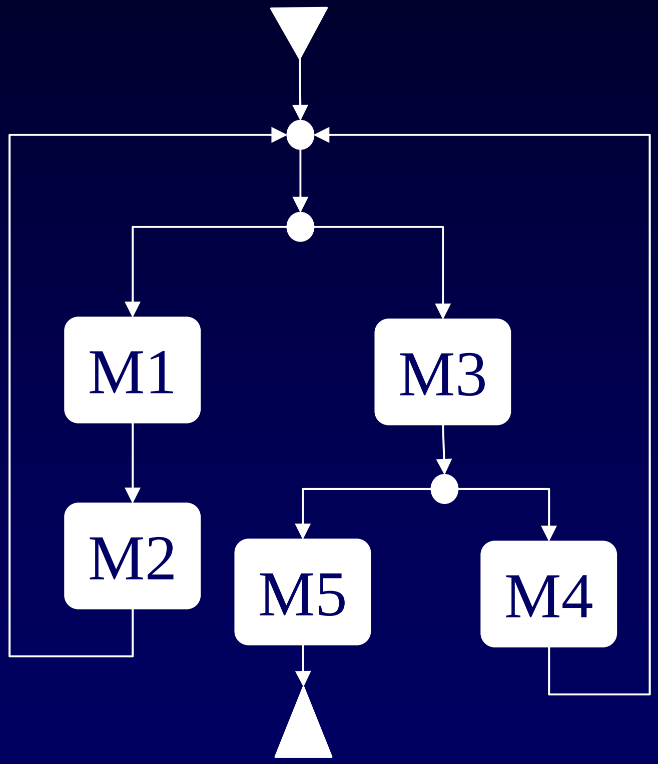
Covert Channel detection



Hypothesis :

To transmit a message of arbitrary length, one needs to iterate some behaviors :

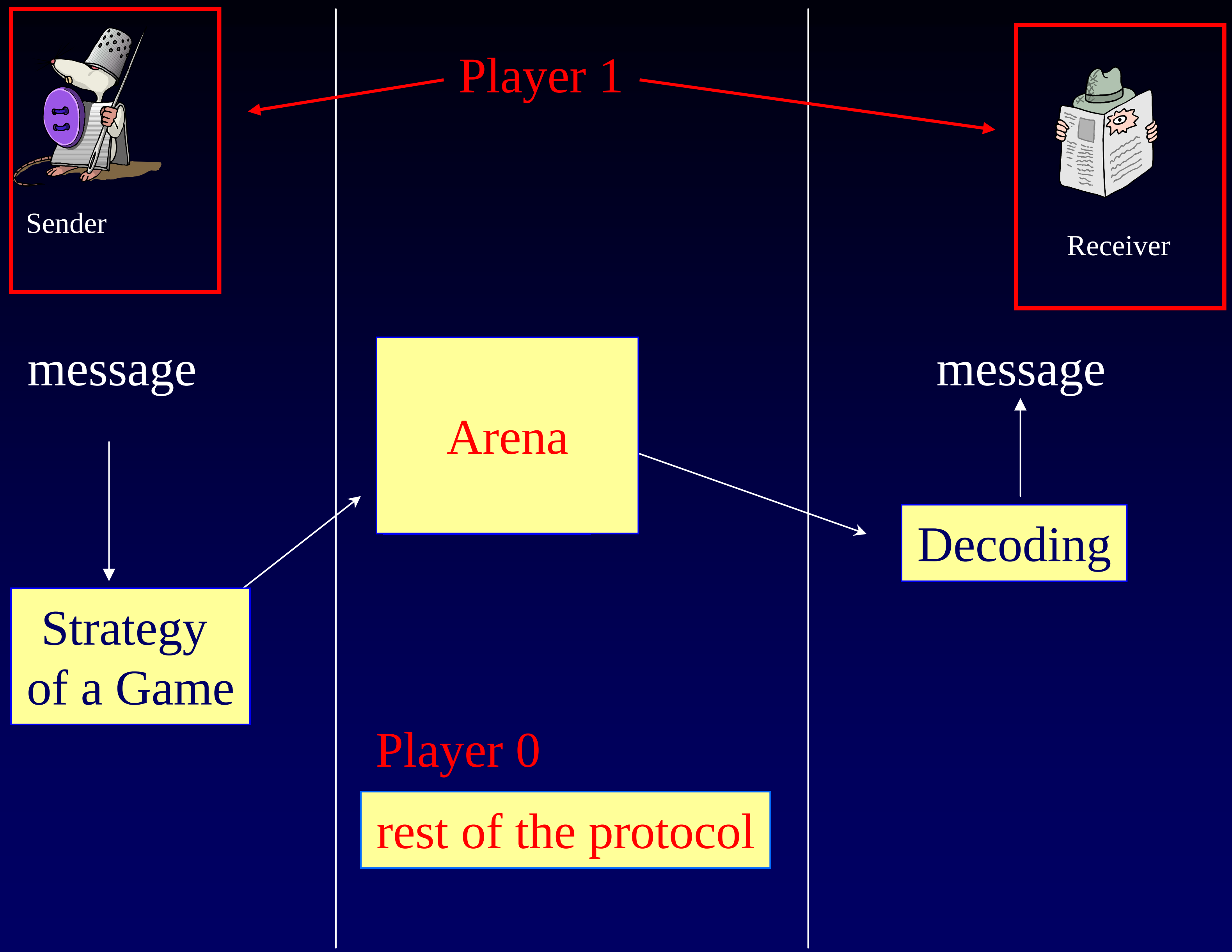
Covert channels only appear in presence of strongly connected components.



Consider a covert channel as a game
where a pair Sender/Receiver wins if they
can transmit messages of unbounded size

- Stay in strongly connected components
- must be able to transmit information

Construction of an arena

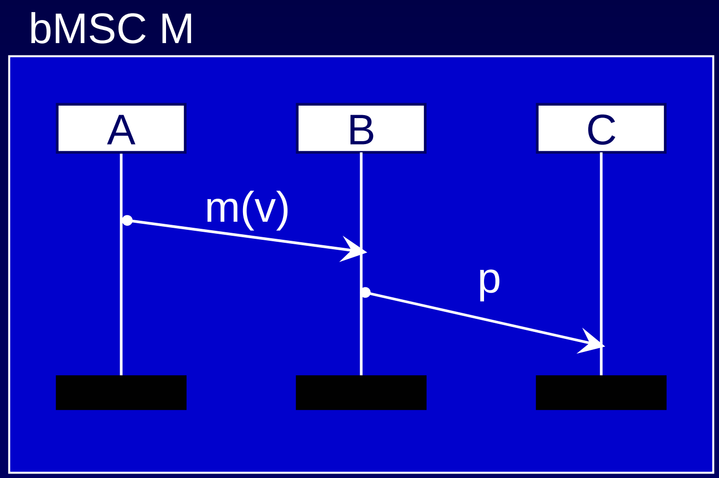

Player 1
Sender
Receiver
message
Arena
message
Decoding
Strategy of a Game
Player 0
rest of the protocol

STEP 1 : Find encoding nodes

Definition :

A bMSC *M* is controlled by an instance *p* iff $\exists!\ e = min(M)$ et $\varphi(e) = p$

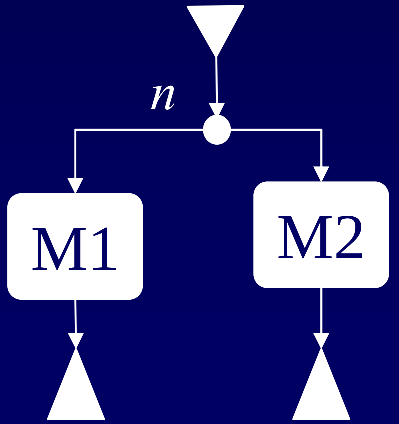
M controlled by *A*



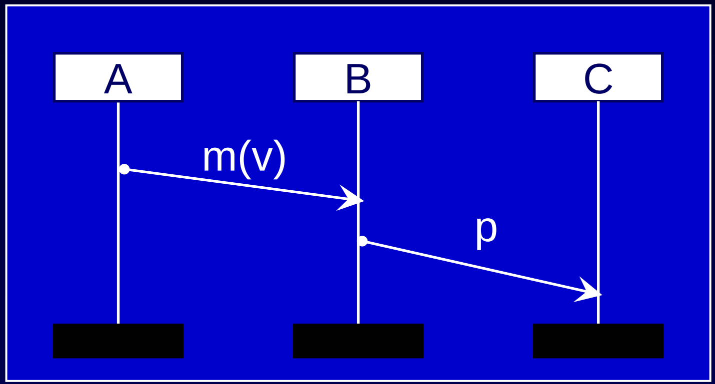
Definition :

