

# Počítačové siete 2

TESLA, bezpečné smerovanie, detekcia chýb

Martin Drozda

# Formulácia problému

Autentifikácia správ v ad hoc sieťach:

- **Symetrická kryptografia:** vyžaduje distribučnú autoritu (key distribution center),  $O(n^2)$  rozdielnych kľúčov
- **Asymetrická kryptografia:** vyžaduje distribučnú autoritu (key distribution center),  $O(n)$  rozdielnych kľúčov, výpočtovo náročné (pre mnoho zariadení)

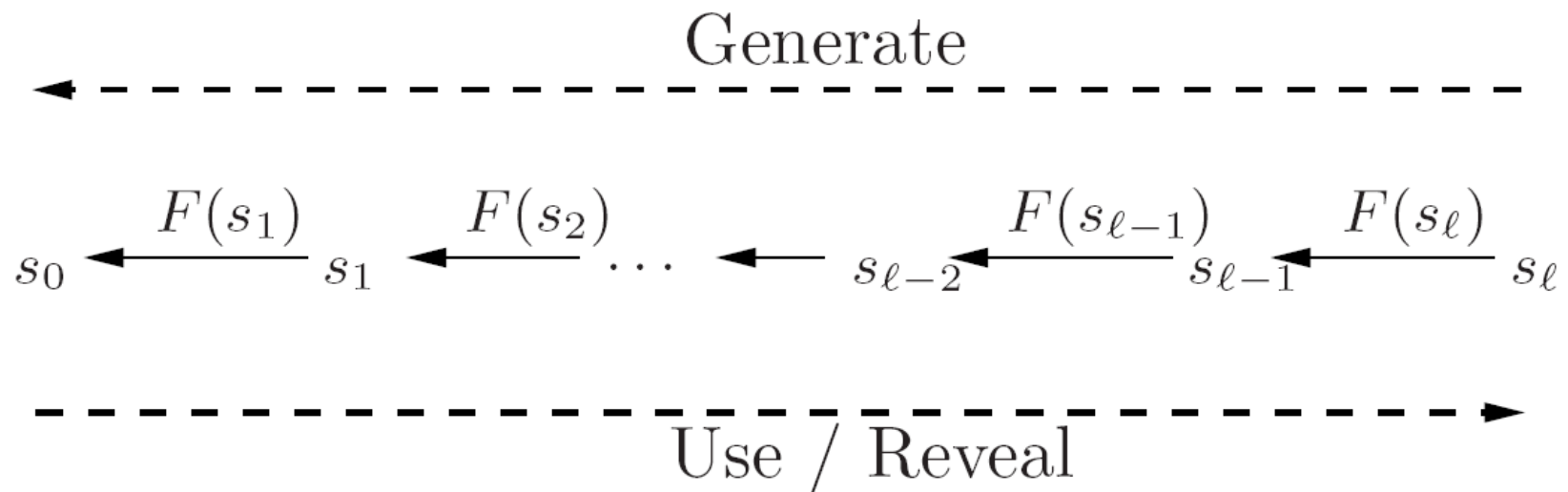
**Bezpečný broadcast:** ←

- Pri broadcaste sa posiela správa viacerým uzlom, ktorých identita dopredu nemusí byť známa (ako šifrovať, keď neviem komu posielam)
- Overiteľnosť, že dáta (ale aj RREQ, ...) sú z daného uzla
- Symetrické kľúče môžu byť ukradnuté
- Asymetrické kľúče nemusia neponúkať potrebnú priepustnosť

# Timed efficient stream loss-tolerant authentication (TESLA)

## Jednosmerné hašovanie:

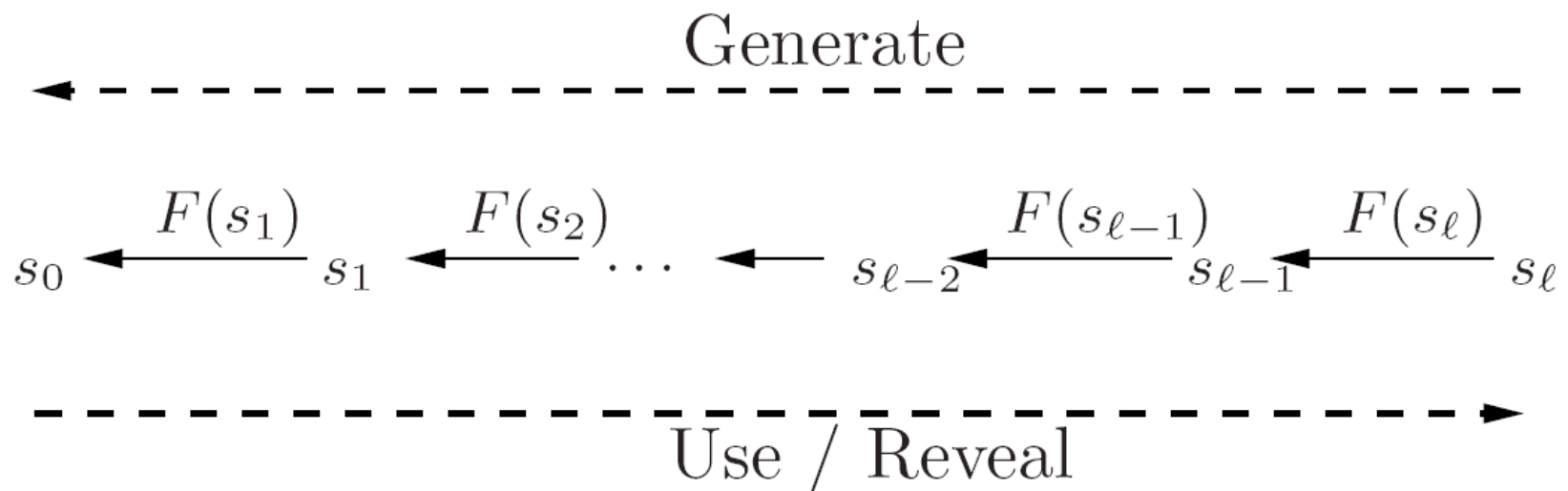
- Na generovanie jednosmernej reťazi hašov použijeme jednosmernú hašovaciu funkciu, napr. gen. náhodných čísel
- Hašovacia funkcia je použitá  $L$ -krát
- Kľúče  $s_i$  sú použité pre autentifikáciu správ (MAC = Message authentication code)



