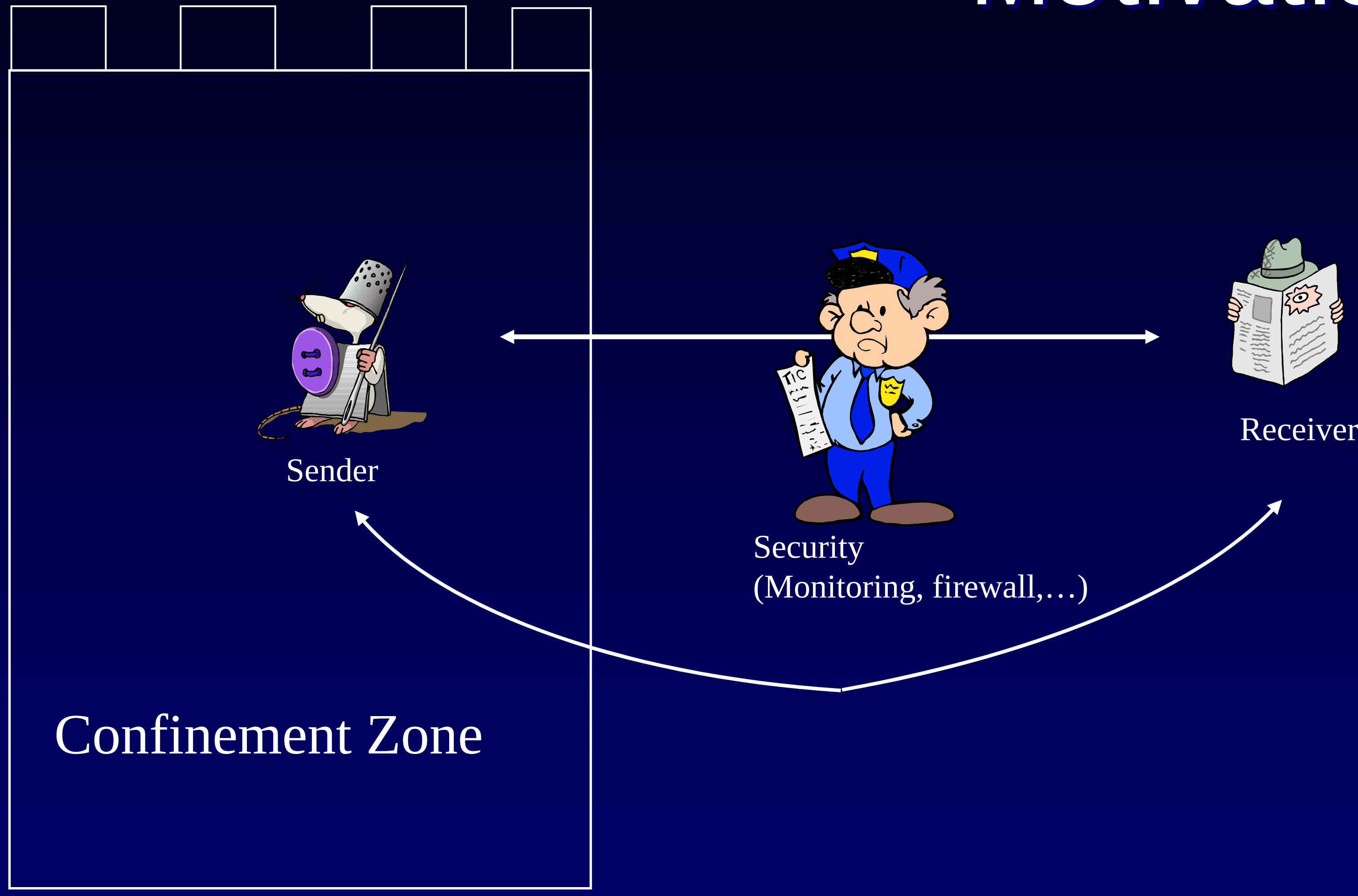
# Covert channels detection in protocols using scenarios

Loïc Hélouët

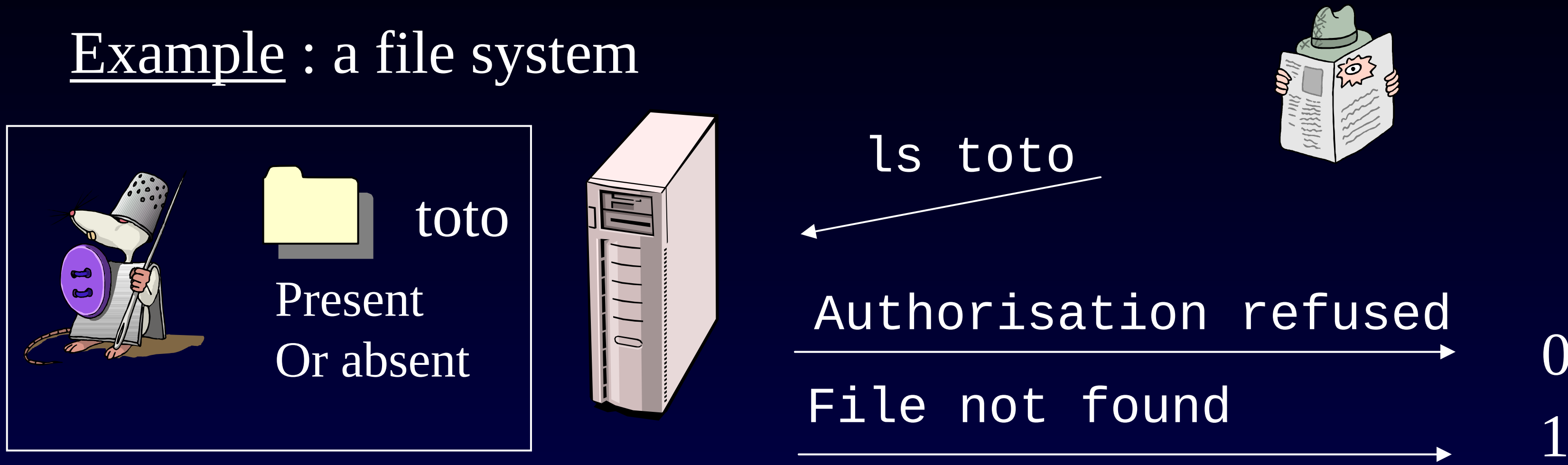
INRIA Rennes

SAM2004

# Motivations



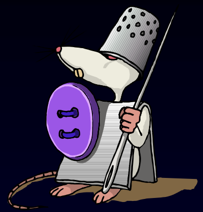
Example : a file system



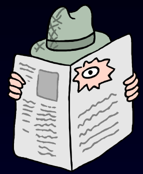

- threat : performance, billing, security, …
- all channels can not be eliminated

Recommandations:

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



Sender



Receiver

message

Encoding

decisions of *sender*
at choice nodes

Protocol
Model
(HMSC)

Compute bandwidth

Test on real
implementation

message

Decoding

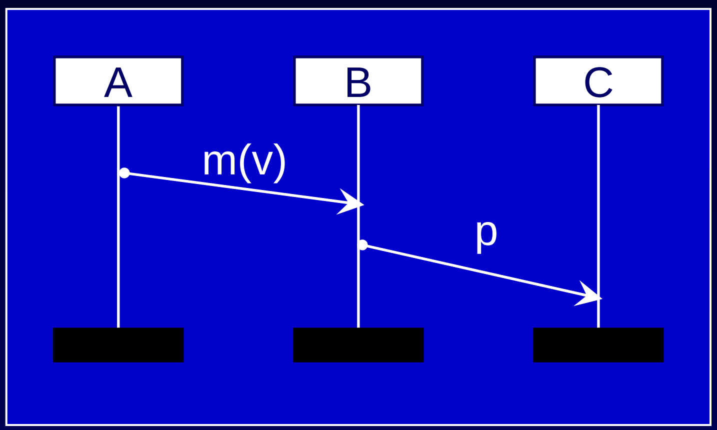
Deduction of choices
performed from
observations
on *receiver*

# PLAN

- Message Sequence Charts
- Covert channels
- Bandwidth evaluation
- RMTP2
- Conclusions & perspectives