A choice node n in a HMSC is controlled by an instance p iff for all path P_i, $i \in 1..K$ starting in n O_{P_i} controlled by p

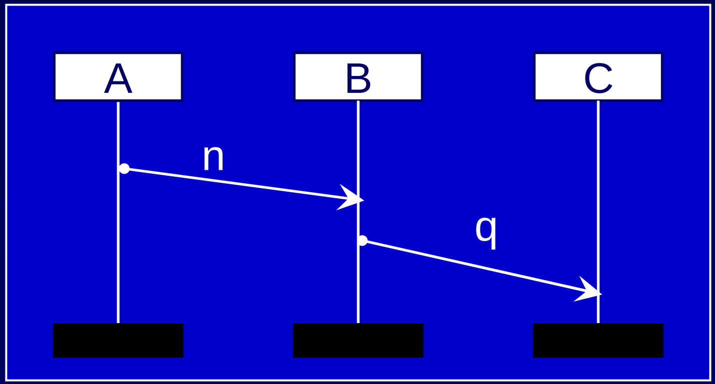
(idem local choice)



bMSC M1

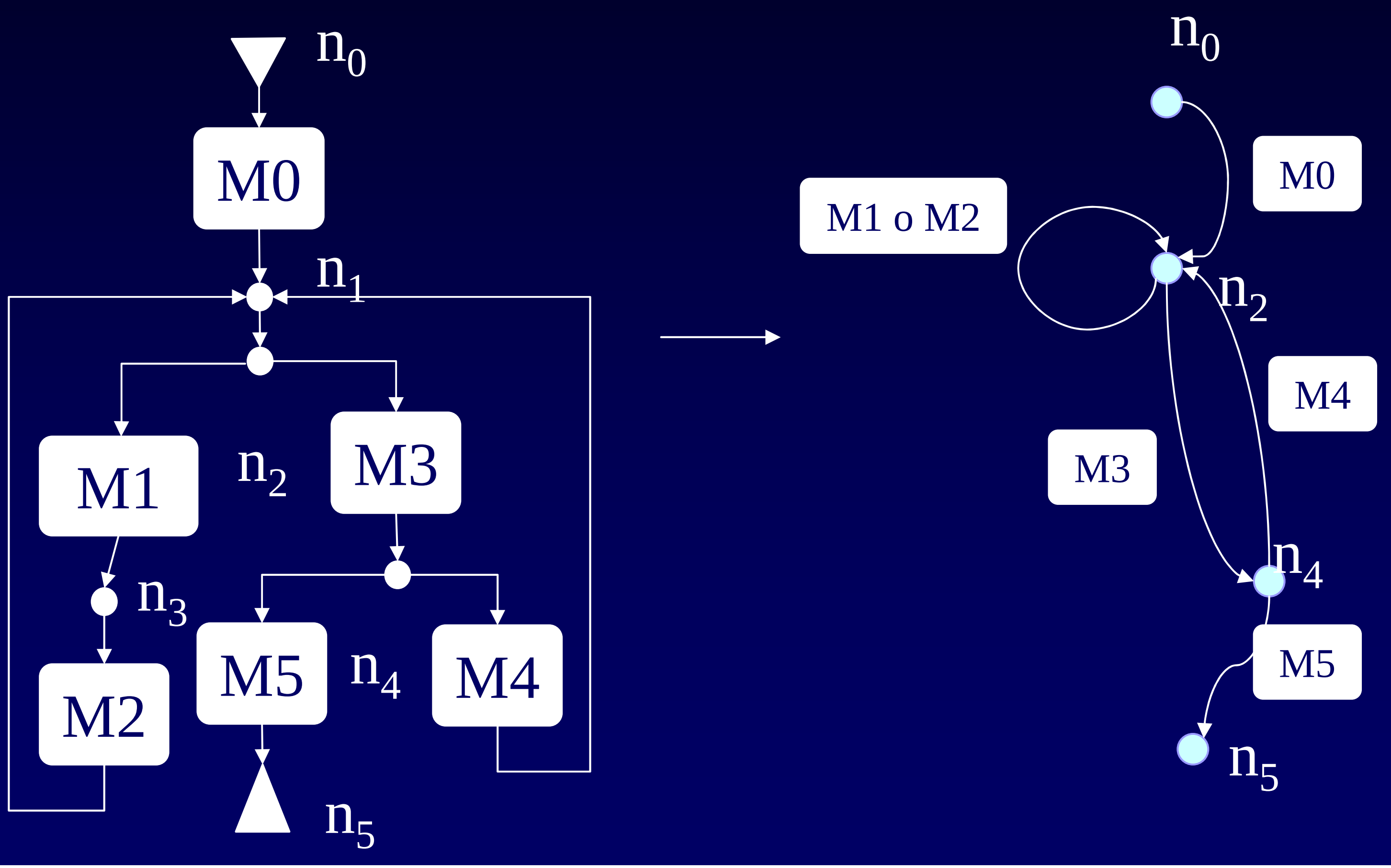


bMSC M2

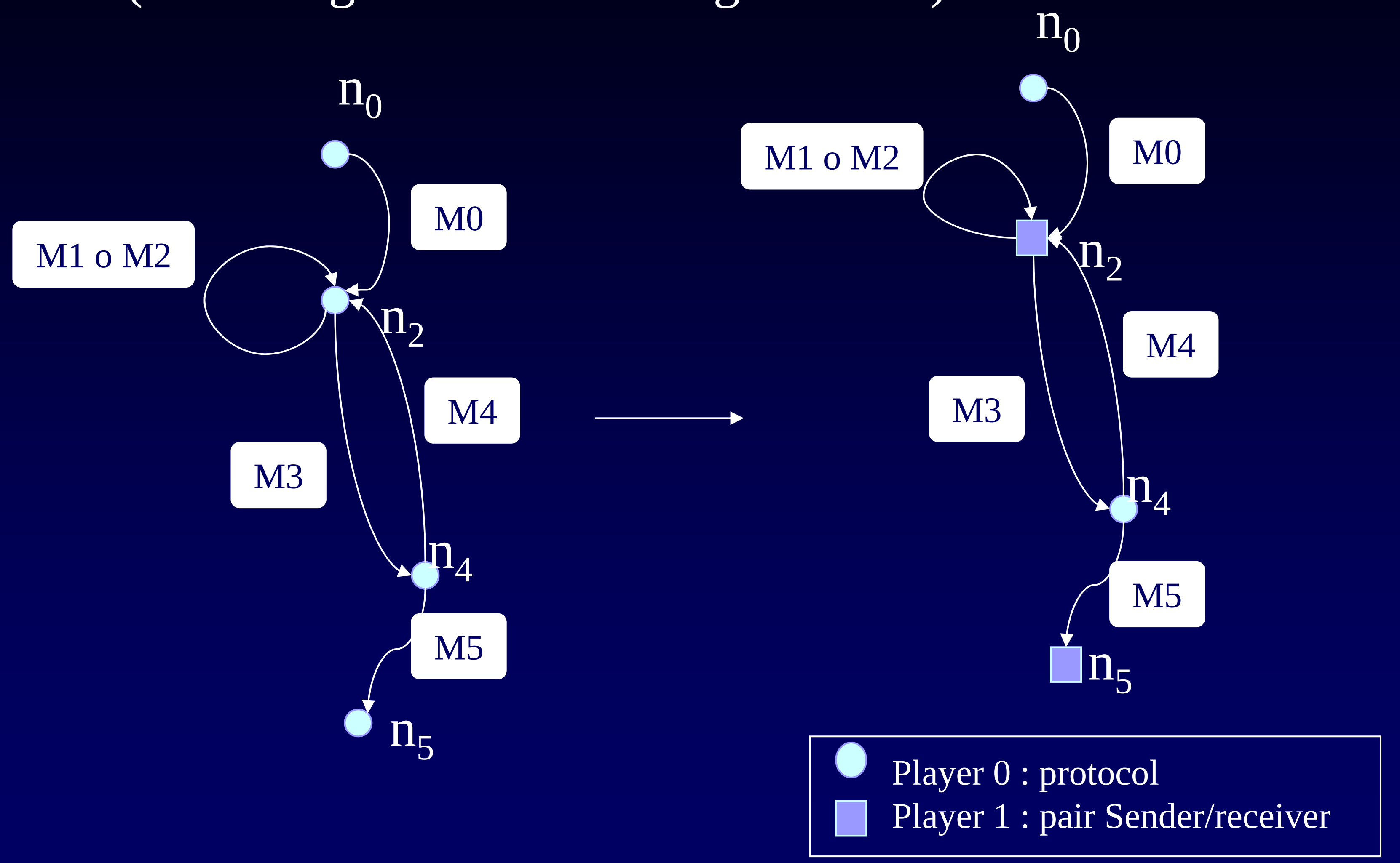


Reduction of a HMSC to an Arena

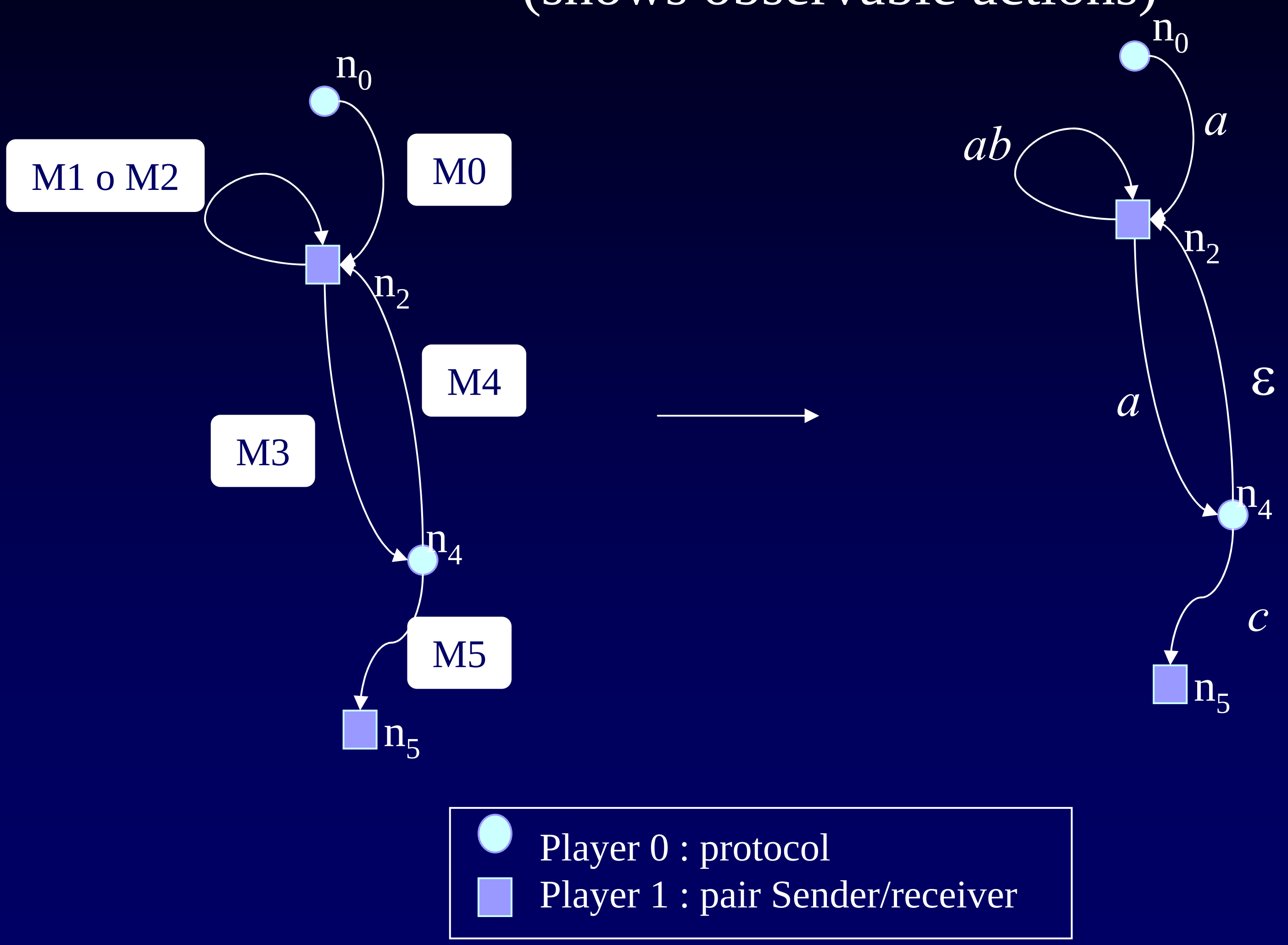
Step 1.1 : consider choice nodes only:



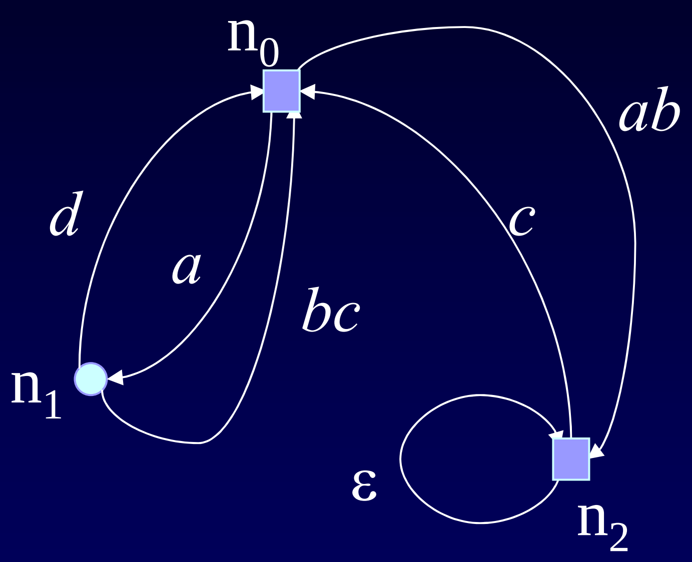
