Surcoût de l'authentification et du consensus dans la sécurité des réseaux sans fil véhiculaires

Jonathan Petit

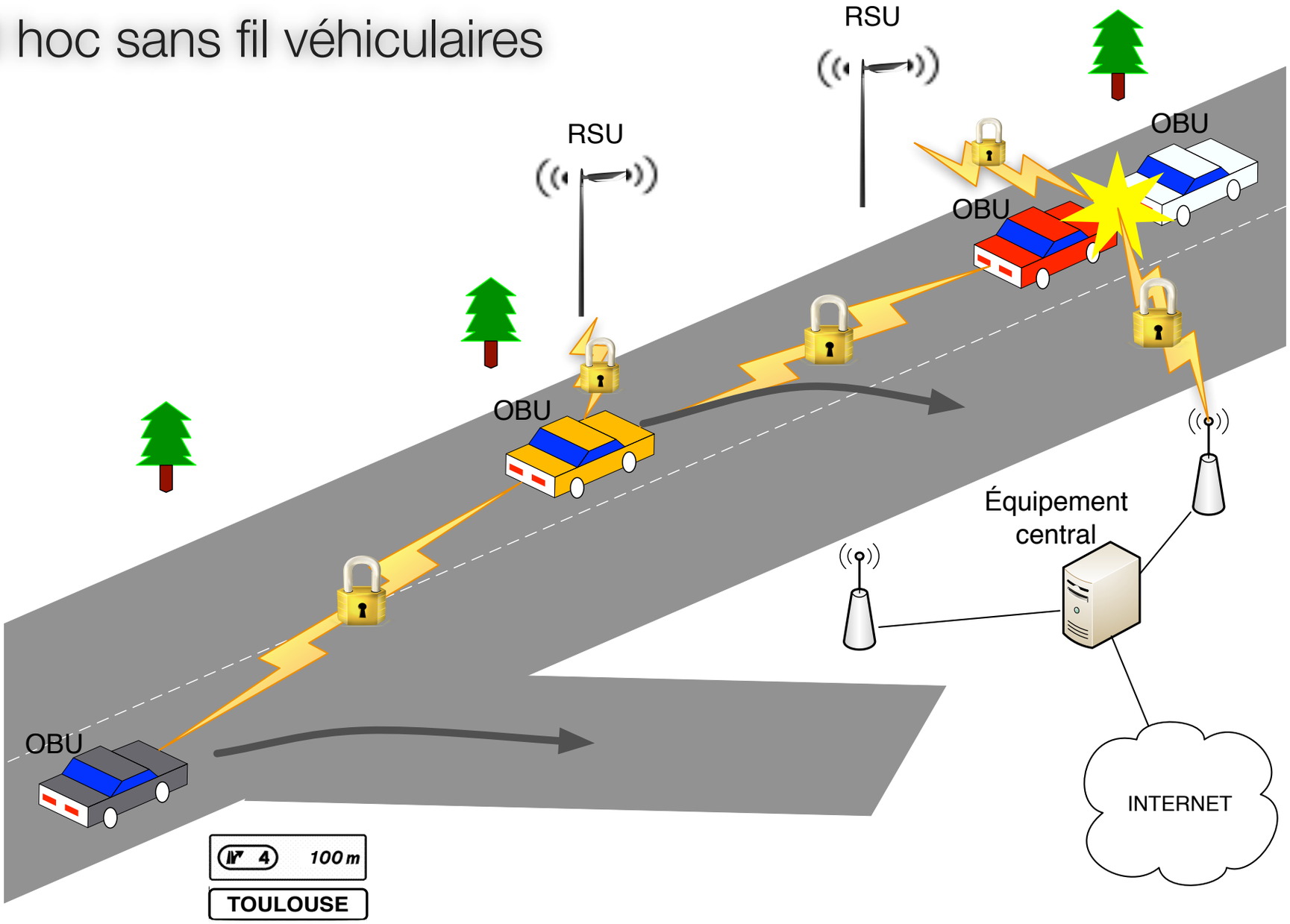
13 Juillet 2011

Thèse dirigée par Zoubir Mammeri

*A*rchitecture
*S*ystèmes
*T*emps
*R*éel
*E*mbarqués

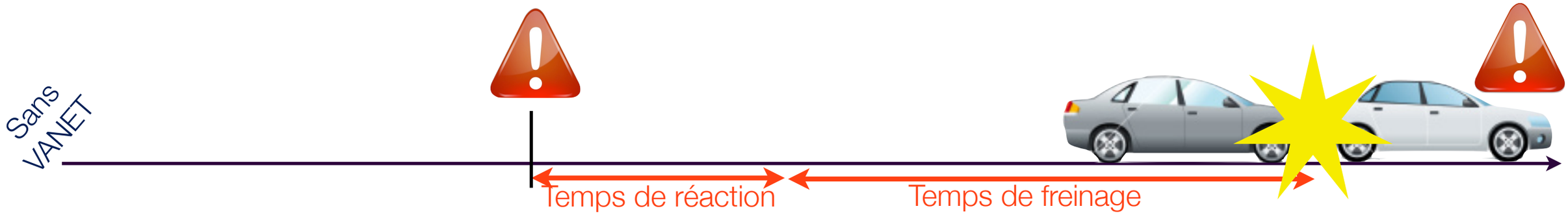
Contexte

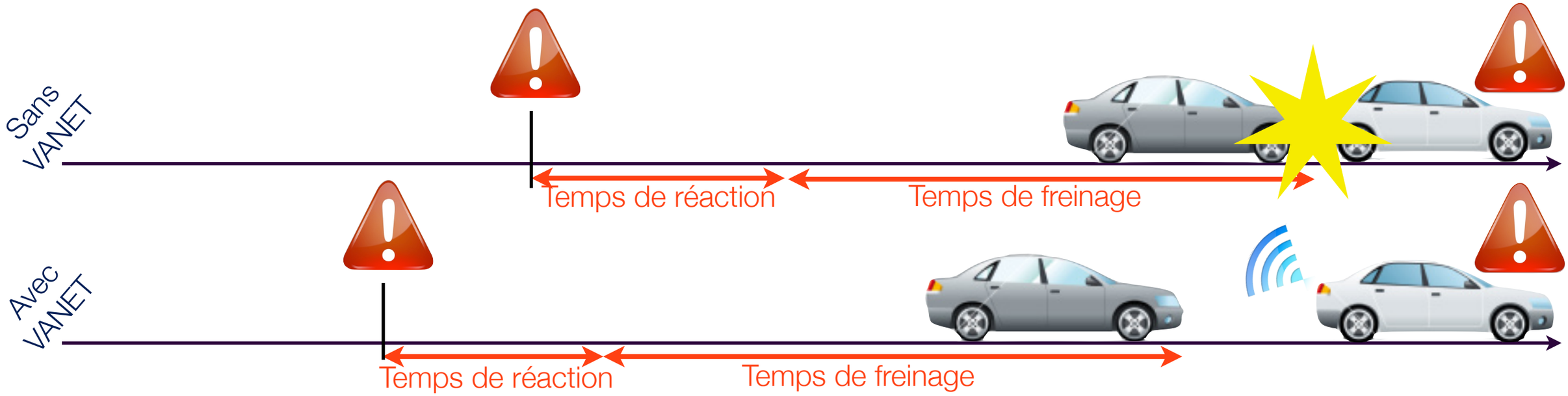
Réseaux ad hoc sans fil véhiculaires

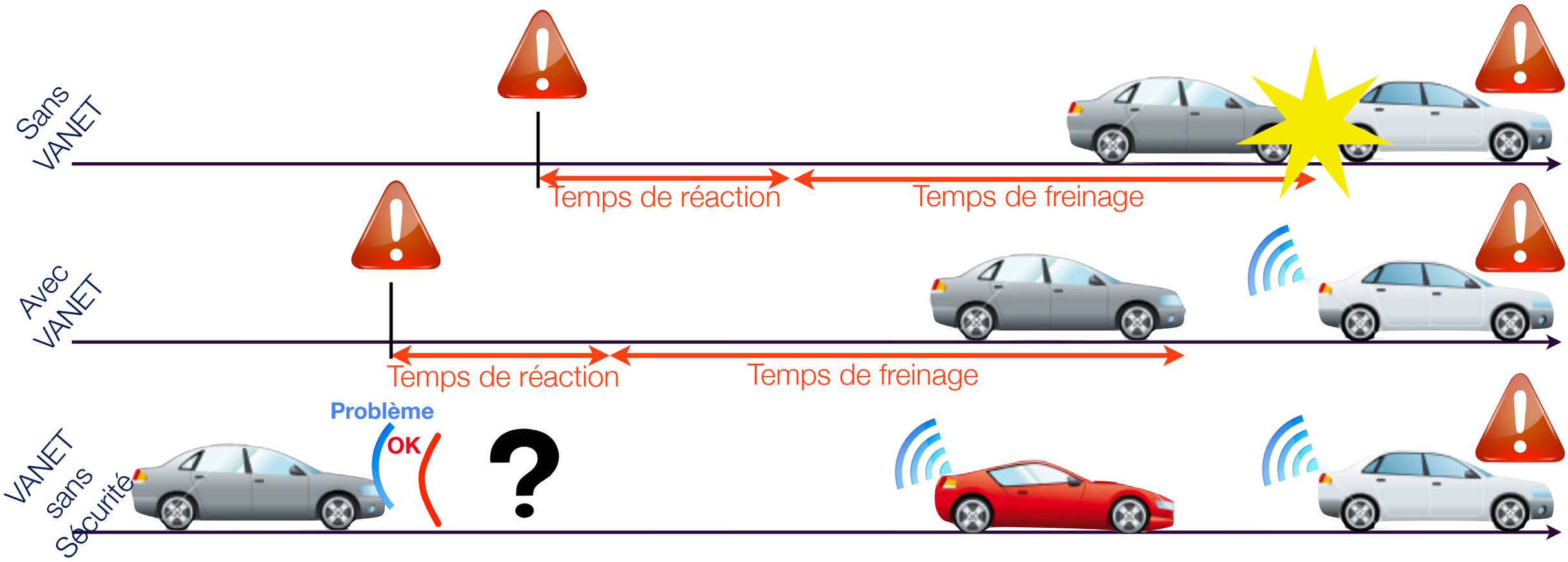


Sans VANET

Sans VANET


Sans
VANET
Temps de réaction
Temps de freinage


Sans VANET
Temps de réaction
Temps de freinage
Avec VANET
Temps de réaction
Temps de freinage


Sans VANET
Temps de réaction
Temps de freinage
Avec VANET
Temps de réaction
Temps de freinage
VANET sans Sécurité
Problème
OK
?

Sans VANET

Temps de réaction

Temps de freinage

Avec VANET

Temps de réaction

Temps de freinage

VANET sans Sécurité

Problème

OK

?

VANET Sécurisé

Opération de sécurité

Temps de réaction

Temps de freinage

Sans VANET

Temps de réaction

Temps de freinage

Avec VANET

Temps de réaction

Temps de freinage

VANET sans Sécurité

Problème

OK

?

VANET Sécurisé

Opération de sécurité

Temps de réaction

Temps de freinage

Opérations de sécurité

Temps de réaction

Temps de freinage

Sans VANET

Temps de réaction

Temps de freinage

Avec VANET

Temps de réaction

Temps de freinage

VANET sans Sécurité

Problème

OK

?

VANET Sécurisé

Opération de sécurité

Temps de réaction

Temps de freinage

Opérations de sécurité

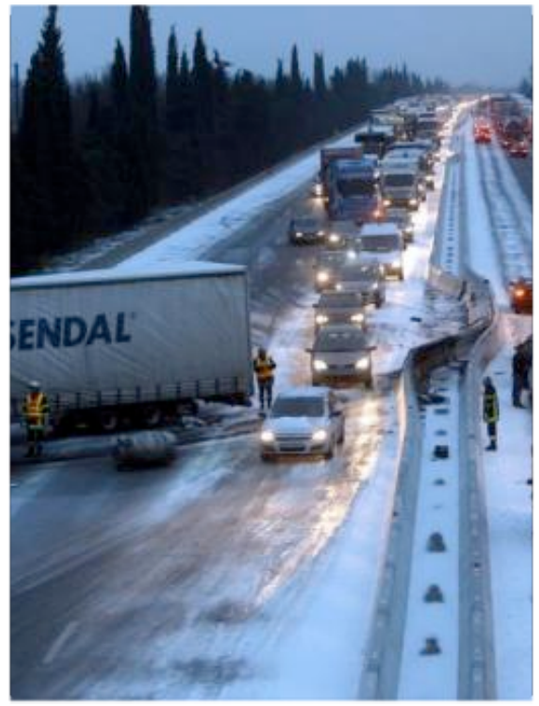
Temps de réaction

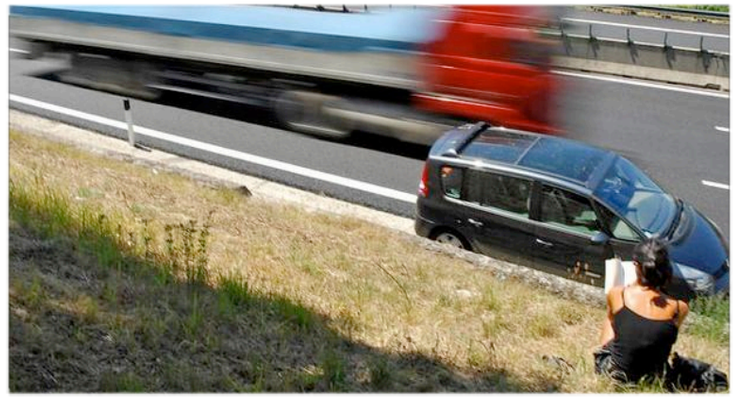
Temps de freinage

?

Applications

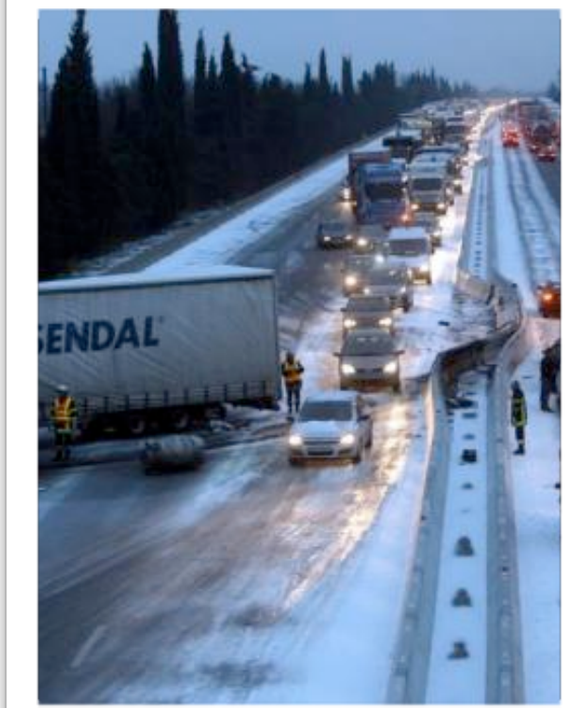
- Sécurité du trafic routier
- Optimisation du trafic routier
- Divertissement

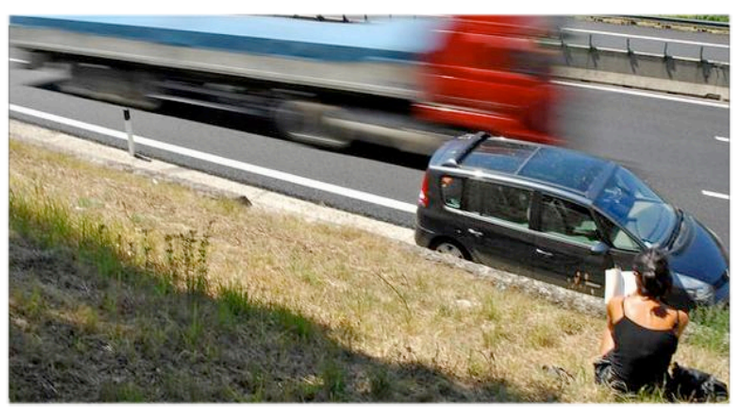




Applications

- Sécurité du trafic routier
- Optimisation du trafic routier
- Divertissement





Paradigme du surcoût

- Authentification
- Consensus
- Disponibilité
- Non-répudiation
- ...

Paradigme du surcoût

- Authentification
- Consensus
- Disponibilité
- Non-répudiation
- ...

$$D_{Authentification} + D_{Consensus} + D_{Disponibilité} + D_{Non-répudiation} + \ldots$$

Paradigme du surcoût

- Authentification
- Consensus
- Disponibilité
- Non-répudiation
- ...

$$\left.\begin{array}{l} D_{Authentification} \\ + \\ D_{Consensus} \\ + \\ D_{Disponibilité} \\ + \\ D_{Non-répudiation} \\ + \\ \ldots \end{array}\right\} = D_{Sécurité}$$

Paradigme du surcoût

- Authentification
- Consensus
- Disponibilité
- Non-répudiation
- ...

$$\left.\begin{aligned} & D_{Authentification} \\ & + \\ & D_{Consensus} \\ & + \\ & D_{Disponibilité} \\ & + \\ & D_{Non-répudiation} \\ & + \\ & \dots \end{aligned}\right\} = D_{Sécurité}$$

Paradigme du surcoût

- Authentification
- Consensus
- Disponibilité
- Non-répudiation
- ...

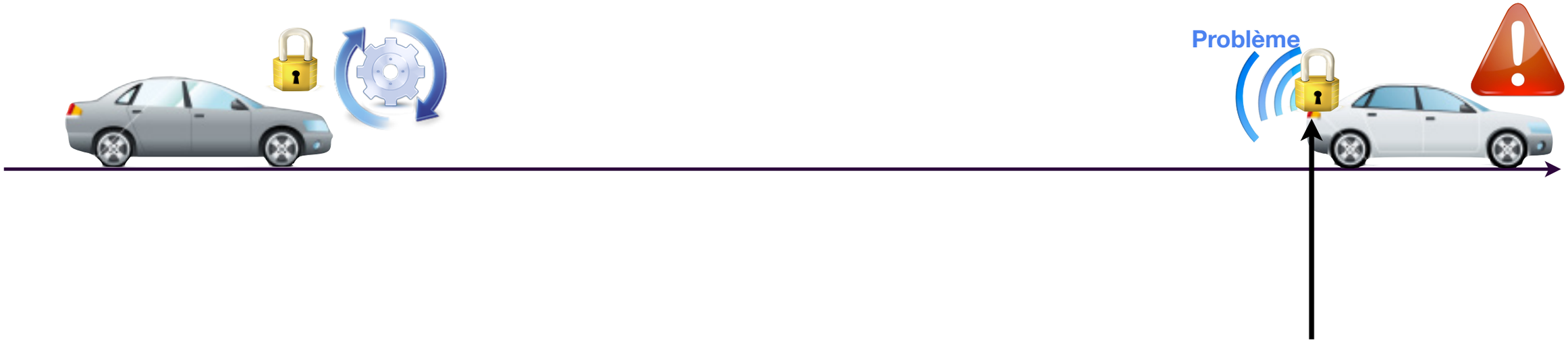
$$\left.\begin{aligned} & D_{Authentification} \\ & + \\ & D_{Consensus} \\ & + \\ & D_{Disponibilité} \\ & + \\ & D_{Non-répudiation} \\ & + \\ & \dots \end{aligned}\right\} = D_{Sécurité}$$

Surcoût de l'authentification

Surcoût de l'authentification

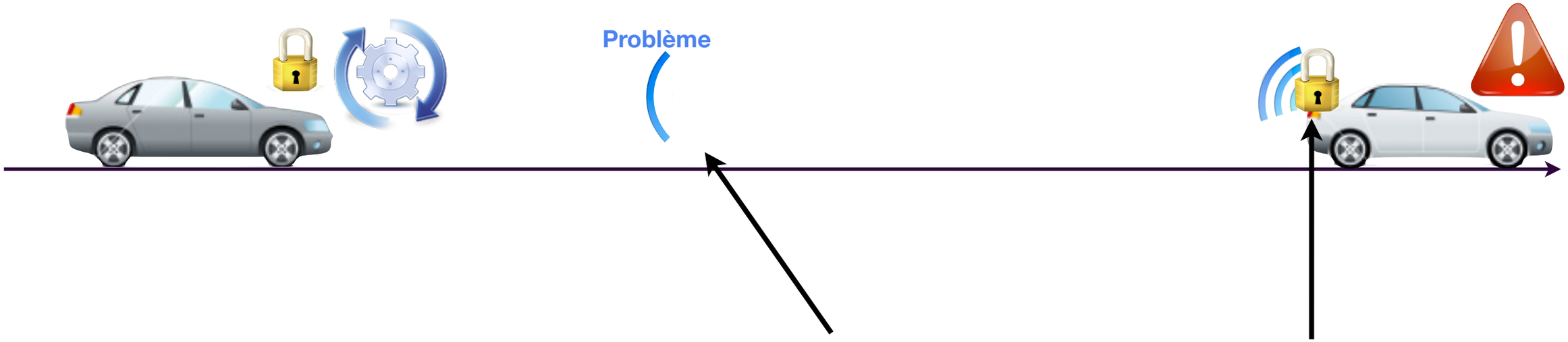
Surcoût de l'authentification

Surcoût de l'authentification

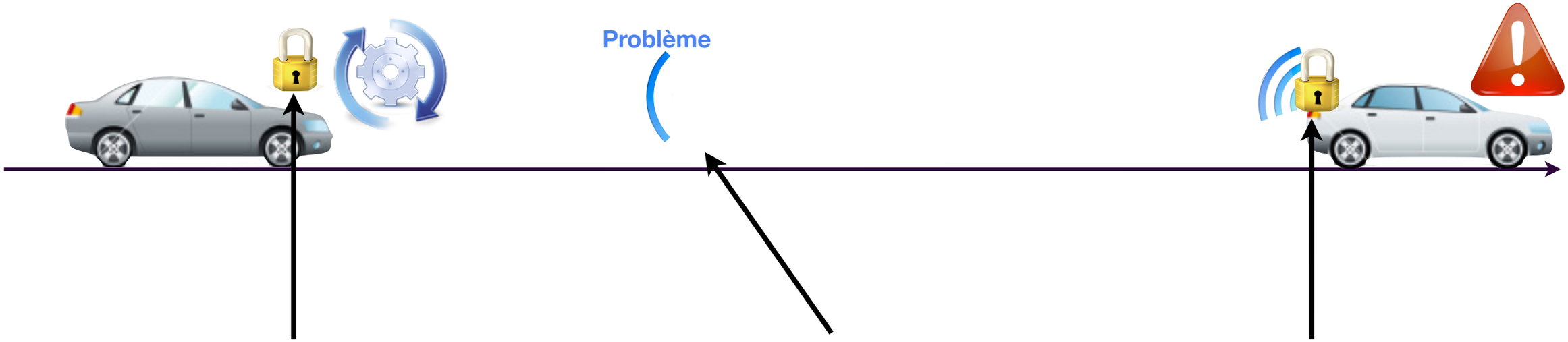


Temps de **génération**
de signature numérique

Surcoût de l'authentification



Surcoût de l'authentification

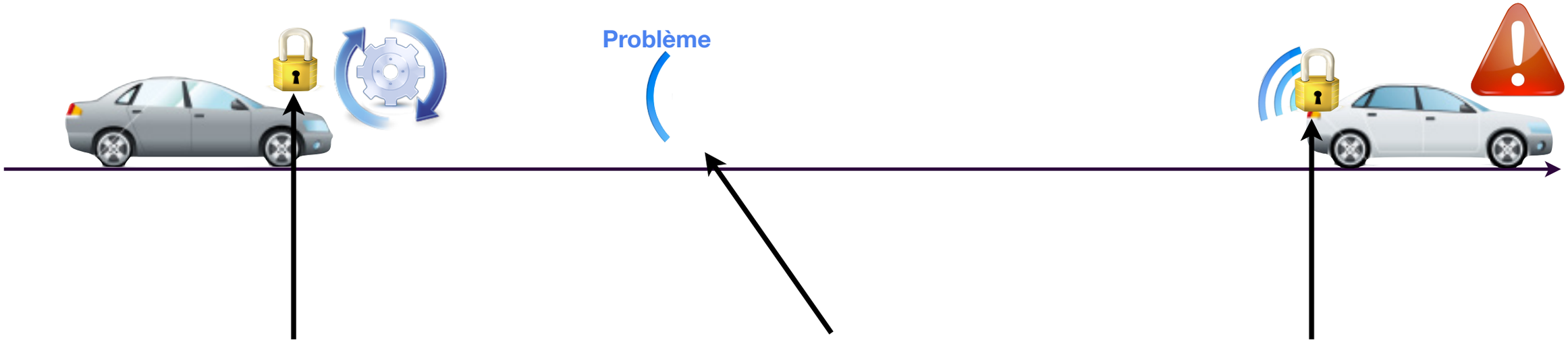


Temps de **vérification** de signature numérique

Temps de **transfert** du message signé

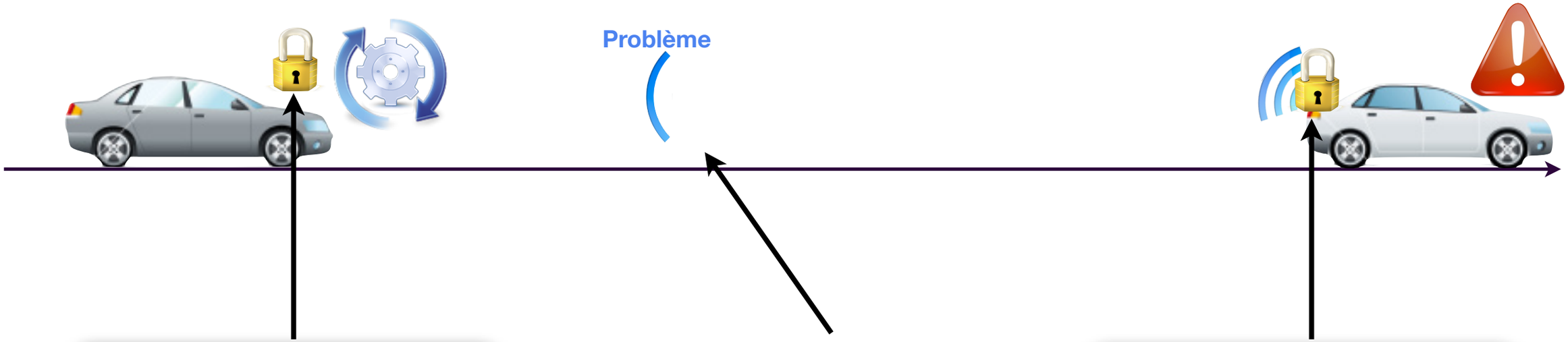
Temps de **génération** de signature numérique

Surcoût de l'authentification



Temps de **vérification** de signature numérique **+** Temps de **transfert** du message signé **+** Temps de **génération** de signature numérique

Surcoût de l'authentification



Temps de **vérification** de signature numérique

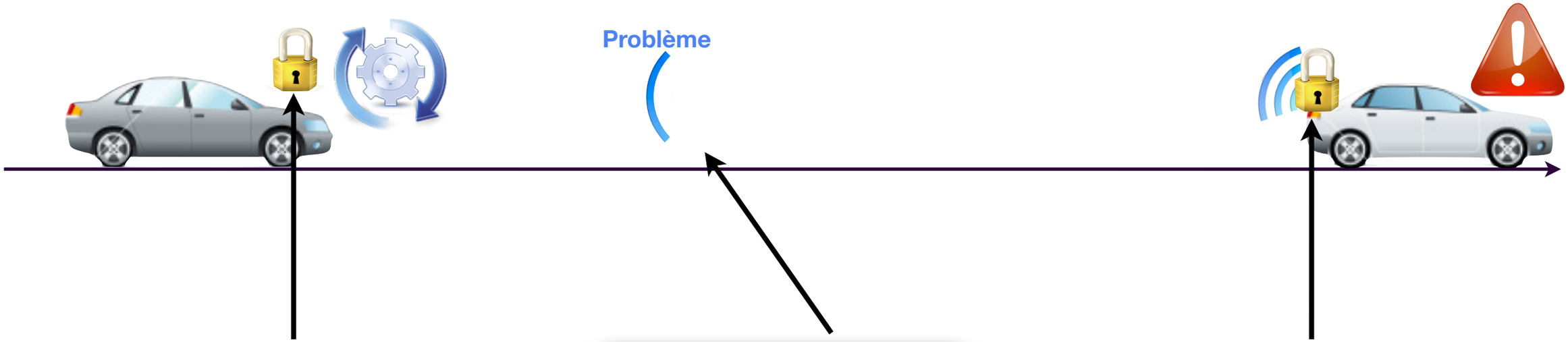
+

Temps de **transfert** du message signé

+

Temps de **génération** de signature numérique

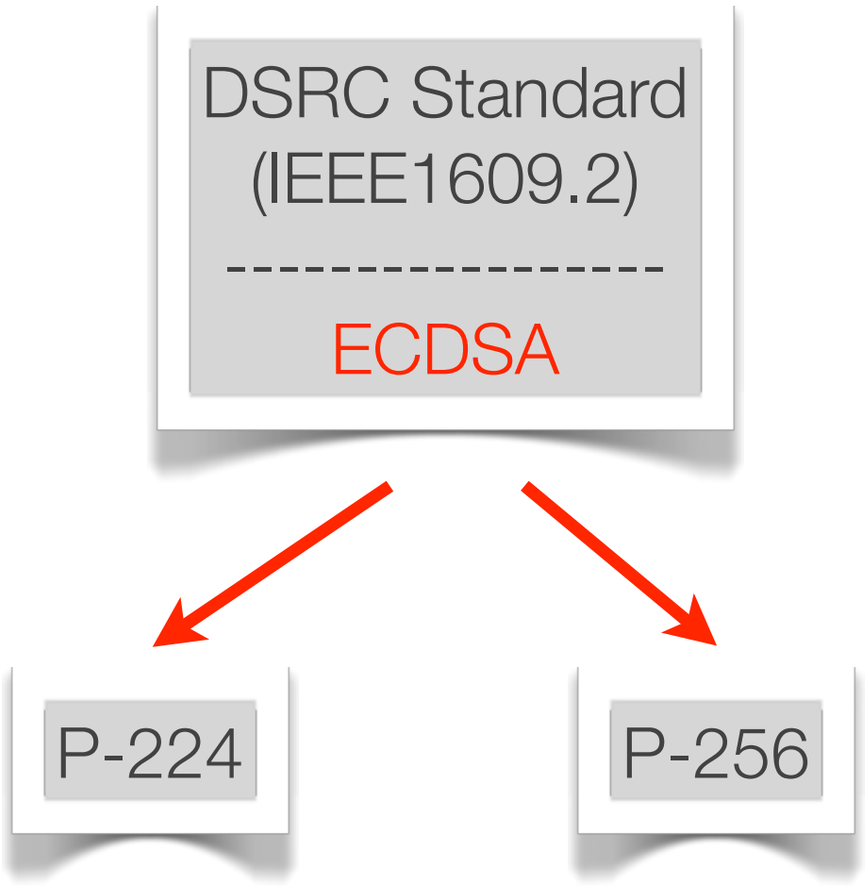
Surcoût de l'authentification



Temps de **vérification** de signature numérique + Temps de **transfert** du message signé + Temps de **génération** de signature numérique

Algorithme d'authentification

Algorithme d'authentification



a. Key generation

1. Obtain a set of elliptic curve domain parameters
   q denotes the size of the underlying field F_q, which can be a large prime or a prime to a power
   $a,b \in F_q$: parameters of elliptic curve E
   $G \in E$: point on E
   n : order of G (n prime greater than 2^{160})
   $h = \frac{ord(E)}{ord(G)}$, where *ord(X)* denotes the order of X
2. Select a random number $d \in [1, n-1]$ as private key
3. Compute the public key $Q = d \times G$

(E,Q,G,n) are public.

b. Signature generation

input: message m and *(d,Q)*

1. Select a random number $k \in [1, n-1]$
2. Compute $k \times G = (x_1, y_1)$ and $r = x_1 \bmod n$
   if $r = 0$ goto 1
3. Compute $s = k^{-1}(e + d \times r) \bmod n$ with $e = H(m)$
   if $s = 0$ goto 1
4. The signature of m is *(r,s)*.

c. Signature verification

input: *(r,s), m, Q*

1. Verify $r, s \in [1, n-1]$
2. Compute $w = s^{-1} \bmod n$
3. Compute $u_1 = e \times w \bmod n$ and $u_2 = r \times w \bmod n$ with $e = H(m)$
4. Compute $X_1 = u_1 \times G + u_2 \times Q$ and $V = X_1 \bmod n$
5. If $V = r$ then signature accepted.