# Message Sequence Charts

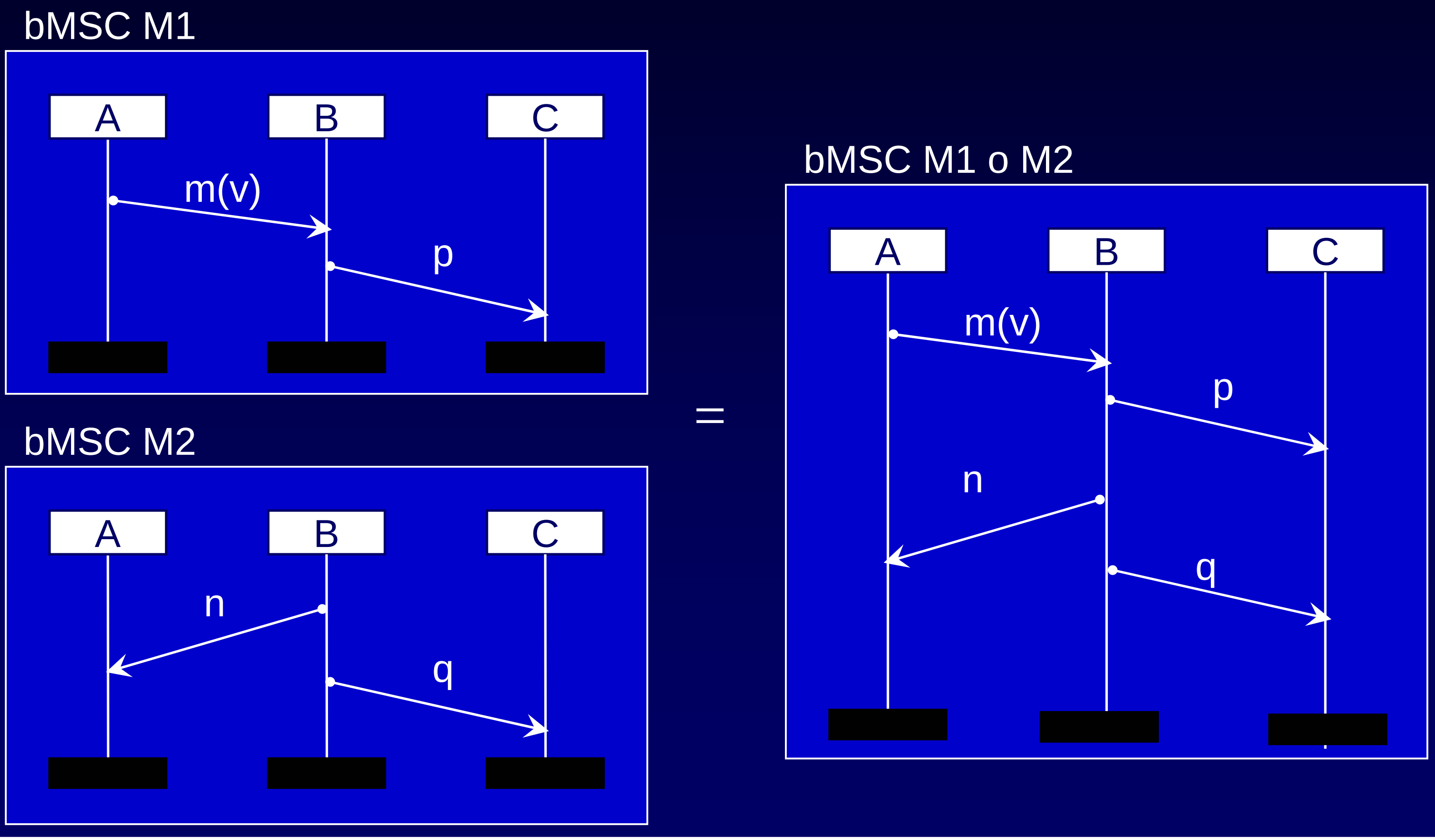
bMSC M




$M = < E, \leq, A, P, \alpha, \varphi, m, V, \sigma >$

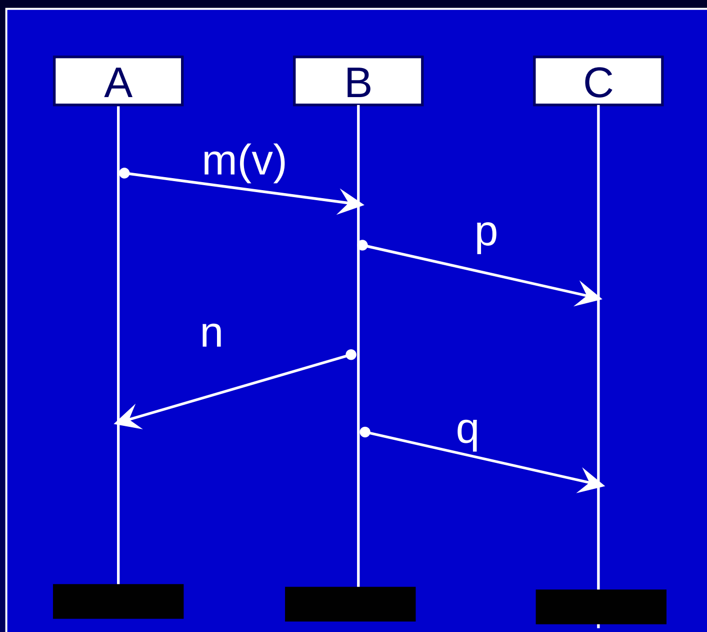
- E : events
- $\leq \subseteq E \times E$ : causal order
- A : action names
- $P$ : Instances
- $\varphi \subseteq E \times P$ : locality
- $\alpha \subseteq E \times A$ : labeling
- $m \subseteq E \times E$ : messages
- V : variables
- $\sigma \subseteq m \times V$ : message parameters

# Sequential composition

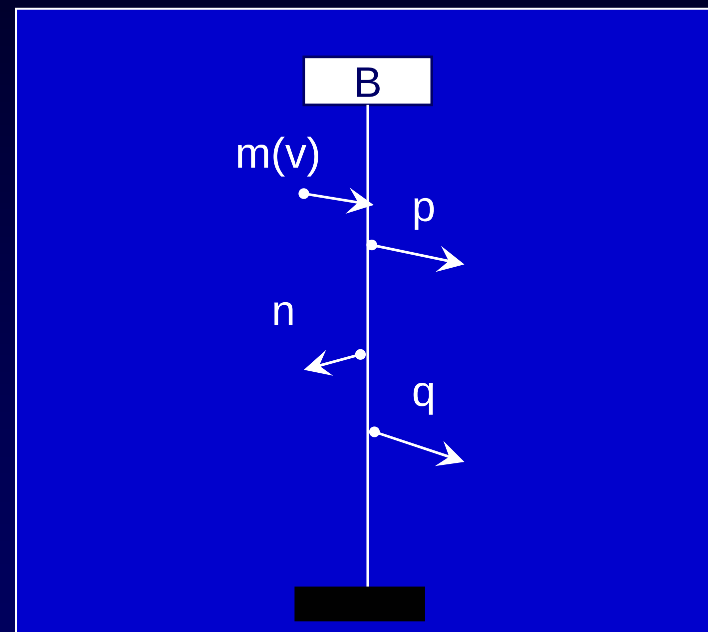


# Projection on an instance

bMSC M



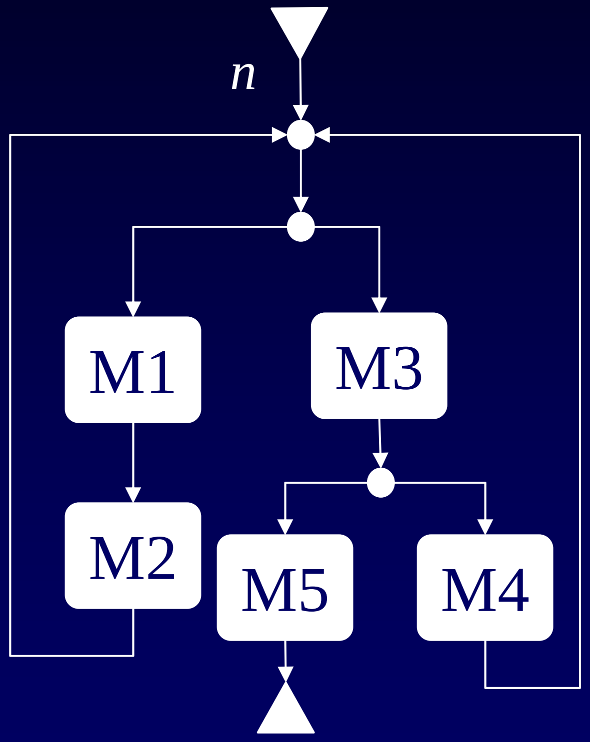

bMSC $\pi_B(M)$




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

# HMSC

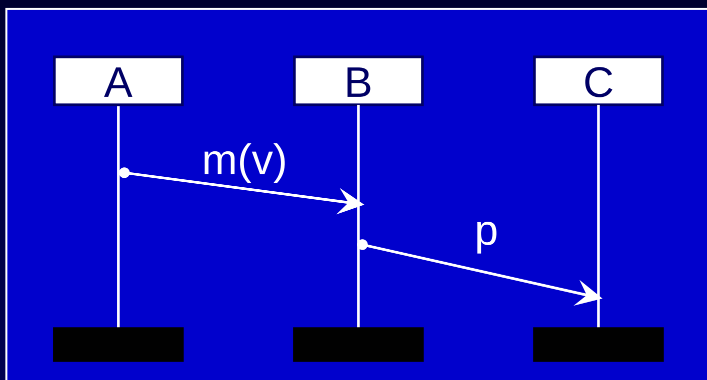
$$H = (N, \rightarrow, \mathcal{M}, n_0)$$



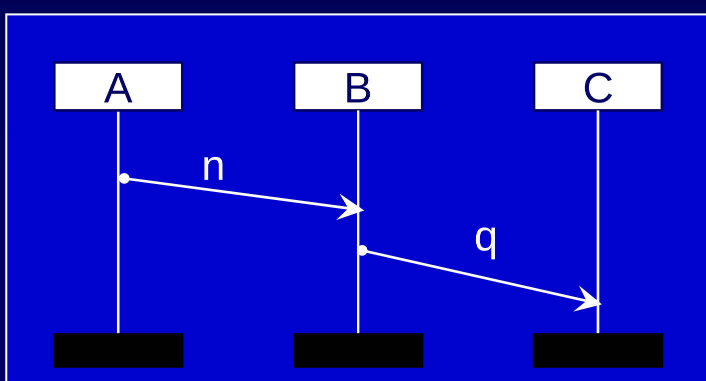

- $N$ : nodes
- $\rightarrow \subseteq N \times \mathcal{M} \times N$ : transitions
- $\mathcal{M}$ : bMSCs
- $n_0$ : initial node