Step 1.2 : chose a sender and a receiver – assign nodes to a player (according to the controlling instance)



Step 1.3 : Project MSCs on receiver's instance (shows observable actions)



Property A : Ambiguity



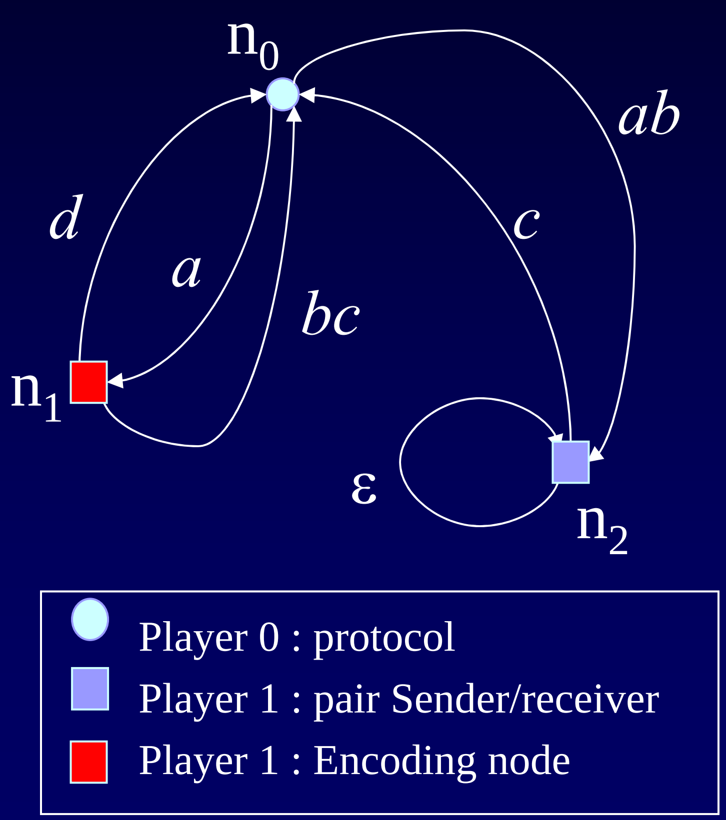
$D=\{n_0 ; n_1 ; n_2 \}$
$A(D,n_0)$
$A(D,n_1)$
$A(D,n_2)$

D strongly connected component

A(D,n) iff :
n not controlled by *sender*
or
n controlled by *sender* and
$\forall t_1,t_2,\ t_1=(n,b,n_1') \ t_2=(n,b,n_1')$

paths starting with
t_1 or t_2 cannot be reliably differentiated
by the receiver.