Obrázok zdroj: Perrig, A. and Canetti, R. and Tygar, JD and Song, D. The TESLA Broadcast Authentication Protocol, RSA CryptoBytes, 2002.

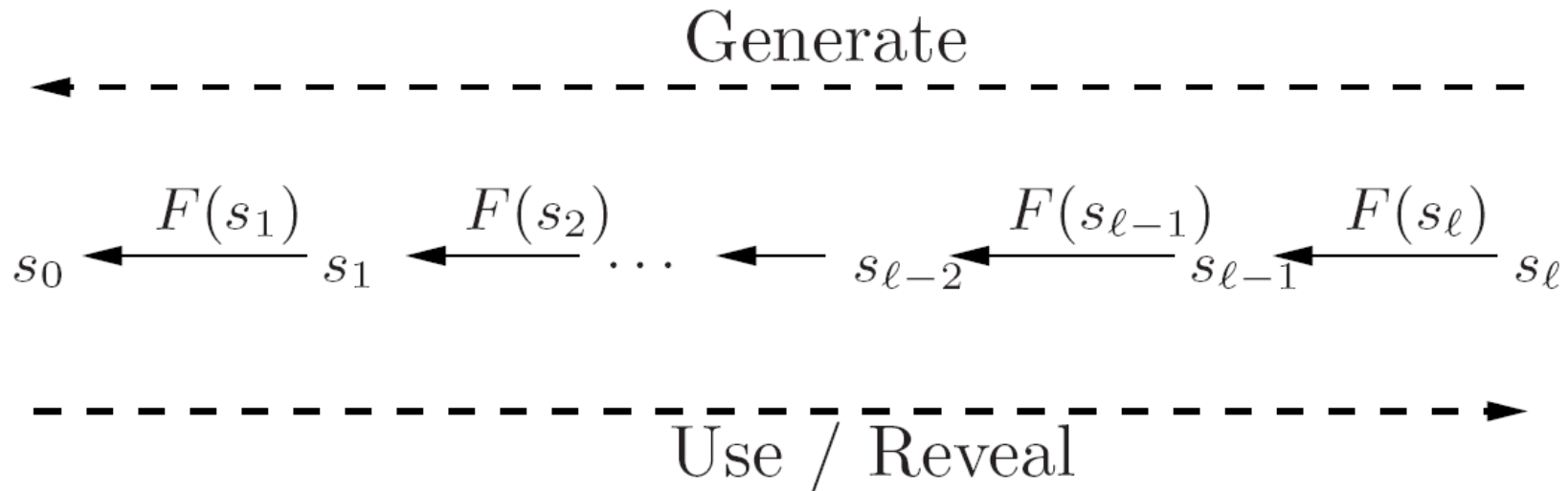
# Timed efficient stream loss-tolerant authentication (TESLA)

- Kľúče sú použité a zverejnené v opačnom poradí ako sú generované
- Kľúče sú zverejnené s časovým oneskorením
- Uzol pred overením správy overí, či kľúč už bol zverejnený, ak áno, správa je zmazaná



# Timed efficient stream loss-tolerant authentication (TESLA)

- Ak sa kľúč stratí, je možné ho generovať z neskoršie zverejnených kľúčov
- TESLA vyžaduje približnú synchronizáciu času, odosielateľ zverejní čas zverejnenia kľúča (oneskorenie po jeho použití)



## Synchronizácia odosielateľa S a prijímateľa R

- R pošle S: Nonce
- S pošle R:  $\{t_s, \text{Nonce}\}$  podpísaný privátnym kľúčom S
- R overí pomocou verejného kľúča S, či je správa podpísaná uzlom S

Horné ohraničenie času odosielateľa:  $t - t_R + t_s$

Nonce je náhodný bit-string s dĺžkou  $h$

$t$  = čas teraz;  $t_s$  = čas odosielateľa;  $t_R$  = čas prijímateľa

Ďalšia možnosť: „microcomputer-compensated crystal oscillator“.  
Presnosť v sekundách v trvaní niekoľko mesiacov.