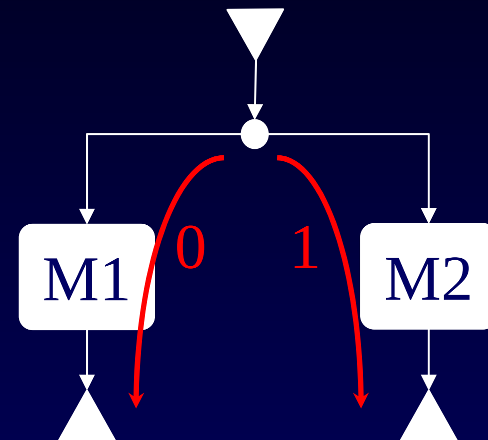
# Covert Channel detection

bMSC M1




bMSC M2



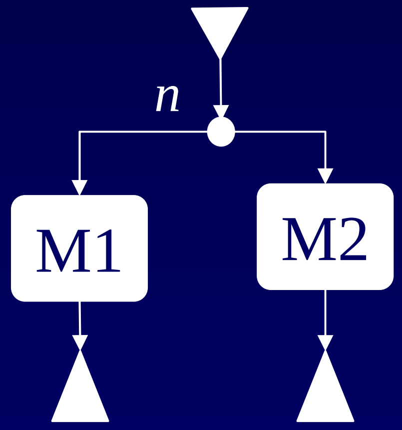




| Events observed on instance C | | events executed on instance A |
|---|---|---|
| ?p | => | !m(v) |
| ?q | => | !n |

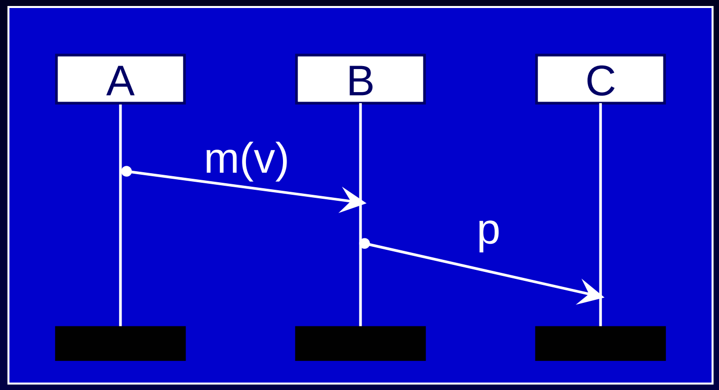
## Definition :

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* $\exists!\, e_i = min(O_{P_i})$ and $\varphi(e_i)=p$

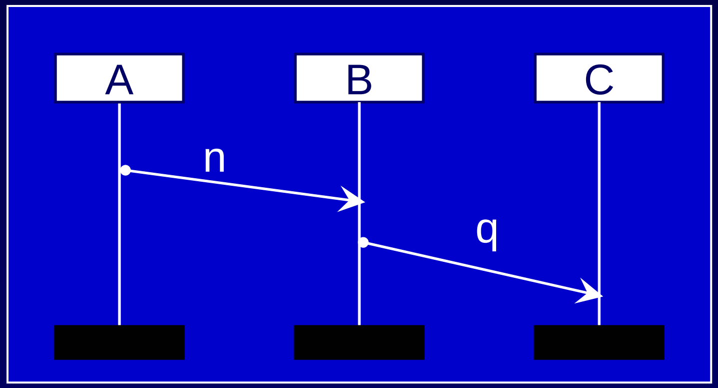
*(idem local choice)*

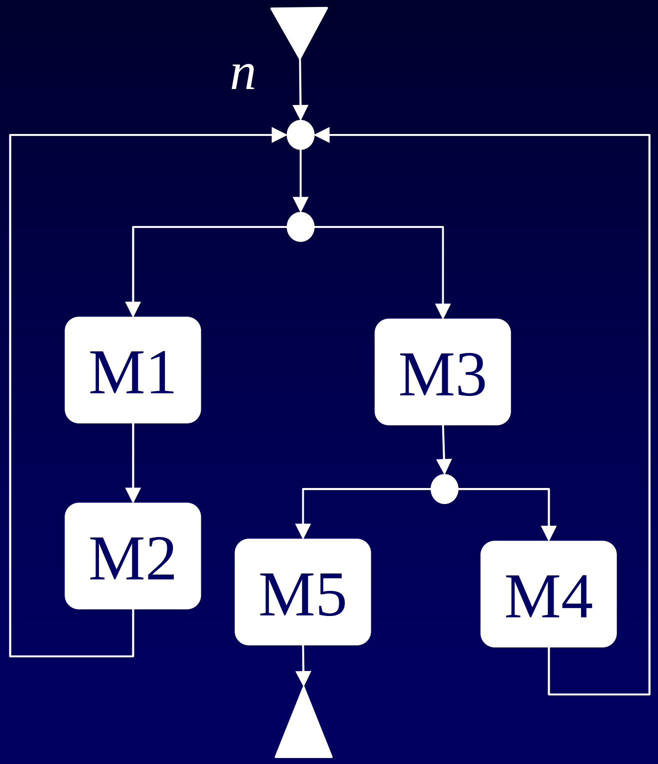



bMSC M1




bMSC M2

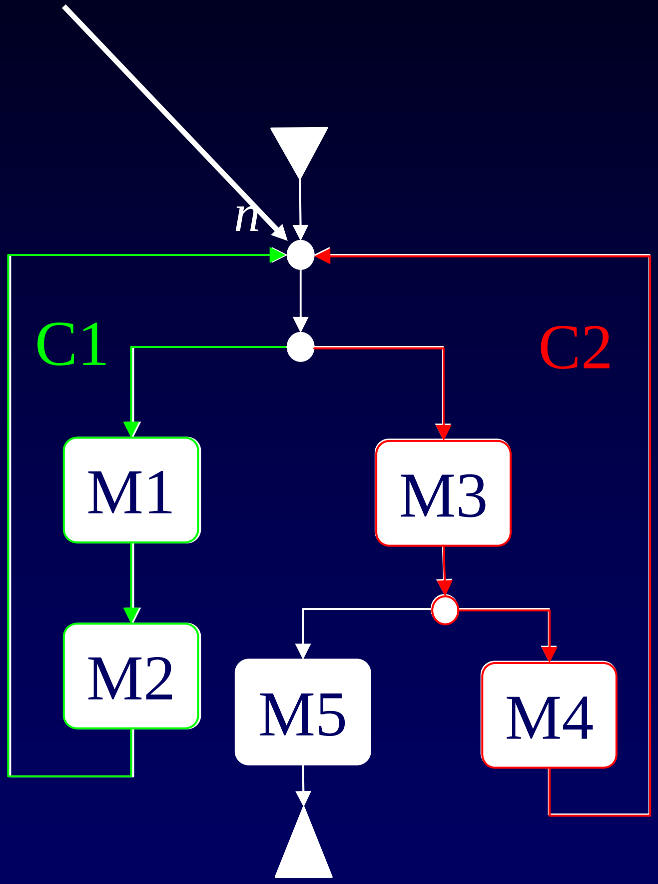





## Hypotheses

- To transmit a message of arbitrary length, one need to iterate some behaviors : CC appear in presence of cycles.
- to encode information, the sender can perform several choices
- For each choice, the observable consequences are ≠ for the receiver

Controlled by *Sender*



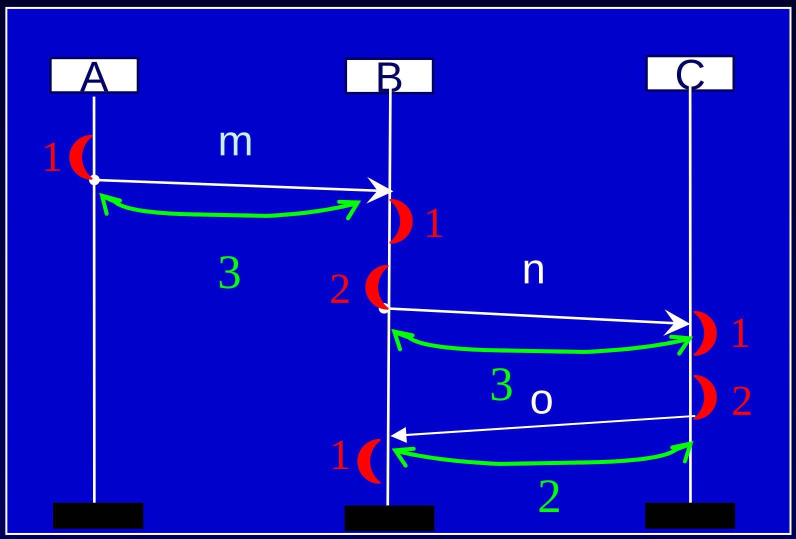

Covert channel from *Sender* to *Receiver*

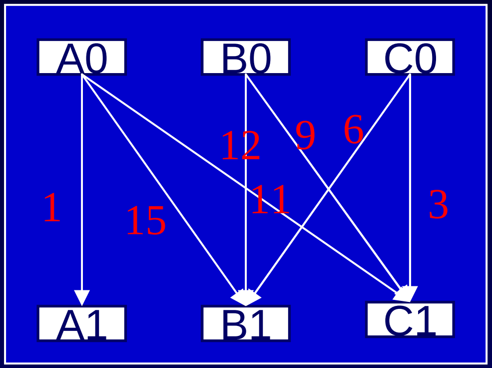
- decision node controlled by *Sender*
- Several Cycles
- ≠ Observations by the *Receiver*