Encoding nodes



$D=\{n_0 ; n_1 ; n_2\}$

$A(D,n_0)$

(not controlled by sender)

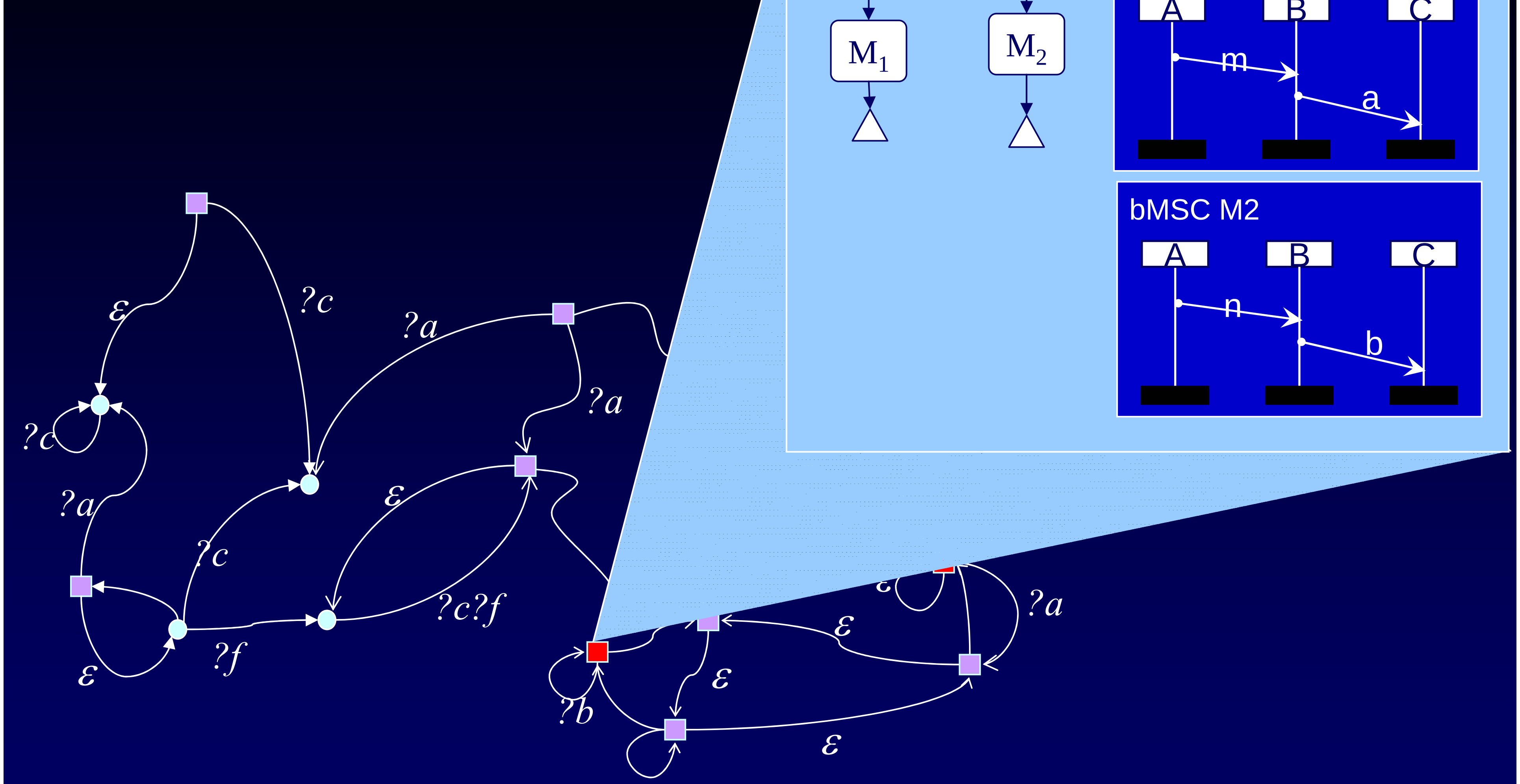
$\neg A(D,n_1)$

(two different observable choices)

$A(D,n_2)$

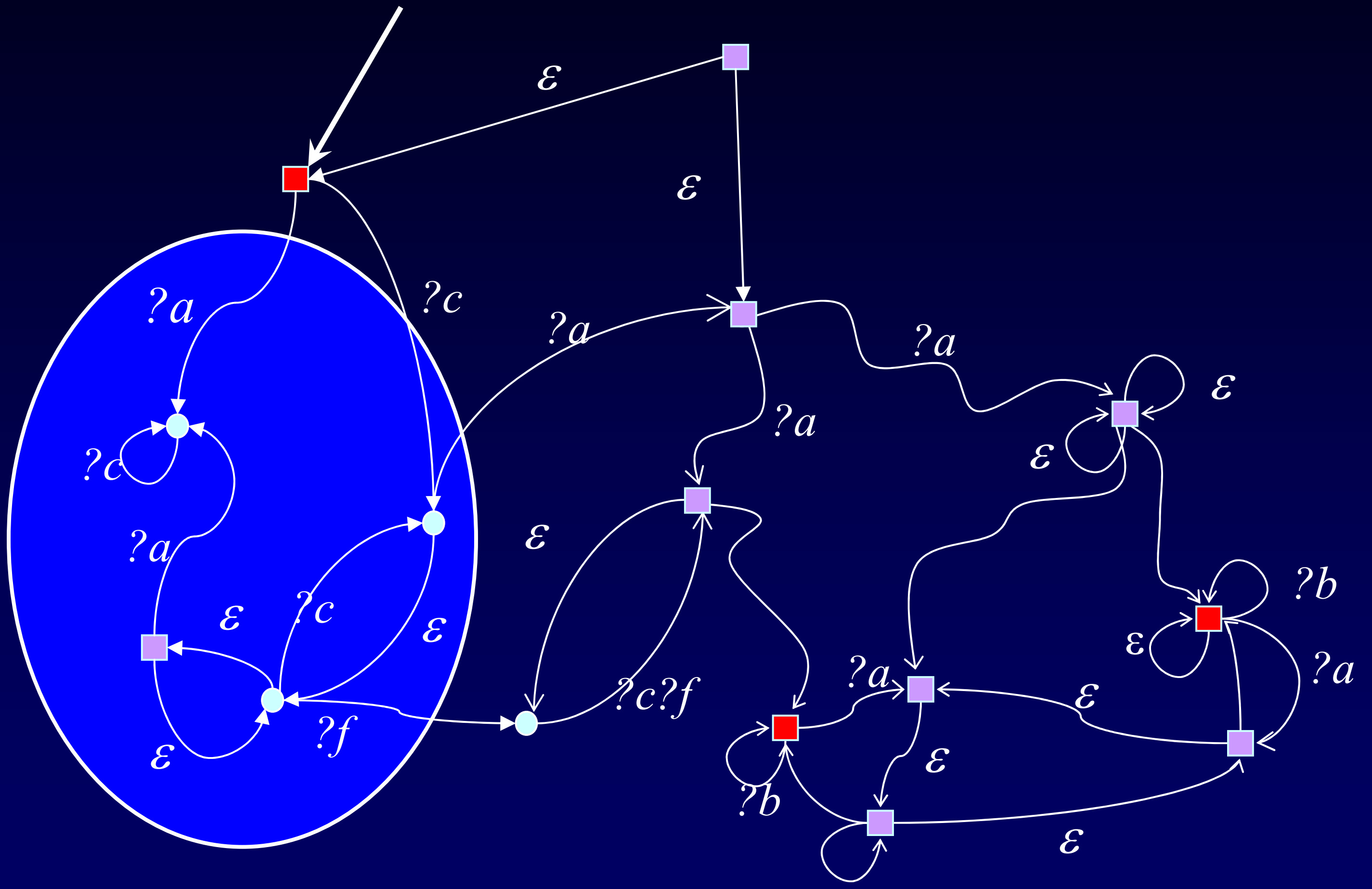
(a single observable choice: *c*)