Algorithme d'authentification

DSRC Standard (IEEE1609.2)

ECDSA

P-224

P-256

a. Key generation

1. Obtain a set of elliptic curve domain parameters

q denotes the size of the underlying field F_q, which can be a large prime or a prime to a power

$a,b \in F_q$: parameters of elliptic curve E

$G \in E$: point on E

n : order of G (n prime greater than 2^{160})

$h = \frac{ord(E)}{ord(G)}$, where *ord(X)* denotes the order of X

2. Select a random number $d \in [1, n-1]$ as private key
3. Compute the public key $Q = d \times G$

(E,Q,G,n) are public.

O(n)+O(M*n)

b. Signature generation

input: message m and *(d,Q)*

1. Select a random number $k \in [1, n-1]$
2. Compute $k \times G = (x_1, y_1)$ and $r = x_1 \bmod n$
   if $r = 0$ goto 1
3. Compute $s = k^{-1}(e + d \times r) \bmod n$ with $e = H(m)$
   if $s = 0$ goto 1
4. The signature of m is *(r,s)*.

c. Signature verification

input: *(r,s), m, Q*

1. Verify $r, s \in [1, n-1]$
2. Compute $w = s^{-1} \bmod n$
3. Compute $u_1 = e \times w \bmod n$ and $u_2 = r \times w \bmod n$ with $e = H(m)$
4. Compute $X_1 = u_1 \times G + u_2 \times Q$ and $V = X_1 \bmod n$
5. If $V = r$ then signature accepted.

Temps de calcul d'ECDSA

$$T_{Surcoût\_ECDSA}(M) = T_{sign}(M) + T_{tx}(M) + T_{vérif}(M)$$

Temps de calcul d'ECDSA

$$T_{Surcoût\_ECDSA}(M) = T_{sign}(M) + T_{tx}(M) + T_{vérif}(M)$$

Pentium D 3,4GHz, 1Go RAM

Taille de la clé (bit)	T_{MUL} (µs)	T_{INV} (µs)	T_{kP} (µs)	T_{HASH} (µs)
224	1.23	18.91	2468.71	8.47
256	1.39	22.01	3297.23	10.09

Taille de la clé (bit)	T_{sign} (ms)	$T_{vérif}$ (ms)
224	2.50	4.97
256	3.33	6.63

Temps de calcul d'ECDSA

$$T_{Surcoût\_ECDSA}(M) = T_{sign}(M) + T_{tx}(M) + T_{vérif}(M)$$

Pentium D 3,4GHz, 1Go RAM

Taille de la clé (bit)	T_{MUL} (µs)	T_{INV} (µs)	T_{kP} (µs)	T_{HASH} (µs)
224	1.23	18.91	2468.71	8.47
256	1.39	22.01	3297.23	10.09

9.96 ms =

Taille de la clé (bit)	T_{sign} (ms)	$T_{vérif}$ (ms)
224	2.50	4.97
256	3.33	6.63

Temps de calcul d'ECDSA

$$T_{Surcoût\_ECDSA}(M) = T_{sign}(M) + T_{tx}(M) + T_{vérif}(M)$$

Pentium D 3,4GHz, 1Go RAM

9.96 ms =

Taille de clé (bit)	T_{MUL} (µs)	T_{INV} (µs)	T_{kP} (µs)	T_{HASH} (µs)
224	1.23	18.91	2468.71	8.47
256	1.39	22.01	3297.23	10.09

Taille de la clé (bit)	T_{sign} (ms)	$T_{vérif}$ (ms)
224	2.50	4.97
256	3.33	6.63

Temps de transfert

$$T_{Surcoût\_ECDSA}(M) = T_{sign}(M) + T_{tx}(M) + T_{vérif}(M)$$

Temps de transfert

$$T_{Surcoût\_ECDSA}(M) = T_{sign}(M) + T_{tx}(M) + T_{vérif}(M)$$

$$T_{tx} = \frac{W-1}{2}[\sigma P_e + T_s P_s + T_c P_c] + (1-\pi)^{n-1}(1-e)T_s + (1-(1-\pi)^{n-1}(1-e))T_c$$

T_s, T_c : Durée de transmission réussie, de collision
W : Taille de la fenêtre de contention
σ : Intervalle de temps
P_e, P_s, P_c : Probabilité de canal libre, de transmission réussie, de collision
n : Nombre de vehicules
e : Probabilité de corruption par le bruit
π : Probabilité de transmission dans un intervalle de temps

Vinel A., Andreev S., Koucheryavy Y., Staehle D., “Estimation of a Successful Beacon Reception Probability in Vehicular Ad-hoc Networks”, *ACM International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly (IWCMC),* pp. 416-420, Leipzig, Germany, June 2009.

Temps de transfert

$$T_{Surcoût\_ECDSA}(M) = T_{sign}(M) + T_{tx}(M) + T_{vérif}(M)$$

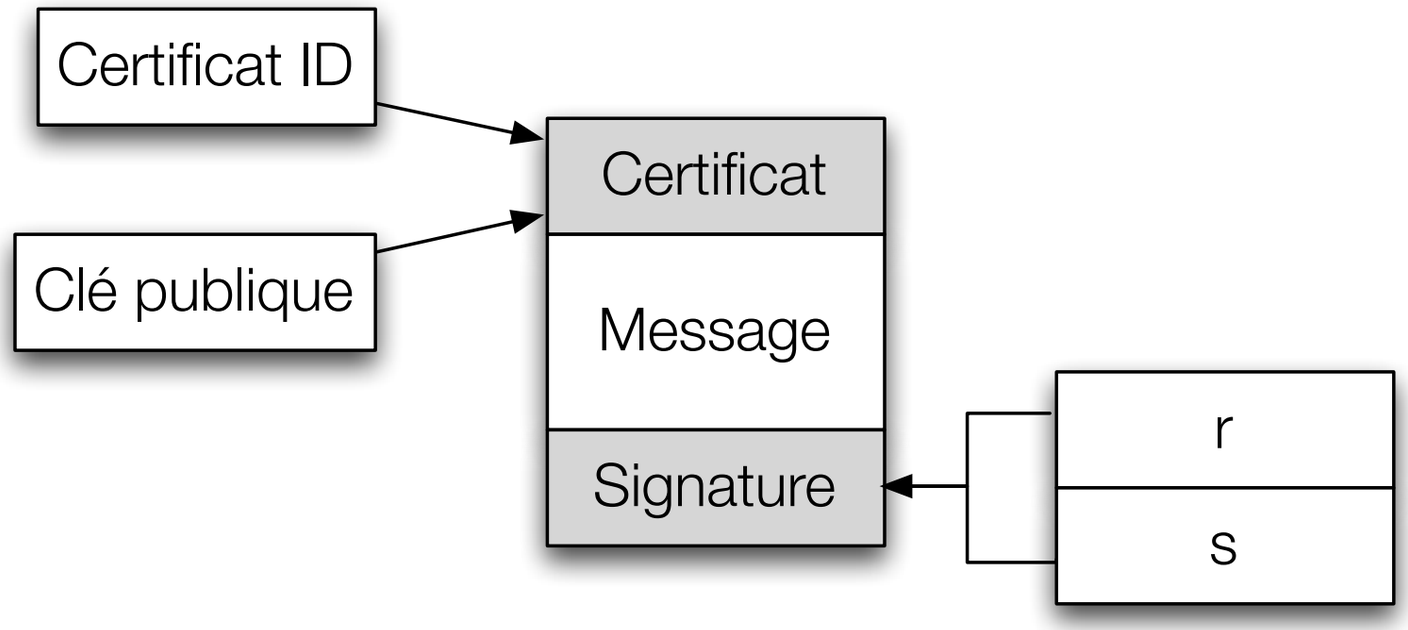
$$T_{tx} = \frac{W-1}{2}[\sigma P_e + T_s P_s + T_c P_c] + (1-\pi)^{n-1}(1-e)T_s + (1-(1-\pi)^{n-1}(1-e))T_c$$

T_s, T_c : Durée de transmission réussie, de collision
W : Taille de la fenêtre de contention
σ : Intervalle de temps
P_e, P_s, P_c : Probabilité de canal libre, de transmission réussie, de collision
n : Nombre de vehicules
e : Probabilité de corruption par le bruit
π : Probabilité de transmission dans un intervalle de temps

Vinel A., Andreev S., Koucheryavy Y., Staehle D., “Estimation of a Successful Beacon Reception Probability in Vehicular Ad-hoc Networks”, *ACM International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly (IWCMC),* pp. 416-420, Leipzig, Germany, June 2009.

Surcoût taille de paquet

Calcul du surcoût : $S_{ov} = S_{cert} + S_{sign}$



Surcoût taille de paquet

Calcul du surcoût : $S_{ov} = S_{cert} + S_{sign}$

- Taille de la signature

$$S_{sign} = \frac{S_{sigmess}}{8} \times 2 = \frac{S_{sigmess}}{4}$$

Taille	Champs		
1	Version de protocole = 1		
1	Type		
1	Information du signataire	Type (certificat ou condensé)	
125		Certificat	
67	Message non signé		
28	Signature	Signature ECDSA	r
28			s

Surcoût taille de paquet

Calcul du surcoût : $$S_{ov} = S_{cert} + S_{sign} = \frac{S_{pu}}{8} + 1 + \frac{S_{sigcert}}{4} + \frac{S_{sigmess}}{4}$$

Taille de la signature

$$S_{sign} = \frac{S_{sigmess}}{8} \times 2 = \frac{S_{sigmess}}{4}$$

Taille du certificat

$$S_{cert} = \left(\frac{S_{pu}}{8} + 1\right) + \left(\frac{S_{sigcert}}{8} \times 2\right) = \left(\frac{S_{pu}}{8} + 1\right) + \left(\frac{S_{sigcert}}{4}\right)$$

<table>
<tr><th>Taille</th><th colspan="3">Champs</th></tr>
<tr><td>1</td><td colspan="3">Version du certificat = 1</td></tr>
<tr><td>8</td><td rowspan="6">Certificat non signé</td><td colspan="2">ID du signataire</td></tr>
<tr><td>21</td><td colspan="2"></td></tr>
<tr><td>1</td><td rowspan="3">Clé(s) publique (s) certifiée(s)</td><td>Taille du champ "Clé publique"</td></tr>
<tr><td>1</td><td>Algorithme utilisé</td></tr>
<tr><td>29</td><td>Clé publique</td></tr>
<tr><td>32</td><td rowspan="2">Signature</td><td rowspan="2">Signature ECDSA</td><td>r</td></tr>
<tr><td>32</td><td>s</td></tr>
</table>

Temps de transfert

$$T_{Surcoût\_ECDSA}(M) = T_{sign}(M) + T_{tx}(M) + T_{vérif}(M)$$

Temps de transfert

$$T_{Surcoût\_ECDSA}(M) = T_{sign}(M) + T_{tx}(M) + T_{vérif}(M)$$

$$T_{tx} = \frac{W-1}{2}[\sigma P_e + T_s P_s + T_c P_c] + (1-\pi)^{n-1}(1-e)T_s + (1-(1-\pi)^{n-1}(1-e))T_c$$

Temps de transfert

$$T_{Surcoût\_ECDSA}(M) = T_{sign}(M) + T_{tx}(M) + T_{vérif}(M)$$

$$T_{tx}(S_{ov}) = \frac{W-1}{2}\left[\sigma P_e + (T_h + \frac{S_{ov}\times 8}{D_R} + DIFS + \delta)P_s + (T_h + \frac{S_{ov}\times 8}{D_R} + EIFS + \delta)P_c\right]$$

$$+(1-\pi)^{n-1}(1-e)(T_h + \frac{S_{ov}\times 8}{D_R} + DIFS + \delta)$$

$$+(1-(1-\pi)^{n-1}(1-e))(T_h + \frac{S_{ov}\times 8}{D_R} + EIFS + \delta)$$

Temps de transfert

$$T_{Surcoût\_ECDSA}(M) = T_{sign}(M) + T_{tx}(M) + T_{vérif}(M)$$

$$T_{tx}(S_{ov}) = \frac{W-1}{2}\left[\sigma P_e + (T_h + \frac{S_{ov}\times 8}{D_R} + DIFS + \delta)P_s + (T_h + \frac{S_{ov}\times 8}{D_R} + EIFS + \delta)P_c\right]$$

$$+(1-\pi)^{n-1}(1-e)(T_h + \frac{S_{ov}\times 8}{D_R} + DIFS + \delta)$$

$$+(1-(1-\pi)^{n-1}(1-e))(T_h + \frac{S_{ov}\times 8}{D_R} + EIFS + \delta)$$

Temps de transfert

$$T_{Surcoût\_ECDSA}(M) = T_{sign}(M) + T_{tx}(M) + T_{vérif}(M)$$

$$T_{tx}(S_{ov}) = \frac{W-1}{2}\left[\sigma P_e + (T_h + \frac{S_{ov}\times 8}{D_R} + DIFS + \delta)P_s + (T_h + \frac{S_{ov}\times 8}{D_R} + EIFS + \delta)P_c\right]$$

$$+(1-\pi)^{n-1}(1-e)(T_h + \frac{S_{ov}\times 8}{D_R} + DIFS + \delta)$$

$$+(1-(1-\pi)^{n-1}(1-e))(T_h + \frac{S_{ov}\times 8}{D_R} + EIFS + \delta)$$

Surcoût global de l'authentification

$$T_{Surcoût\_ECDSA}(M) = T_{sign}(M) + T_{tx}(M) + T_{vérif}(M)$$

$$T_{ov}(M) = T_{sign}(M) + T_{tx}(S_{ov}) + T_{verif}(M)$$

$$= (6n+2)T_{MUL} + T_{INV} + 5nT_{SQR} + T_{HASH}$$

$$+\frac{W-1}{2}\left[\sigma P_e + \left(T_h + \frac{S_{pu} + 2\times(S_{sigcert} + S_{sigmess}) + 8}{D_R} + DIFS + \delta\right)P_s\right.$$

$$\left. + \left(T_h + \frac{S_{pu} + 2\times(S_{sigcert} + S_{sigmess}) + 8}{D_R} + EIFS + \delta\right)P_c\right]$$

$$+(1-\pi)^{n-1}(1-e)\left(T_h + \frac{S_{pu} + 2\times(S_{sigcert} + S_{sigmess}) + 8}{D_R} + DIFS + \delta\right)$$

$$+\left(1-(1-\pi)^{n-1}(1-e)\right)\left(T_h + \frac{S_{pu} + 2\times(S_{sigcert} + S_{sigmess}) + 8}{D_R} + EIFS + \delta\right)$$

$$+(12n+2)T_{MUL} + T_{INV} + 10nT_{SQR} + T_{HASH}$$

Surcoût global de l'authentification

$$T_{Surcoût\_ECDSA}(M) = T_{sign}(M) + T_{tx}(M) + T_{vérif}(M)$$

$$T_{ov}(M) = T_{sign}(M) + T_{tx}(S_{ov}) + T_{verif}(M)$$

$$= (6n+2)T_{MUL} + T_{INV} + 5nT_{SQR} + T_{HASH}$$

$$+\frac{W-1}{2}\left[\sigma P_e + \left(T_h + \frac{S_{pu} + 2\times(S_{sigcert} + S_{sigmess}) + 8}{D_R} + DIFS + \delta\right)P_s\right.$$

$$\left. + \left(T_h + \frac{S_{pu} + 2\times(S_{sigcert} + S_{sigmess}) + 8}{D_R} + EIFS + \delta\right)P_c\right]$$

$$+(1-\pi)^{n-1}(1-e)\left(T_h + \frac{S_{pu} + 2\times(S_{sigcert} + S_{sigmess}) + 8}{D_R} + DIFS + \delta\right)$$

$$+\left(1-(1-\pi)^{n-1}(1-e)\right)\left(T_h + \frac{S_{pu} + 2\times(S_{sigcert} + S_{sigmess}) + 8}{D_R} + EIFS + \delta\right)$$

$$+(12n+2)T_{MUL} + T_{INV} + 10nT_{SQR} + T_{HASH}$$

Surcoût global de l'authentification

$$T_{Surcoût\_ECDSA}(M) = T_{sign}(M) + T_{tx}(M) + T_{vérif}(M)$$

$$T_{ov}(M) = T_{sign}(M) + T_{tx}(S_{ov}) + T_{verif}(M)$$

$$= (6n+2)T_{MUL} + T_{INV} + 5nT_{SQR} + T_{HASH}$$

$$+ \frac{W-1}{2}\left[\sigma P_e + \left(T_h + \frac{S_{pu} + 2\times(S_{sigcert} + S_{sigmess}) + 8}{D_R} + DIFS + \delta\right)P_s\right.$$

$$\left. + \left(T_h + \frac{S_{pu} + 2\times(S_{sigcert} + S_{sigmess}) + 8}{D_R} + EIFS + \delta\right)P_c\right]$$

$$+ (1-\pi)^{n-1}(1-e)\left(T_h + \frac{S_{pu} + 2\times(S_{sigcert} + S_{sigmess}) + 8}{D_R} + DIFS + \delta\right)$$

$$+ \left(1-(1-\pi)^{n-1}(1-e)\right)\left(T_h + \frac{S_{pu} + 2\times(S_{sigcert} + S_{sigmess}) + 8}{D_R} + EIFS + \delta\right)$$

$$+ (12n+2)T_{MUL} + T_{INV} + 10nT_{SQR} + T_{HASH}$$

Surcoût global de l'authentification

$$T_{Surcoût\_ECDSA}(M) = T_{sign}(M) + T_{tx}(M) + T_{vérif}(M)$$

$$T_{ov}(M) = T_{sign}(M) + T_{tx}(S_{ov}) + T_{verif}(M)$$

$$= (6n+2)T_{MUL} + T_{INV} + 5nT_{SQR} + T_{HASH}$$

$$+ \frac{W-1}{2}\left[\sigma P_e + \left(T_h + \frac{S_{pu} + 2\times(S_{sigcert} + S_{sigmess}) + 8}{D_R} + DIFS + \delta\right)P_s\right.$$

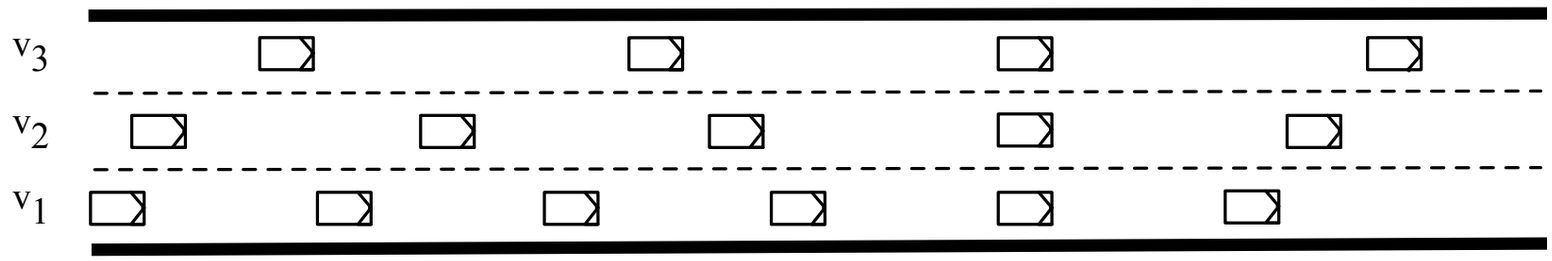
$$\left. + \left(T_h + \frac{S_{pu} + 2\times(S_{sigcert} + S_{sigmess}) + 8}{D_R} + EIFS + \delta\right)P_c\right]$$

$$+ (1-\pi)^{n-1}(1-e)\left(T_h + \frac{S_{pu} + 2\times(S_{sigcert} + S_{sigmess}) + 8}{D_R} + DIFS + \delta\right)$$

$$+ \left(1-(1-\pi)^{n-1}(1-e)\right)\left(T_h + \frac{S_{pu} + 2\times(S_{sigcert} + S_{sigmess}) + 8}{D_R} + EIFS + \delta\right)$$

$$+ (12n+2)T_{MUL} + T_{INV} + 10nT_{SQR} + T_{HASH}$$

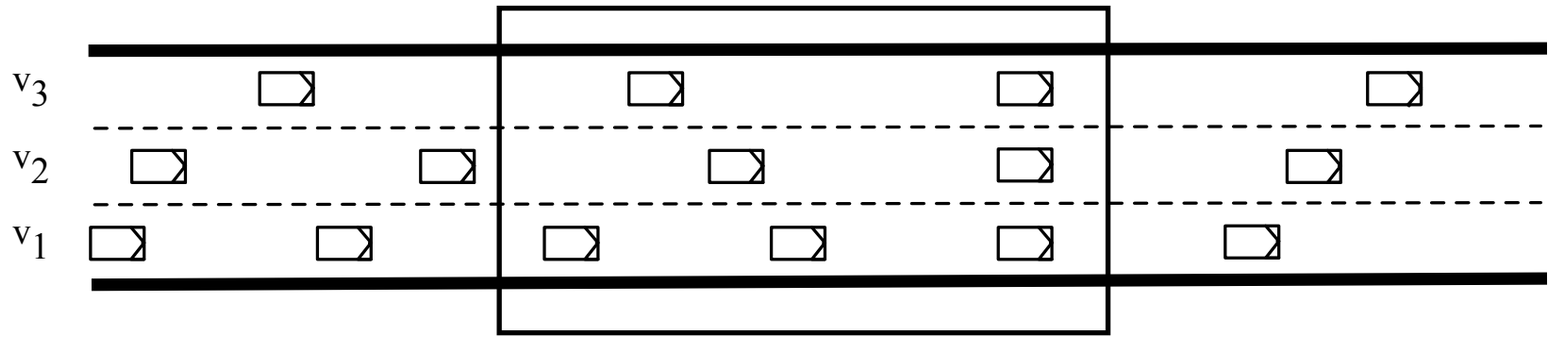
Simulation



NS-2

- Couche PHY et MAC : 802.11p
- Modèle de propagation : Nakagami m=3
- Autoroute, 5 km, 3 voies (v_1=27.7 m/s, v_2=30.5 m/s, v_3=36.1 m/s)
- Fréquence d'envoi : 10 paquets/s
- Portée de communication : 300 m

Simulation

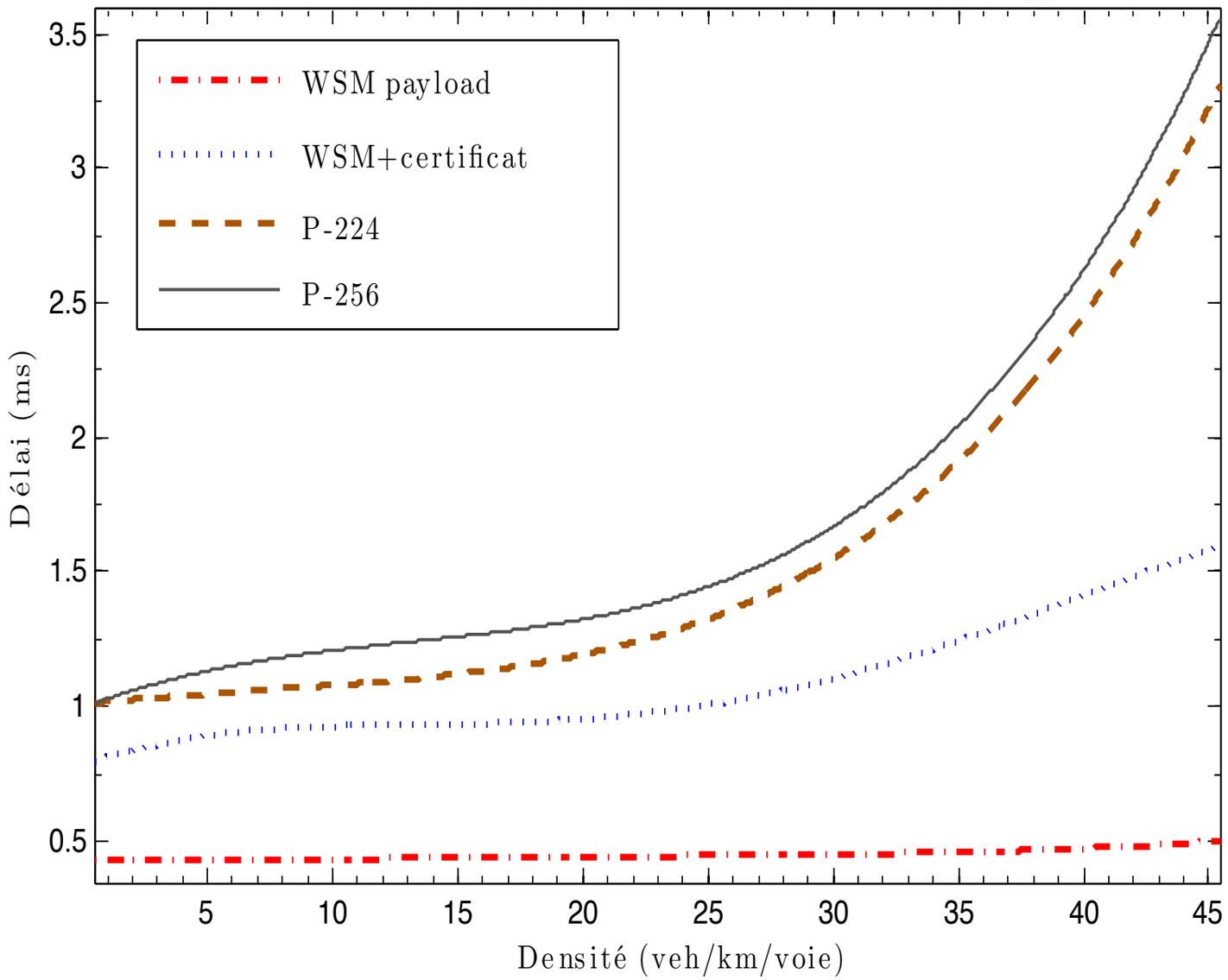


NS-2

- Couche PHY et MAC : 802.11p
- Modèle de propagation : Nakagami m=3
- Autoroute, 5 km, 3 voies (v_1=27.7 m/s, v_2=30.5 m/s, v_3=36.1 m/s)
- Fréquence d'envoi : 10 paquets/s
- Portée de communication : 300 m

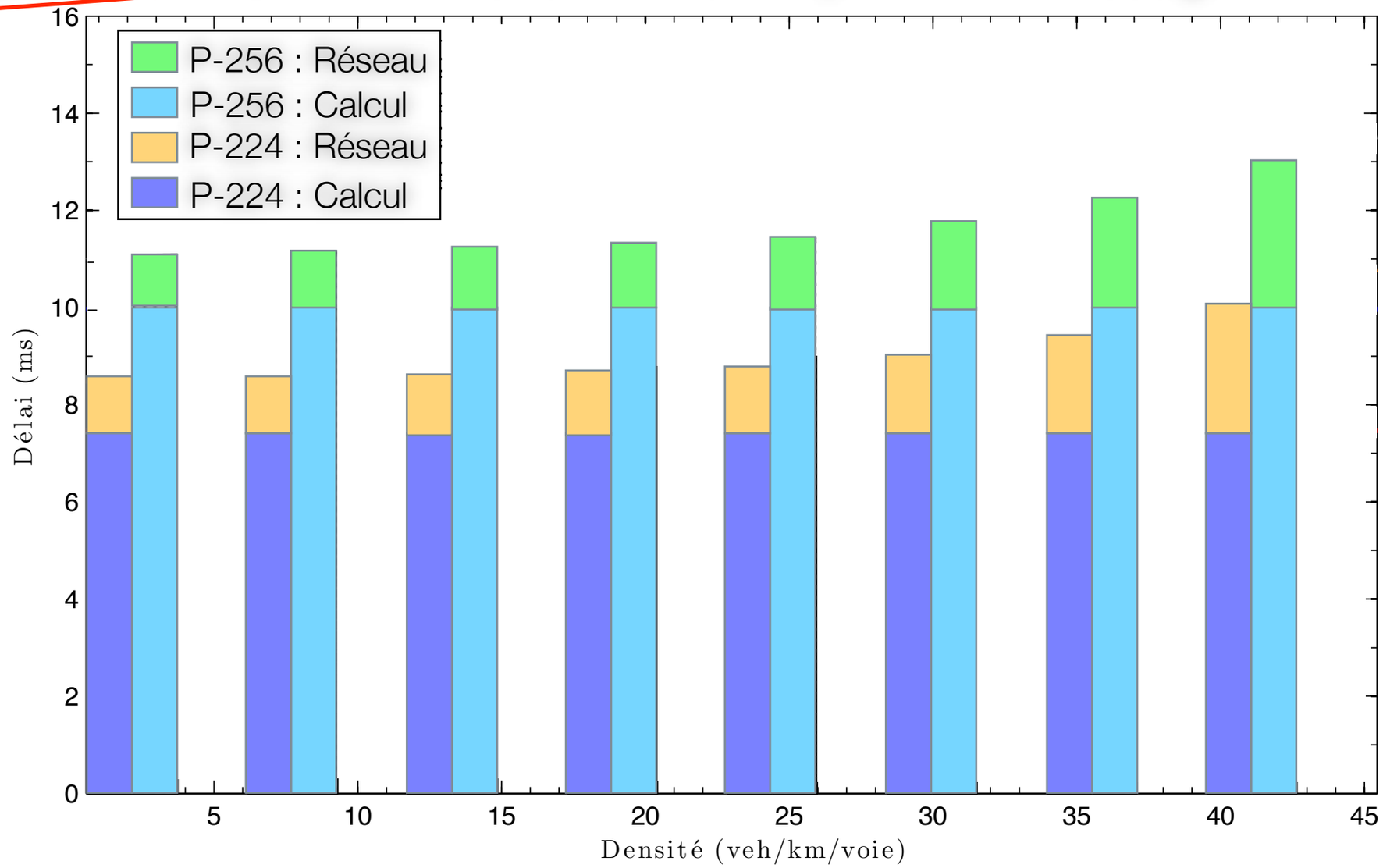
Résultats de simulation (1/4)