## DSR + TESLA

Autentifikácia RREQ: príjemca overí autenticitu a čerstvosť RREQ

## TESLA aplikovaná každým uzlom

Získanie cesty:

- žiaden uzol nevie odstrániť iný uzol zo zoznamu v RREQ/RREP
- cieľový uzol vie autentifikovať zdrojový uzol (kto poslal RREQ)
- Zdrojový uzol vie autentifikovať každý uzol v zozname uzlov RREP

RREQ:

(Route request, initiator, target, id, time interval, hash chain, node list, MAC list)

RREP:

(Route reply, target, initiator, time interval, node list, MAC list, target MAC, key list)

time interval: pesimistický odhad času prijatia RREP



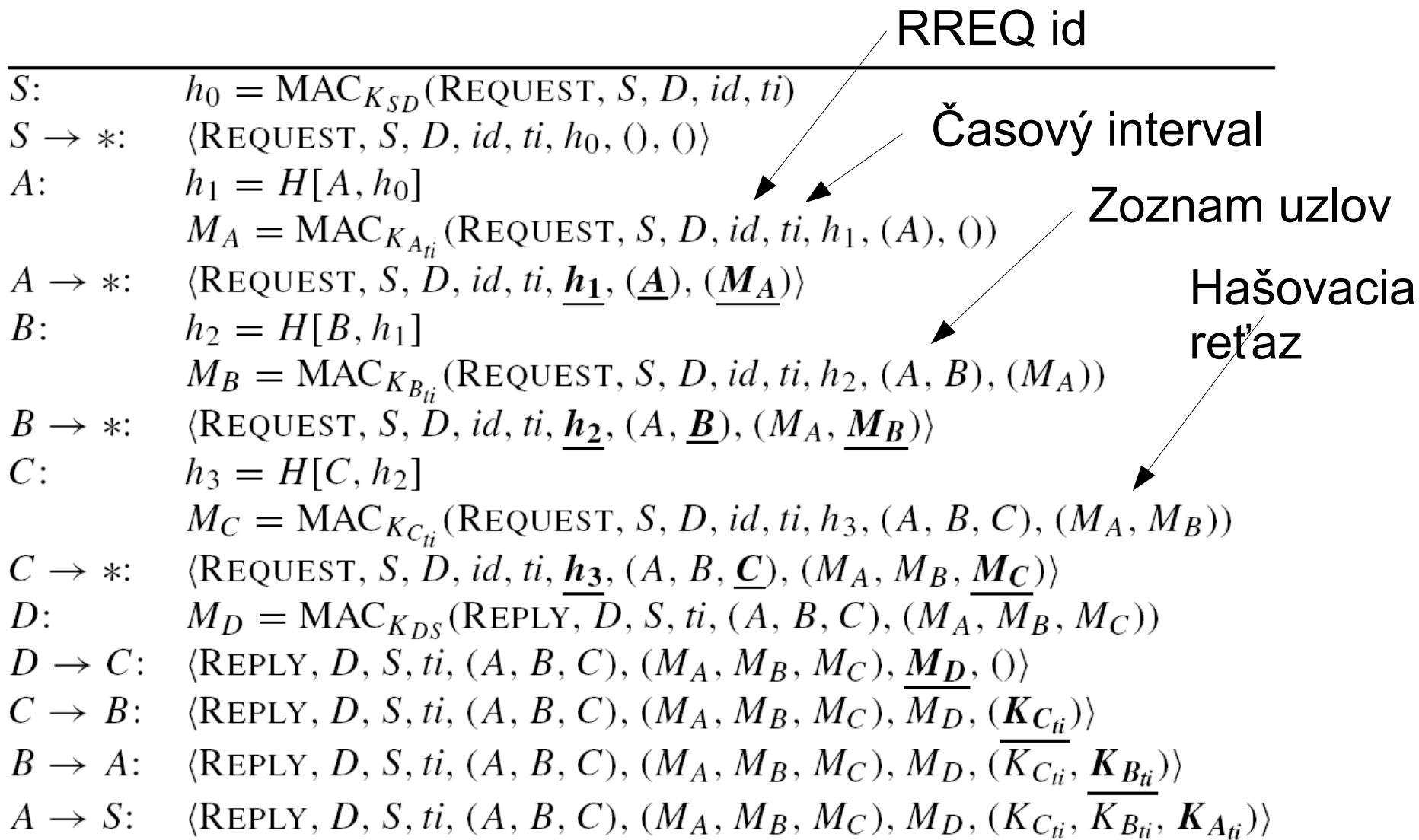
- Cieľový uzol overí, že hašovacia reťaz je rovná:

$H[\eta_n, H[\eta_{n-1}, H[\dots, H[\eta_1, \text{MAC}_{\text{KSD}}(\text{initiator}, \text{target}, \text{id}, \text{time interval})]\dots]]]$