Step 1 : identify interference places

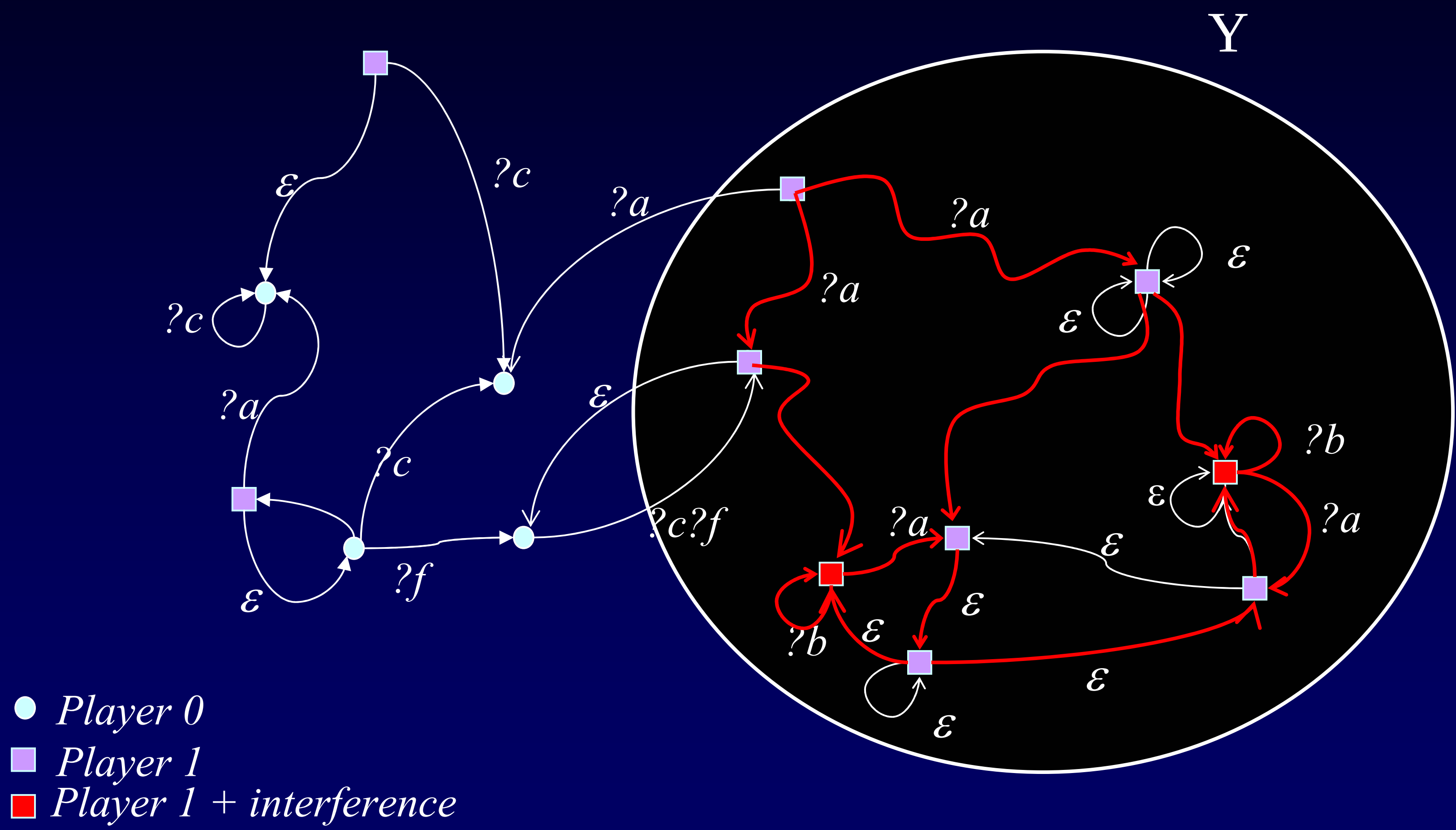


Interference places : no liveness !

(is it really a covert channel ?)



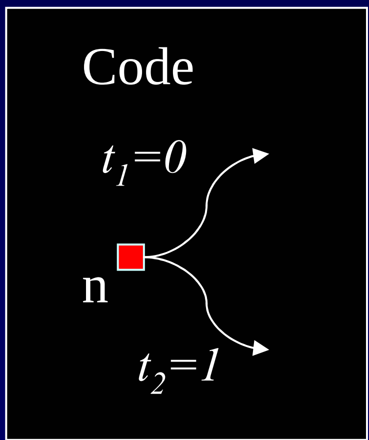
Step 2 : Search a winning subset Y in which
player 1 has a winning strategy f_Y to pass infinitely often through red
Vertices while producing observable events