Délai de transfert



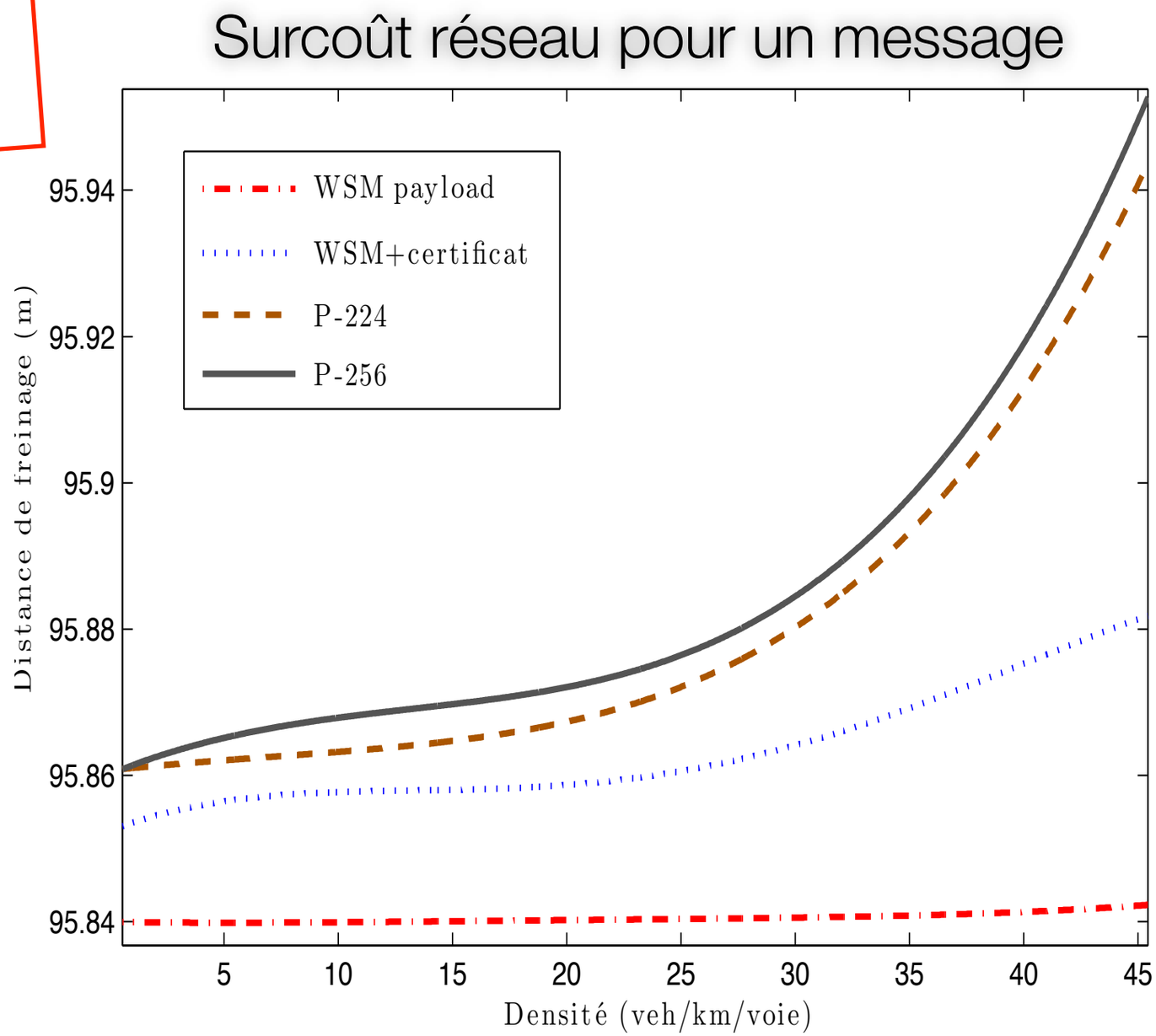
Résultats de simulation (2/4)

Délai de transfert



Résultats de simulation (3/4)

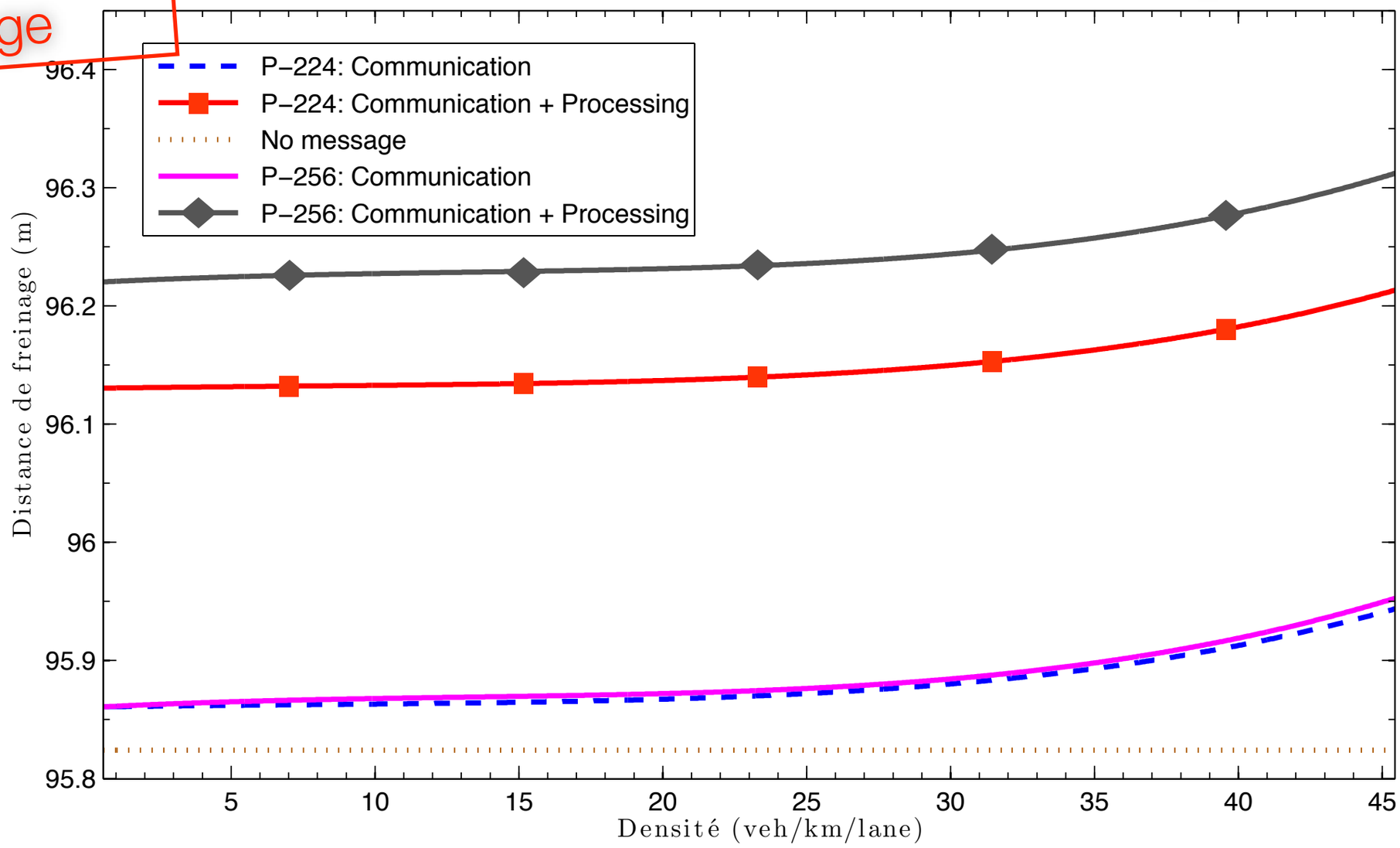
Distance de freinage



Résultats de simulation (4/4)

Distance de freinage

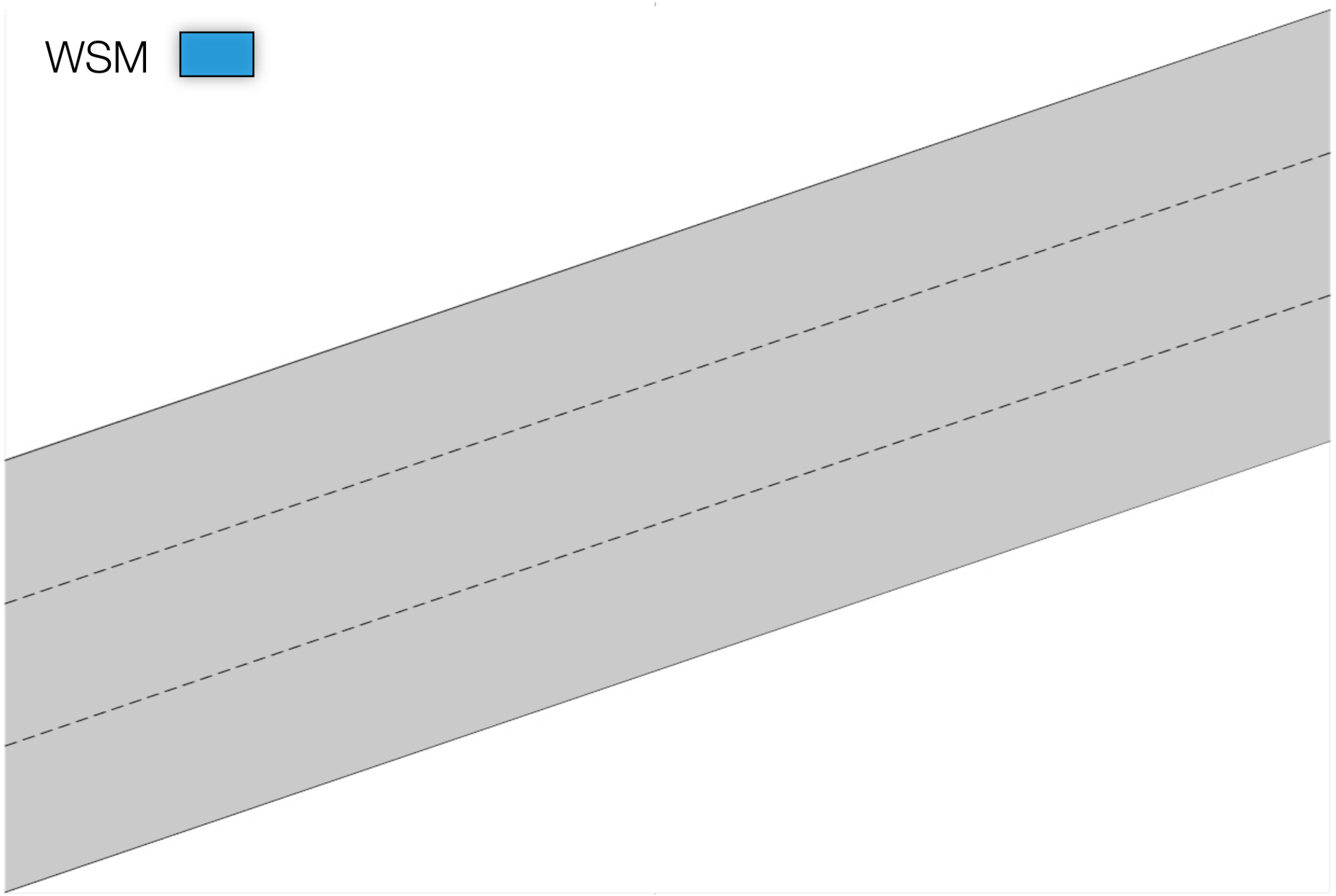
Surcoût réseau et calcul pour un message



Surcoût du consensus

Problématique

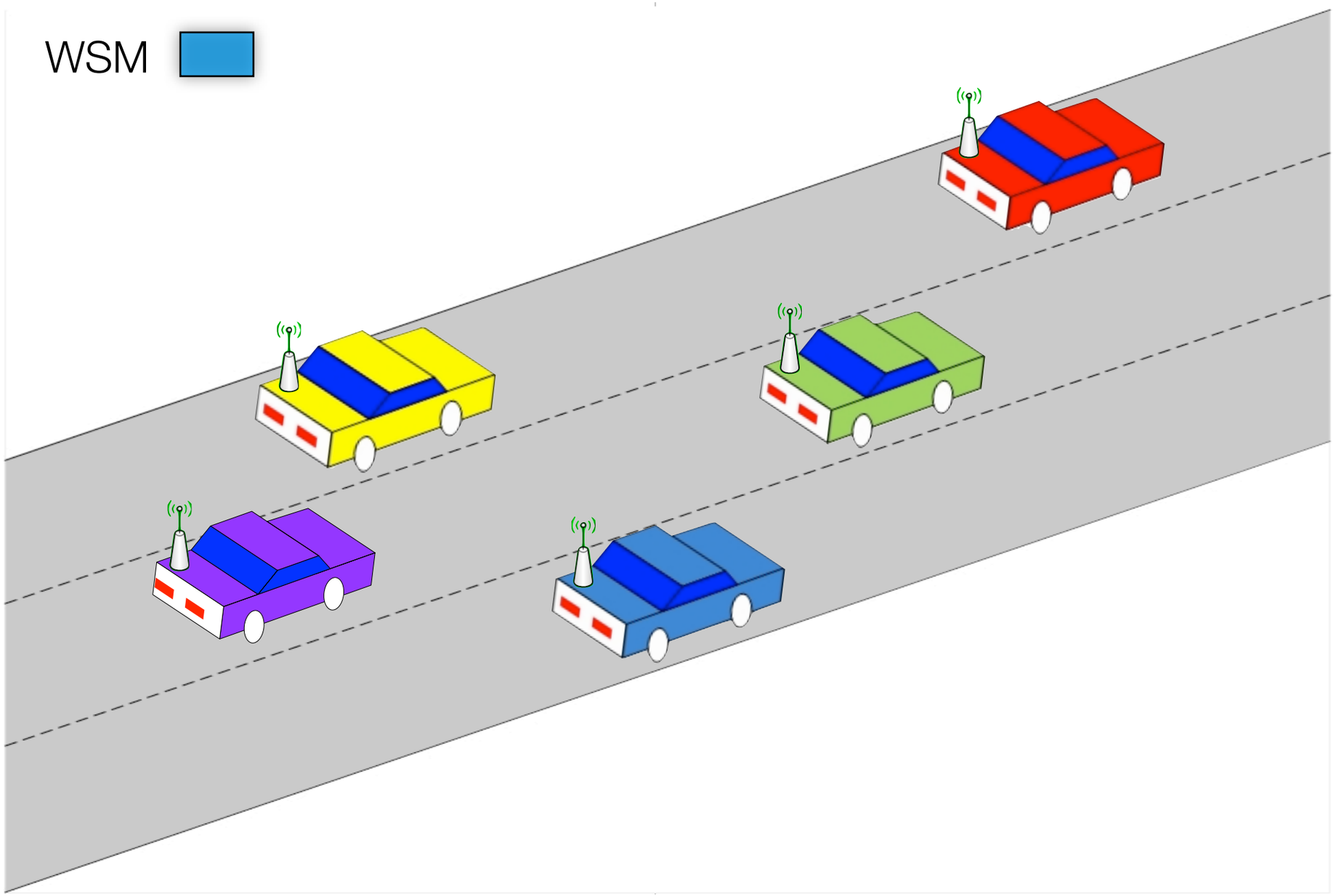
But:
Augmenter la confiance



Problématique

But:
Augmenter la confiance

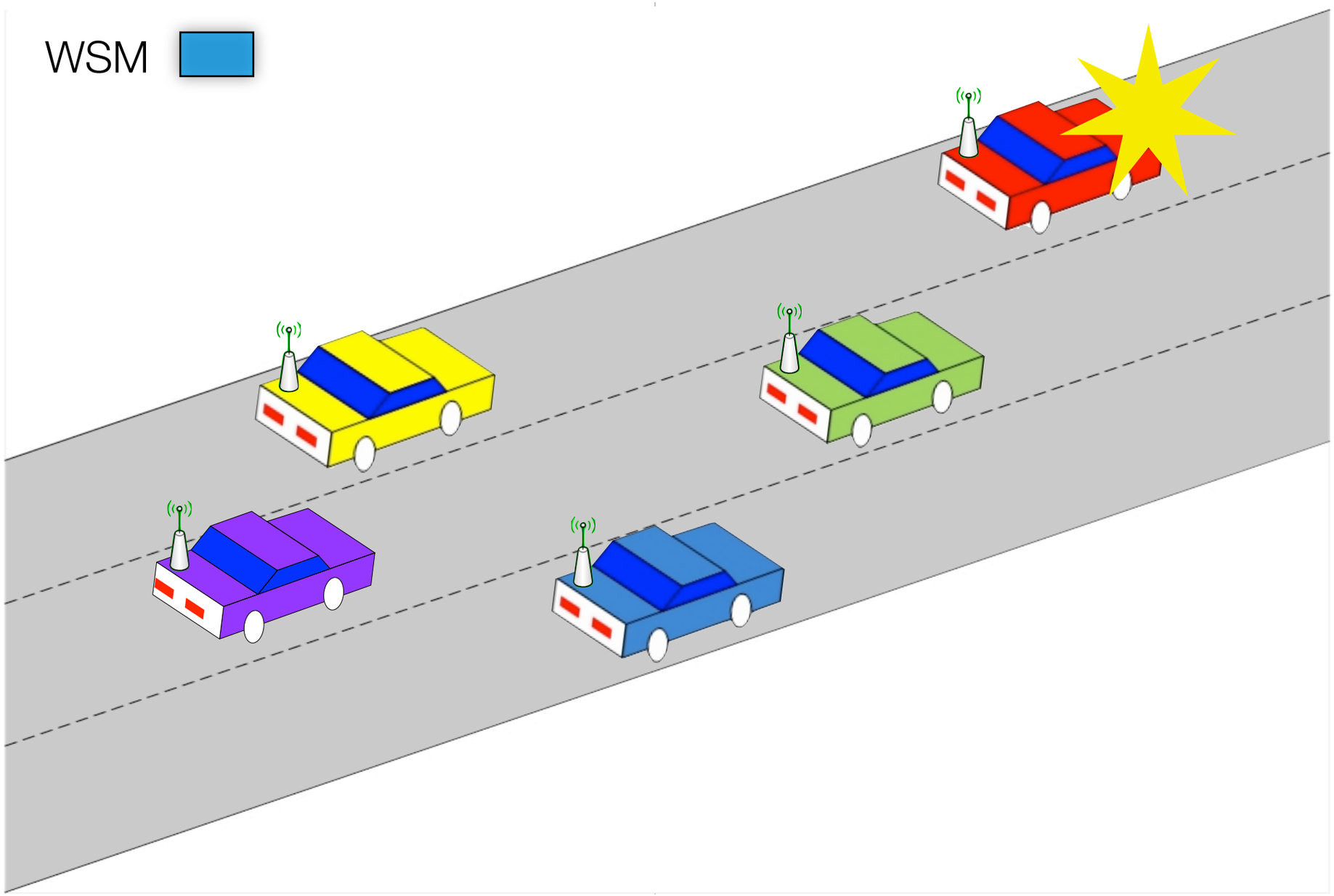
WSM



Problématique

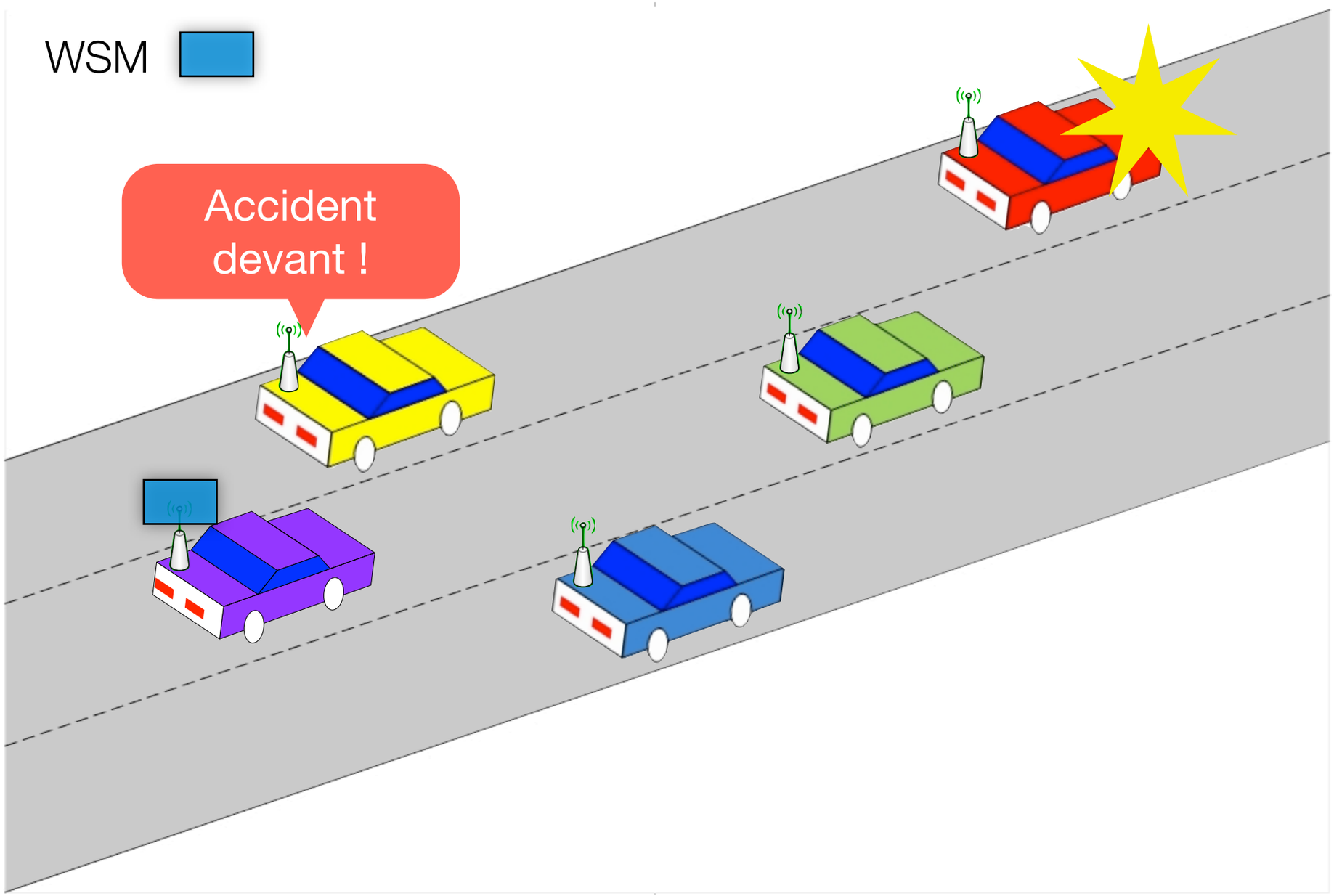
But:
Augmenter la confiance

WSM



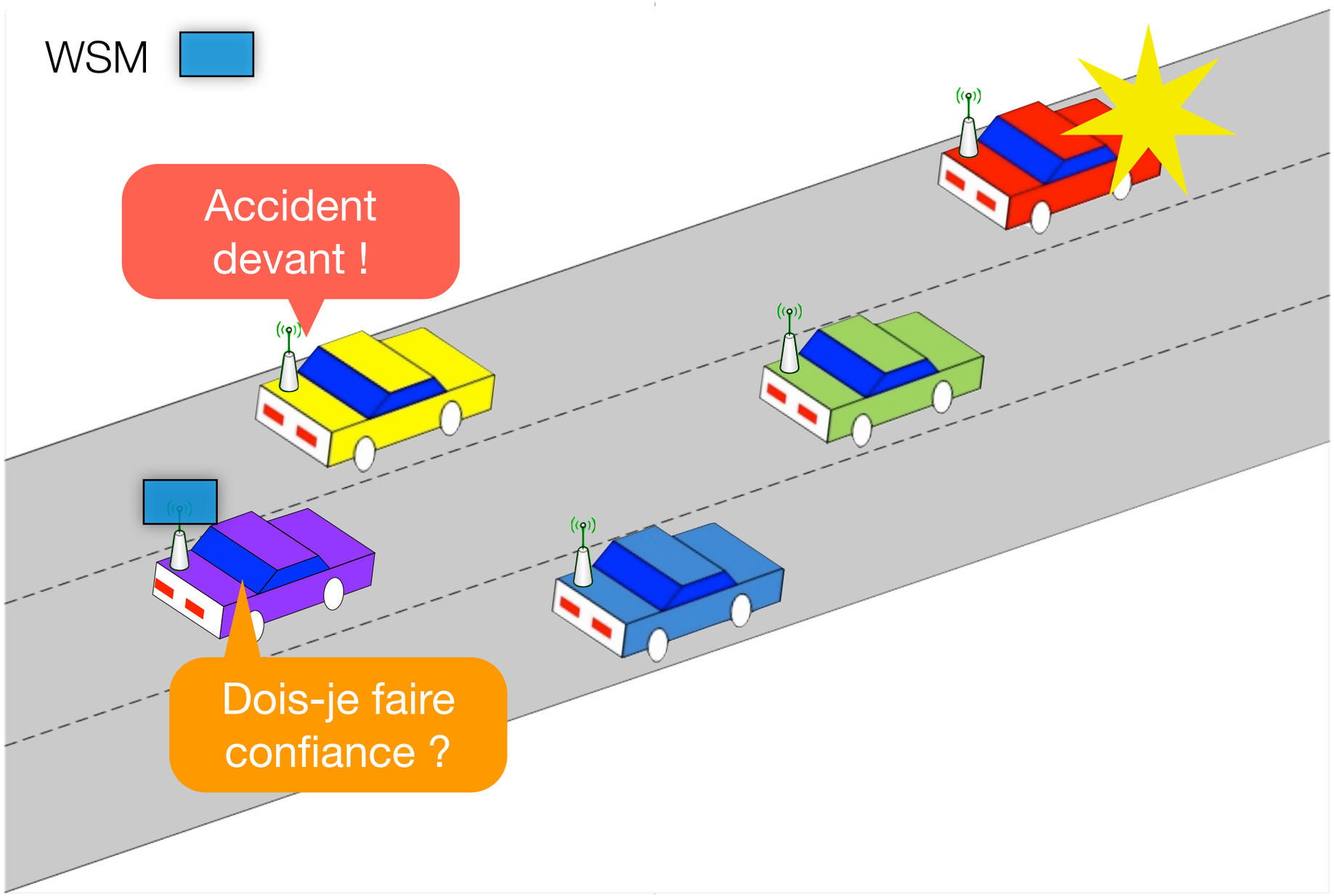
Problématique

But:
Augmenter la confiance



Problématique

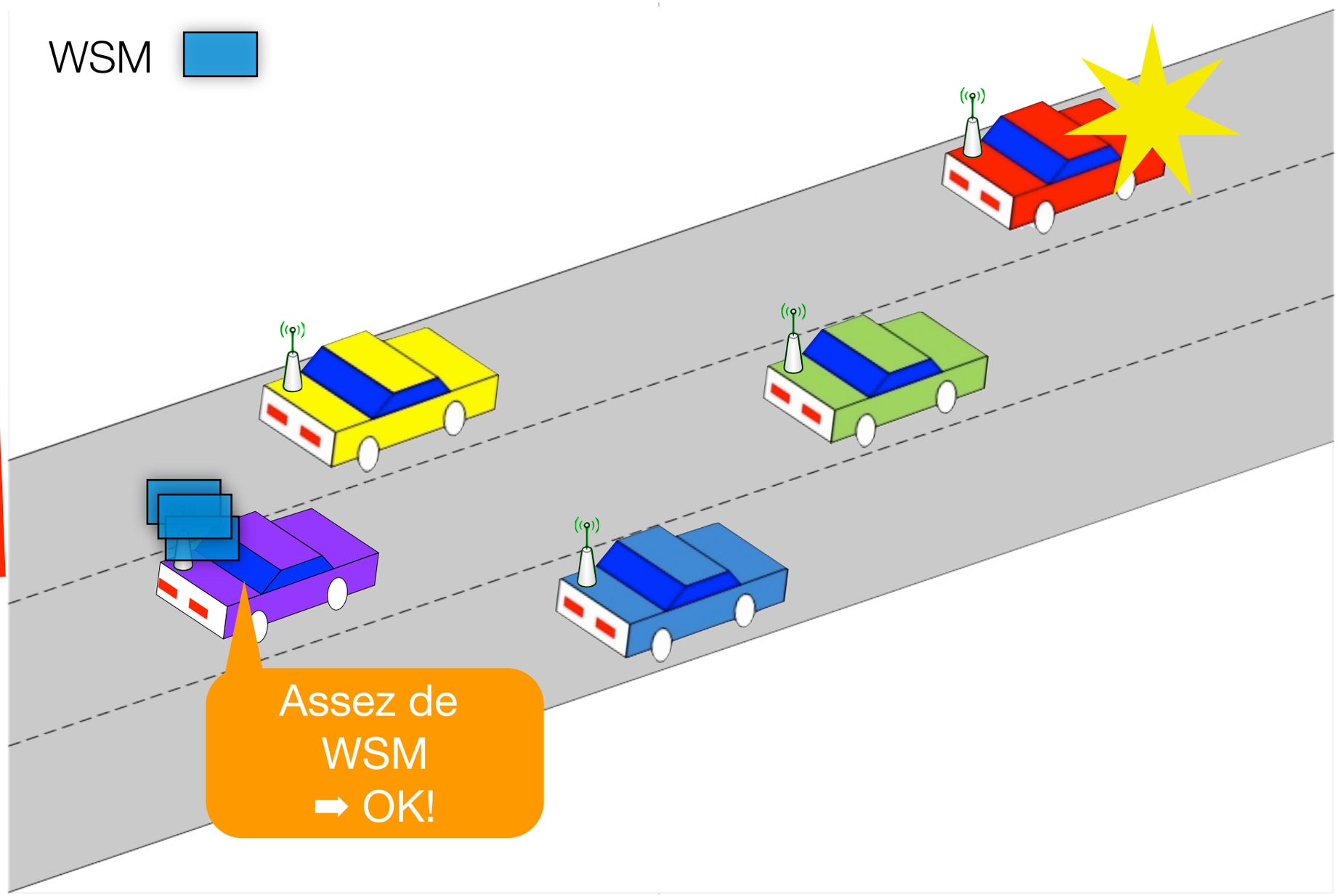
But:
Augmenter la confiance



Problématique

But:
Augmenter la confiance

Problème:
Définir “assez”