$$\pi_{Receiver}(M_1 o M_2) \neq \pi_{Receiver}(M_3 o M_4)$$

# Bandwidth

bMSC M



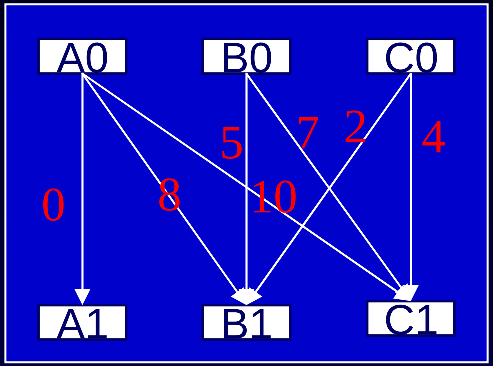




+ temporal annotations

- for events
- for messages

Definition of scenario duration

- $d_{x,y}(M)$
- $D(M) = \max \{ d_{x,y} \}$




$$D(M^n) = max\ \{\ d_{x,y}\ (M^n)\ \}$$

Mean durations:

$$md(M^\omega) = \lim_{n \to \infty} \frac{1}{n} . D(M^n)$$

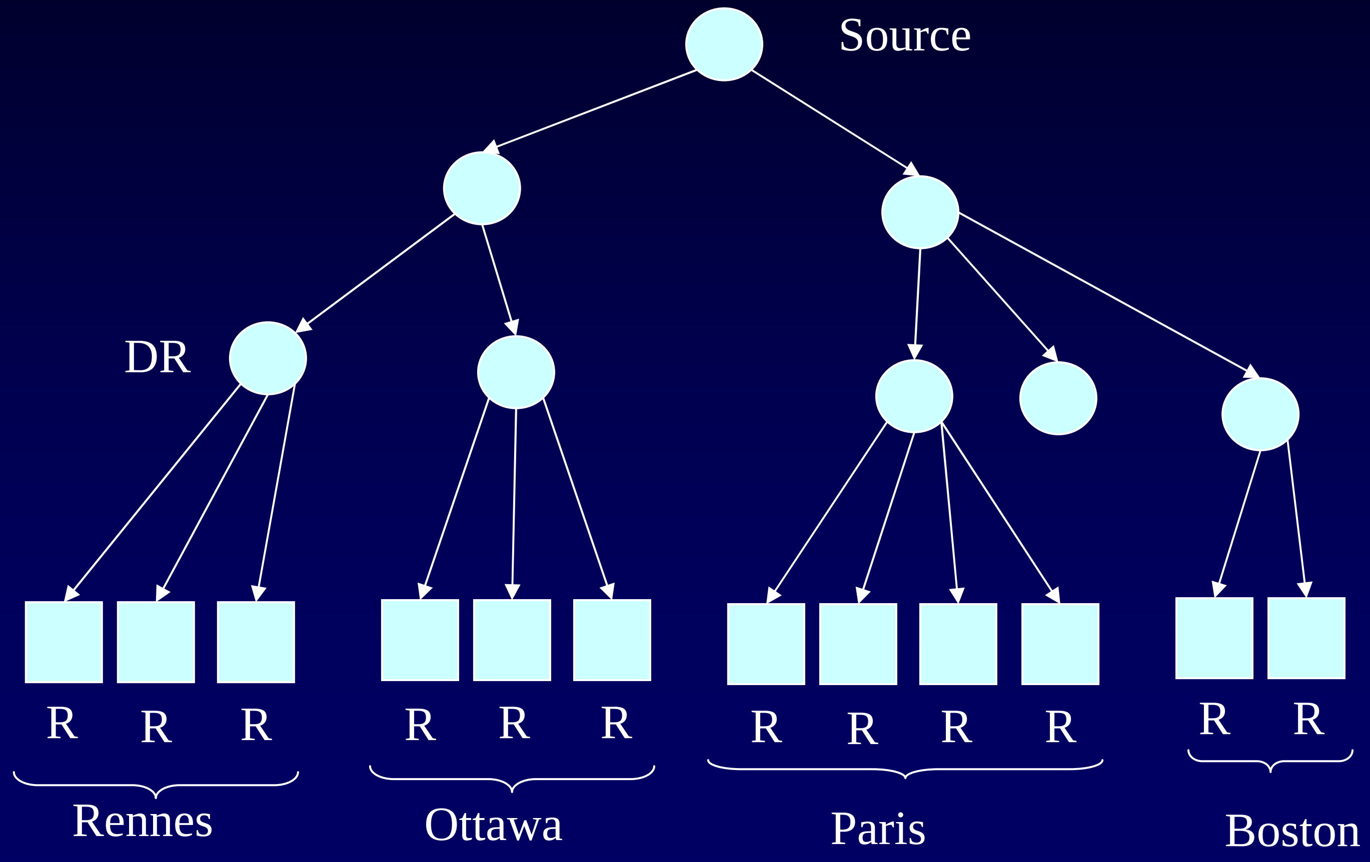
$$md_{x,y}(M^\omega) = \lim_{n \to \infty} \frac{1}{n} . d_{x,y}(M^n)$$

Bandwidth :

If *M* can be used to transfert *b* bits from *x* to *y* :