When Y and f_Y exist

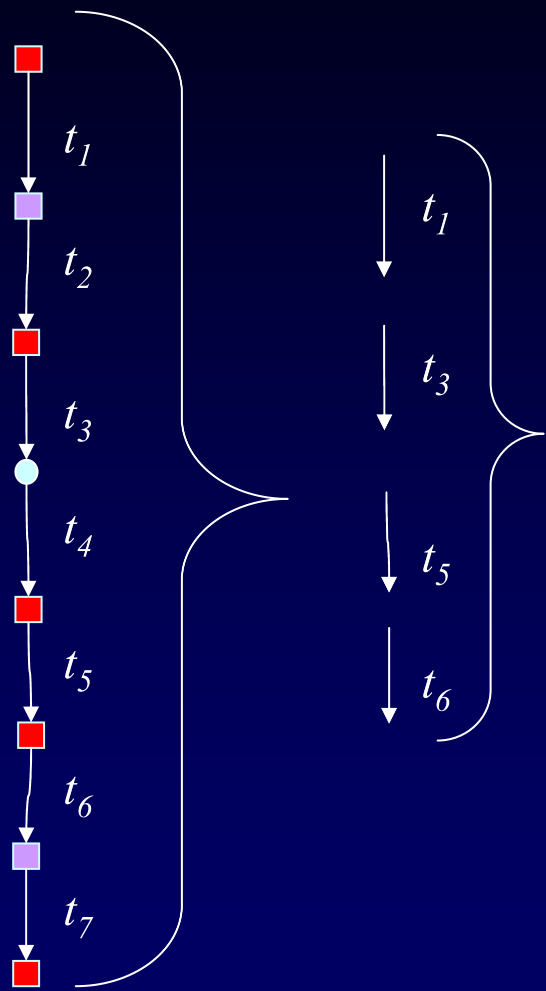
Receiver's Observation

?a
?b
!e
?f
?b
?a
?f
?f
!x
?c
?d
?e



Execution

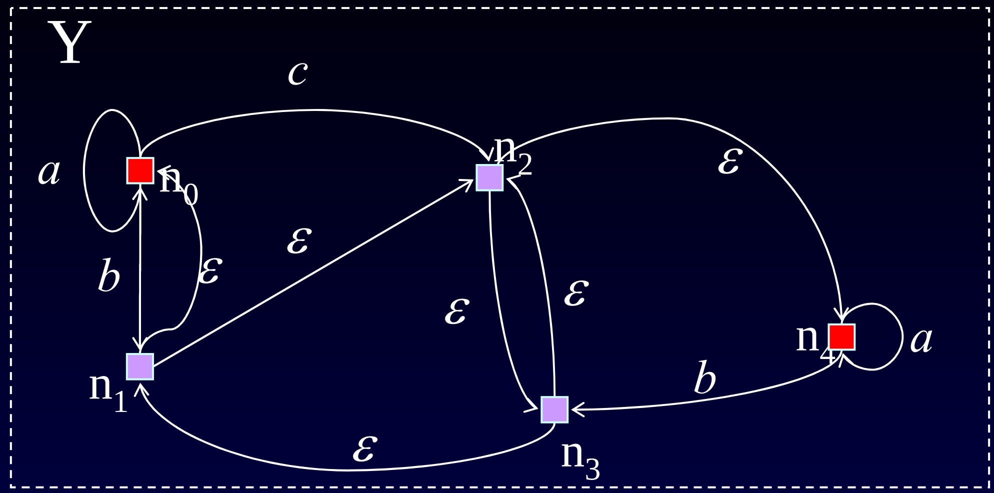
Interferences



Message

0
1
0
1

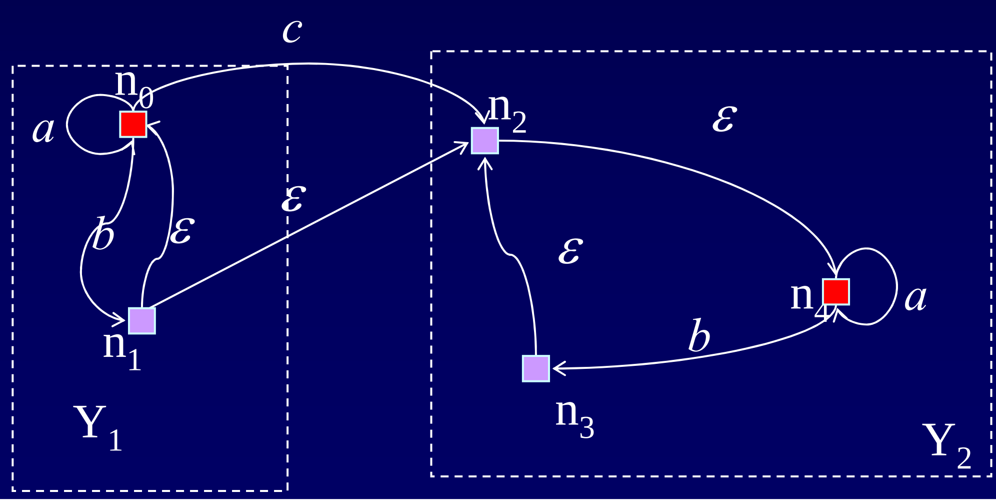
f_Y = strategy in a Büchi game



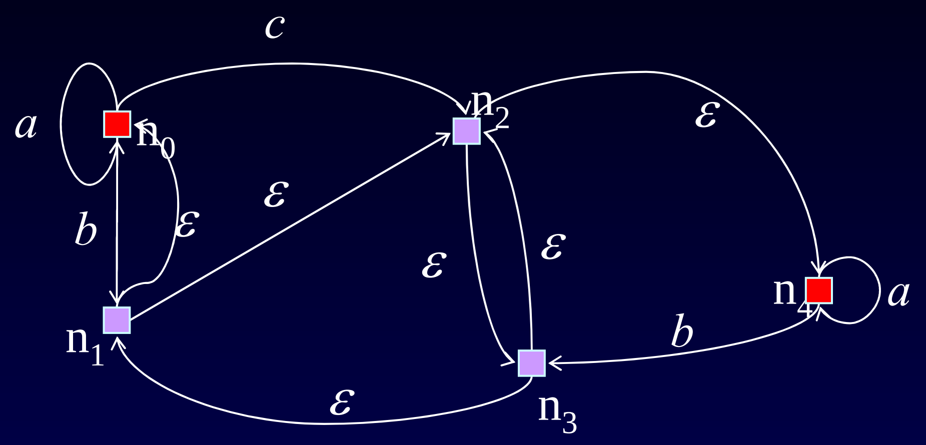
π winning play iff $Inf(\pi) \cap Win(Y) \neq \emptyset$

~~Win = Y~~ , $\pi=(n_1.n_2.n_3)^*$ winning play

Win = { n0,n4 }



f_Y = strategy in a Muller Game $G=(A_H, Win(Y))$



π winning play iff $Inf(\pi) \in Win(Y)$

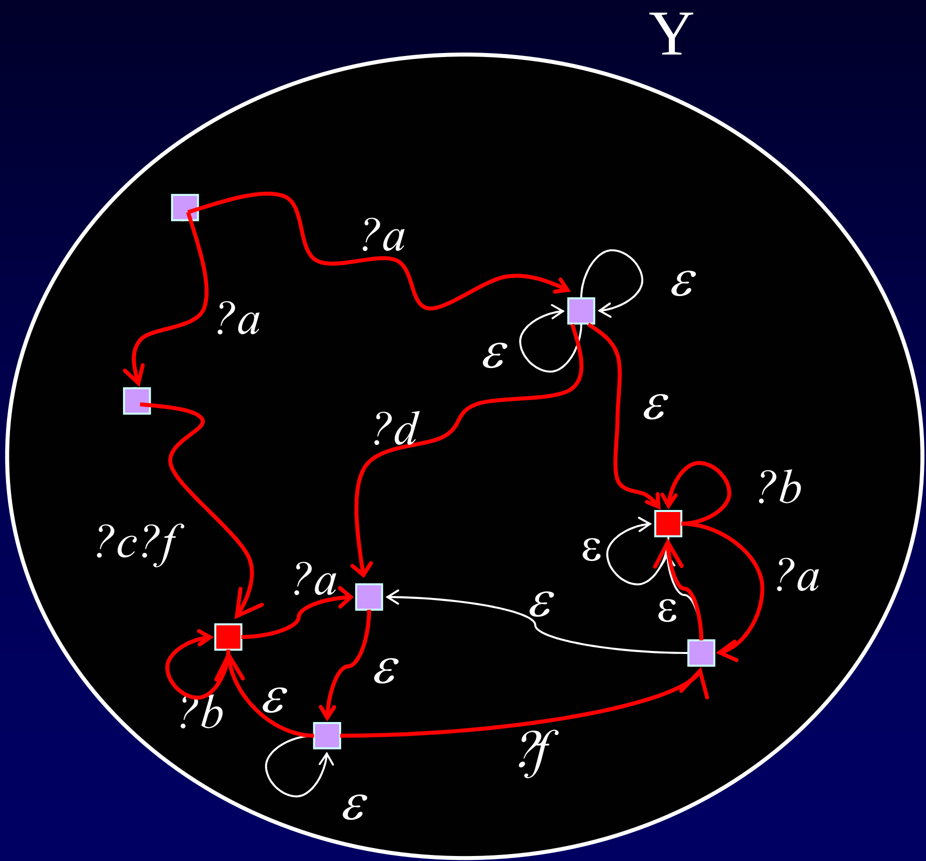
Not a purely positional game

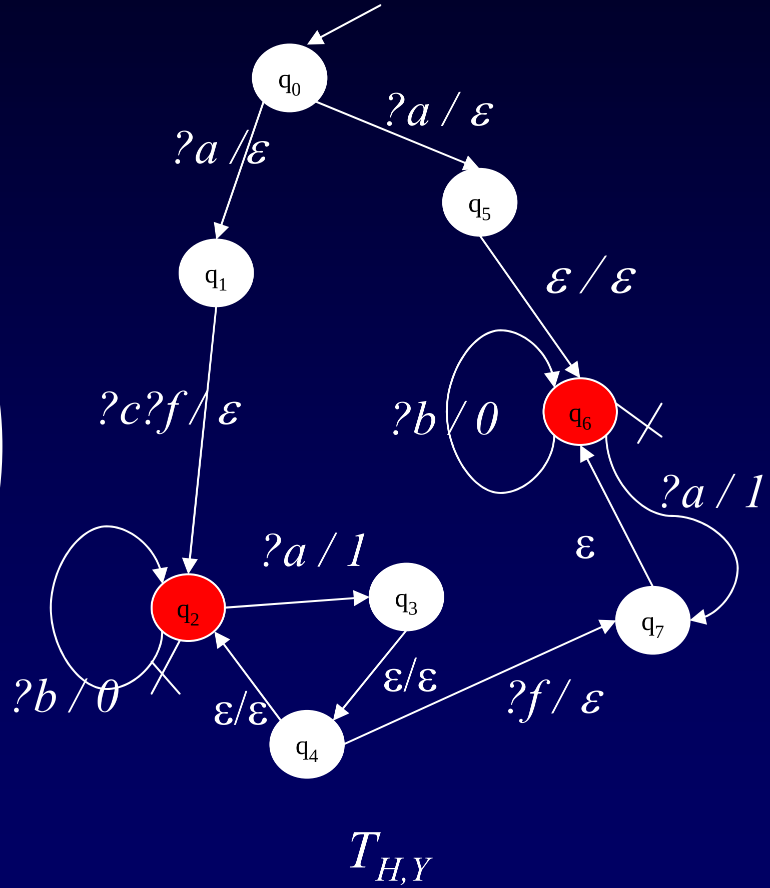
$$Win(Y) = 2^Y - \{ D \in 2^Y \mid D \; scc \wedge \forall d \in D, E(D,d) \}$$

$$Win(Y) = 2^Y - \{n_1, n_2, n_3\}$$

f_Y uses more transitions (under certain memory conditions)