$\eta_i$  je adresa uzla na pozícii  $i$

- Uzol, ktorý preposiela RREP čaká pokým môže zverejniť svoj kľúč
- Zdrojový uzol overí, že každý kľúč v reťazi je platný, každý MAC v zozname MAC je platný

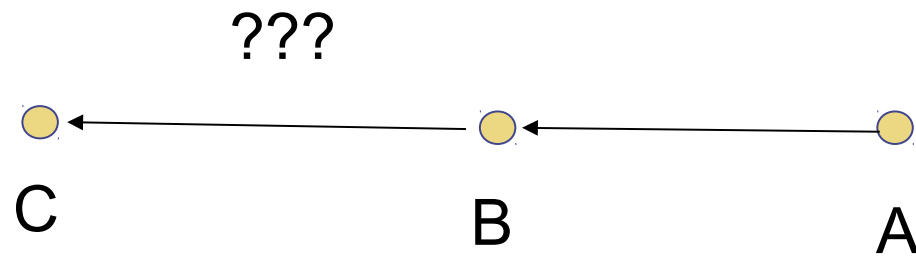
# ARIADNE: RREQ/RREP



$K_{SD}$  = symetrický kľúč;  $K_{A_{ti}}$  = plán zverejnenia kľúča;  $H$  = jednosmerná hašovacia funkcia

# Watchdog

Uzol A v promiskuitnom móde pozoruje, či dátové pakety, ktoré tento uzol poslal B, sú ďalej preposielané.



## Ciele:

- Vysoká detekcia chýb
- Nízky počet falošných poplachov
- Detekcia nových chýb
- Energetická úspornosť
- Nízky počet prahových hodnôt definovaných používateľom
- Adaptivita
- Špecifickosť



Ako?

# “The Adaptive Immune System Interacts with the Innate Immune System to Generate Adaptive Immunity” (Janeway 2001)

## Ciele:

- Vysoká detekcia chýb
- Nízky počet falošných poplachov
- Detekcia nových chýb
- Energetická úspornosť
- Nízky počet prahových hodnôt definovaných používateľom
- Adaptivita
- Špecifickosť

Biologický imúnny systém

Klasifikácia s

- a) vysokým počtom falošných poplachov (**simple**)
- b) nízkym počtom falošných poplachov (**complex**)

# Challenge #2

Klasifikácia, ktorá je

a) energicky neúsporná (**simple**)

b) energicky úsporná (**complex**)