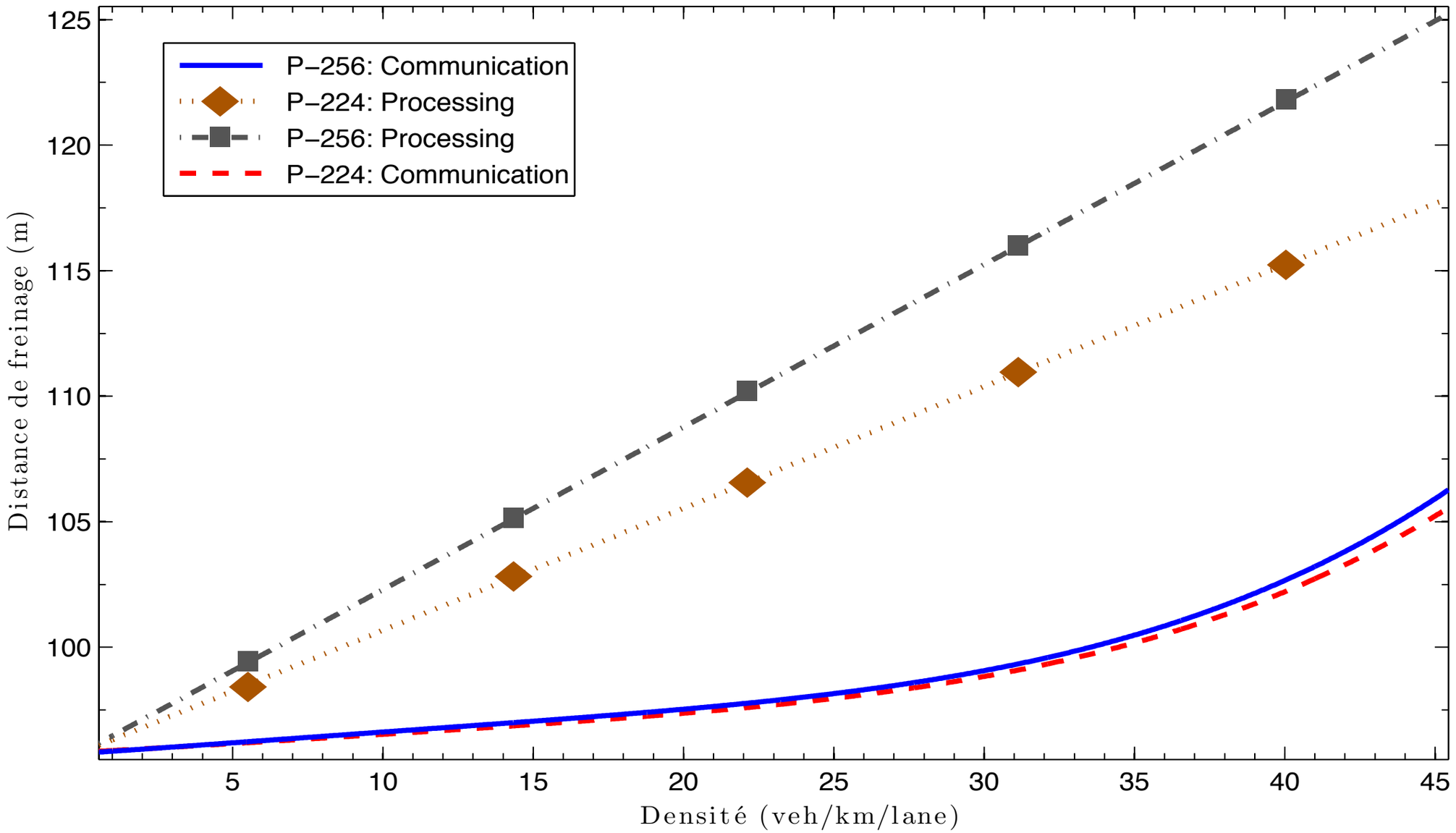
Méthodes de décision

- Naïve

Méthodes de décision

- Naïve

Distance de freinage en fonction de la densité

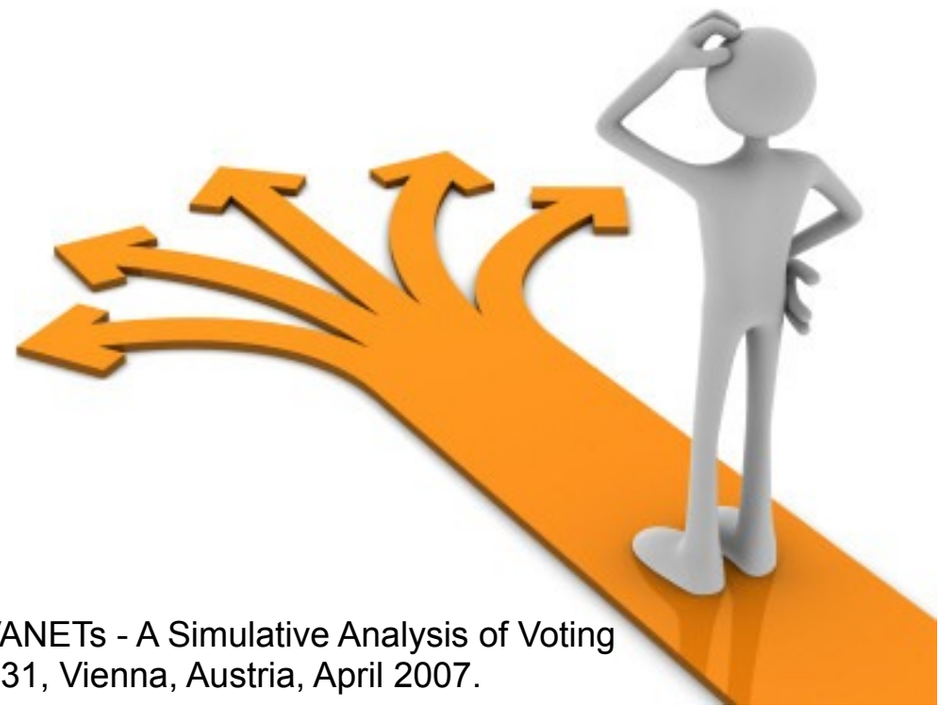


Méthodes de décision

- Naïve
- Majorité

Méthodes de décision

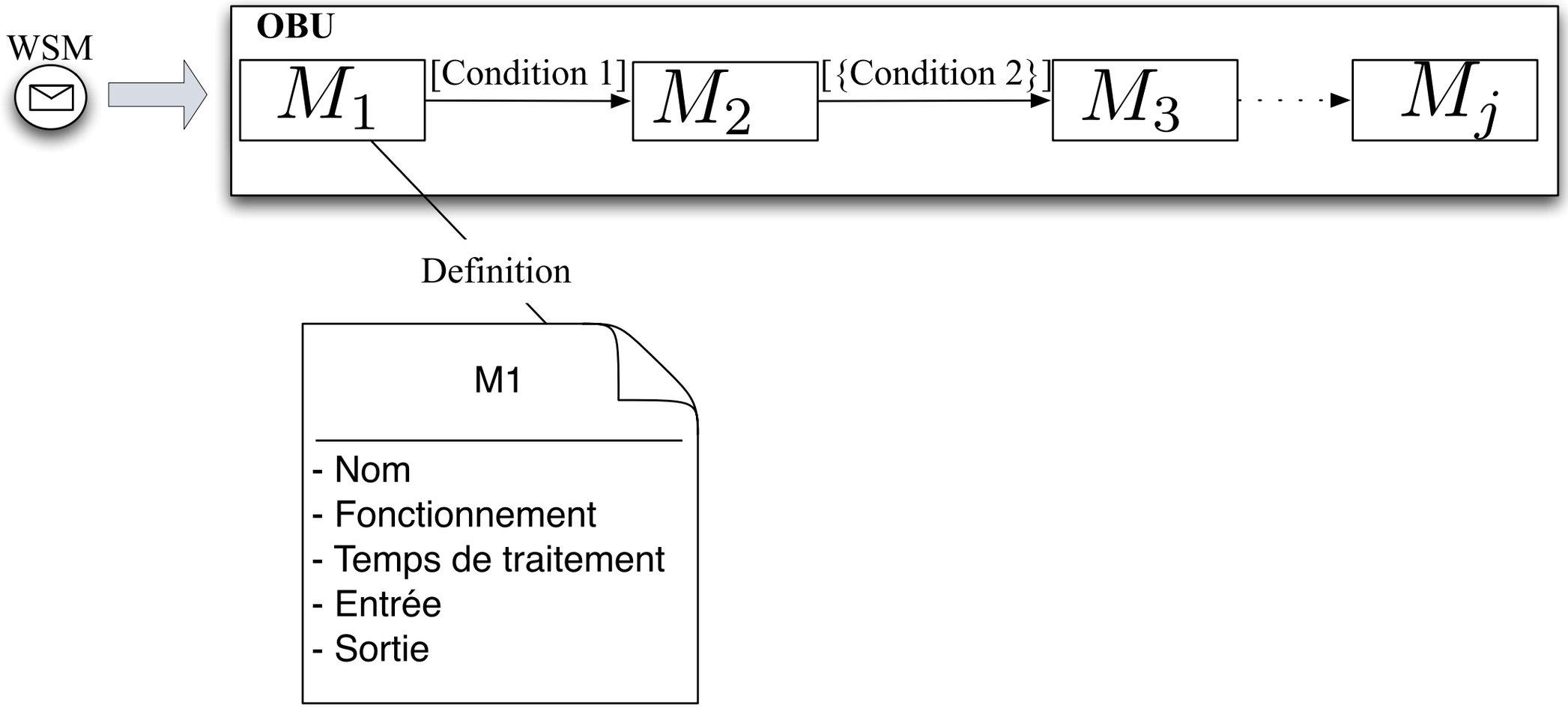
- Naïve
- Majorité
- *Majority of freshest **X** with **Threshold***



Ostermaier B., Dötzer F., Strassberger M., “Enhancing the Security of Local Danger Warnings in VANETs - A Simulative Analysis of Voting Schemes”, *2nd International Conference on Availability, Reliability and Security (ARES),* pp. 422-431, Vienna, Austria, April 2007.

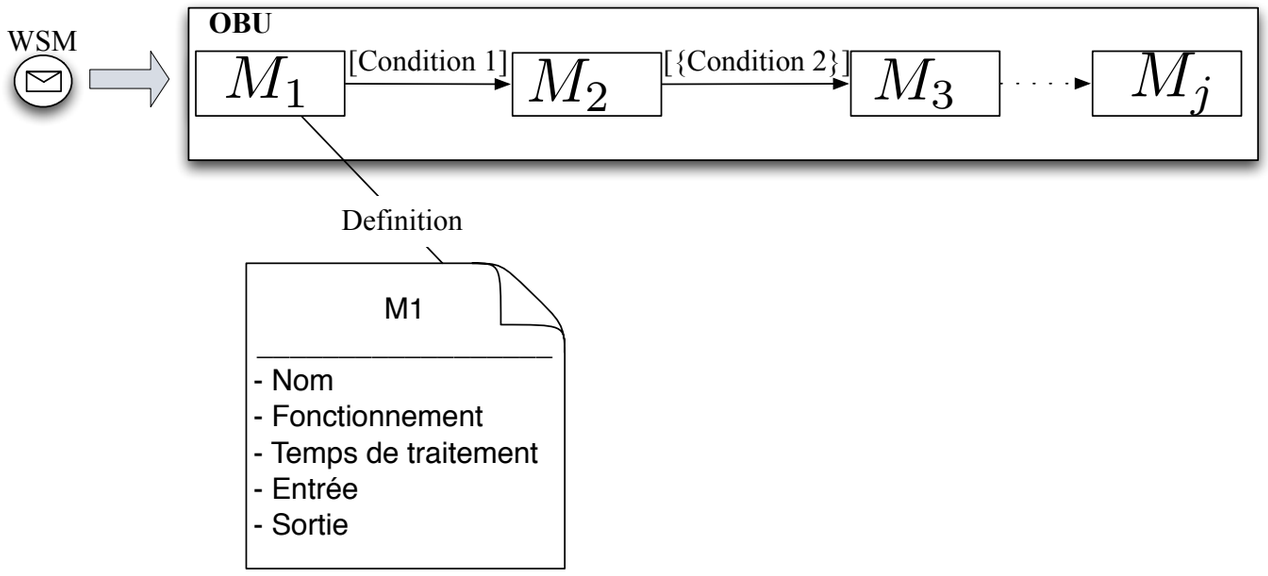
Modélisation

Conceptuelle



Modélisation

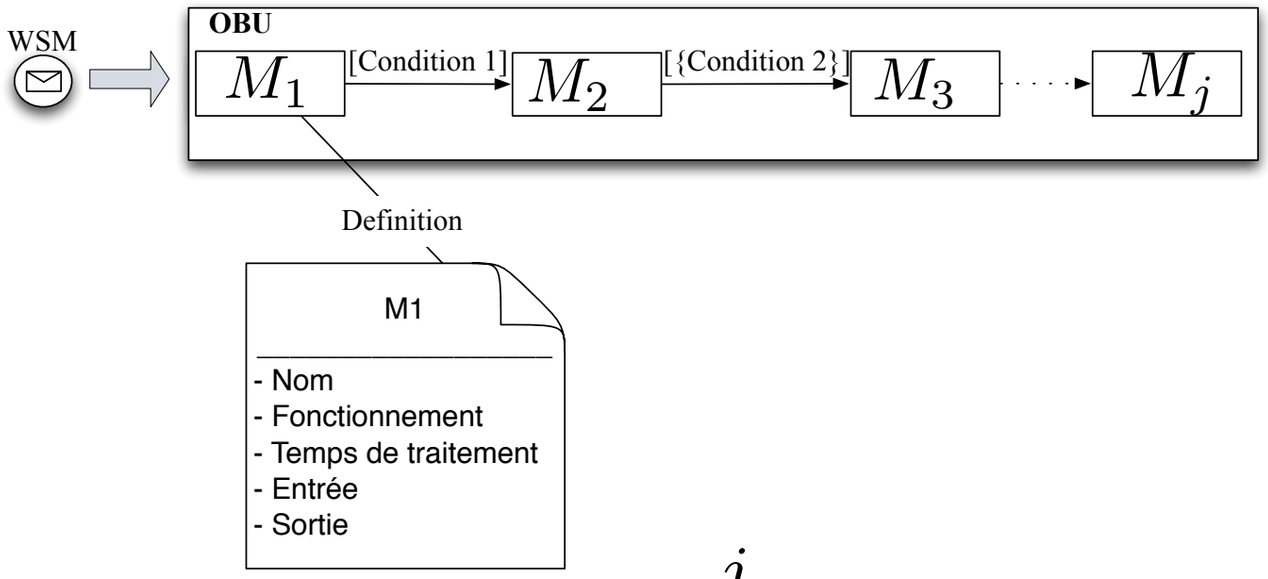
- Conceptuelle



- Analytique
  - Délai de décision
  - Niveau de confiance

Modélisation

- Conceptuelle



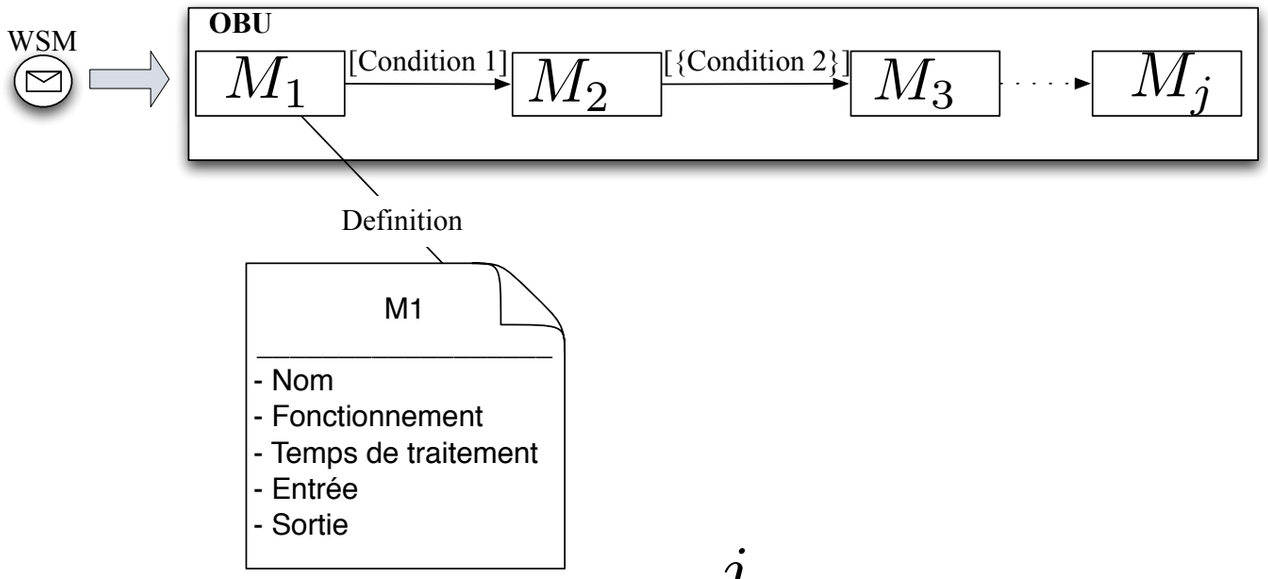
- Analytique
  - Délai de décision

$$Délai_{décision} = \sum_{k=1}^{j} D_k$$

  - Niveau de confiance

Modélisation

- Conceptuelle



- Analytique
  - Délai de décision

$$Délai_{décision} = \sum_{k=1}^{j} D_k$$

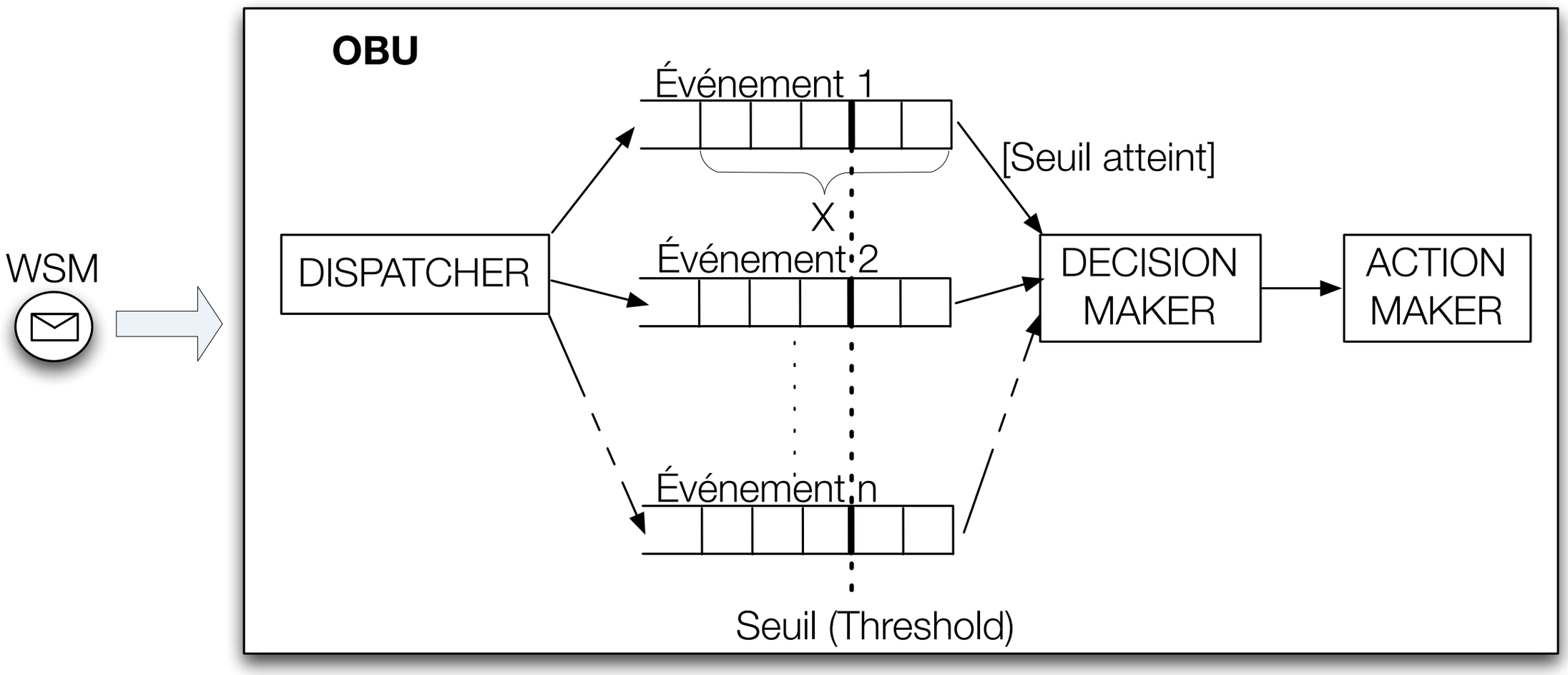
  - Niveau de confiance

$$F(e_k^i) = G(s(V_k), f(\tau(V_k), \lambda(i)))$$

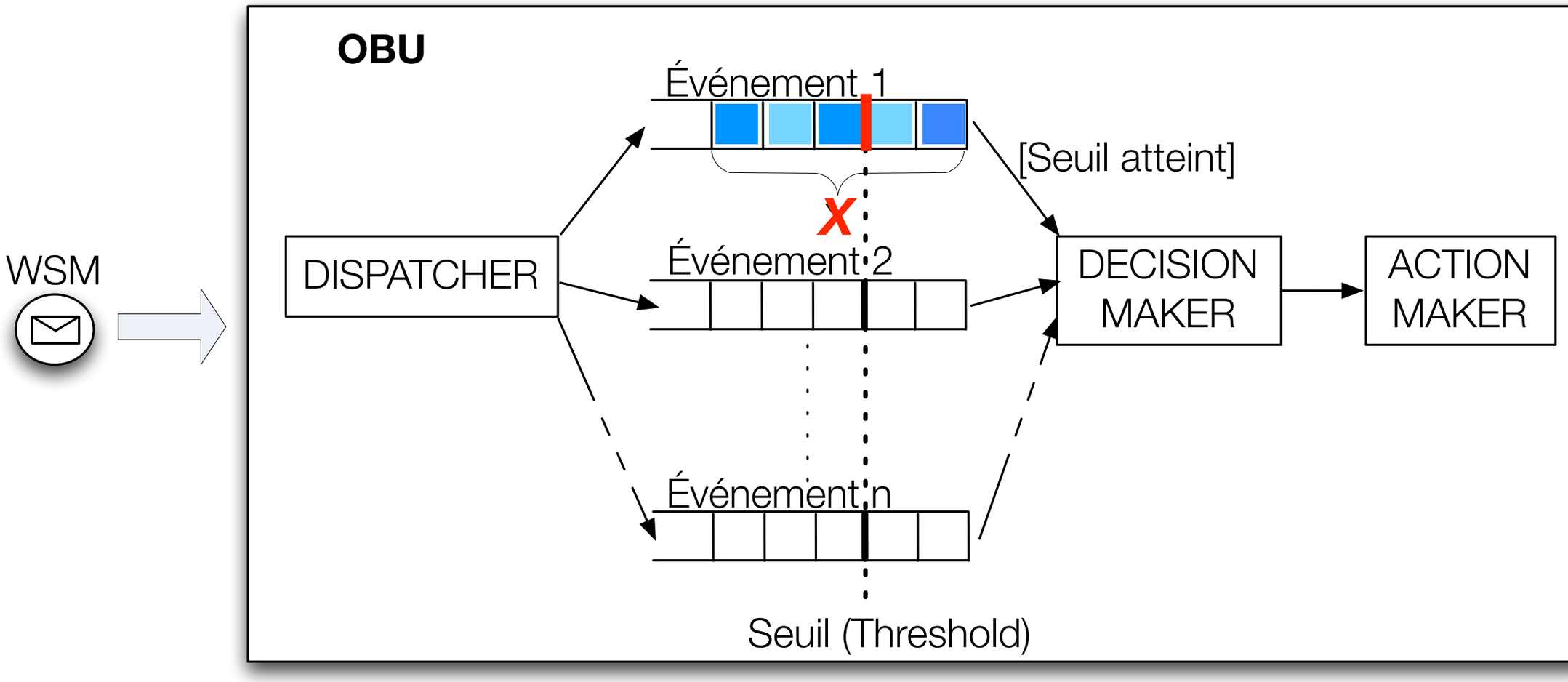
révoqué ? confiance par défaut type d'événement

*Majority of freshest **X** with **Threshold***

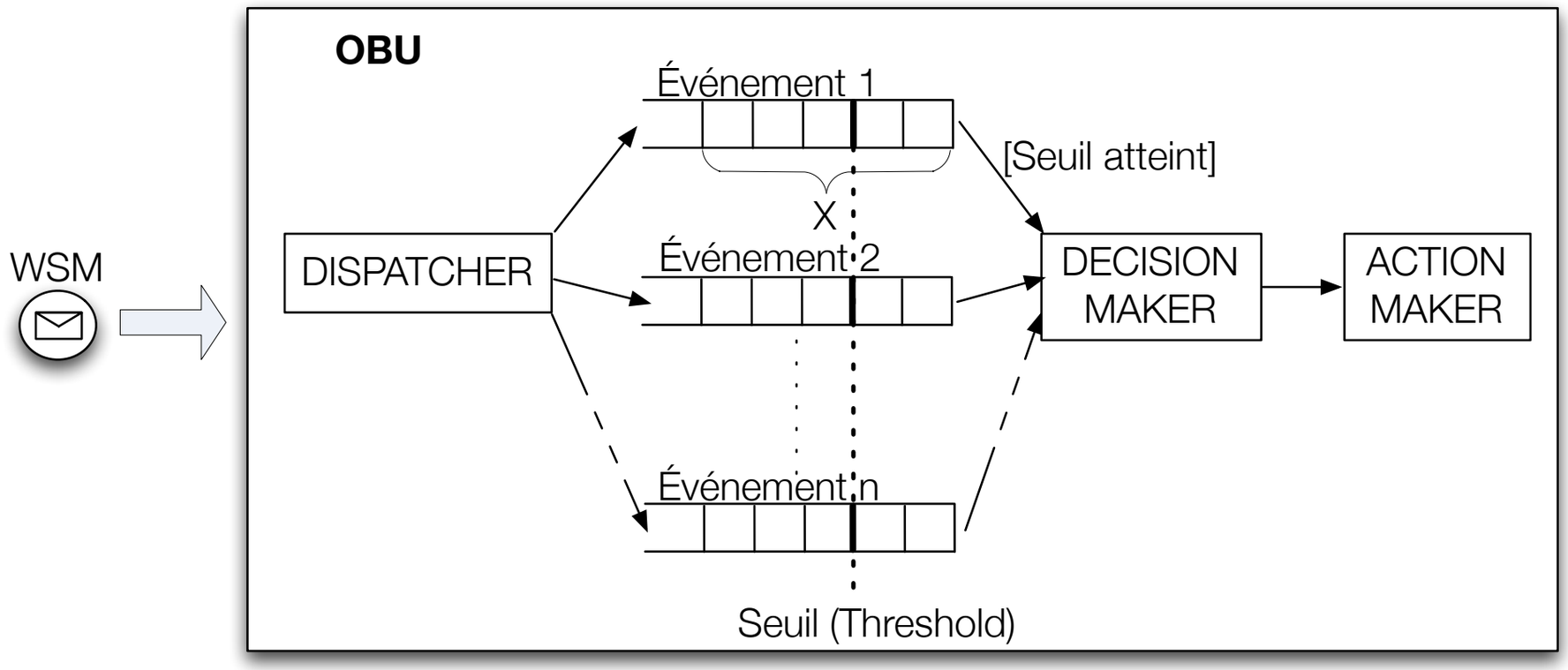
*Majority of freshest **X** with **Threshold***



*Majority of freshest **X** with **Threshold***



*Majority of freshest **X** with **Threshold***



- Niveau de confiance (OBU)

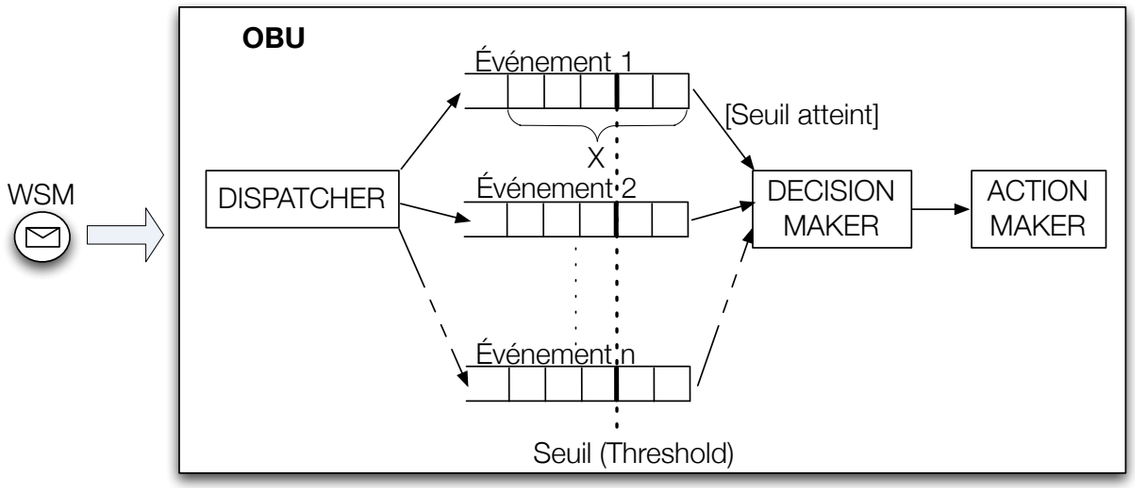
$$d_i = \sum_{k=1}^{N_{TX}} F(e_k^i), \text{ si } X > Threshold$$