Building a decoder





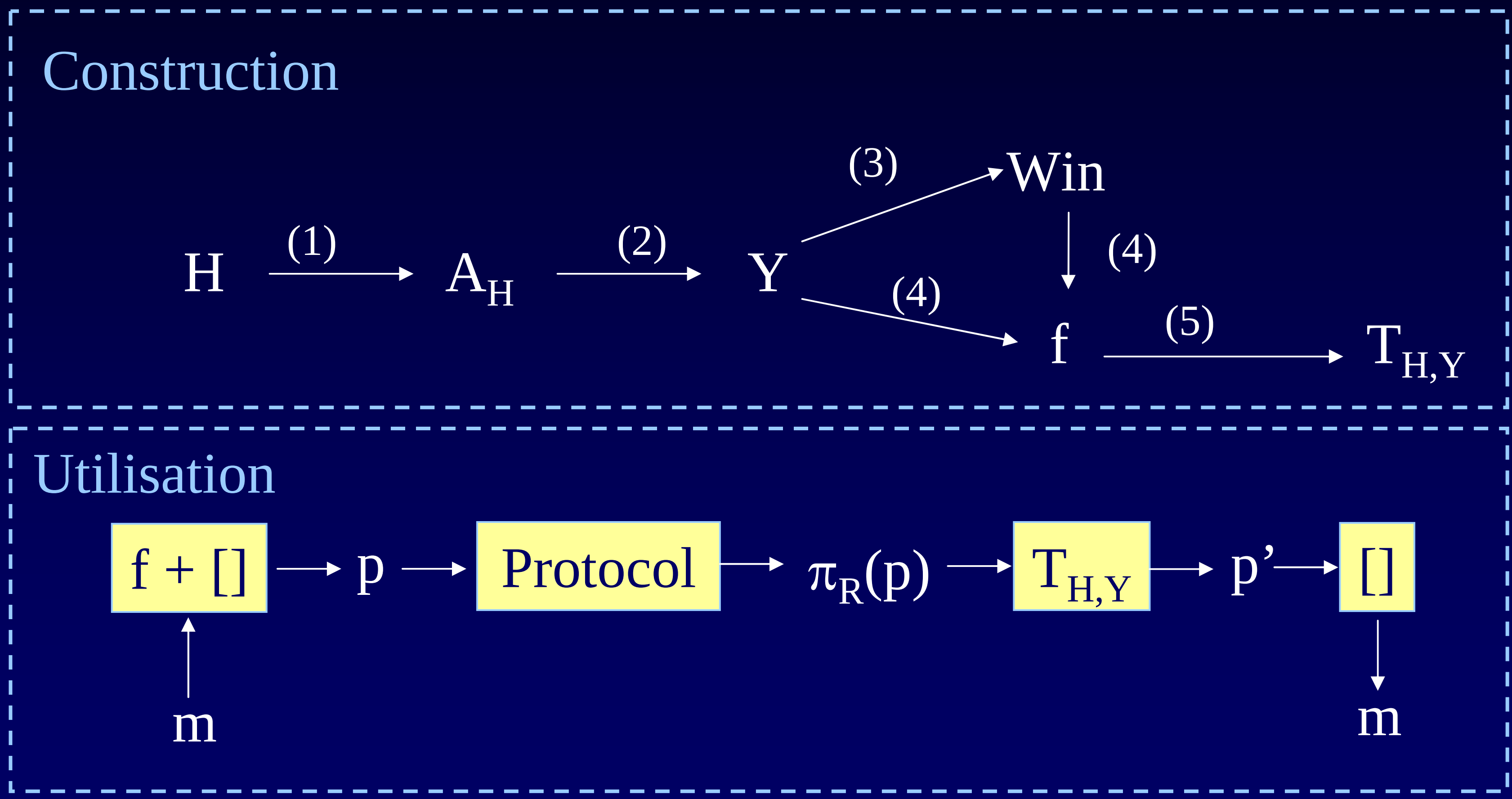
Theorem :

Let H be a HMSC, and A_H be the associated arena.
Let Y be the winning set computed from A_H, $Win(Y)$ be the corresponding winning subsets and f_Y be a strategy for the Muller game $(A_H, Win(Y))$. If $T_{H,Y}$ is functional, then

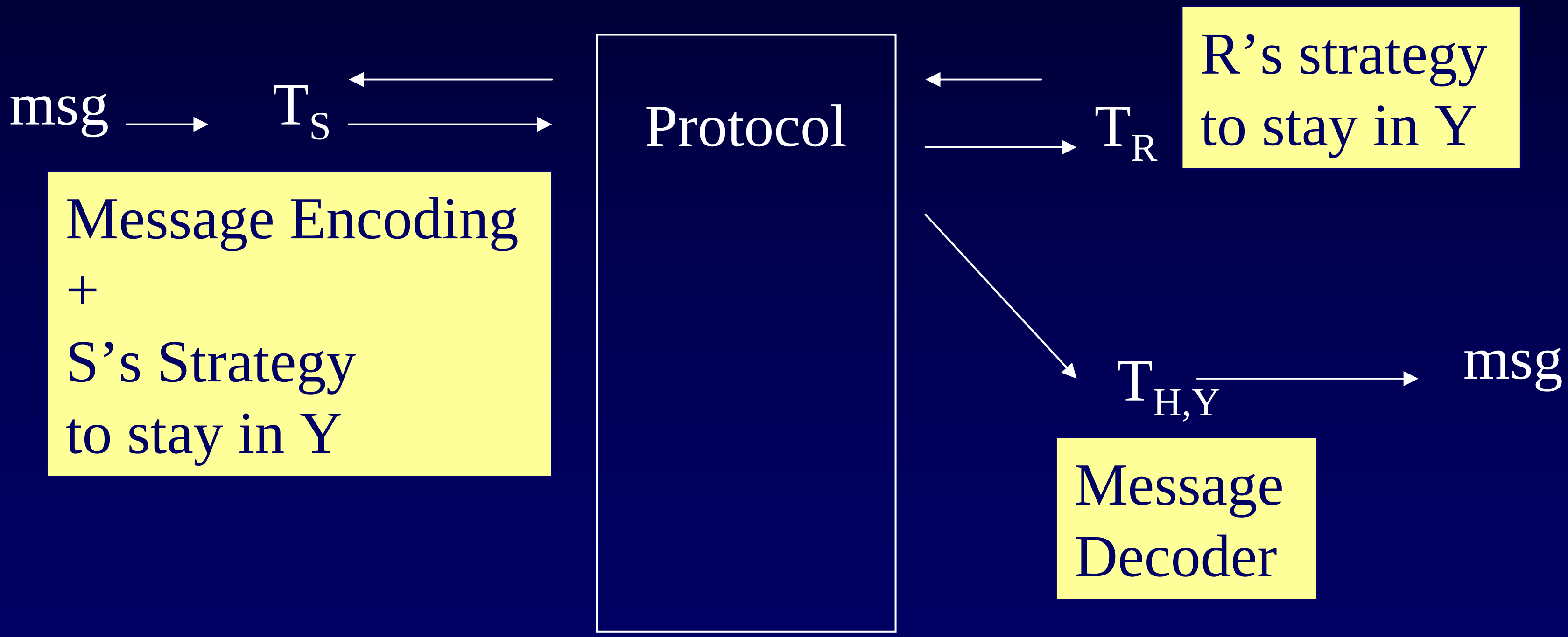
$$\exists\, [\ ] : \{\varepsilon\} \cup \rightarrow\ \rightarrow \{\varepsilon, 0, 1\} \text{ such that}$$
$$\forall y \in Y,\ \forall m \in \{0, 1\}^*,\ \exists p=(y,b,y').t_1 \ldots t_k,$$
$$[\, T_{H,Y}(\pi_R(p))\,] \equiv m$$

Transmission of any message with a bounded number of decisions !

Conclusion


Construction
(3)
Win
H
(1)
A_H
(2)
Y
(4)
(4)
f
(5)
T_H,Y
Utilisation
f + []
p
Protocol
π_R(p)
T_H,Y
p'
[]
m
m

But we are in a distributed world …
Which leads to a more generic framework
with UNCERTAINTY and DISTIBUTION



Once a potential covert channel is found :

- compute its theoretical bandwidth
- test on an implementation
- Scenarios are provided for free !