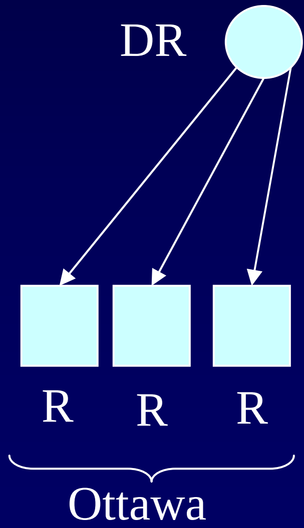
$$Bw = \frac{b}{md_{x,y}(M^\omega)}$$

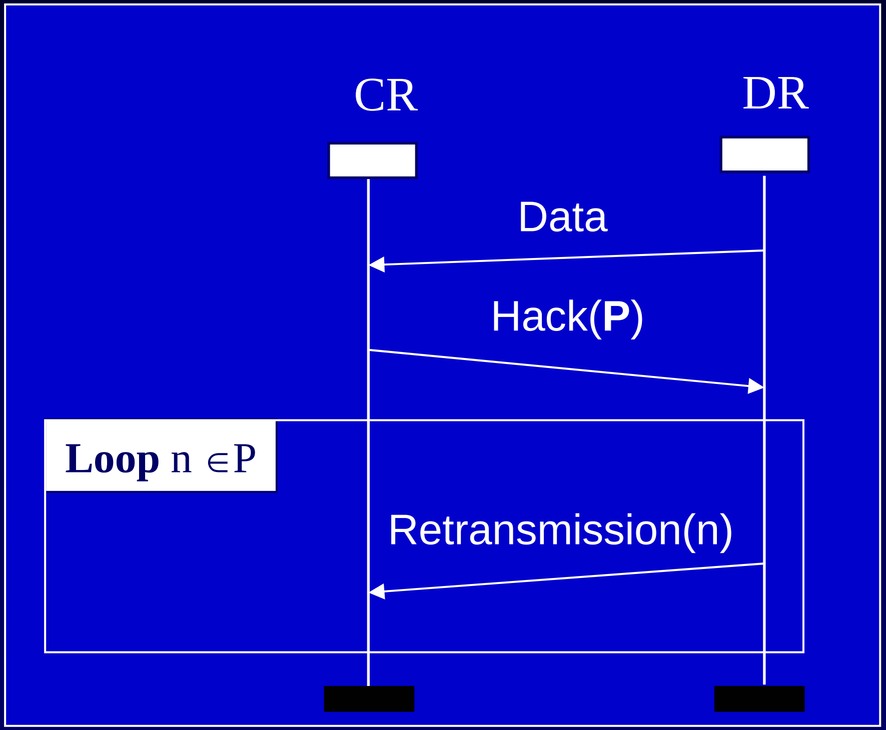
# Example : RMTP2



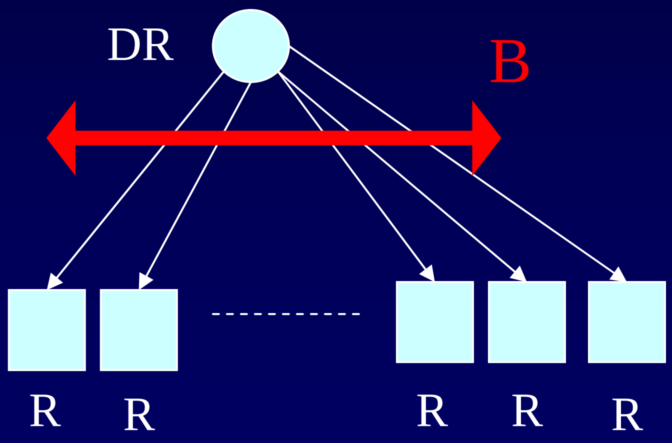
# RMTP2 : Data retransmission

P : bitmap representation of lost/received packets



# RMTP2 Parameters




B : Branching Factor

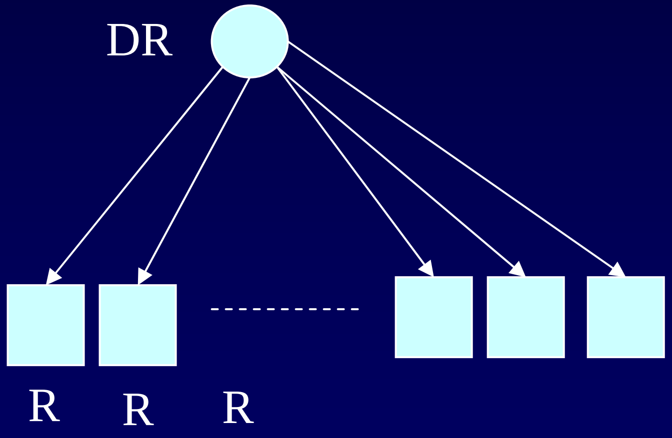
Maximal number of children for a node

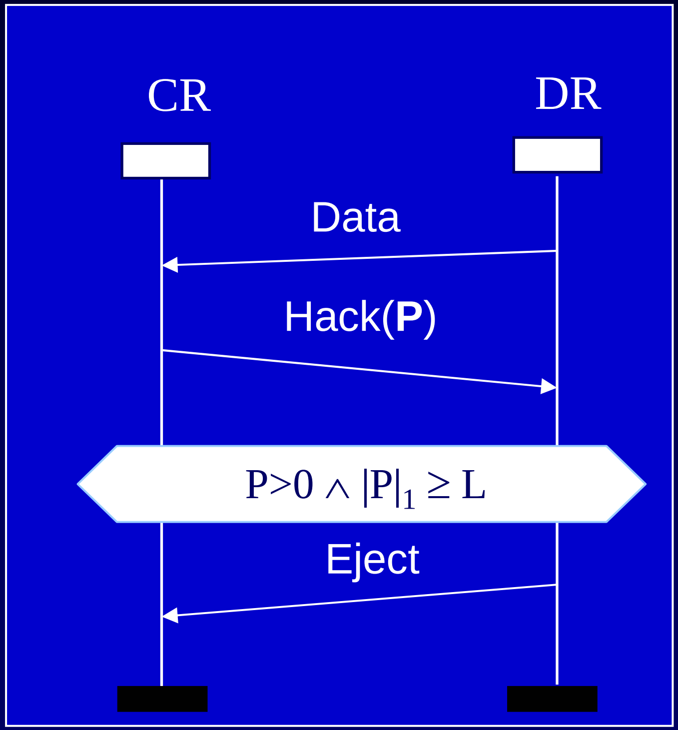
A child can ask for retransmission every B data packet

# RMTP2 Parameters

S : Bitmap size

L: maximal loss rate allowed

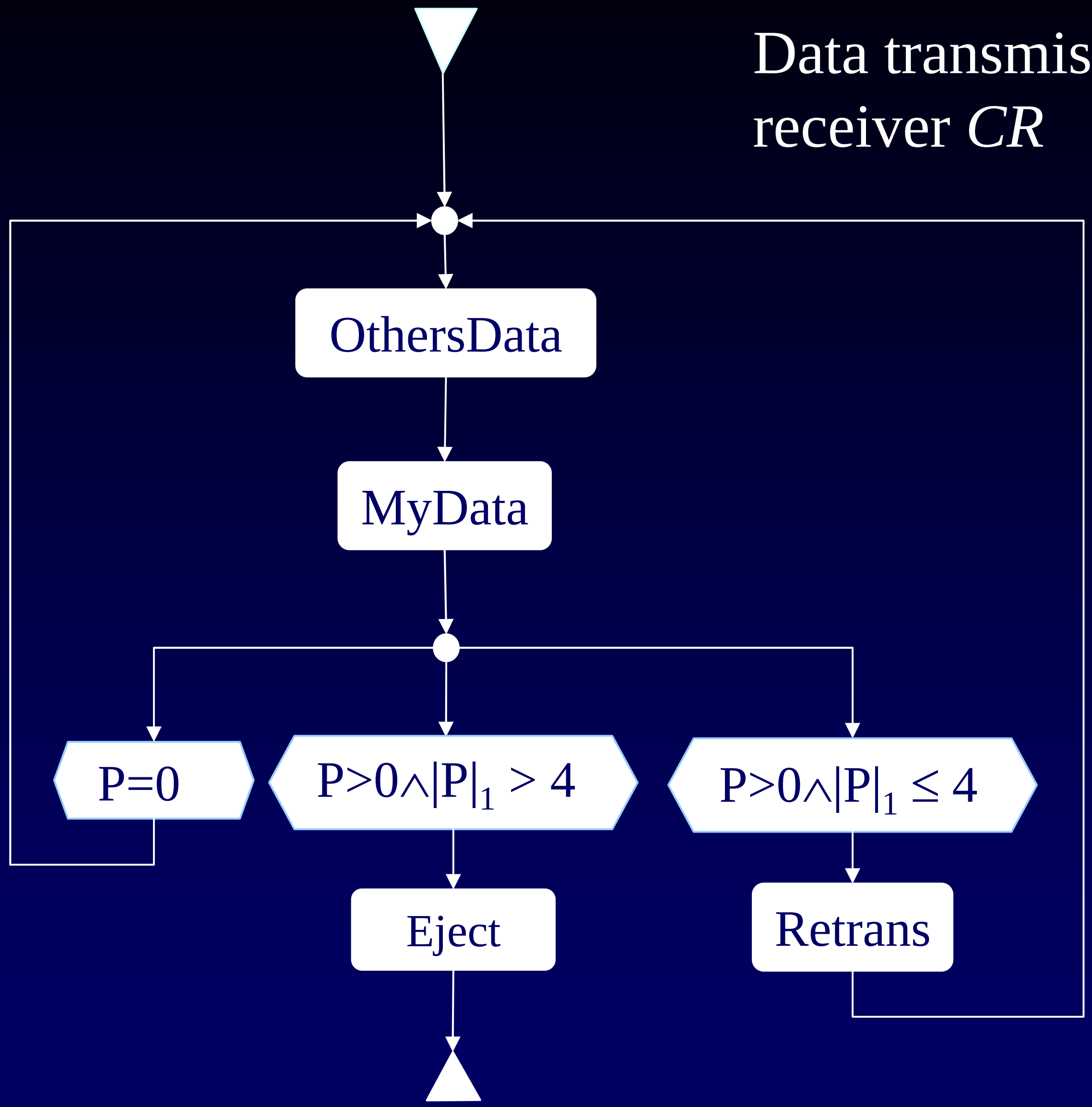


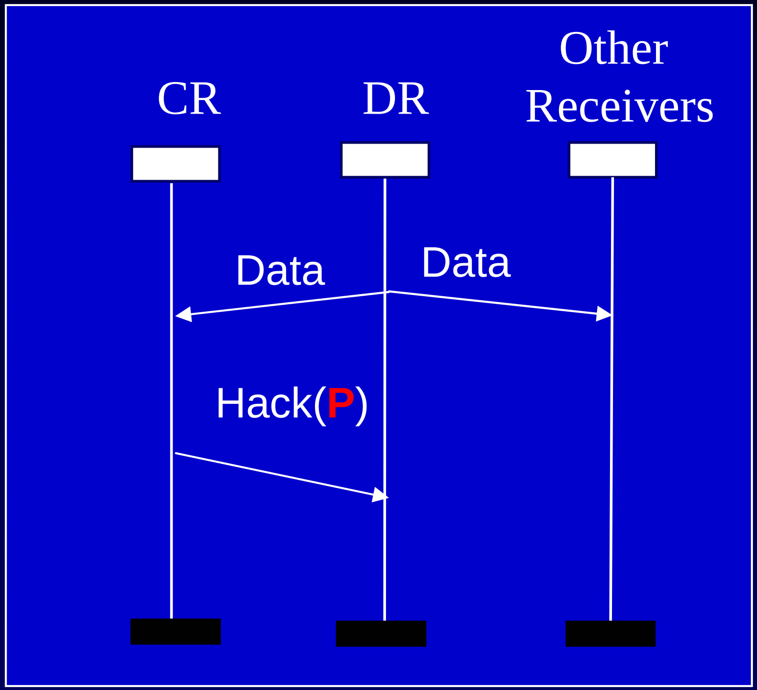

Ex: S=16, L=25%     `Hack(0100 1010 0110 1100)`

Example

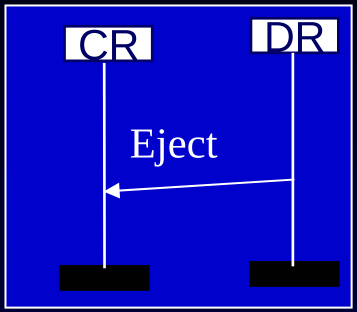
Data transmission seen from a receiver *CR*