- Délai de décision

$$Délai_{décision} = X \times (T_{tx} + T_{vérif}) \text{avec } X > Threshold$$

*Majority of freshest **X** with **Threshold***

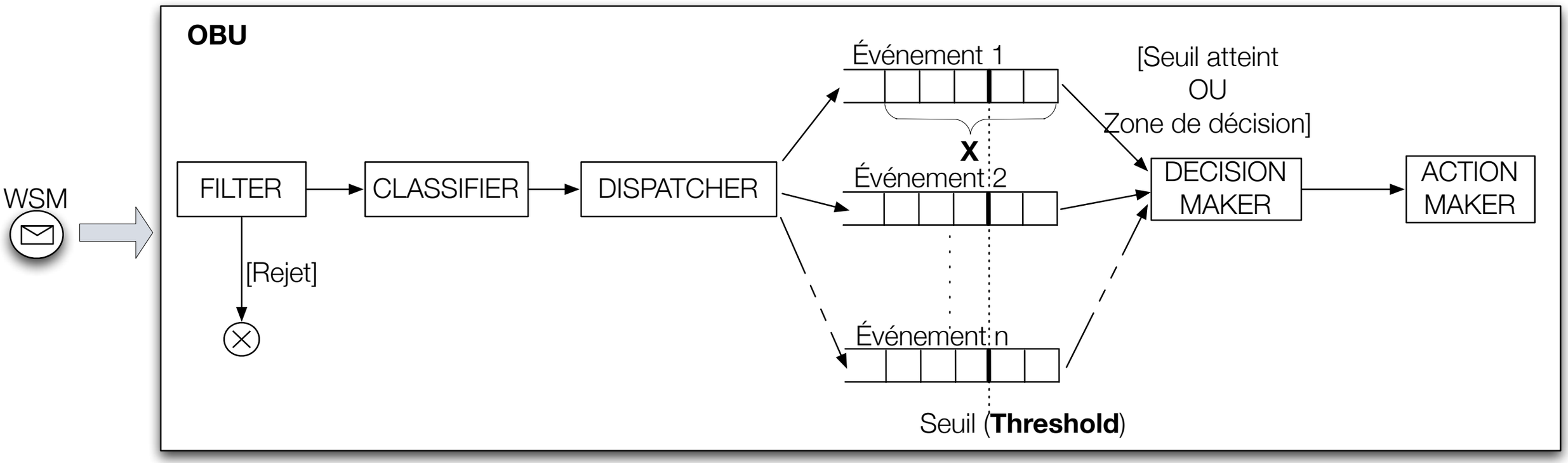
- Protection contre les attaques d'injection de fausses informations
- Fraîcheur



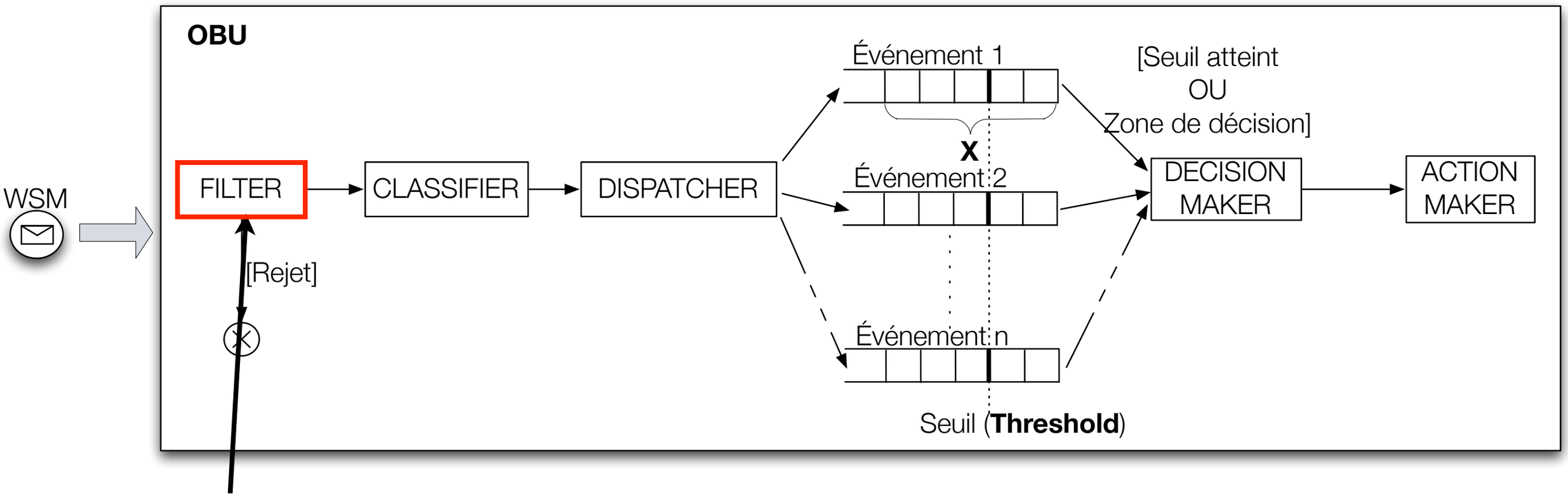
- Comment définir ces paramètres ?
- Non-utilisation du contenu de l'information

Notre proposition

Notre proposition

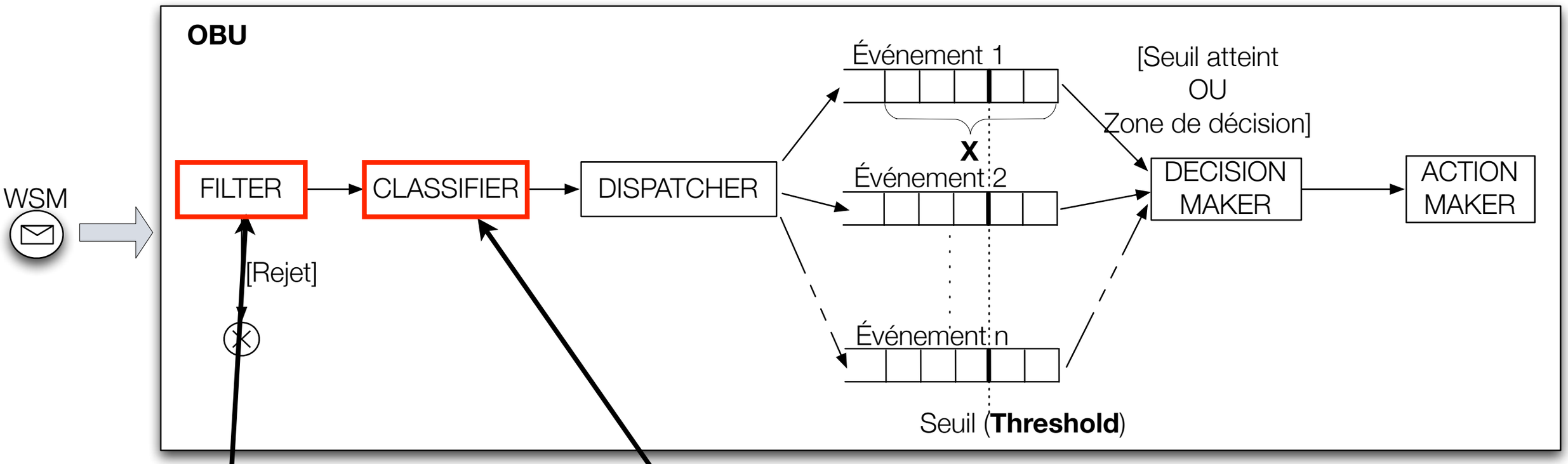


Notre proposition



Pour éliminer les paquets inutiles (distance, voie)

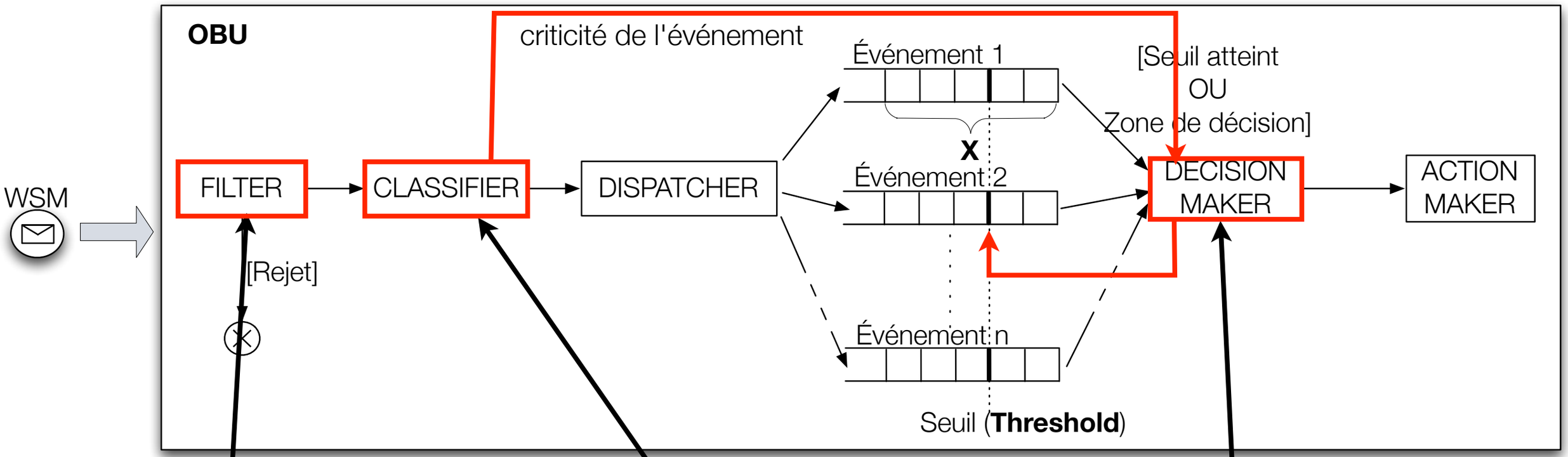
Notre proposition



Pour éliminer les paquets inutiles (distance, voie)

Pour calculer la criticité de l'événement

Notre proposition

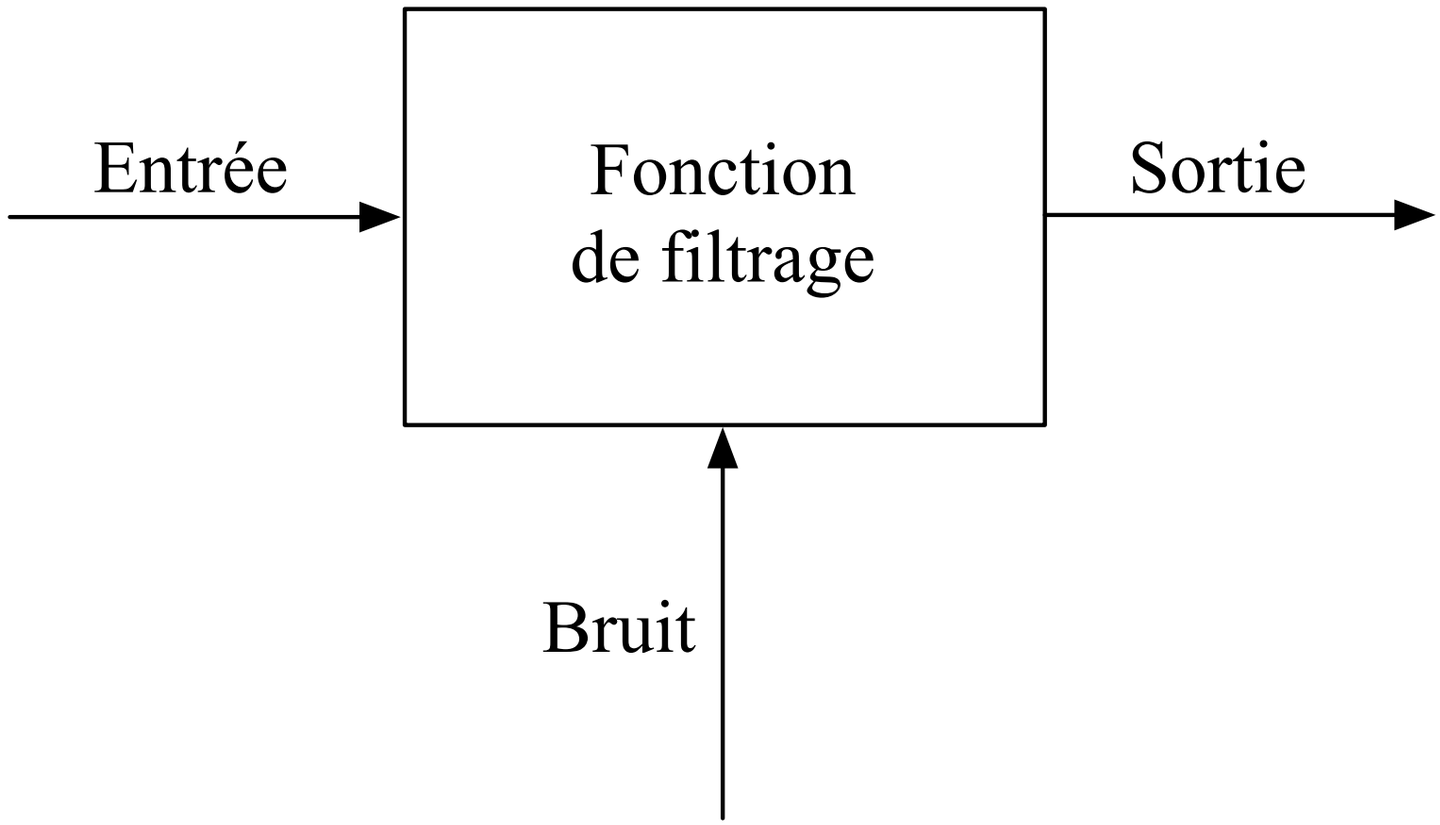


Pour éliminer les paquets inutiles (distance, voie)

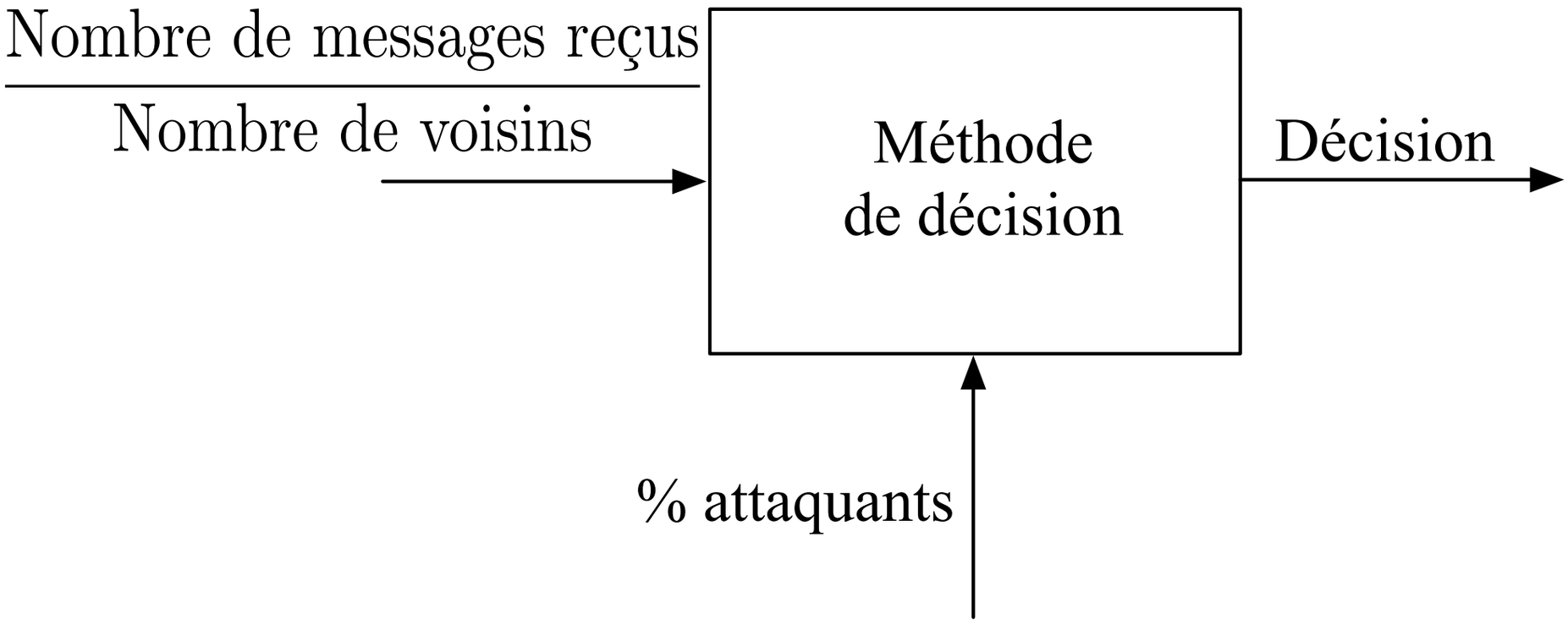
Pour calculer la criticité de l'événement

Pour fixer les paramètres de consensus (*X*, *Threshold*)