# Zložitosť riešenia

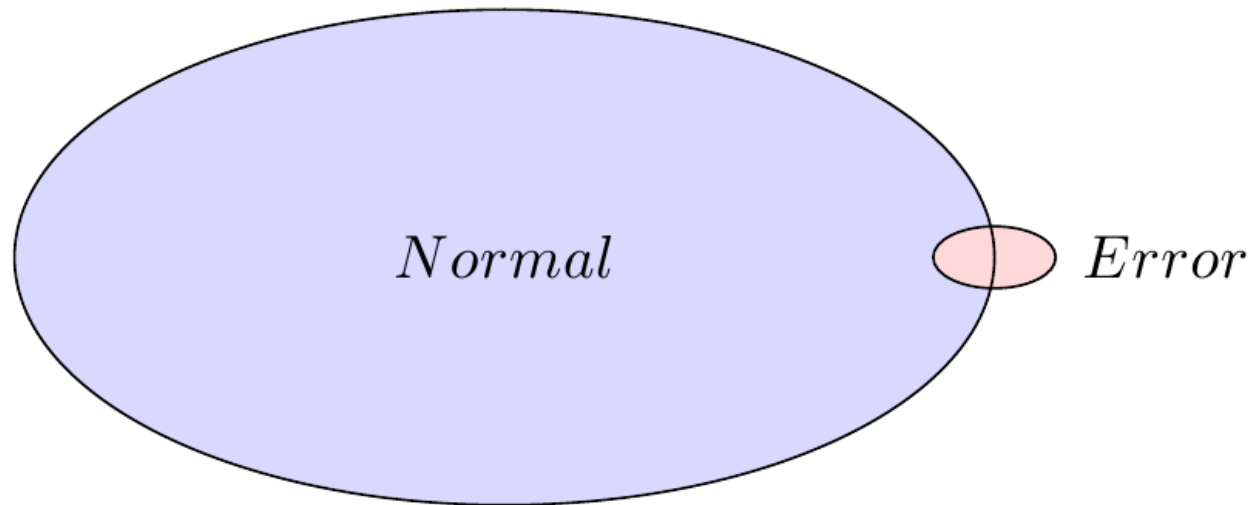
simple + simple = maybe simple

complex + complex = complex

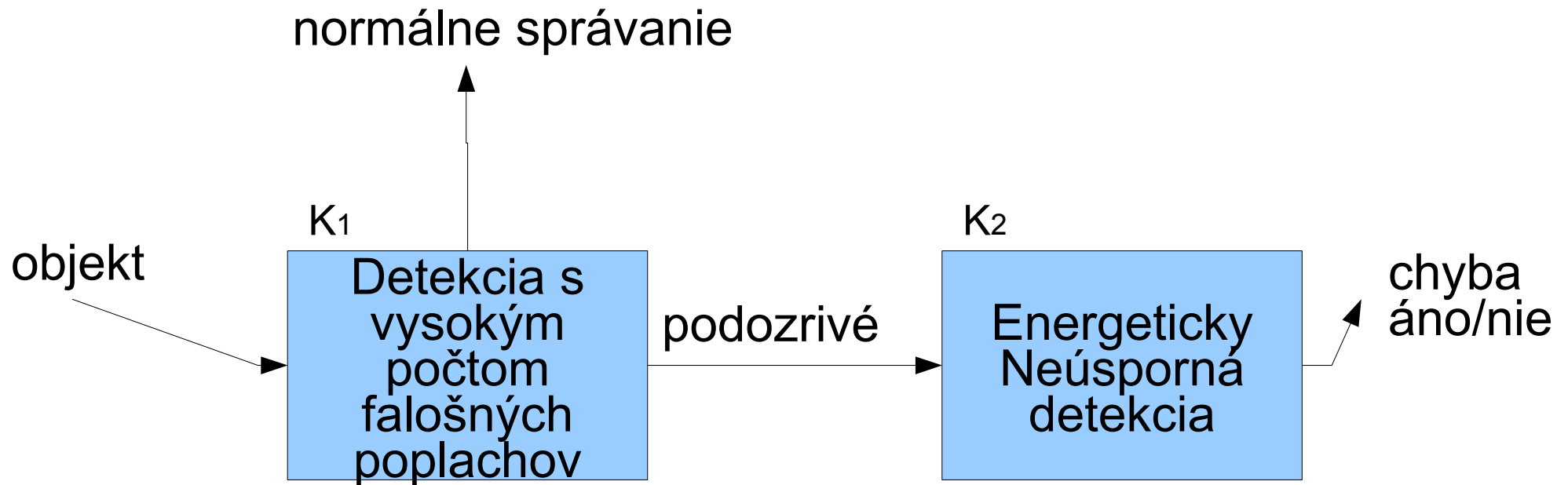
simple + complex = complex



# Normálne správanie vs chyby



Normálne správanie je dominantné v správne navrhnutých systémoch



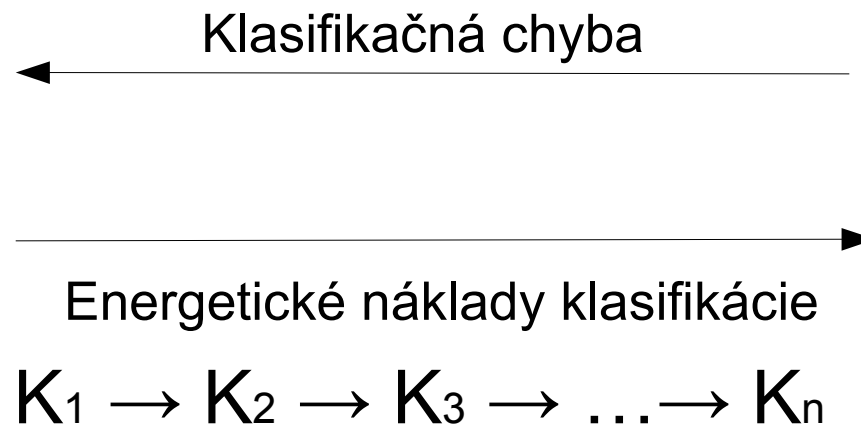
Dve možnosti:

- Vývoj detekčného systému, ktorý je energeticky úsporný
- Minimalizácia používania existujúceho energeticky neúsporného systému

# Kaskádová klasifikácia

Kaynak&Alpaydin (2000): "at the next stage, using a costlier classifier, we build a *more complex* rule to cover those uncovered patterns of the previous stage"

Realita: *menej komplexné pravidlo* (pretože čím je nižšia energetická úspornosť, tým je vyššia presnosť zozbieraných dát a teda pravidlá sú menej zložité)