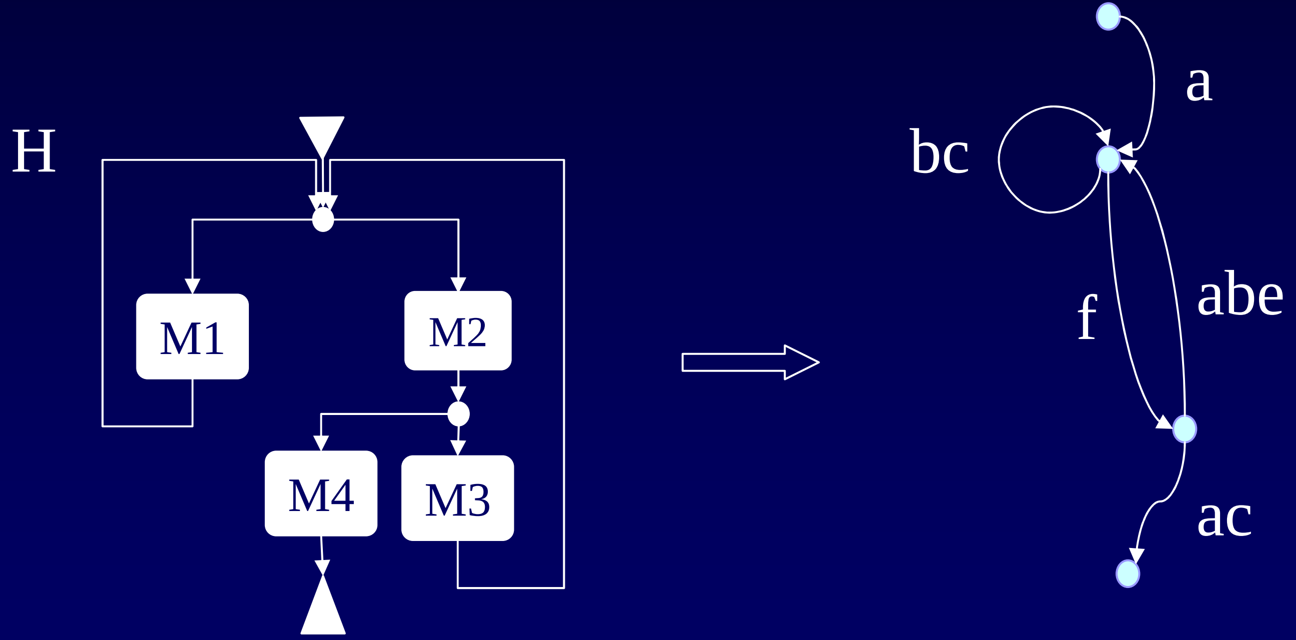
Future research directions:

- Distributing a strategy ?
- Accept uncertainty in decoding
- Study CCs with information theory
- Teams of sender/receivers
- Generalize non-interference using games

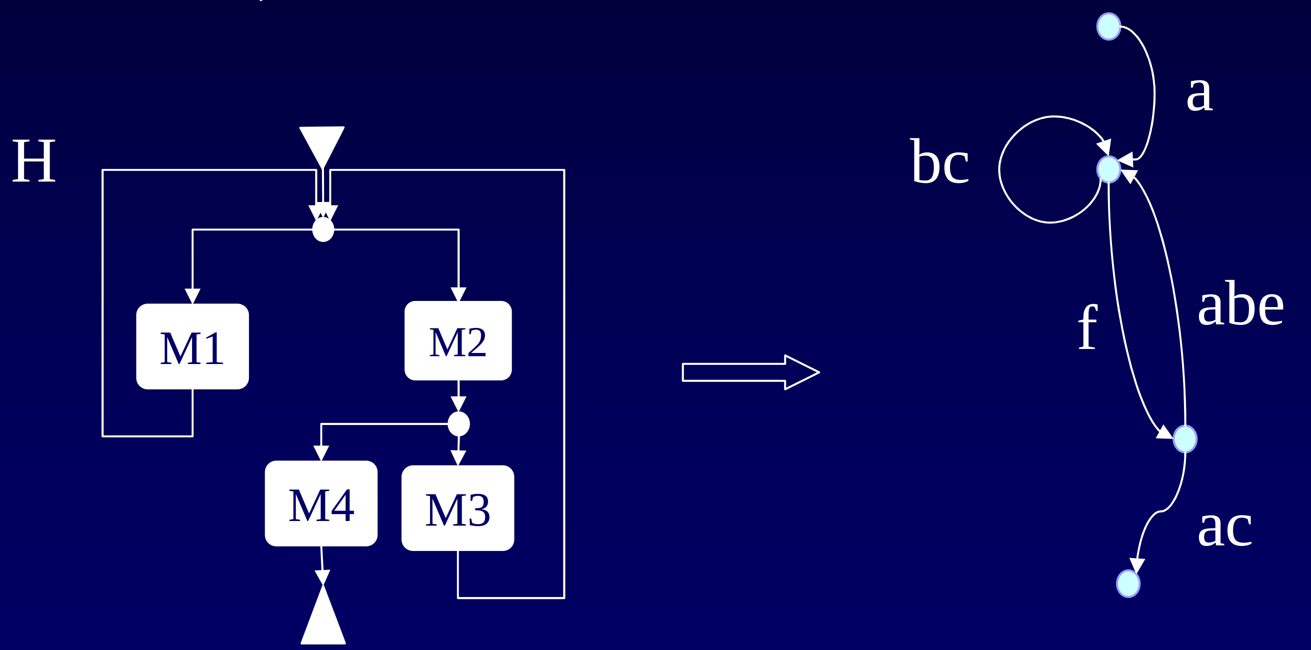
More...

HMSCs vs automata ?

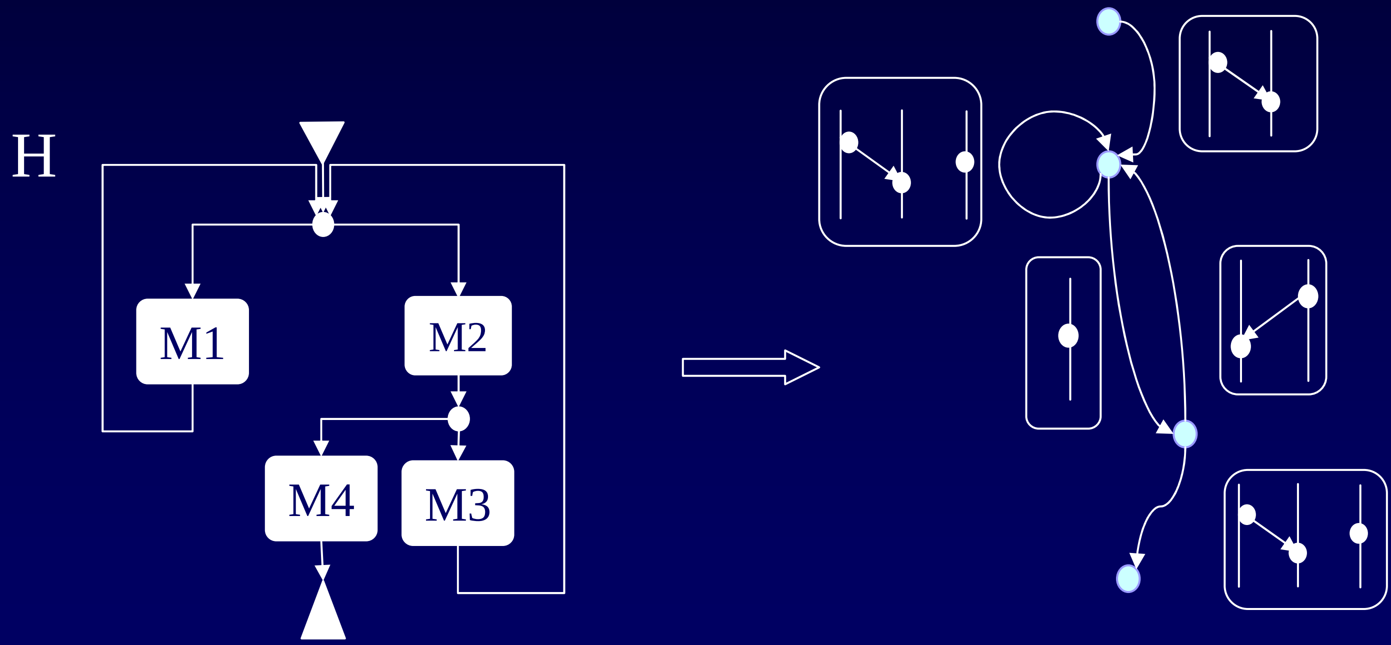
So far, 1 sender, 1 receiver



n senders, 1 receiver



n senders, *k* receivers



Pbs to decide ambiguity ?

More covert channels