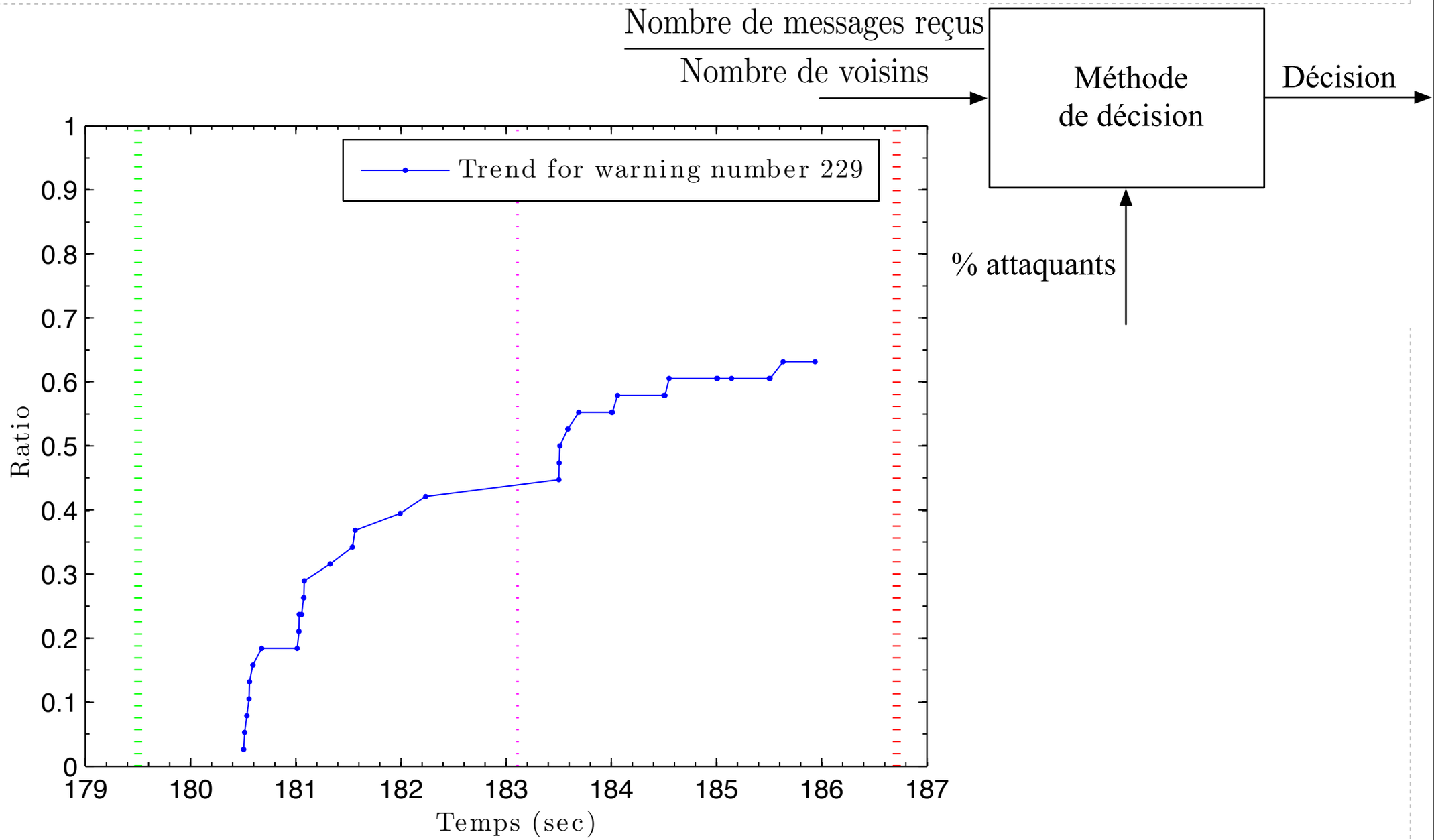
Modélisation du *decision maker*



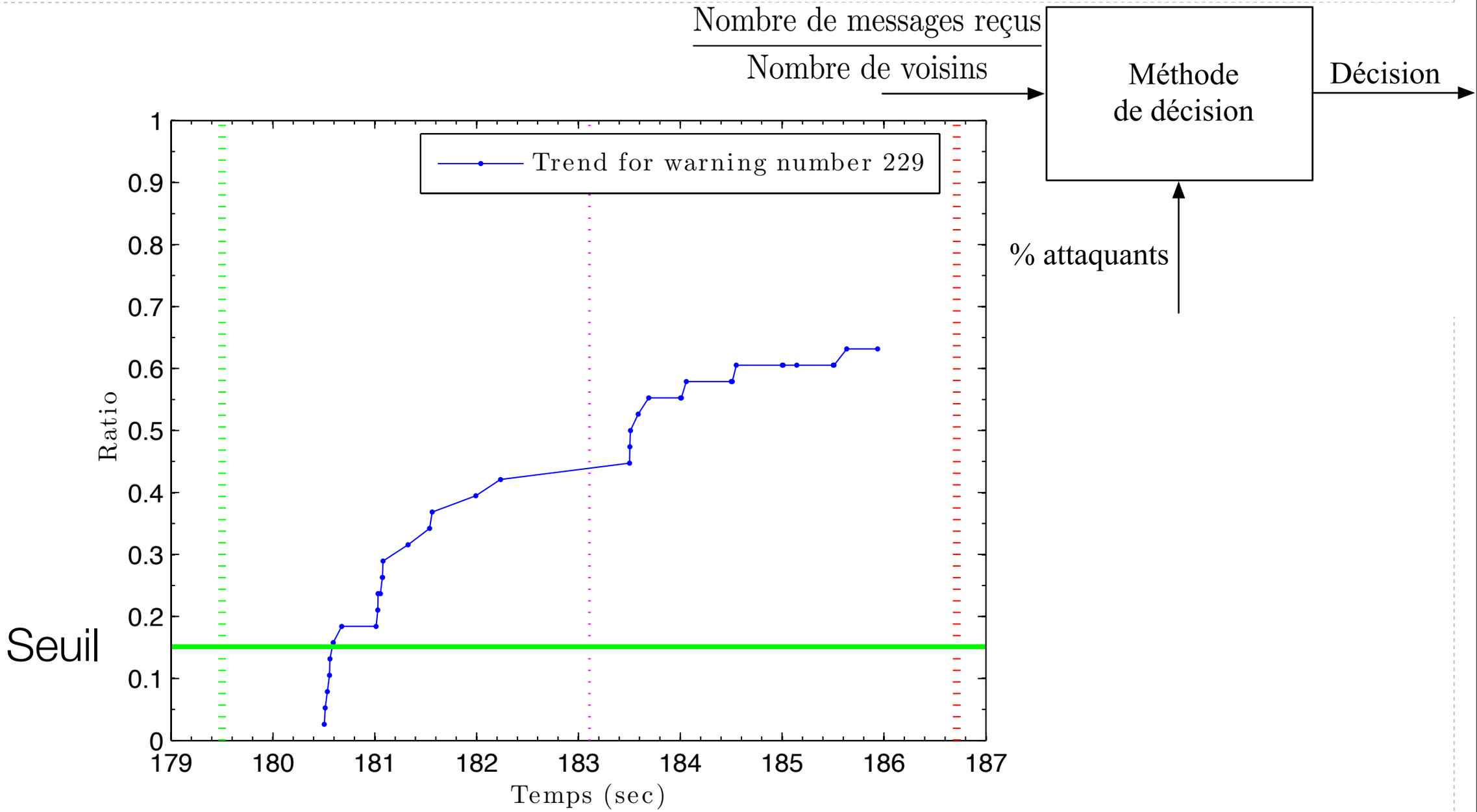
Modélisation du *decision maker*



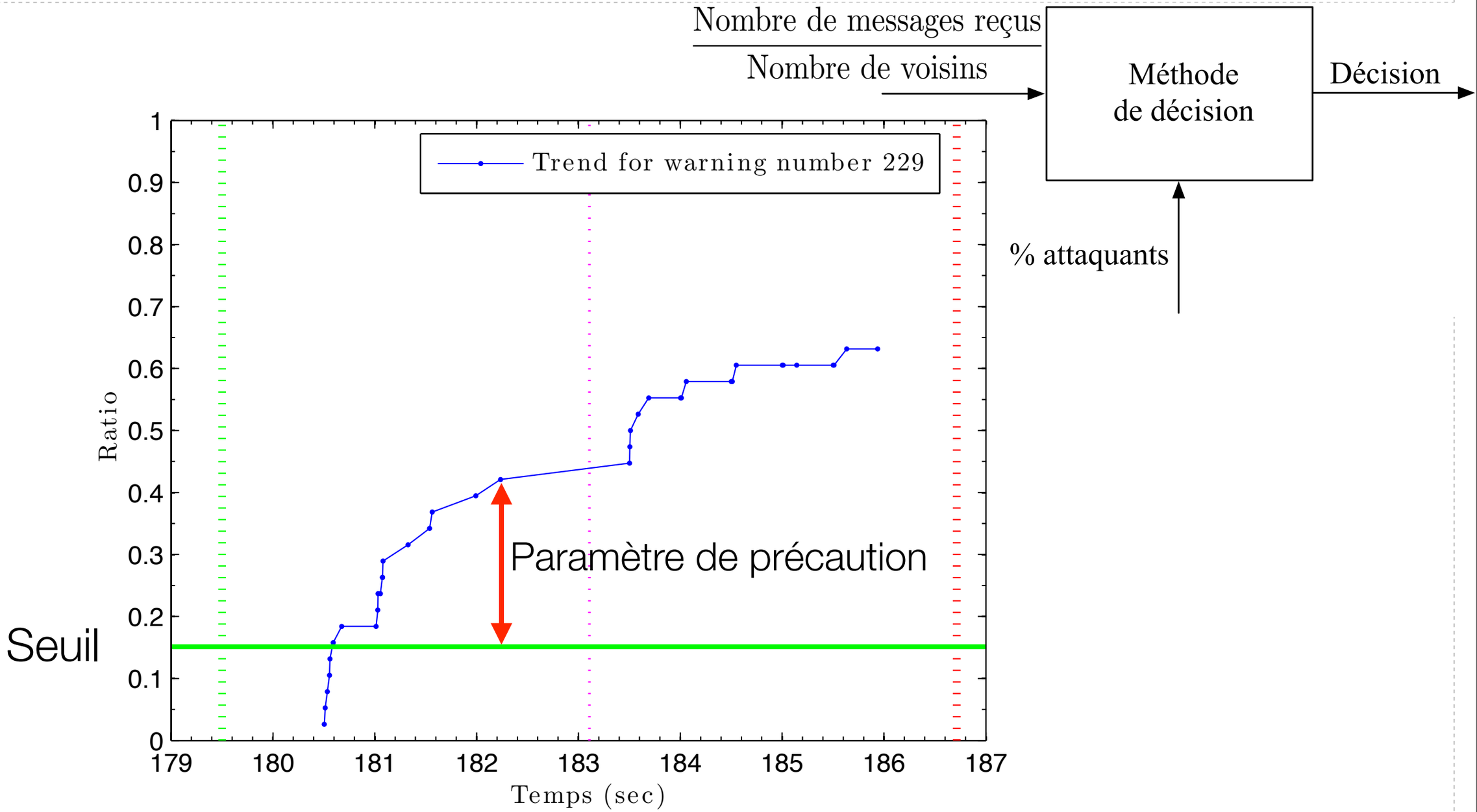
Modélisation du *decision maker*



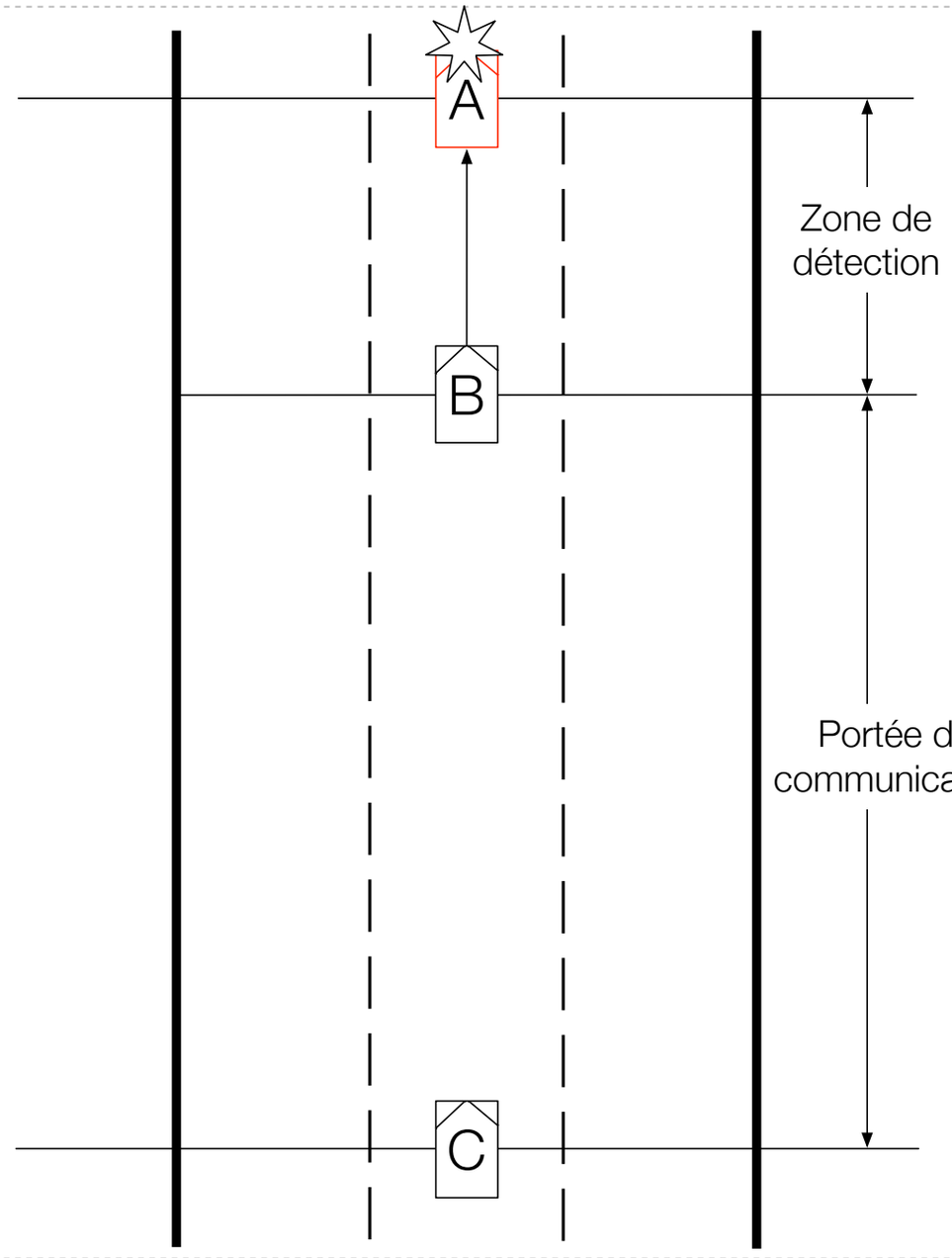
Modélisation du *decision maker*



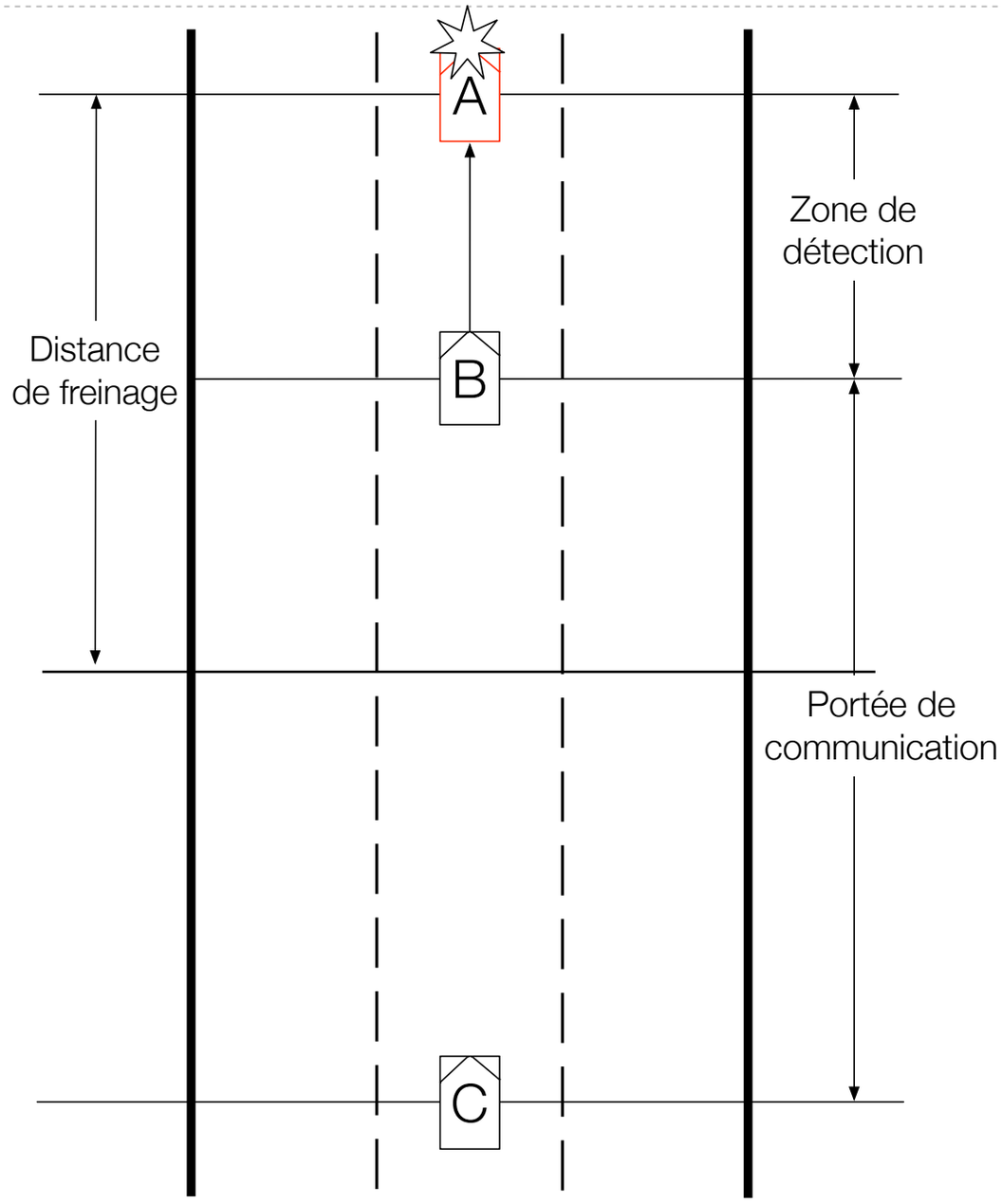
Modélisation du *decision maker*



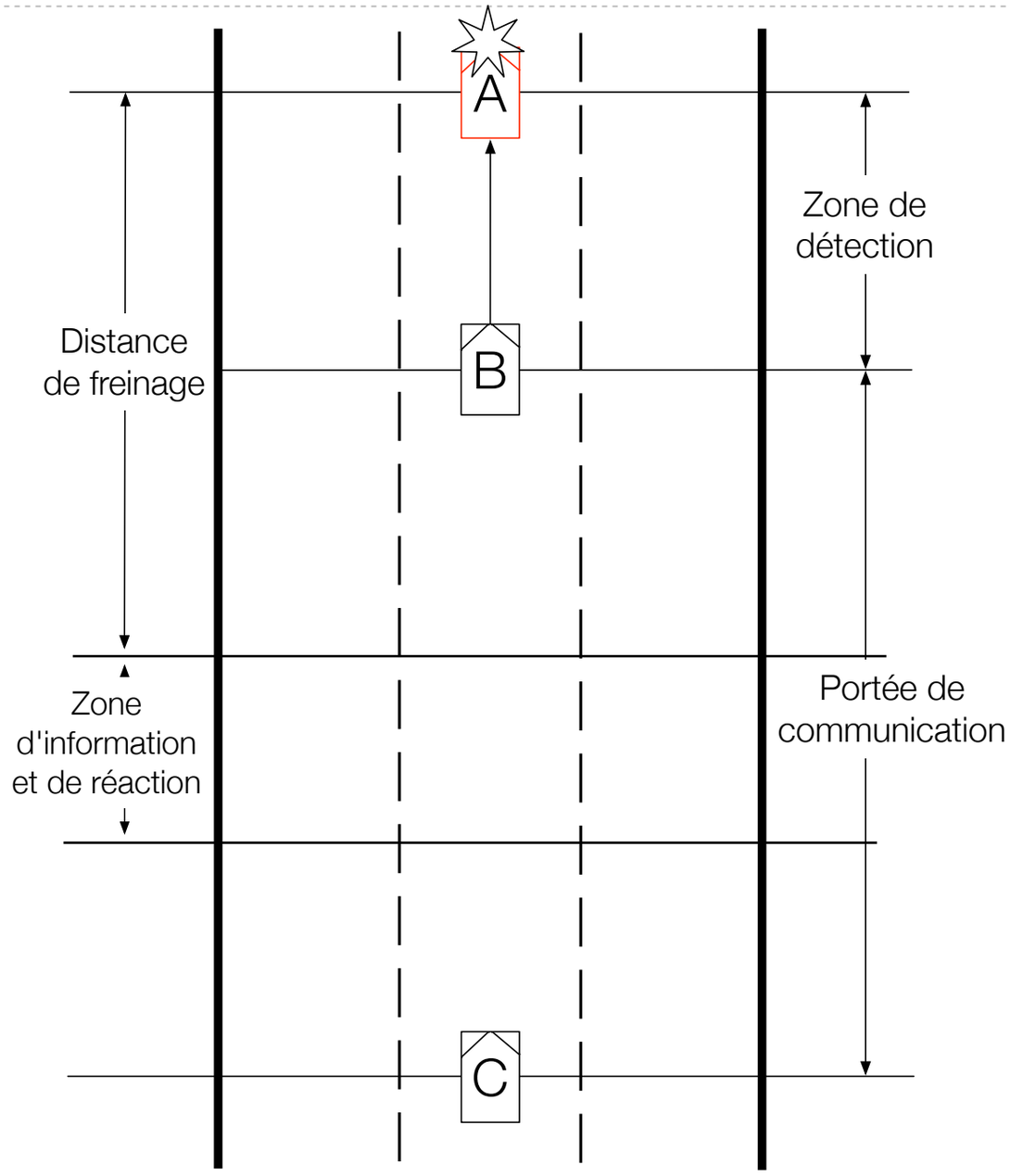
Modèle et criticité



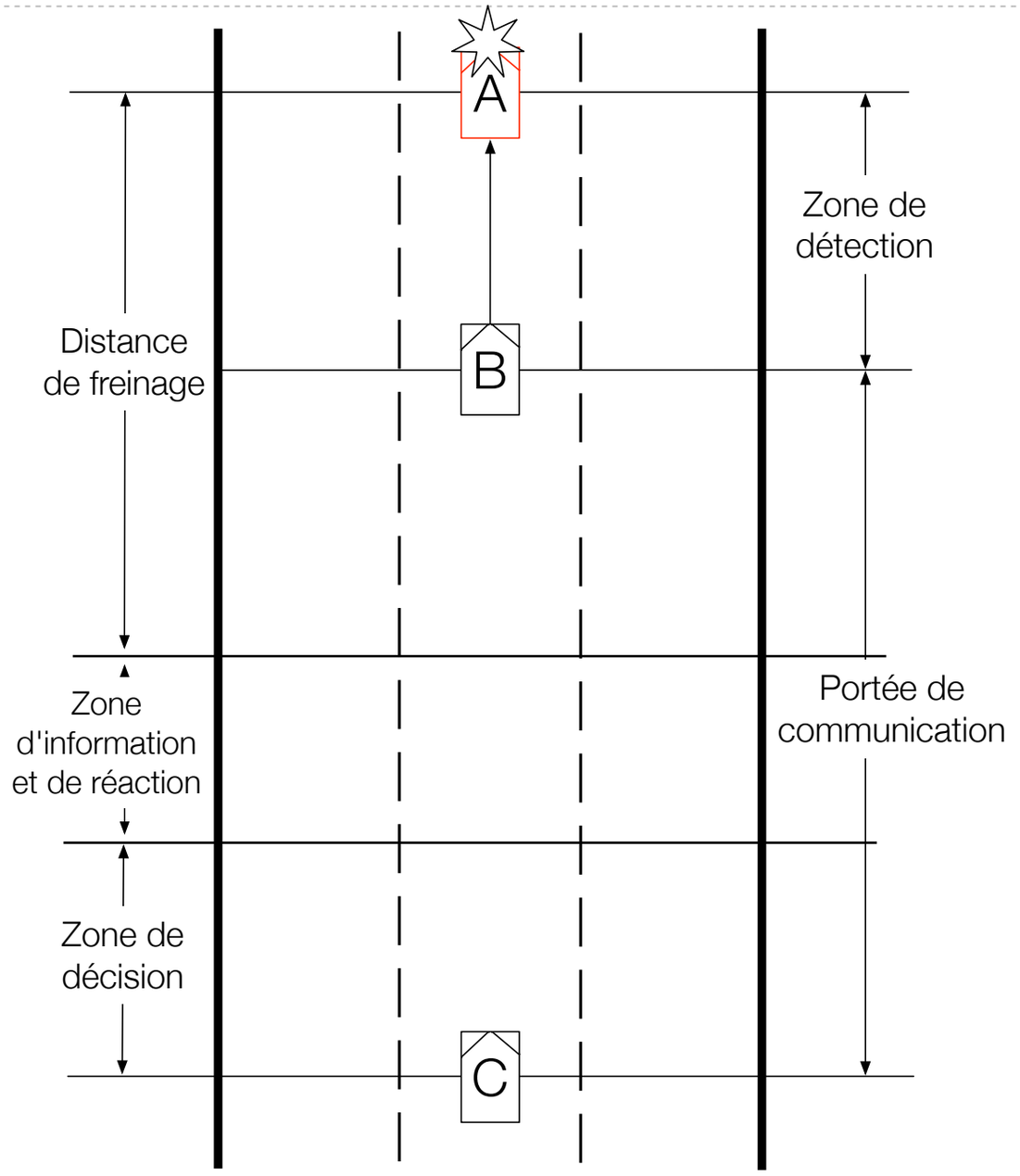
Modèle et criticité



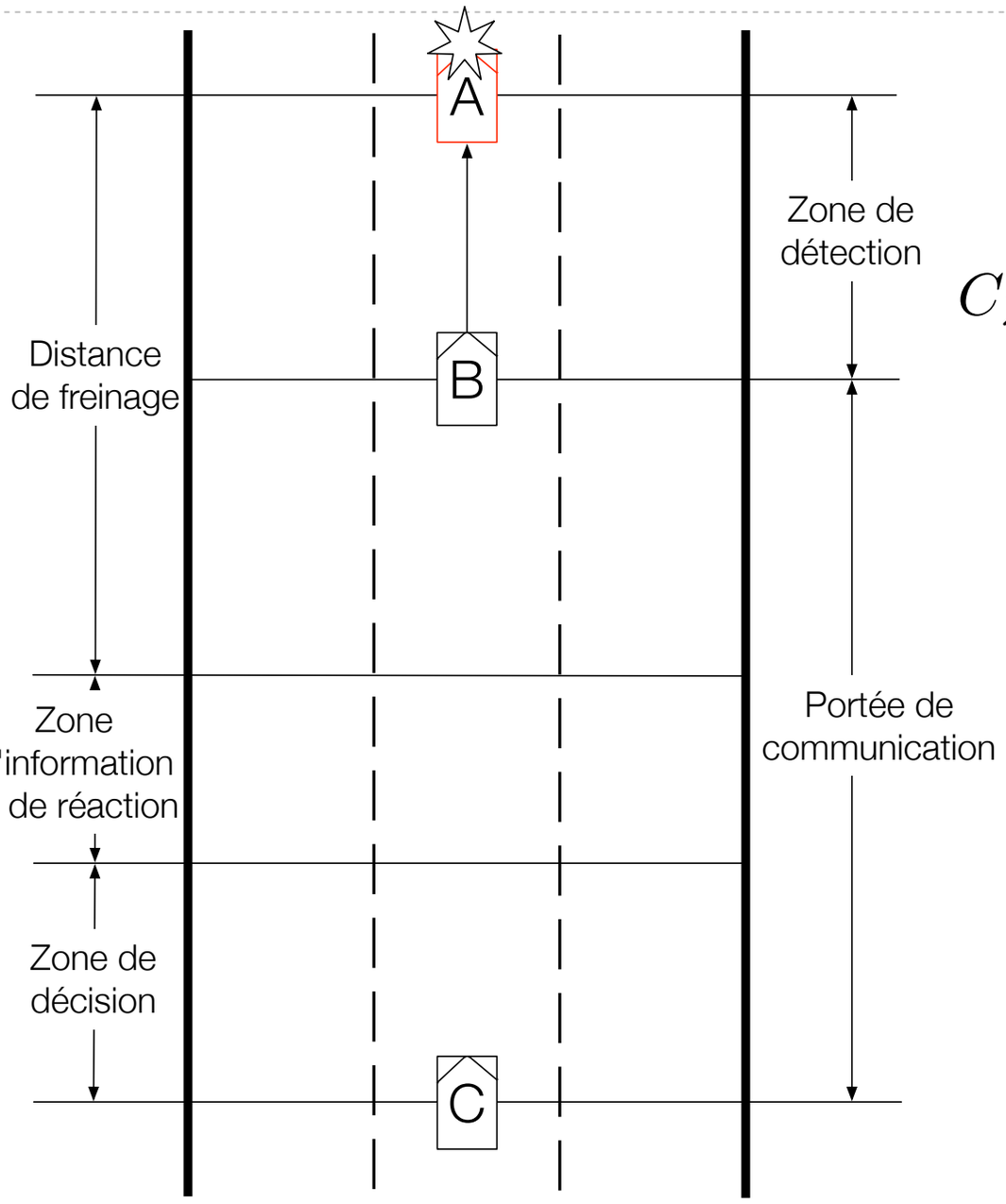
Modèle et criticité



Modèle et criticité

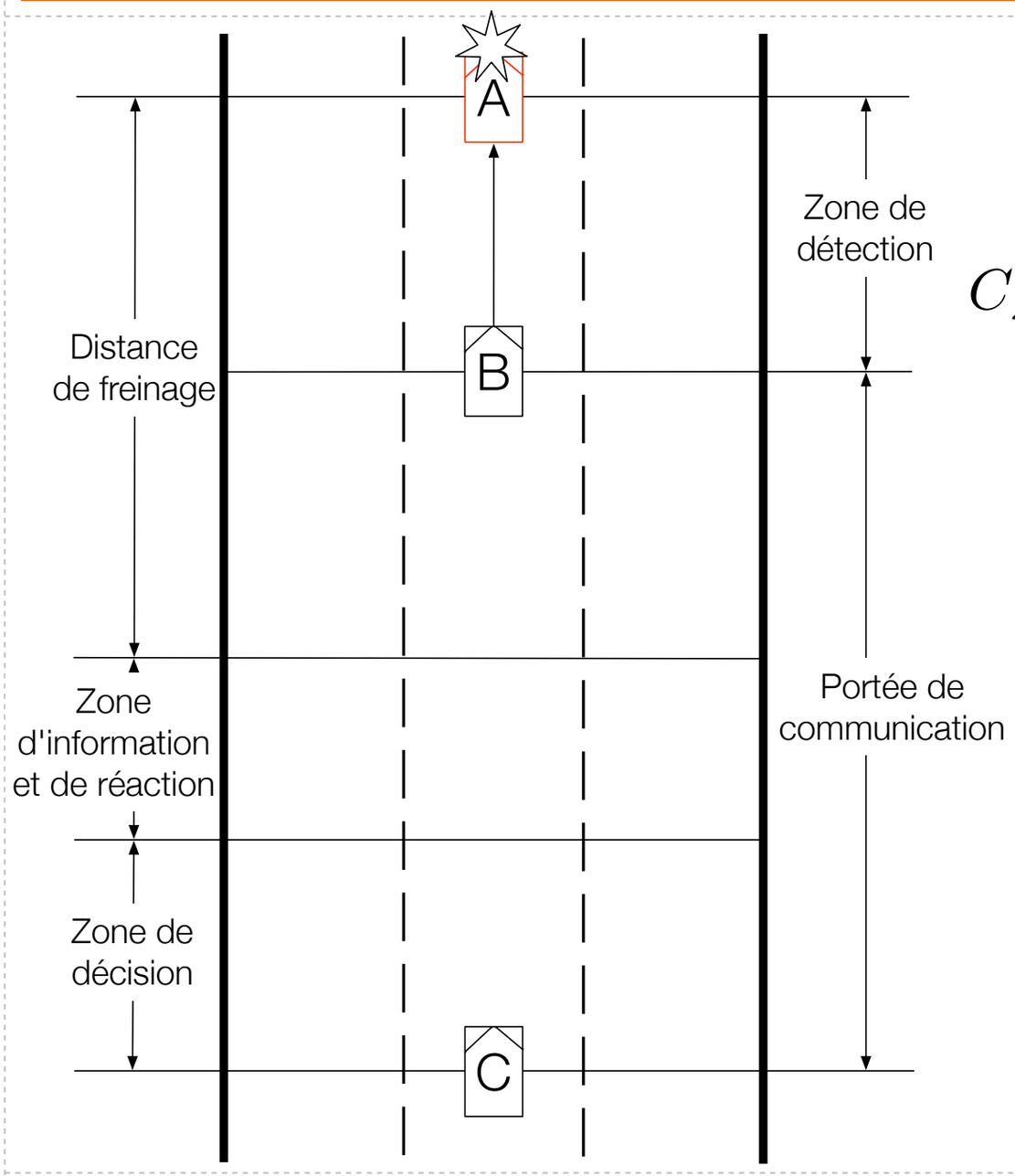


Modèle et criticité

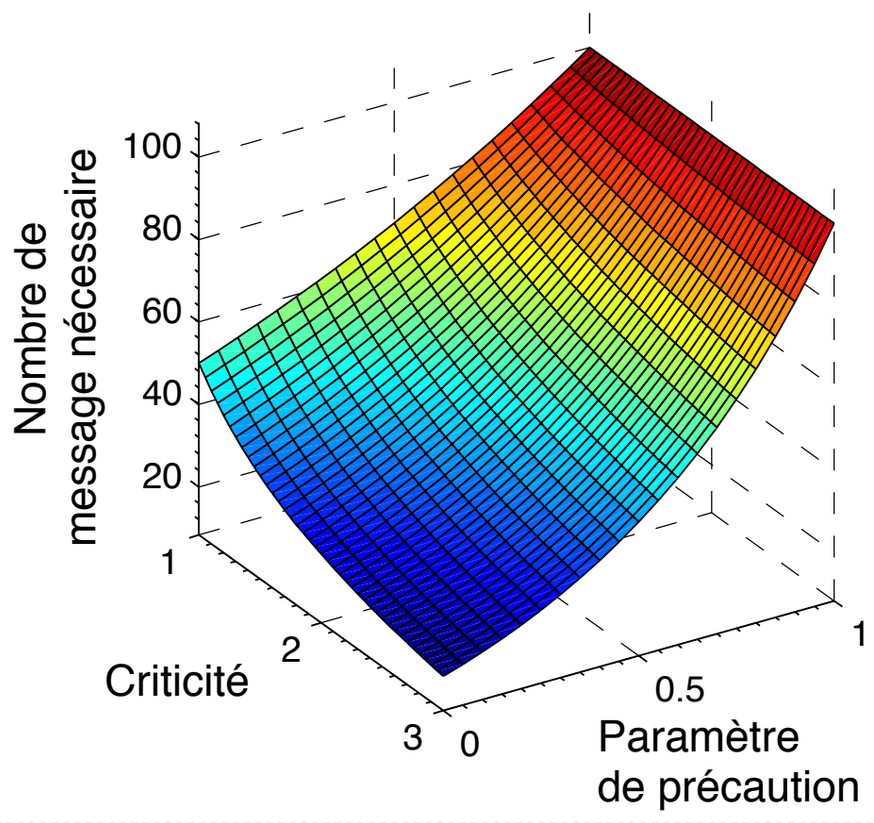


$$C_{\lambda(i)} = \begin{cases} 1, \text{ si } \Delta T_i > T_{dist\_sécurité} \\ 1 + \frac{1}{\Delta T_i}, \text{ si } T_{dist\_sécurité} > \Delta T_i > T_{collision} \end{cases}$$

Modèle et criticité



$$C_{\lambda(i)} = \begin{cases} 1, \text{ si } \Delta T_i > T_{dist\_sécurité} \\ 1 + \frac{1}{\Delta T_i}, \text{ si } T_{dist\_sécurité} > \Delta T_i > T_{collision} \end{cases}$$



Rappels : Limites (Ostermaier)

- Contexte de l'événement inutilisé
- Non prise en compte de la contrainte temporelle applicative
- Valeurs *X* et *Threshold* fixées statiquement

Rappels : Limites (Ostermaier)

- Contexte de l'événement inutilisé → $C_{\lambda(i)}$
- Non prise en compte de la contrainte temporelle applicative
- Valeurs *X* et *Threshold* fixées statiquement

Rappels : Limites (Ostermaier)

- Contexte de l'événement inutilisé $\longrightarrow$ $C_{\lambda(i)}$
- Non prise en compte de la contrainte temporelle applicative $\longrightarrow$ T_{MAX}
- Valeurs *X* et *Threshold* fixées statiquement

Rappels : Limites (Ostermaier)

- Contexte de l'événement inutilisé → $C_{\lambda(i)}$
- Non prise en compte de la contrainte temporelle applicative → T_{MAX}
- Valeurs *X* et *Threshold* fixées statiquement → p

Notre proposition

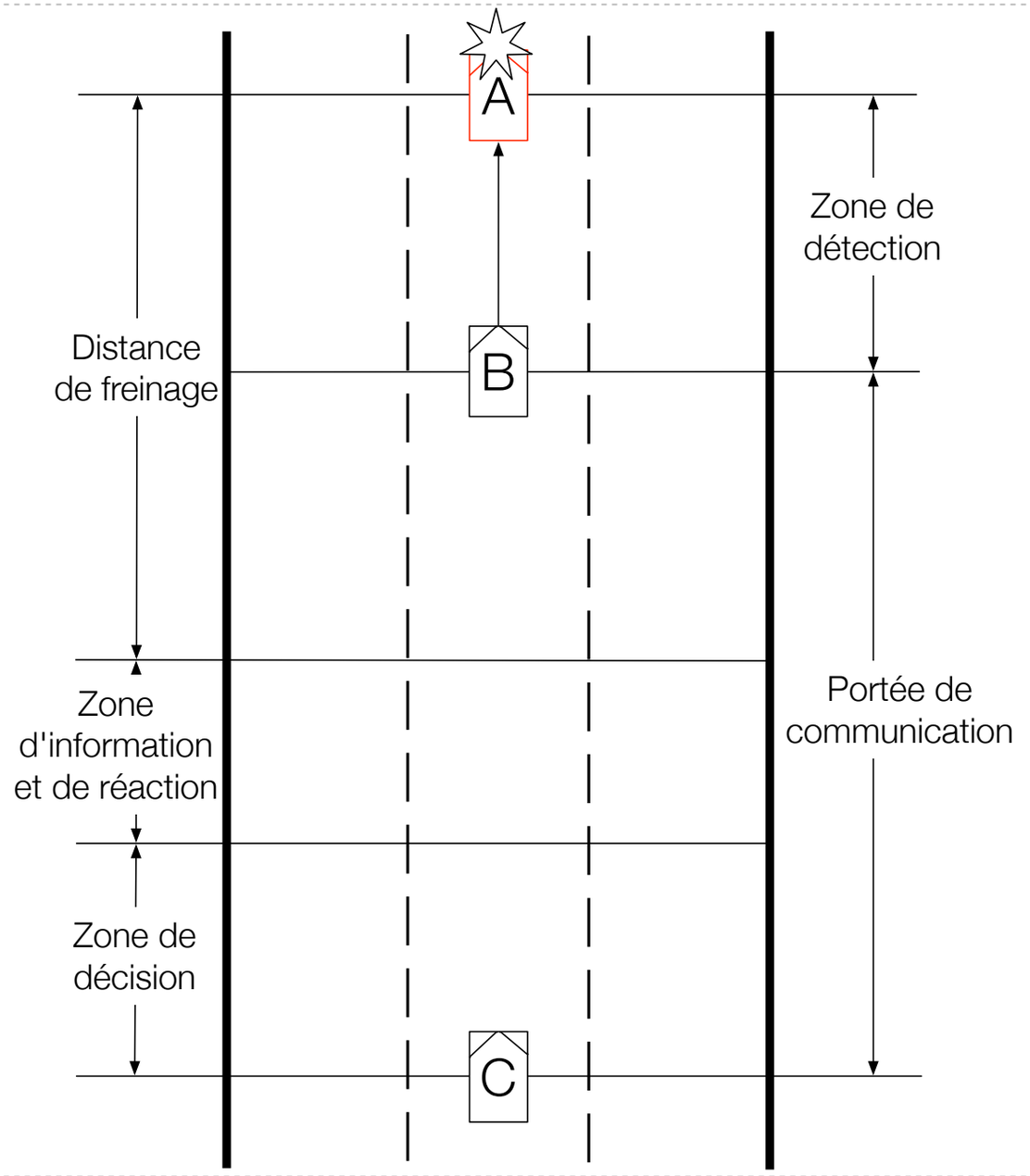
- Changer dynamiquement le seuil

$$Threshold = p \times \frac{Ahead(N_{TX}(t), R)}{2}$$

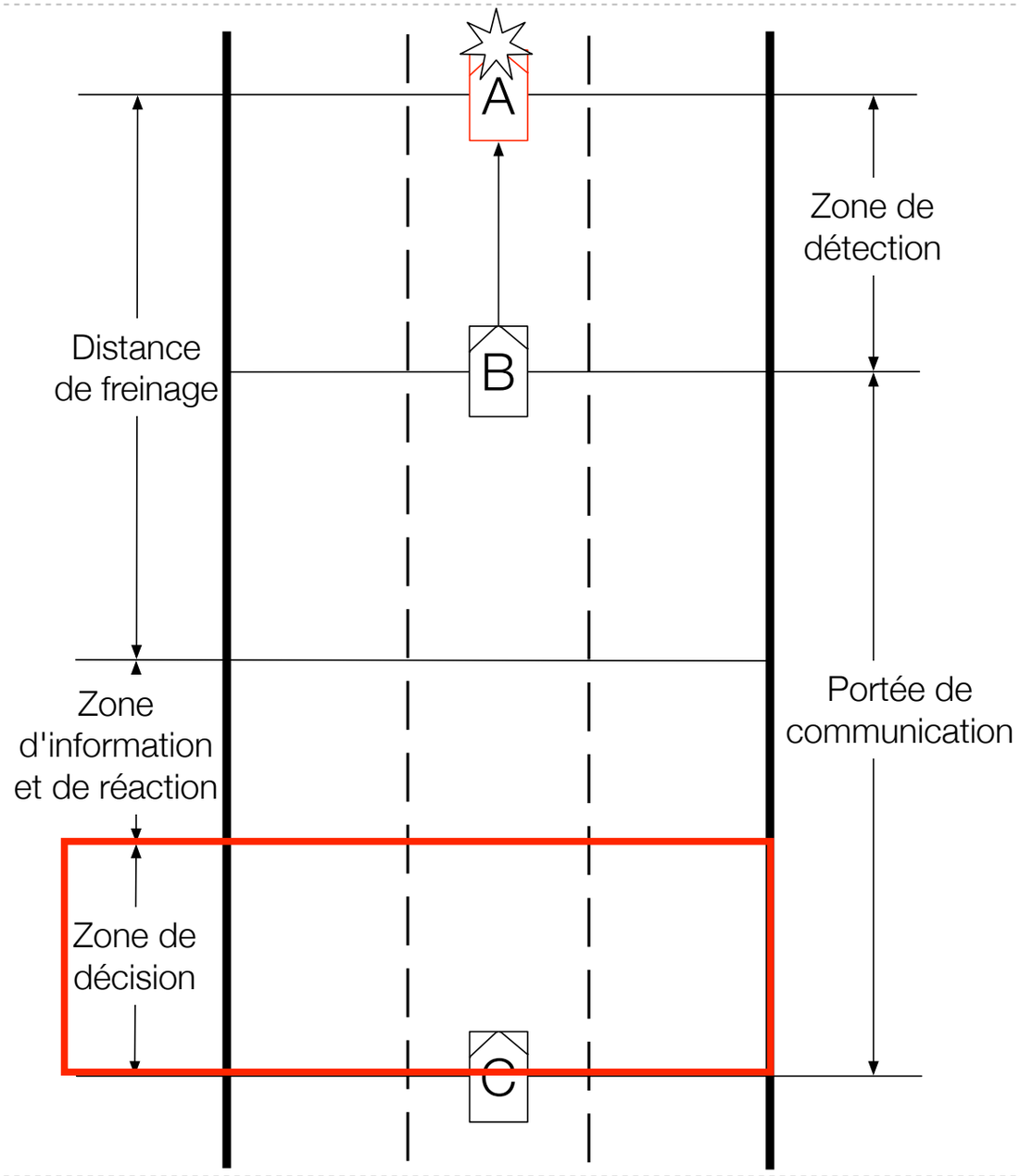
- Changer dynamiquement *X*

$$X = min((\frac{(2 \times C_{\lambda(i)})^{pc}}{C_{\lambda(i)})} \times \frac{(Ahead(N_{TX}(t), R))}{2}, x_{MAX})$$