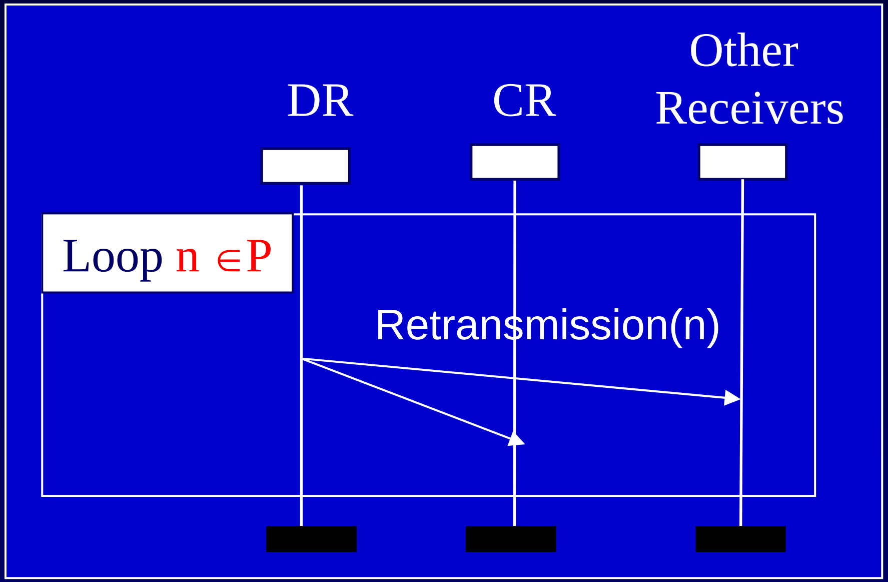
bMSC MyData




bMSC Eject

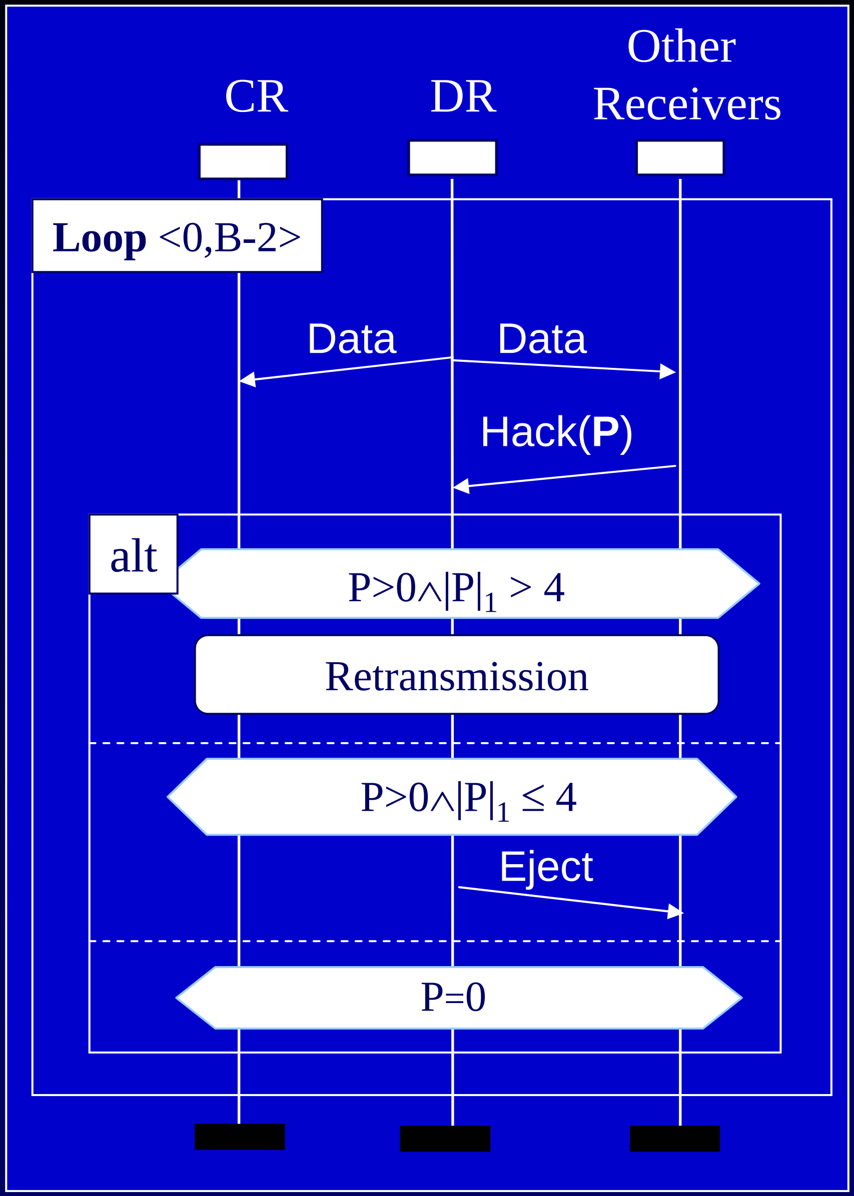



bMSC Retransmission




# Example

bMSC OthersData

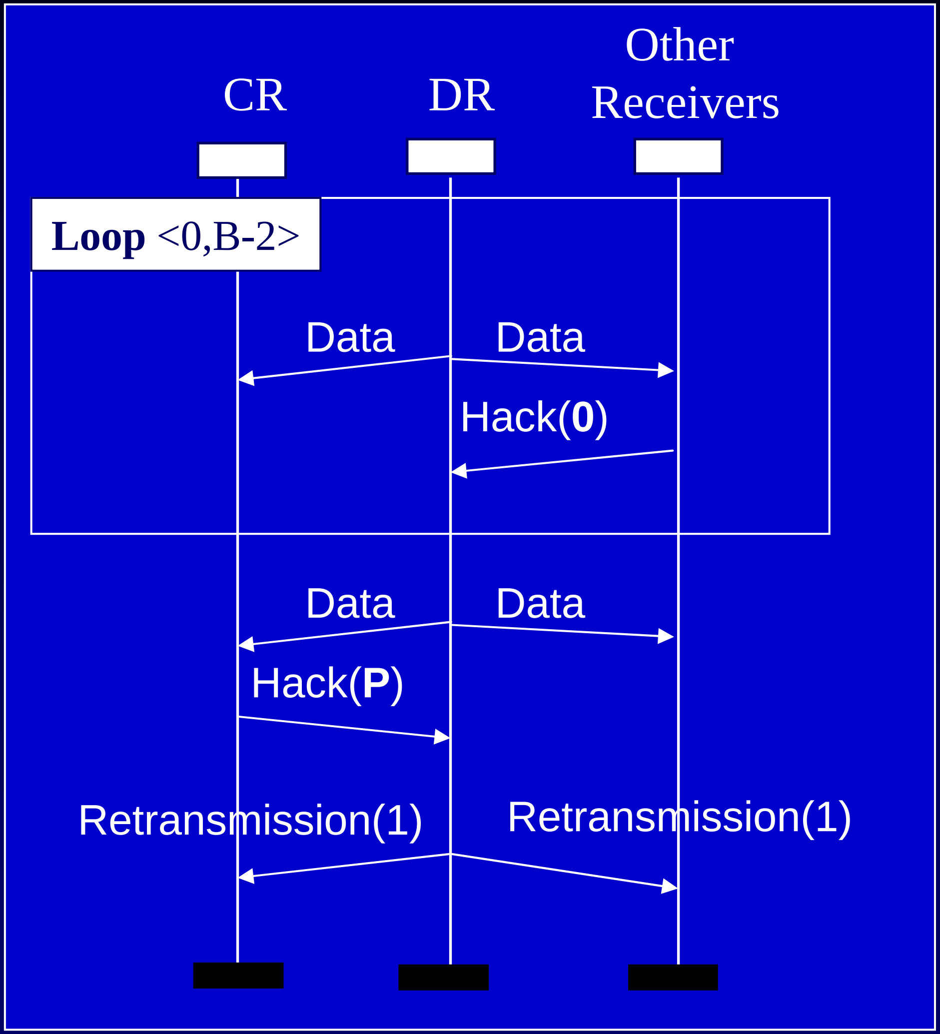



# Example

Covert channel from *CR* to any receiver in *Other Receivers*

Creation of fake bitmaps to force observable retransmissions

bMSC Shortest Scenario




## Example

Let $L=25\%$ , S = $16$

Number of possible fake bitmaps :