# Watchdog je neúsporný?

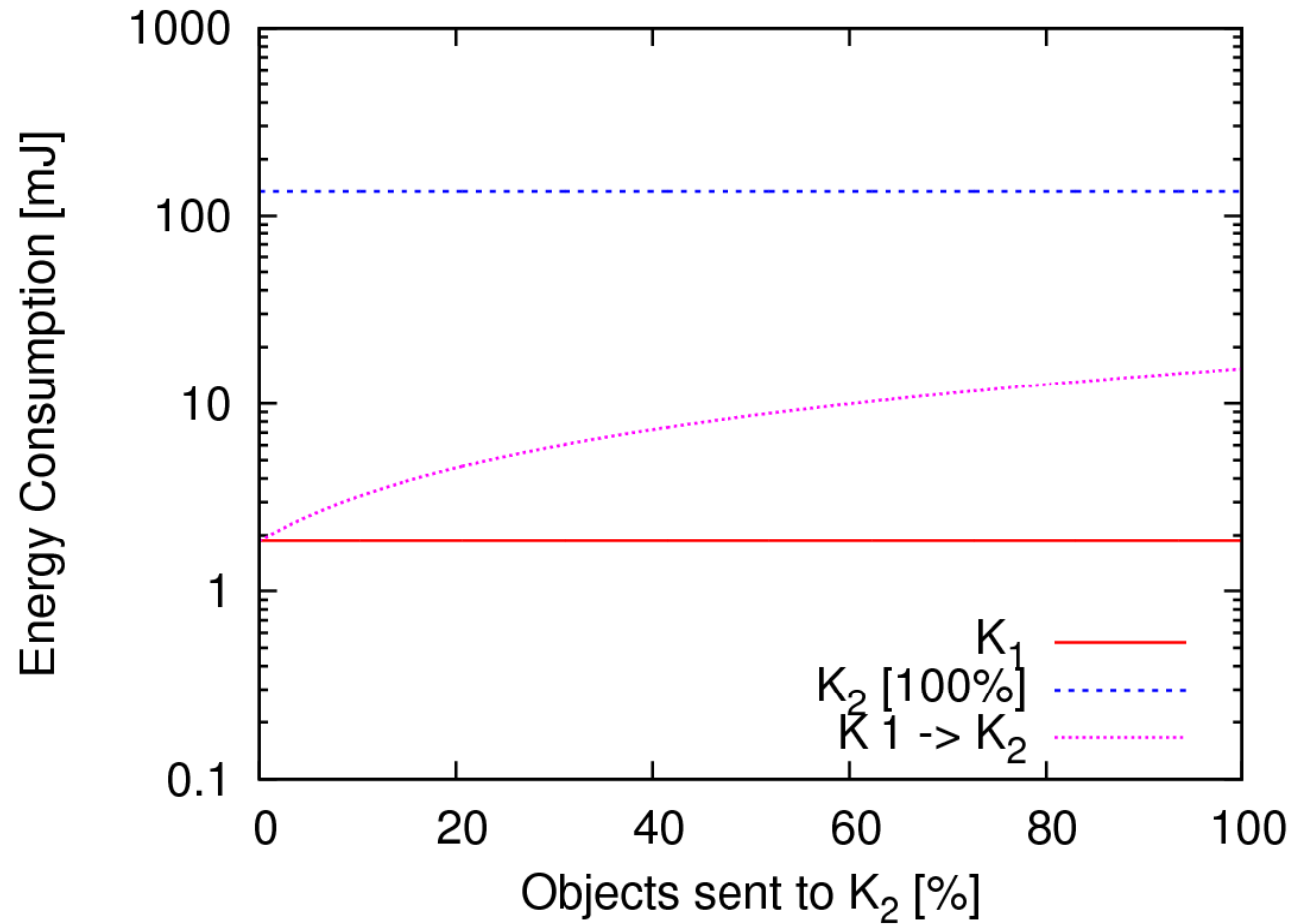
Watchdog je energeticky neúsporný

Watchdog = ACK zo vzdialenosti 2 (od suseda suseda)

Kumulatívne ACK-2 je úsporné:

- ACK pre niekoľko paketov naraz

# K1, K2: experiment

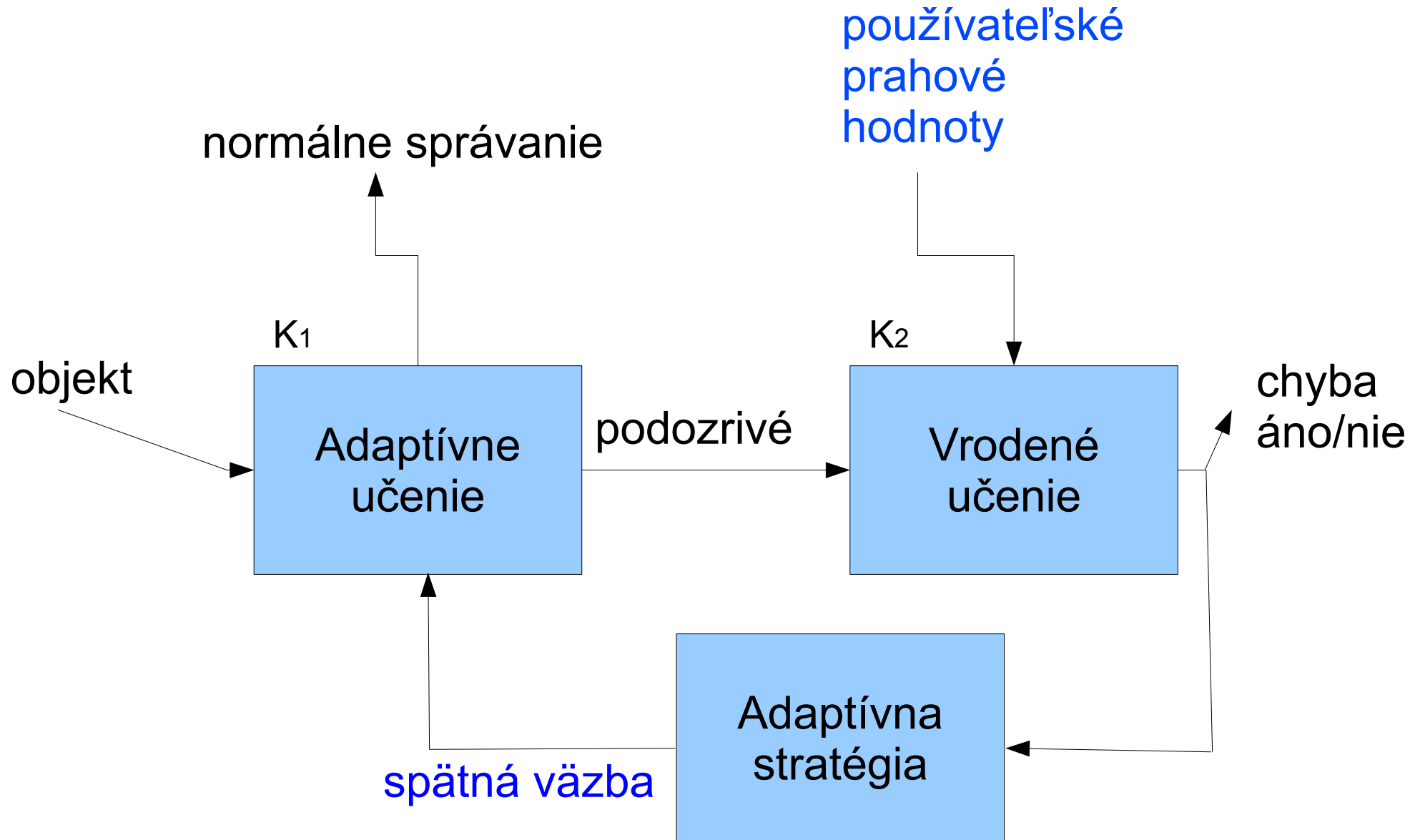


# Falošný poplach?

Pri kaskádovej klasifikácii K1, K2 môže byť výsledný počet falošných poplachov nižší ako počet falošných poplachov K2

- Potvrdené experimentálnymi výsledkami
- Objekty, ktoré K2 nevie správne klasifikovať sú správne klasifikované K1