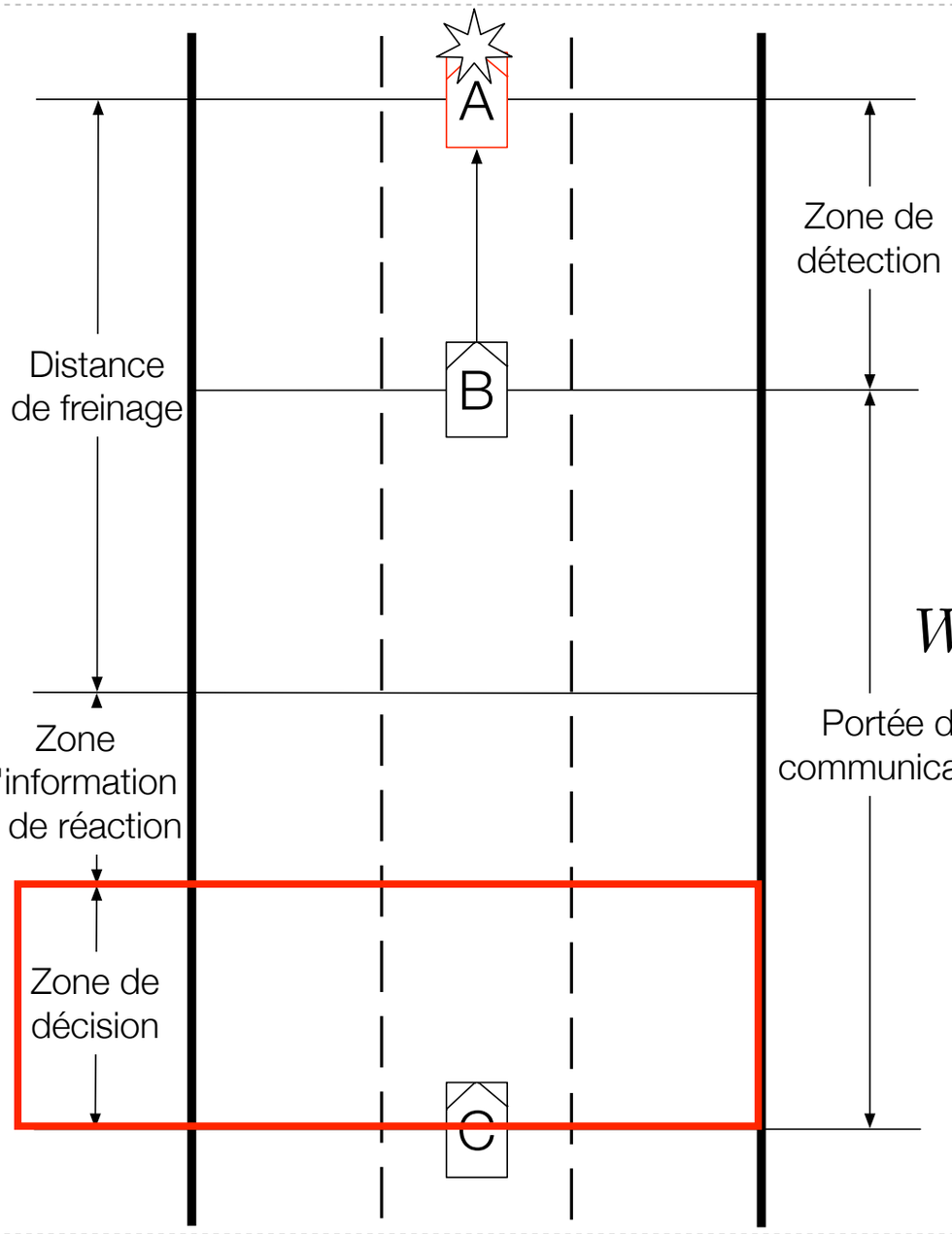
Délai de décision



Délai de décision



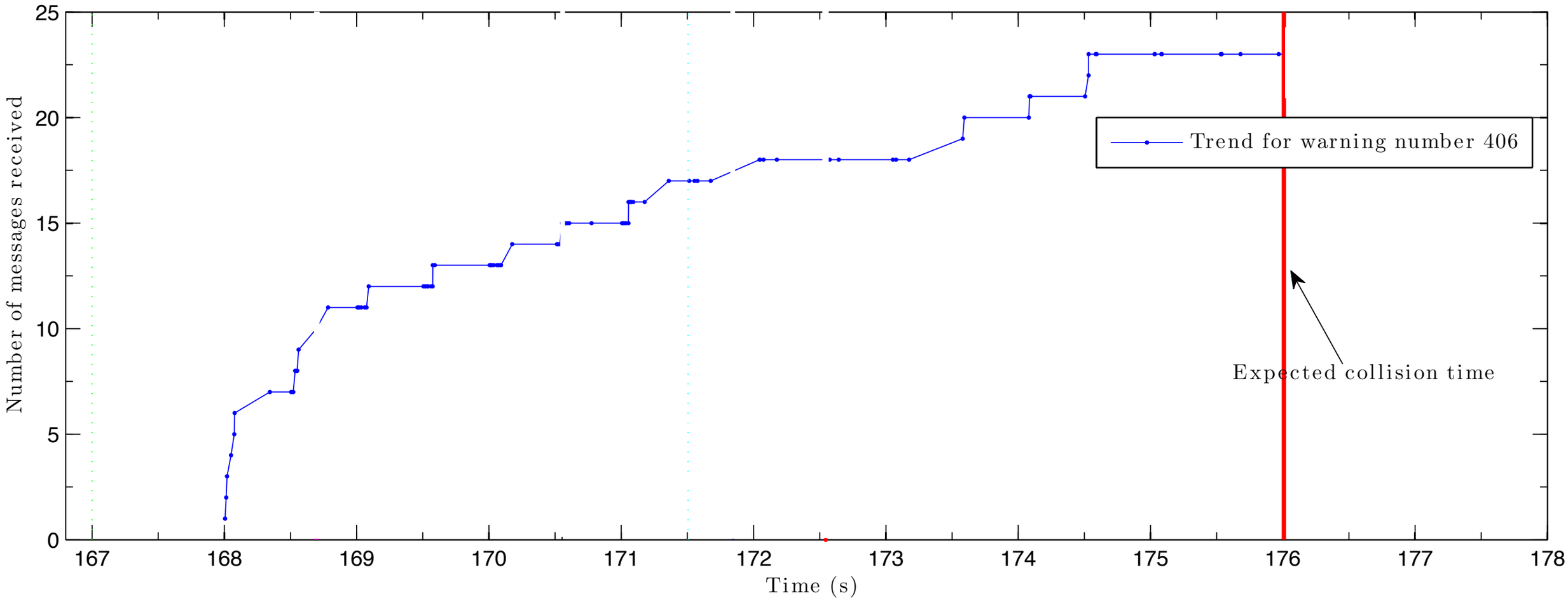
Délai de décision



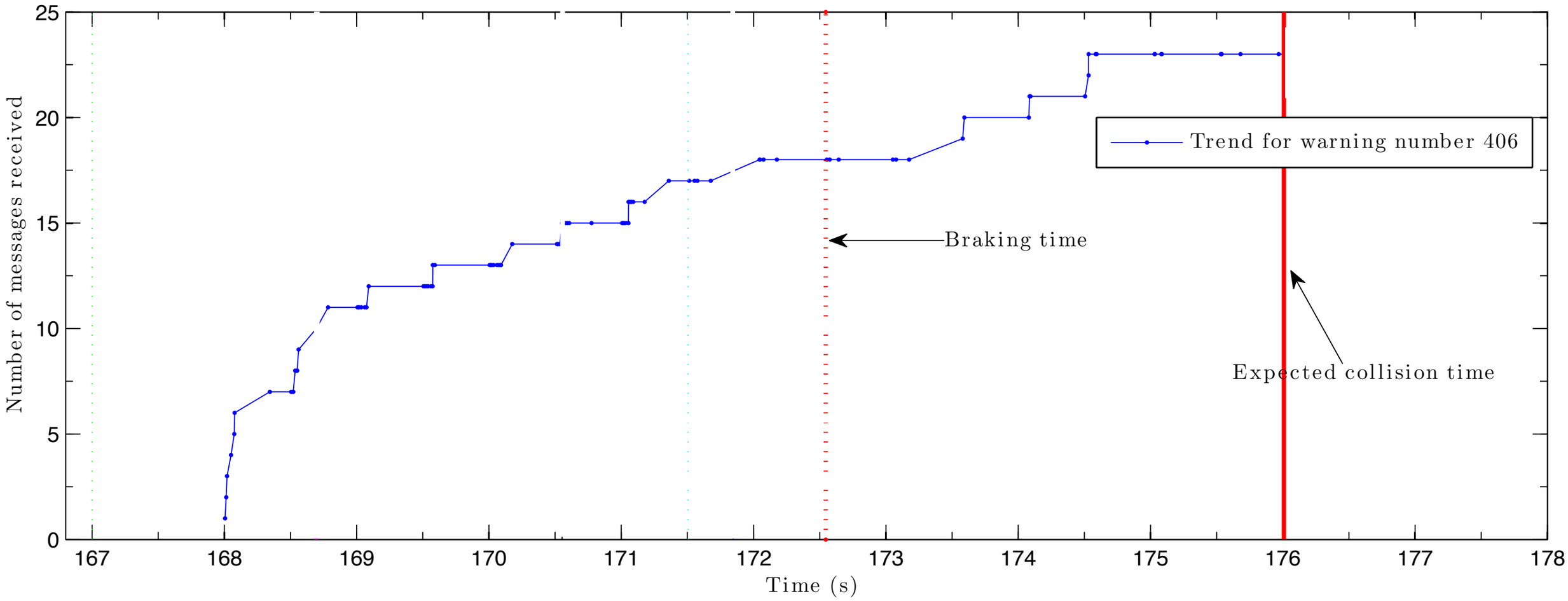
$$Délai_{decision} = (Threshold + W(X)) \times T_{ov}$$

$$W(X) = \begin{cases} X - Threshold, \text{ si } |Q_{e_k^i}| \geq X \text{ avant } T_{MAX} \\ \omega \times (|Q_{e_k^i}| - Threshold), \text{ si } T_{MAX} \text{ écoulé} \end{cases}$$

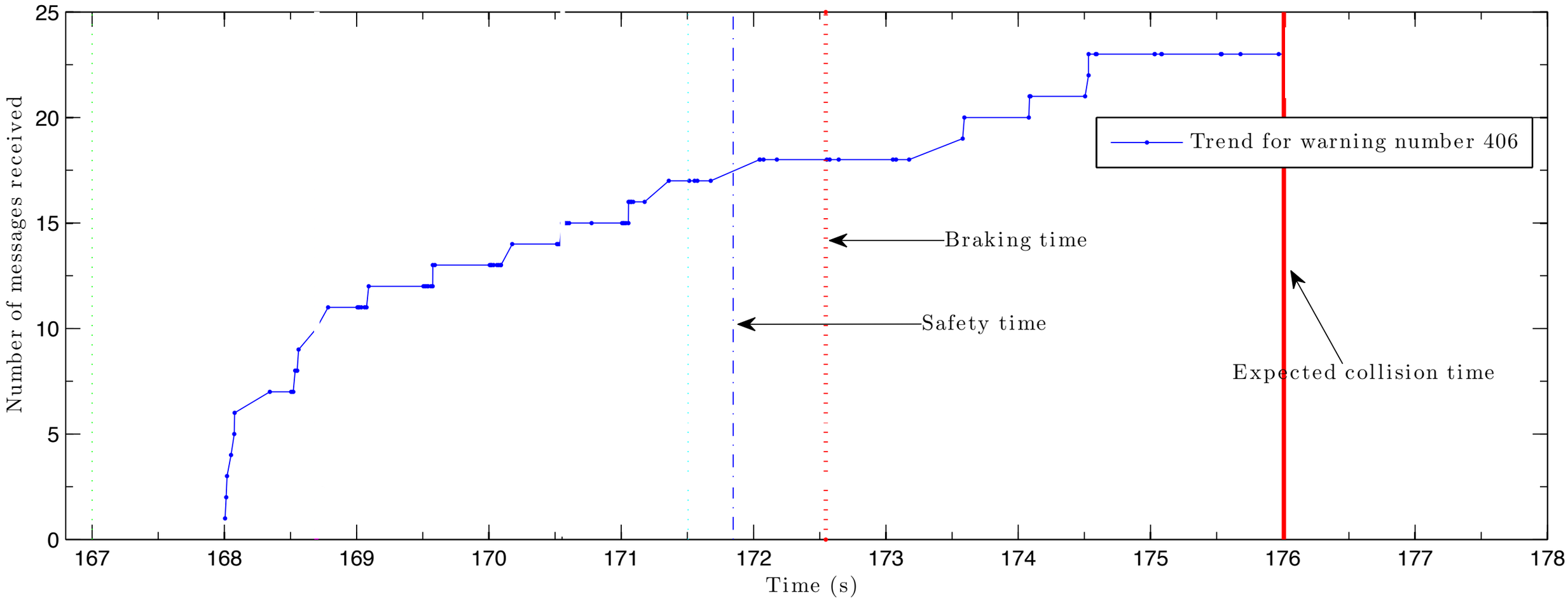
Résultats de simulation (1/2)



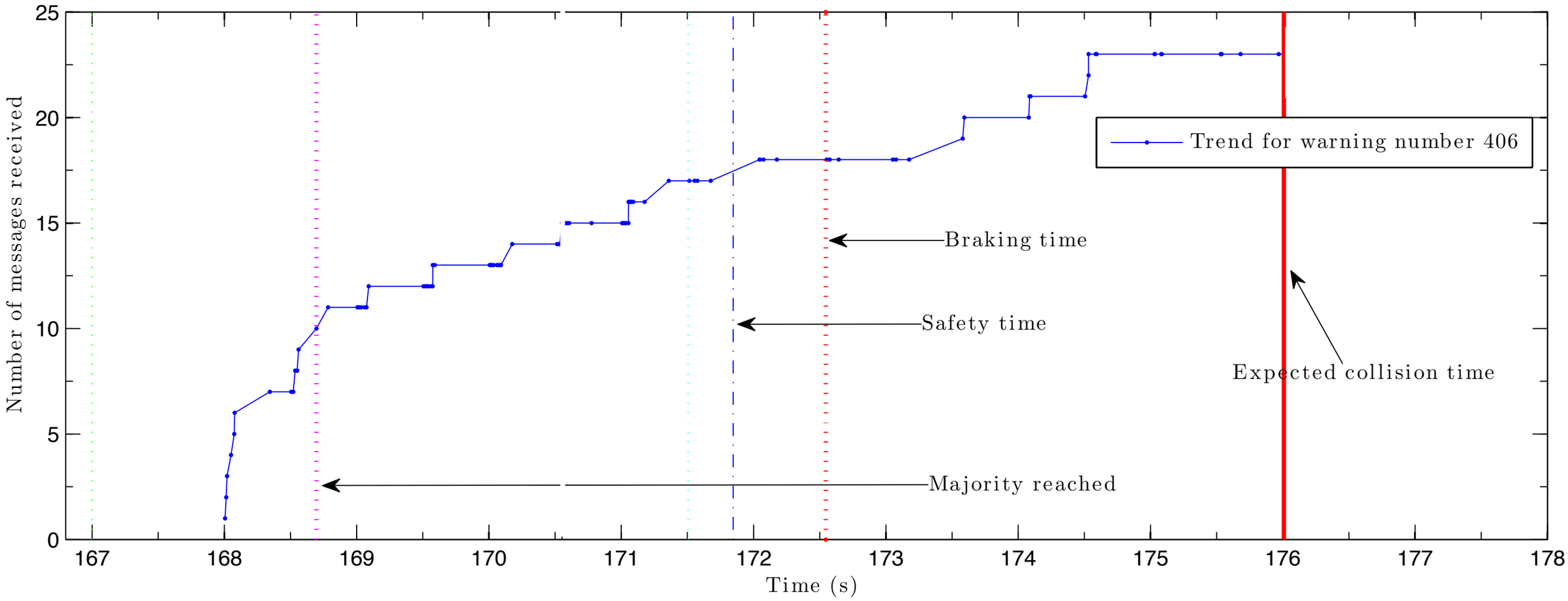
Résultats de simulation (1/2)



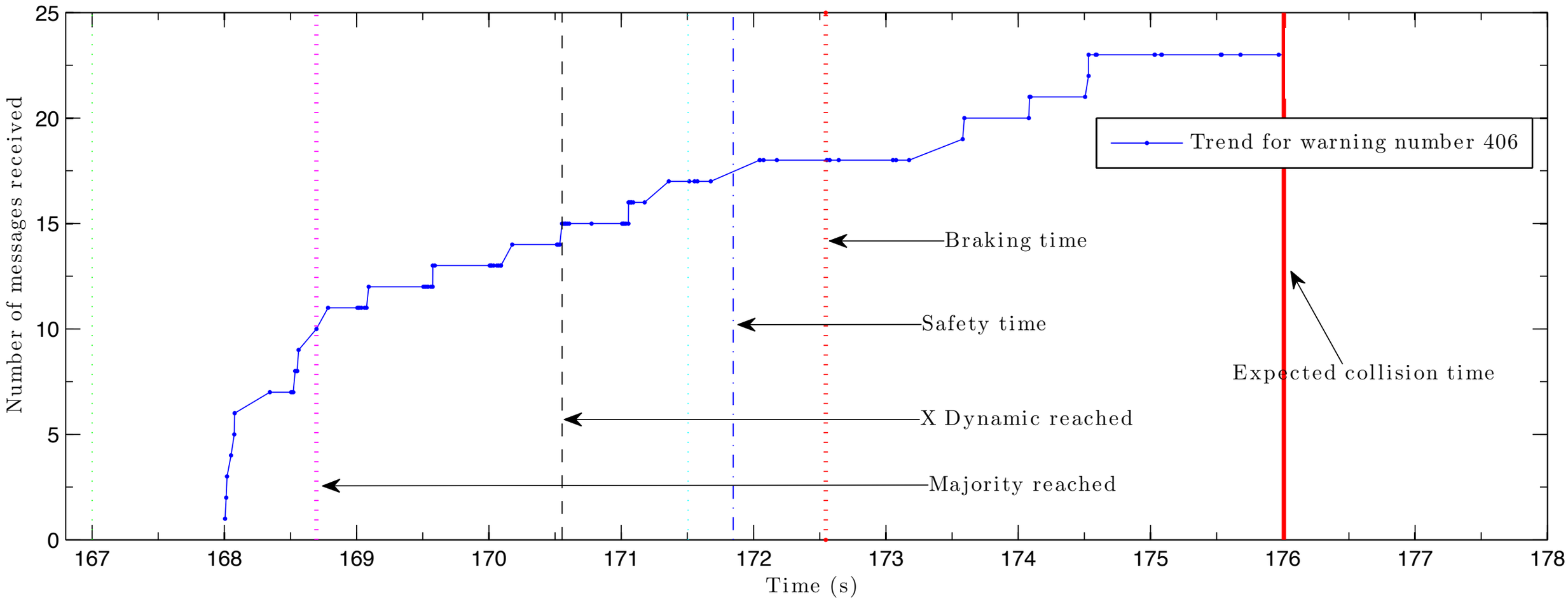
Résultats de simulation (1/2)



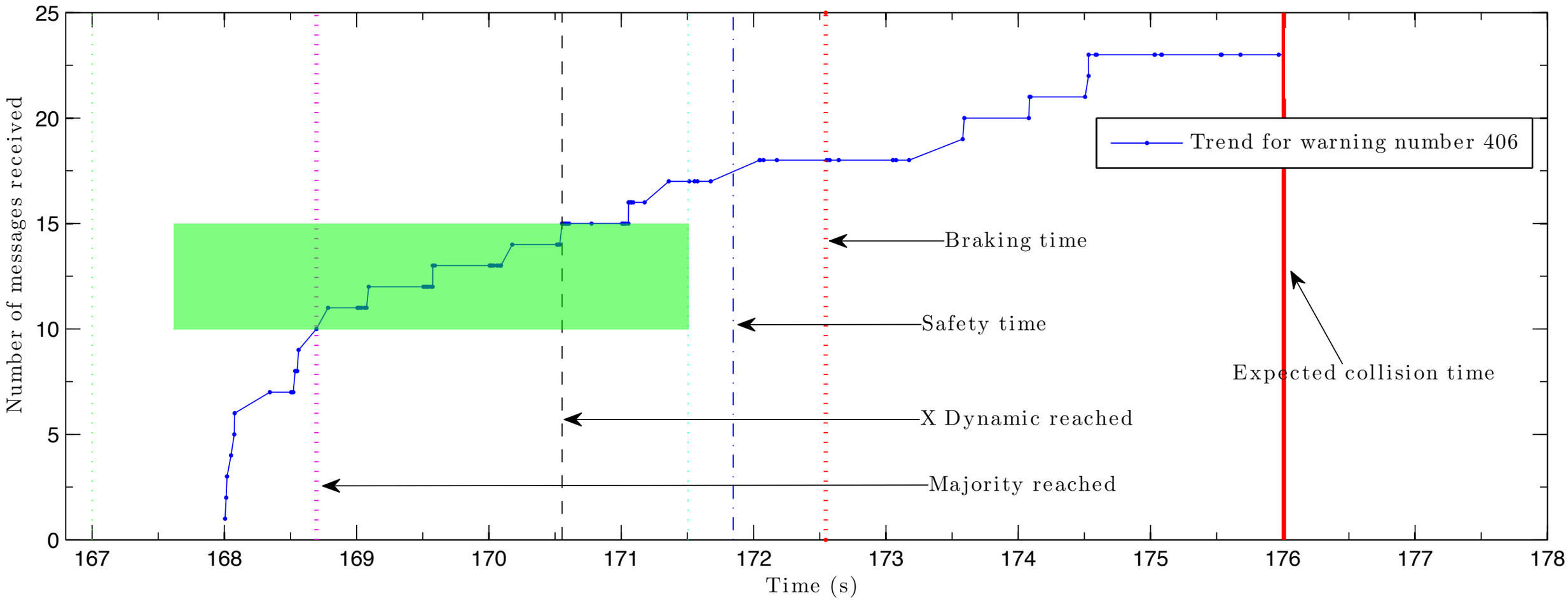
Résultats de simulation (1/2)



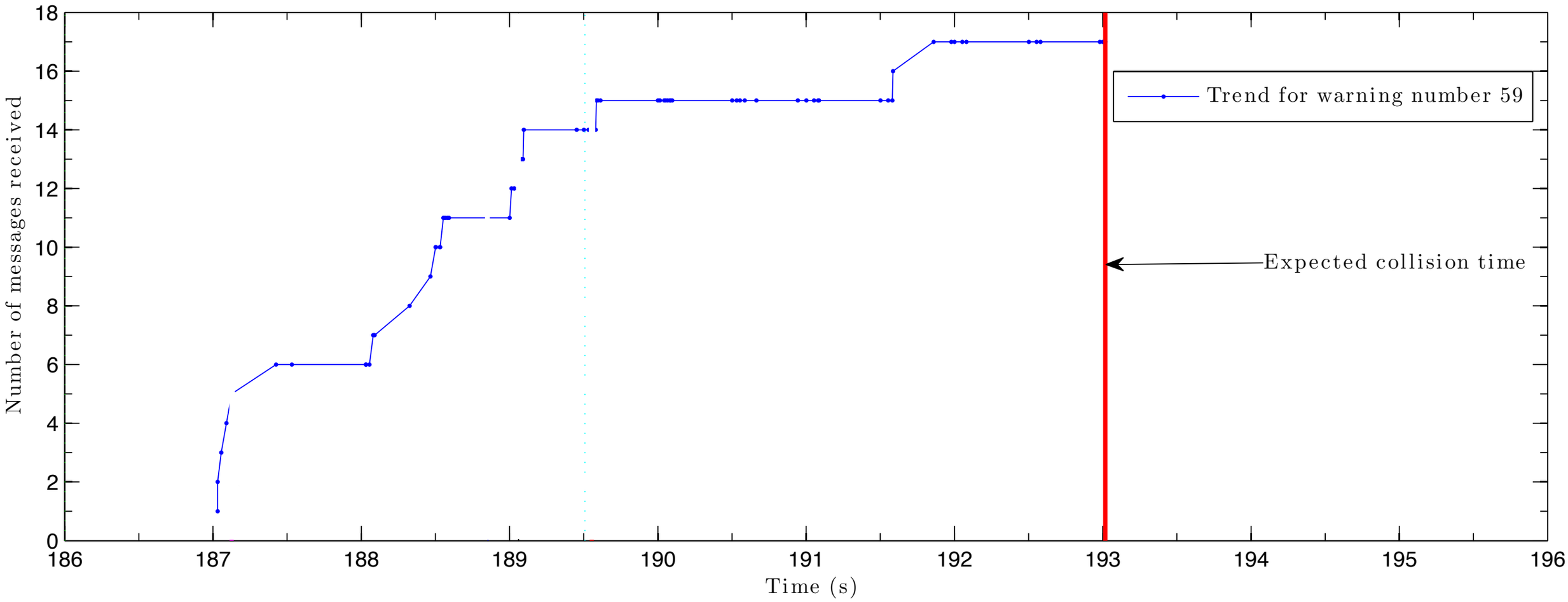
Résultats de simulation (1/2)



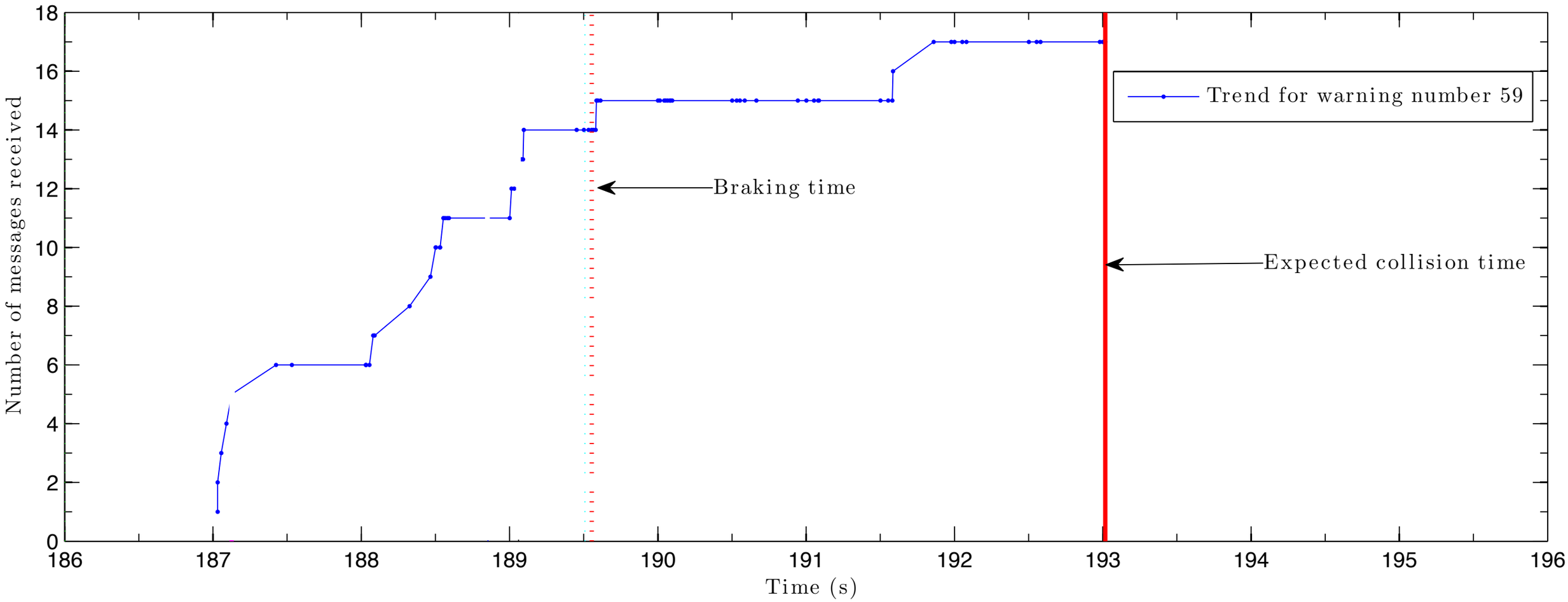
Résultats de simulation (1/2)



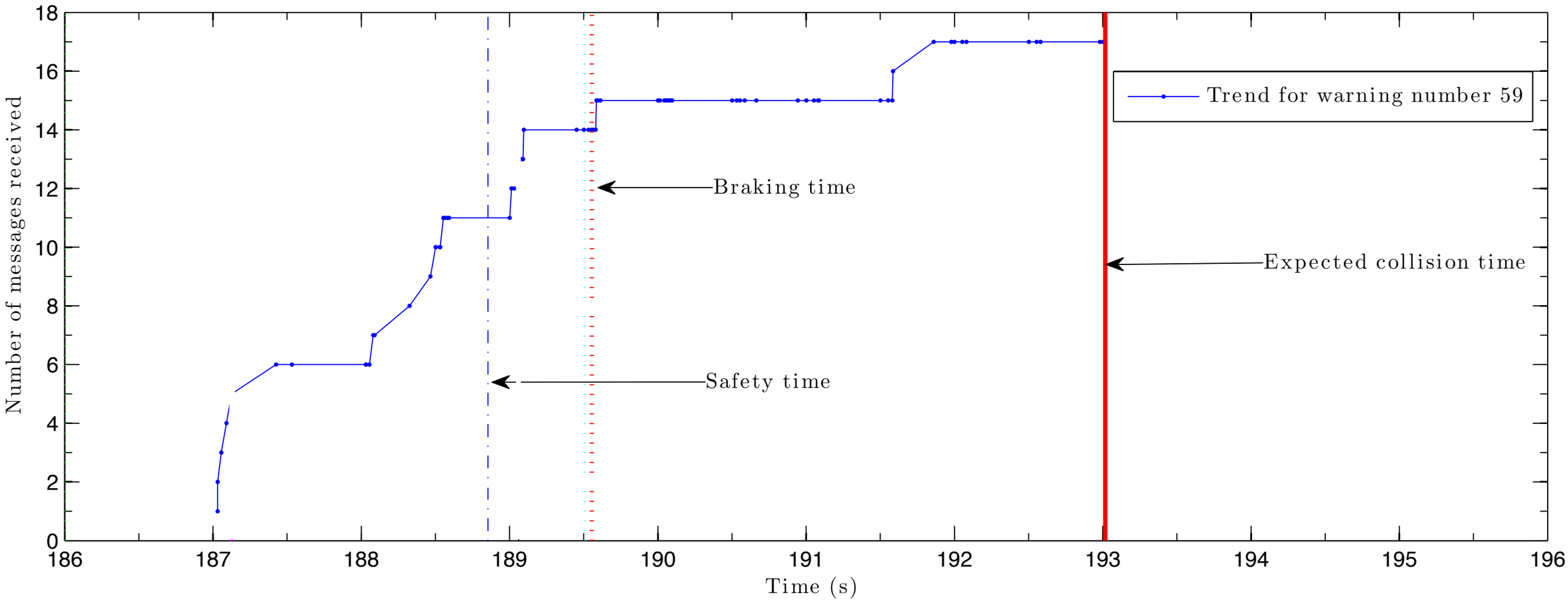
Résultats de simulation (2/2)