$$B = \sum_{i=1..4} \frac{16!}{i!\,.\,(16-i)!} = 2516$$

Number of bits transmitted at each covert channel use

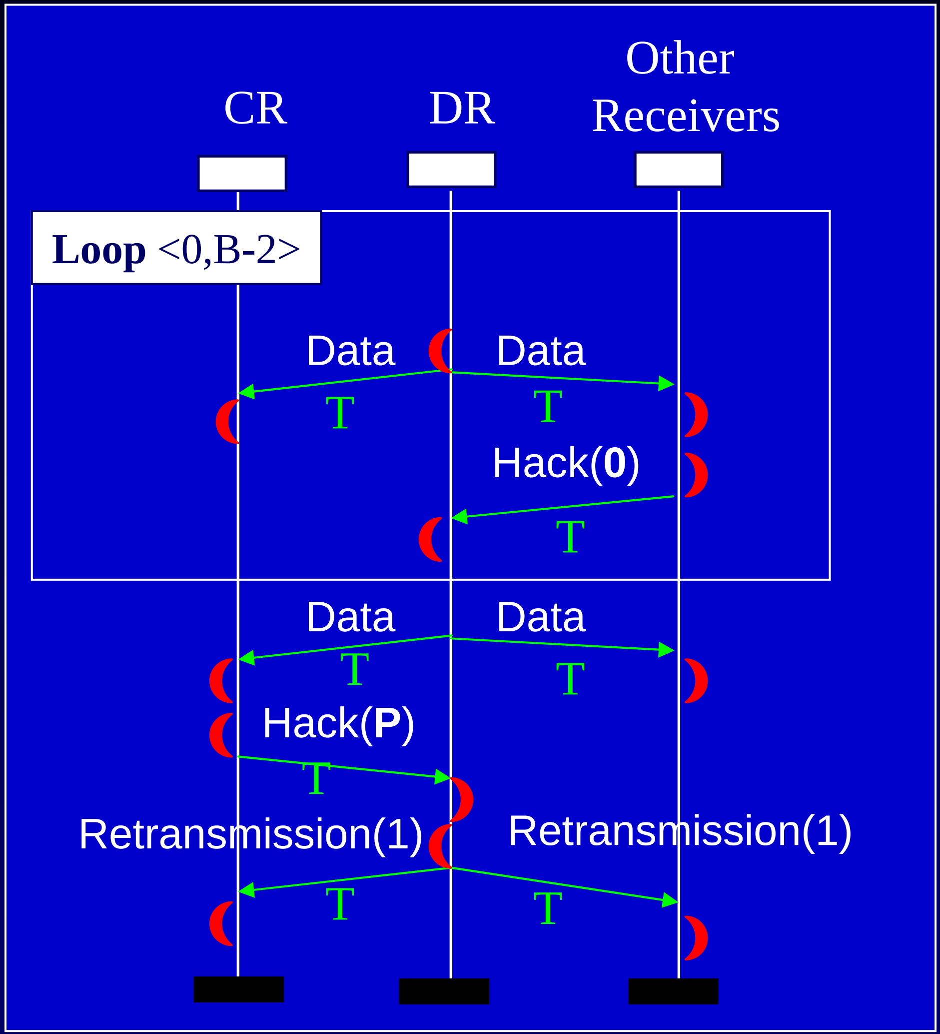
$$b = \log_2(2516)=11.297$$

Bandwidth upper bound:

$$Bw = \frac{b}{md_{cr,Other\ Receivers}(Shortest^{\omega})}$$

Example

bMSC Shortest Scenario




D : event duration

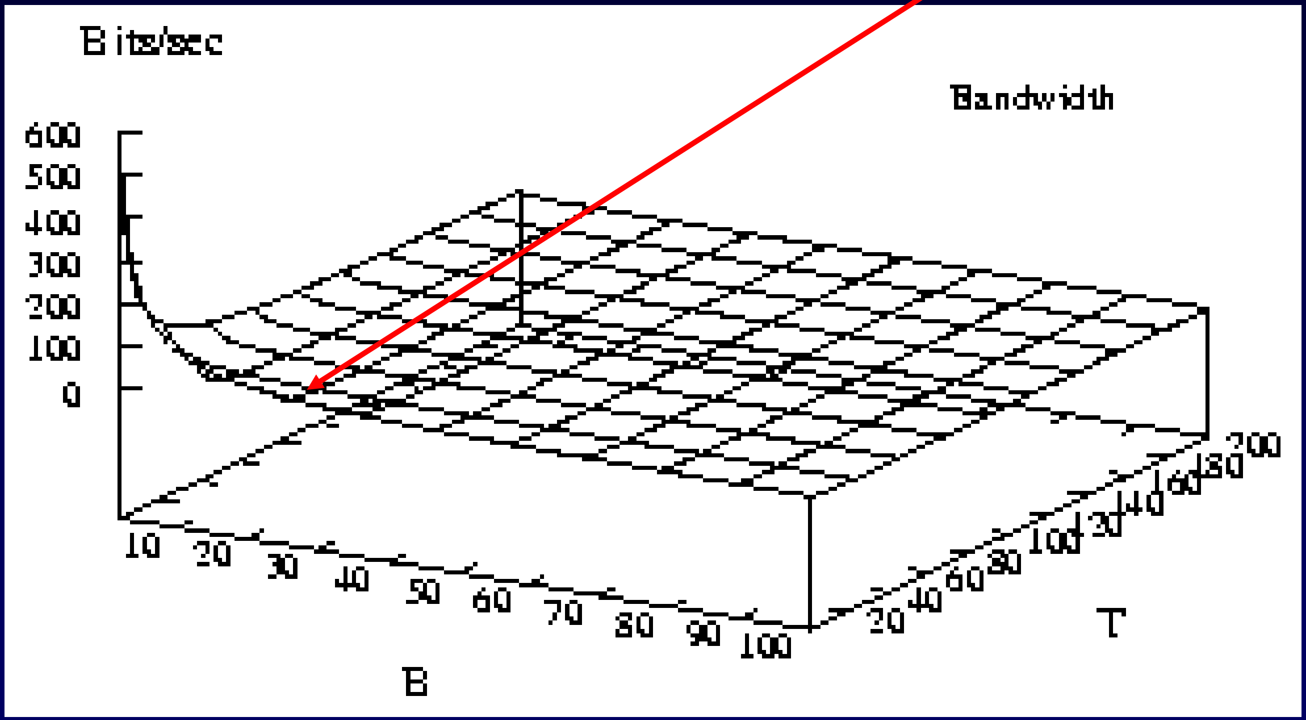
T : transmissions duration

## Example

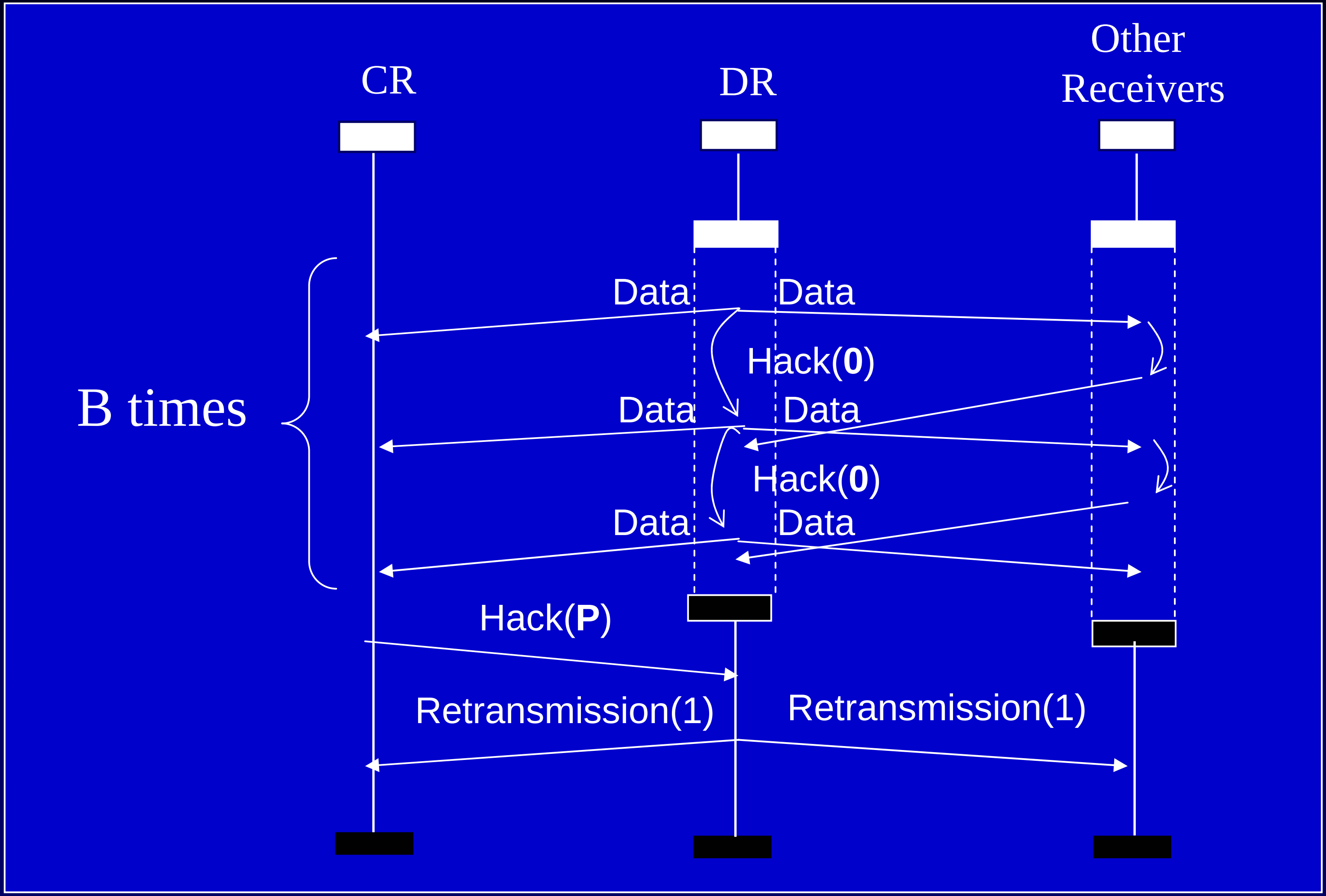
$$Bw = \frac{b}{(4B+1).D + 2B.T}$$

B=20, T=20ms
Bw=11.74 b/s

Bw evolution for *D= 2ms*



bMSC Shortest Scenario



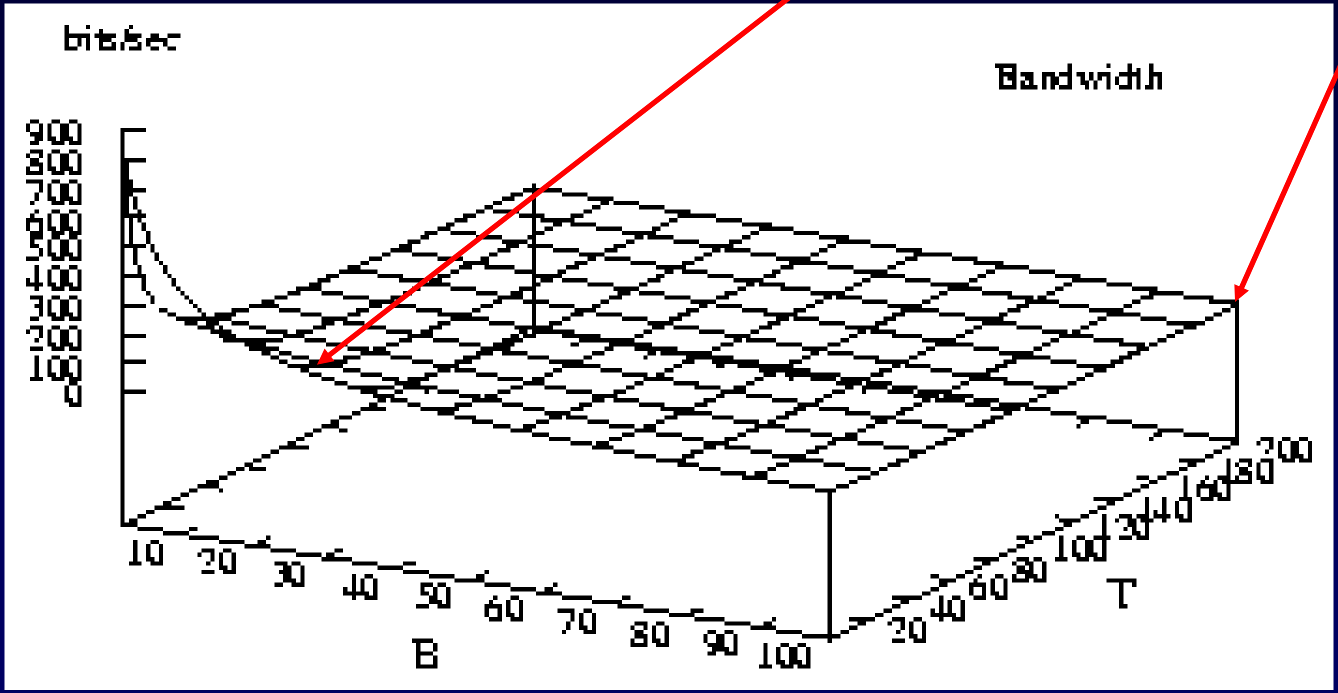

Example

$$Bw = \frac{b}{(B+5).D + 3.\,T}$$

B=20, T=20ms
Bw=102.7 b/s

B=100, T=200ms
Bw=22.40 b/s

Bw evolution for *D= 2ms*



# Conclusion

Covert channel in RMTP2 :

- undetectable receiver
- usable bandwidth

<u>Future work :</u>

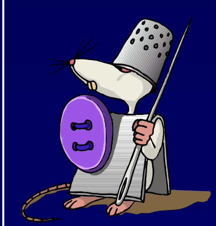
- More elaborated strategies under study
- Covert channels with noise
- Need to « desynchronize » sequential composition CMSCs ?

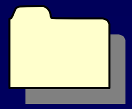
# Covert Channels

Def : communication channel that violates a system’s security policy

Storage channels : implies writing a value somewhere

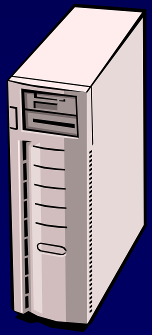
Example : a file system



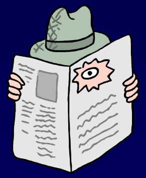


toto

Present
Or absent



ls toto



Authorisation refused → 0

File not found → 1

Some facts about covert channels

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

Recommandations : depend on the security level required for the system under study : NSCS30 (light pink book)

Analysis:

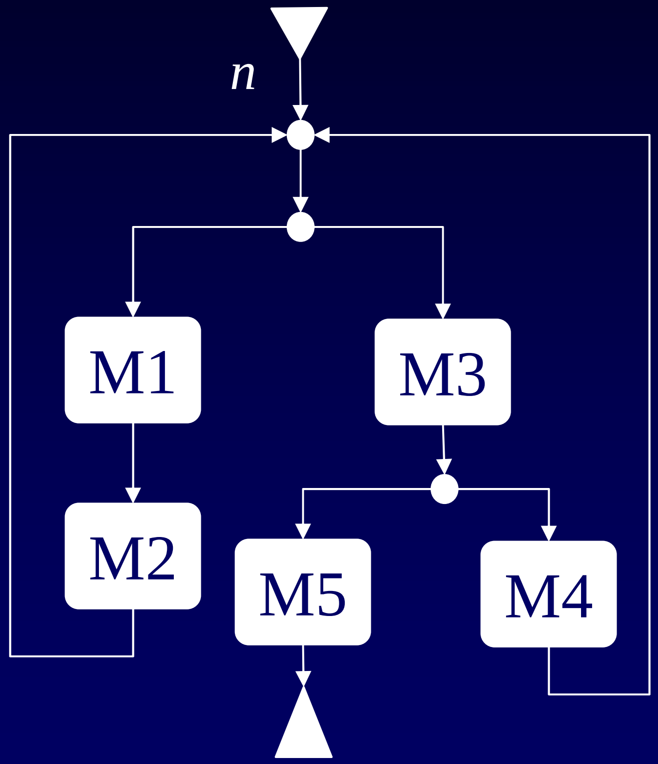
- Identify covert channels
- Illustrate their use through scenarios
- Compute their bandwidth

Solutions :

- Elimination (for systems with high security level)
- Add noise to most important channels
- monitor other channels

Idea : start from informal descriptions of protocol behavious given as scenarios, try to detect potential information flows and compute their bandwidth in order to provide solutions as early as possible during design stages.

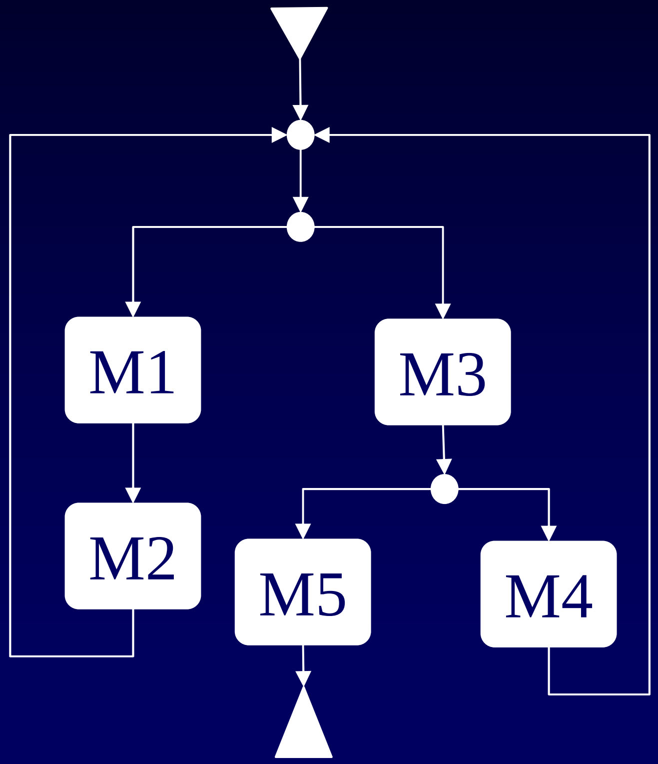
# Covert Channel detection




Hypothesis 1 :

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

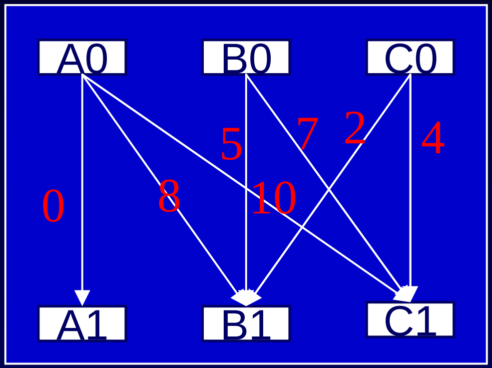
CC can appear in presence of cycles.




Hypothesis 2 :

To transmit a message of arbitrary length, the set of instances participating to a covert channel must cooperate to stay in a chosen set of cyclic behaviors *Q* where information passing is possible, and make sure that the rest of the protocol can not force them to leave Q.

# Asymptotic Durations




$$D(M^n) = max \{ d_{x,y} (M^n) \}$$

<u>Mean durations:</u>

$$md(M^\omega) = \lim_{n \to \infty} \frac{1}{n} . D(M^n)$$

$$md_{x,y}(M^\omega) = \lim_{n \to \infty} \frac{1}{n} . d_{x,y}(M^n)$$

Warning : asynchronous communications

$D(M^n) \leq n . D(M)$ and $md_{x,y}(M^\omega) \leq d_{x,y}(M)$