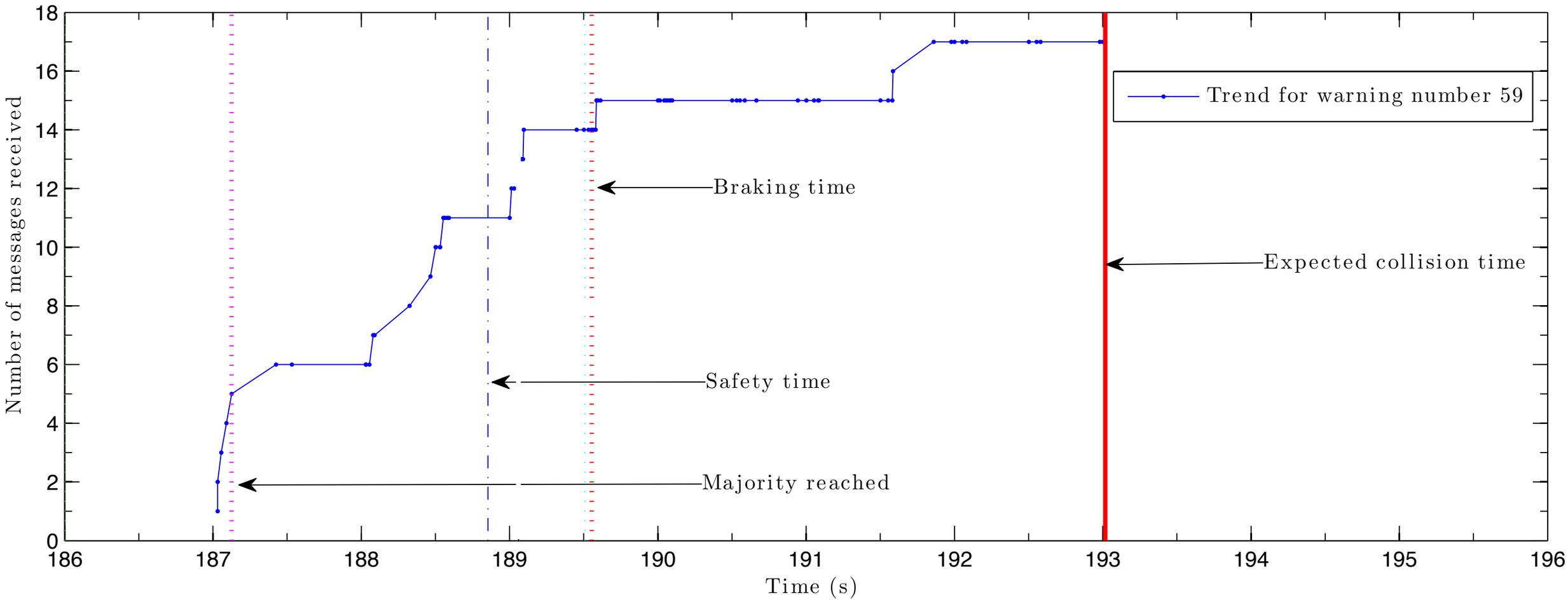
Résultats de simulation (2/2)



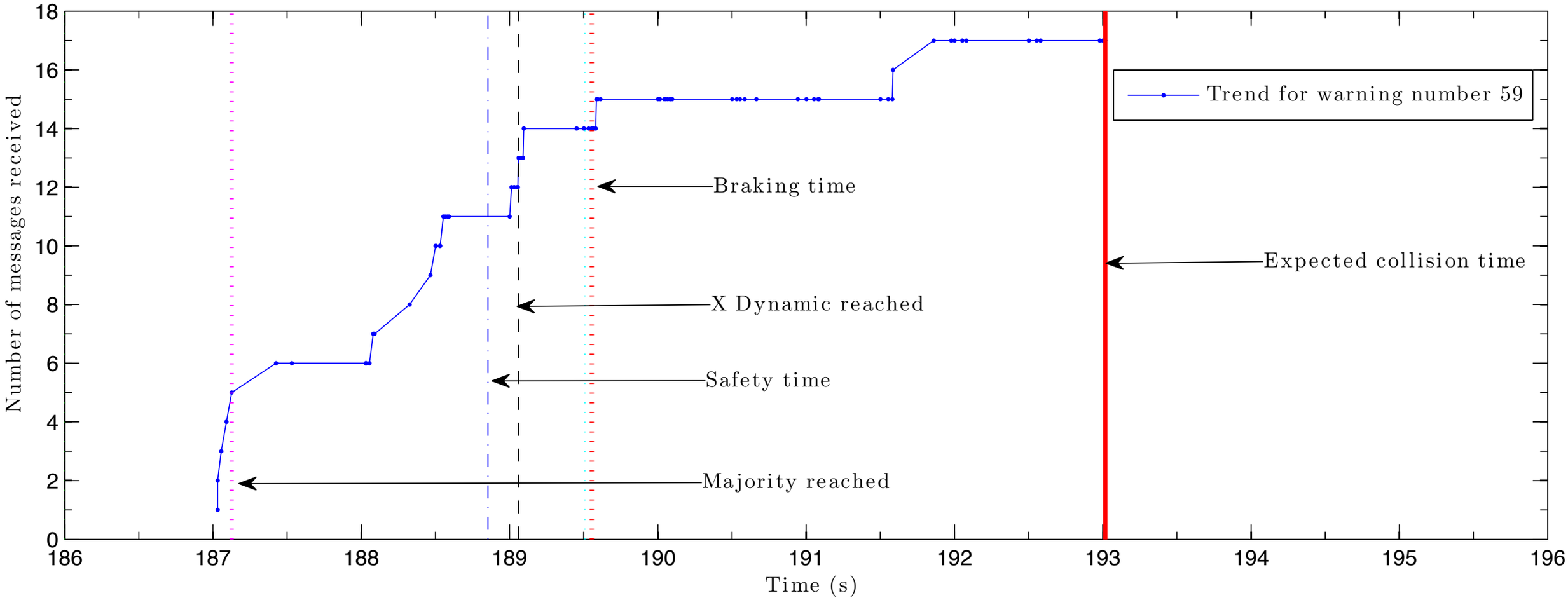
Résultats de simulation (2/2)



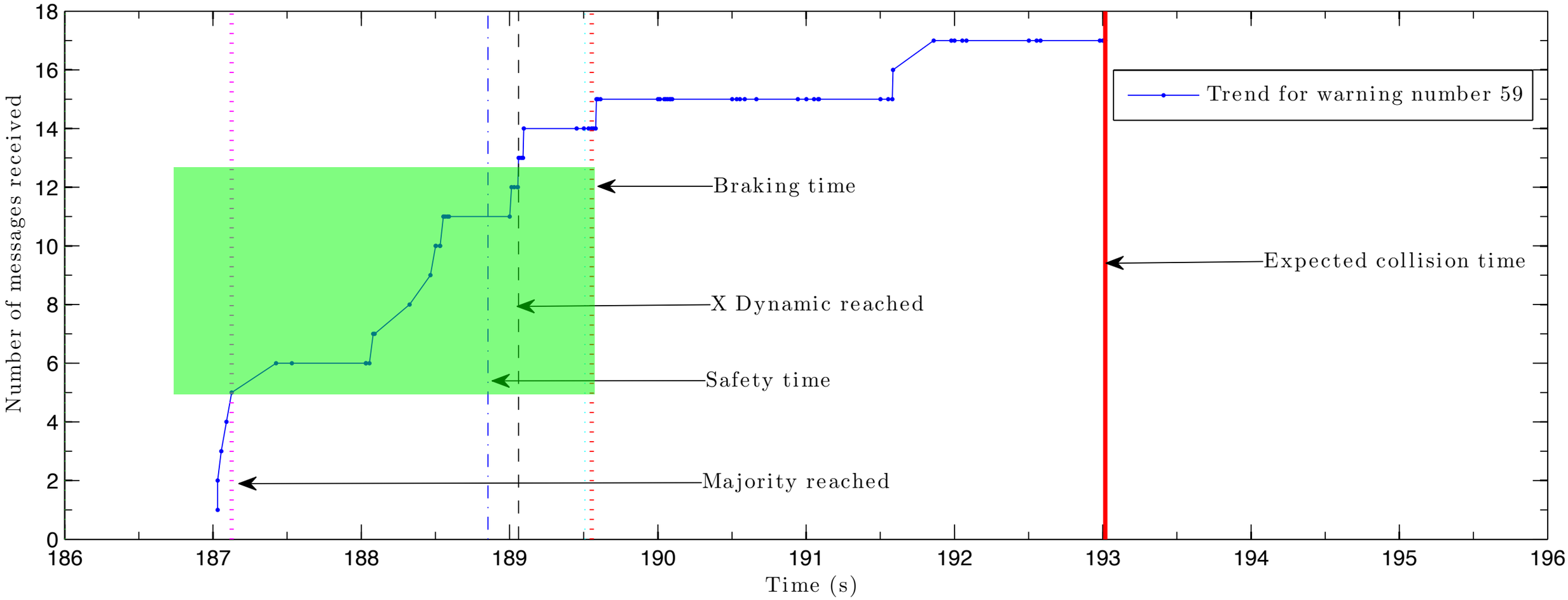
Résultats de simulation (2/2)



Résultats de simulation (2/2)



Résultats de simulation (2/2)

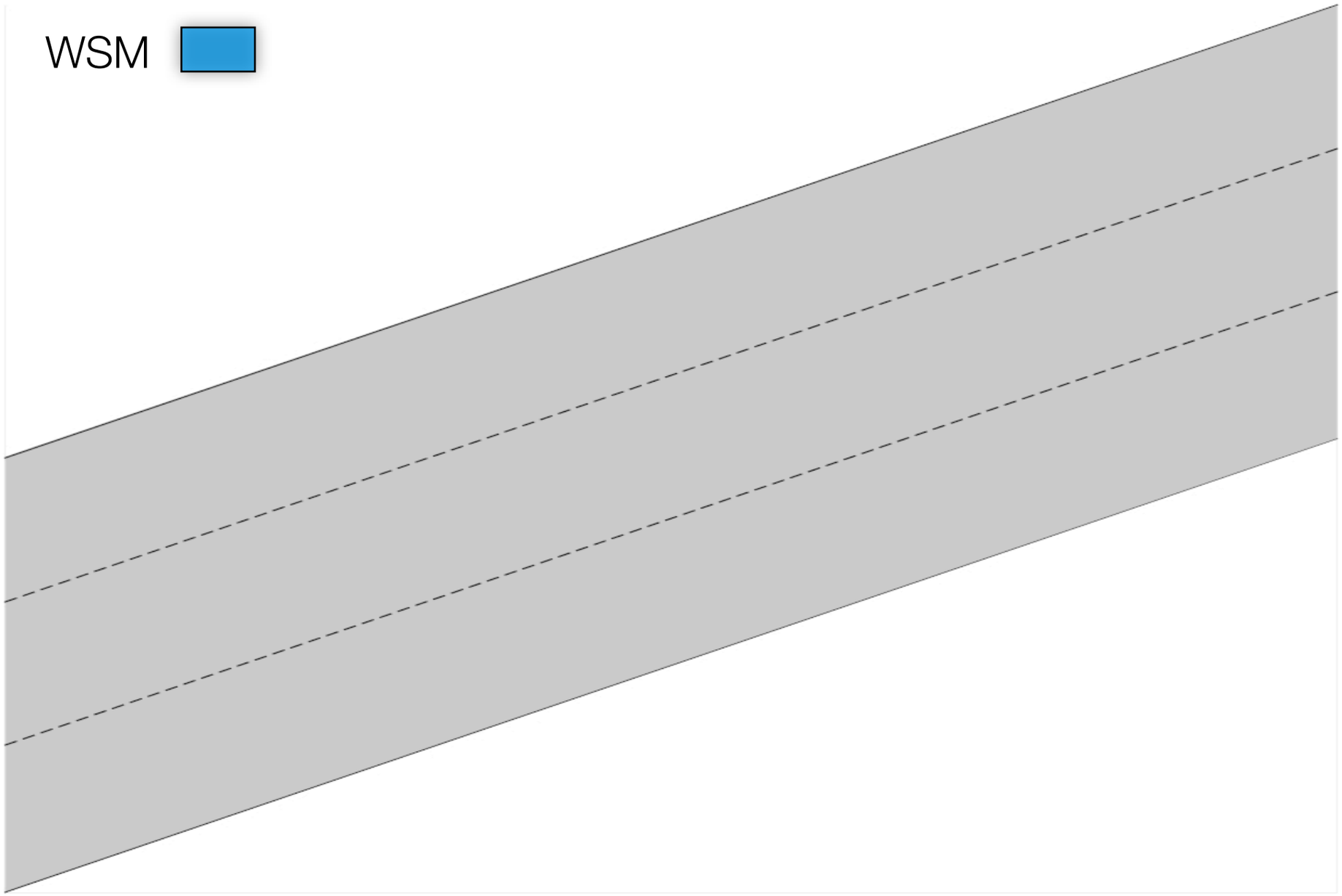


Avantages

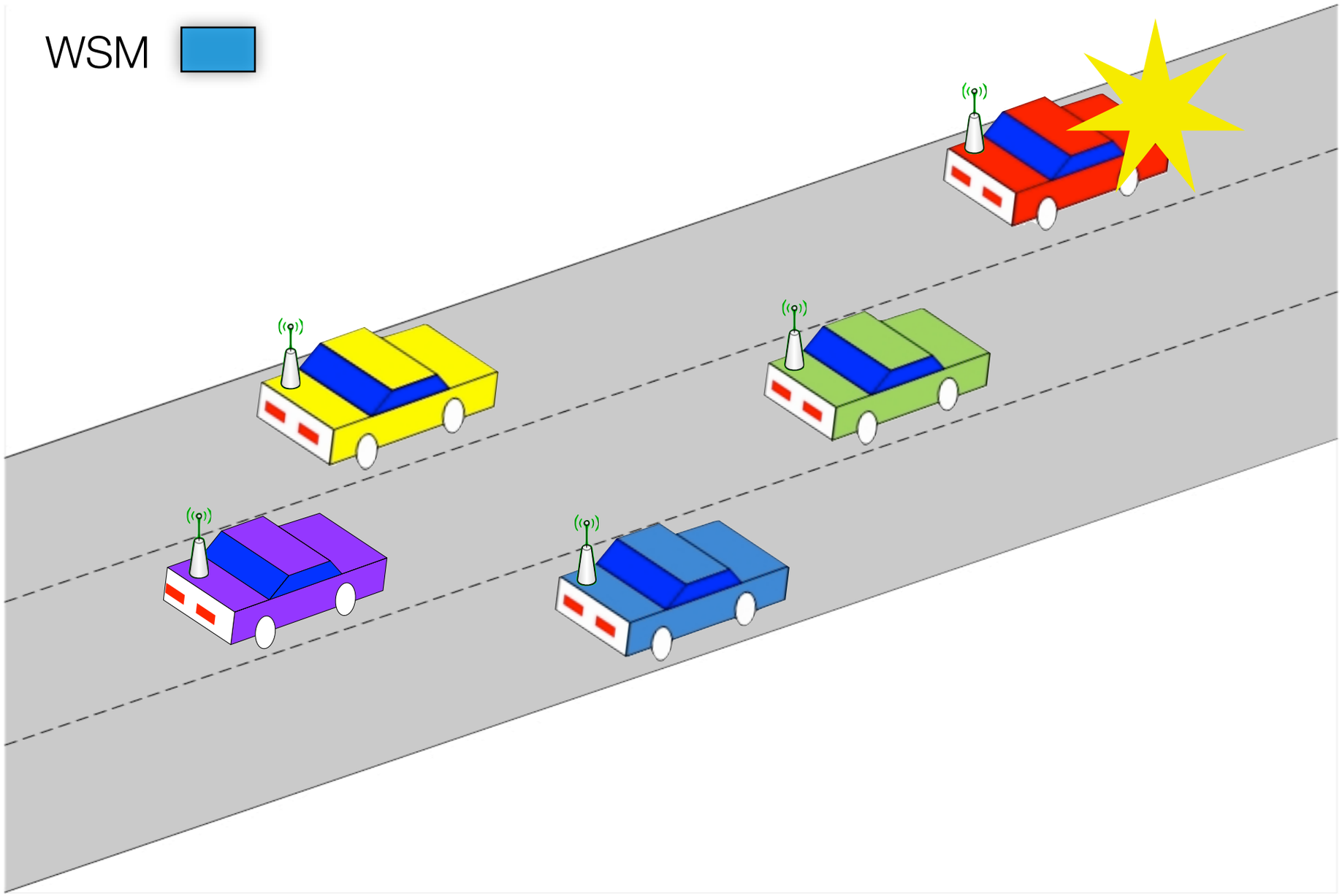
- Fléxibilité
- Sensibilité au contexte (vitesse, position)
- Limitation du surcoût

Authentification + Consensus

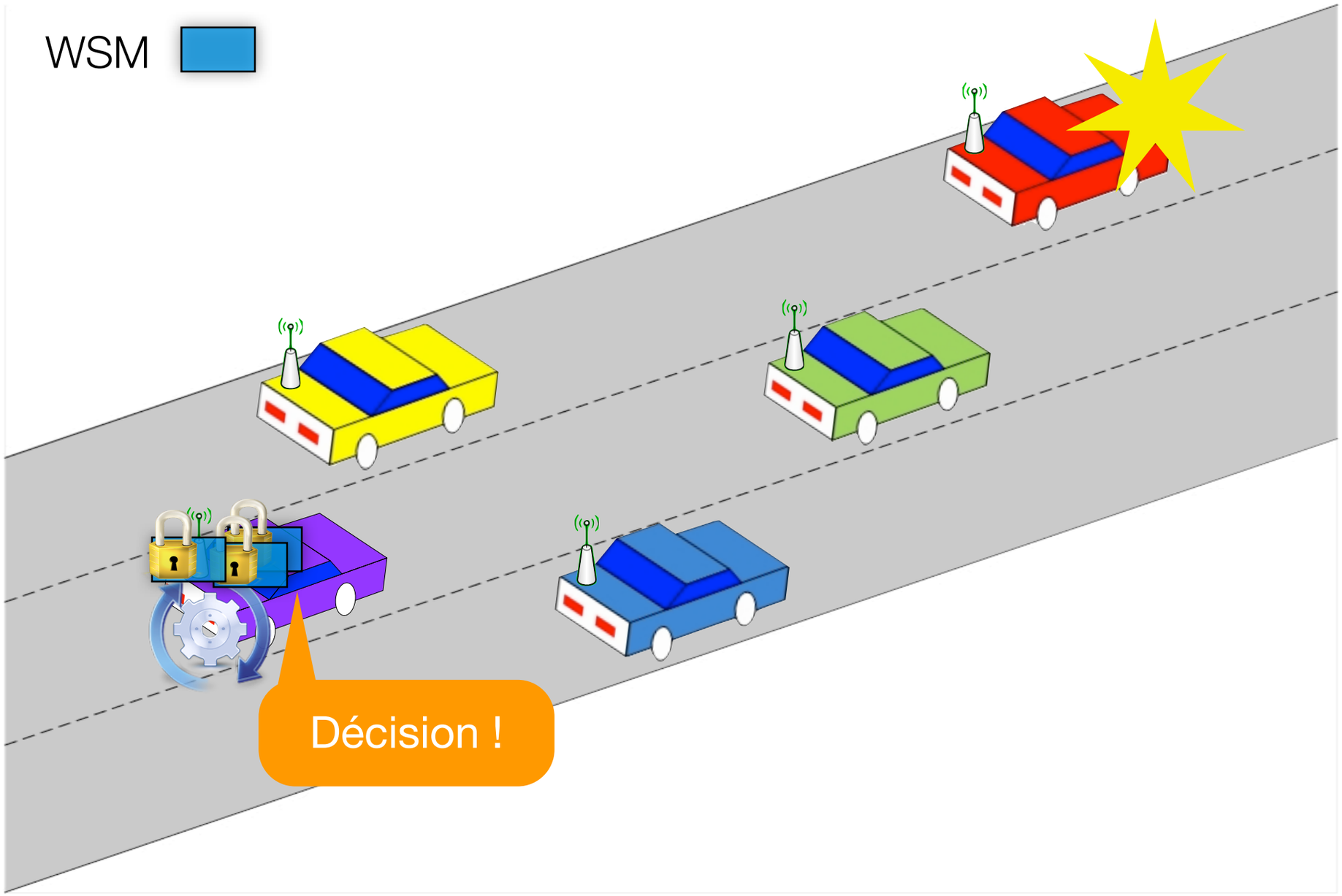
Authentification + Consensus



Authentification + Consensus



Authentification + Consensus



Authentification + Consensus

$$D_{sécurité} = D_{authentification} + D_{consensus} + D_{disponibilité} + \dots$$

Authentification + Consensus

$$D_{sécurité} = D_{authentification} + D_{consensus} + D_{disponibilité} + \dots$$

$$D_{Sécurité} = \quad X_i \times$$

Authentification + Consensus

$$D_{sécurité} = D_{authentification} + D_{consensus} + D_{disponibilité} + \dots$$

$$D_{Sécurité} = \quad X_i \times (D_{authentification}$$

Authentification + Consensus

$$D_{sécurité} = D_{authentification} + D_{consensus} + D_{disponibilité} + \dots$$

$$D_{Sécurité} = \quad X_i \times (D_{authentification} + D_{filter} + D_{classifier}) + D_{decision\_maker} + \dots$$

Authentification + Consensus

$$D_{sécurité} = D_{authentification} + D_{consensus} + D_{disponibilité} + \dots$$

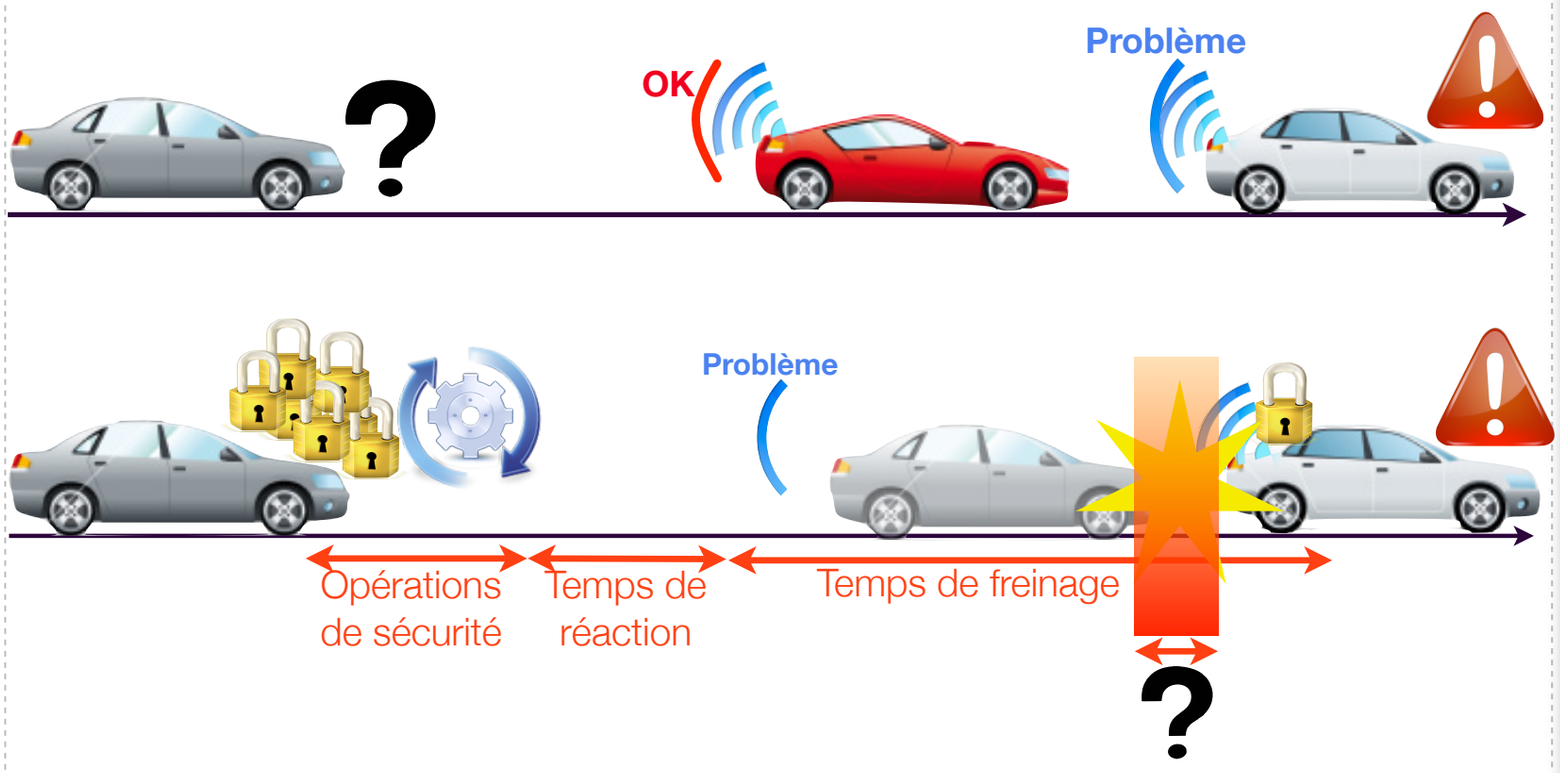
$$D_{Sécurité} = \sum_{i=1}^{N_E} X_i \times (D_{authentification} + D_{filter} + D_{classifier}) + D_{decision\_maker} + \dots$$

Conclusion

Problématique

Conclusion

Problématique

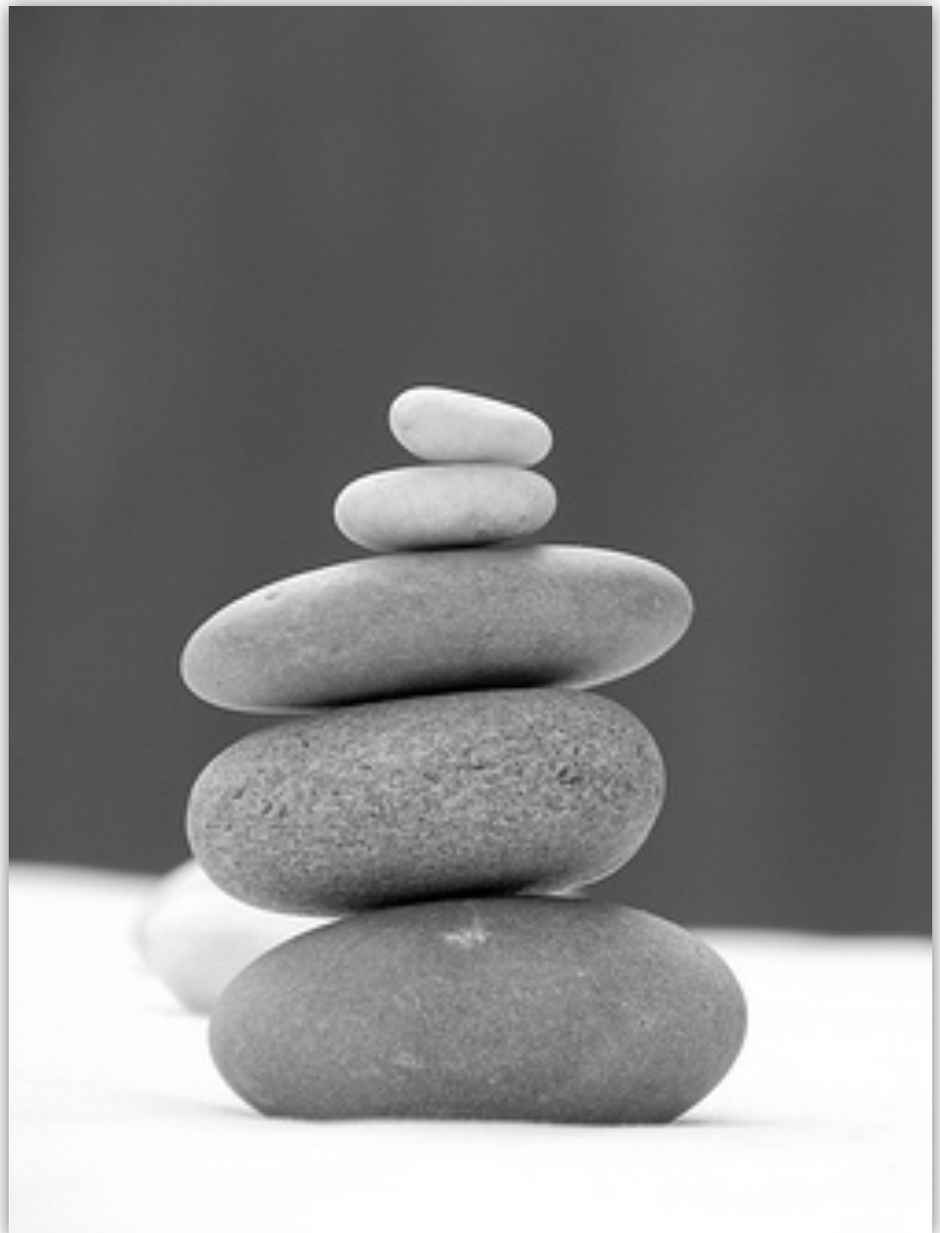


Conclusion

- Problématique
- Estimation du surcoût de l'authentification
- Estimation du surcoût du consensus
  - Méthode de décision dynamique
  - Définition des paramètres
- Combinaison des 2 services

Perspectives

- À court et moyen terme
  - Surcoût de l'authentification : Certificat
  - Optimisation de la gestion des certificats
  - Consensus basé sur le délai de transfert
  - Méta-heuristiques pour améliorer les décisions
- À long terme
  - Modèle global du surcoût de la sécurité (respect de la vie privée, non-répudiation,...)



Merci de votre attention

Merci de votre attention

13 Juillet 2011