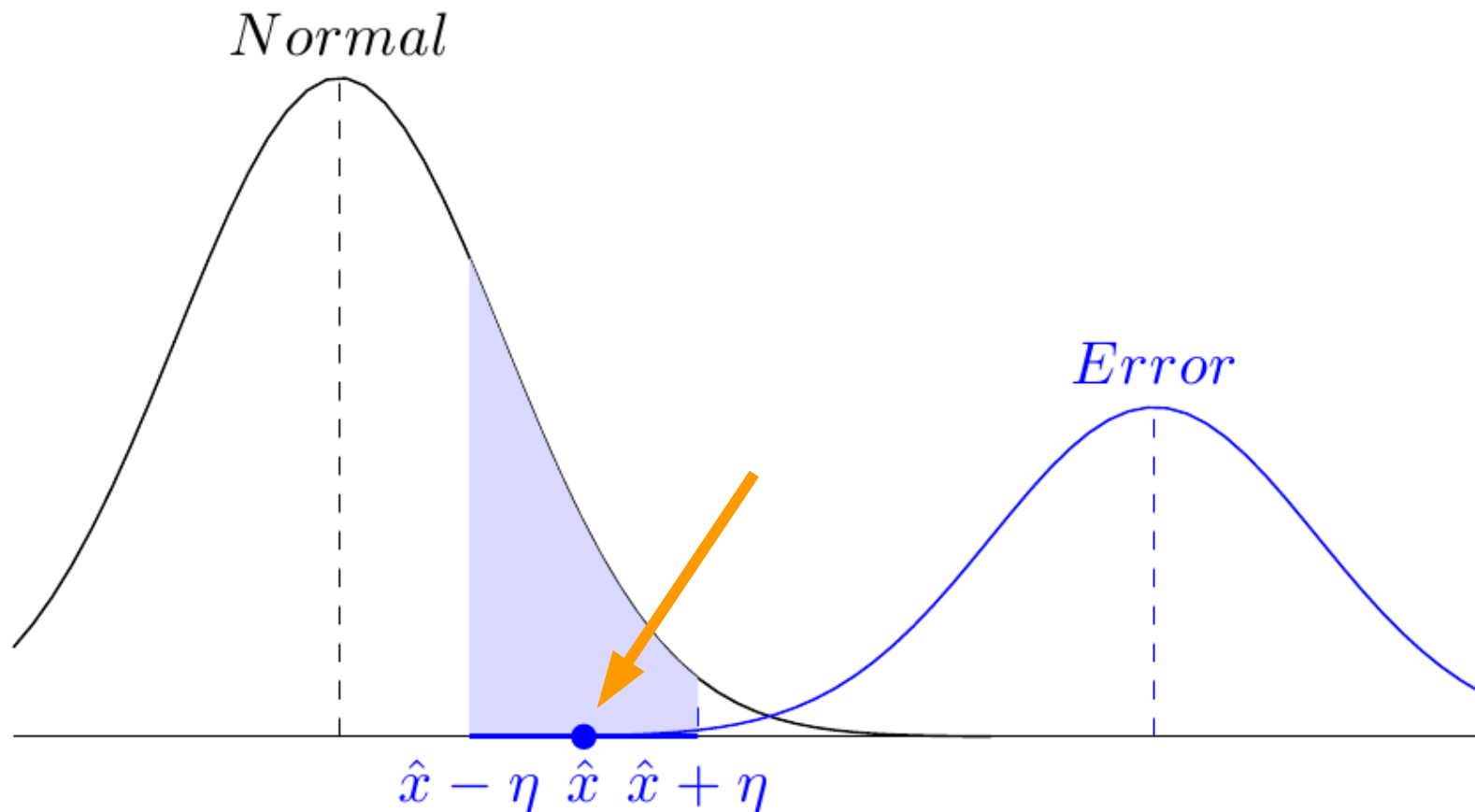
# So spätnou väzbou



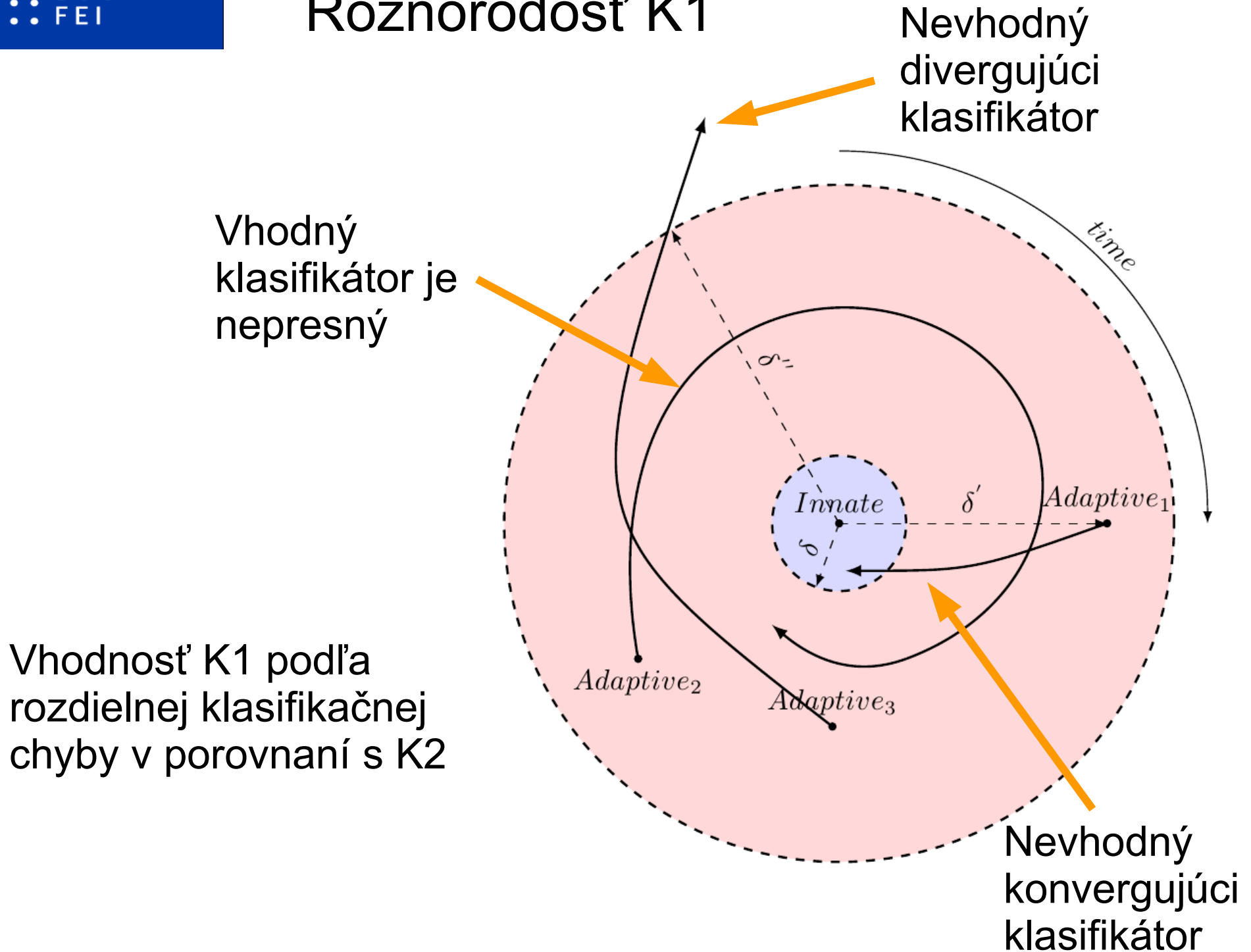


# Priming bias: zaujatost' pri učení

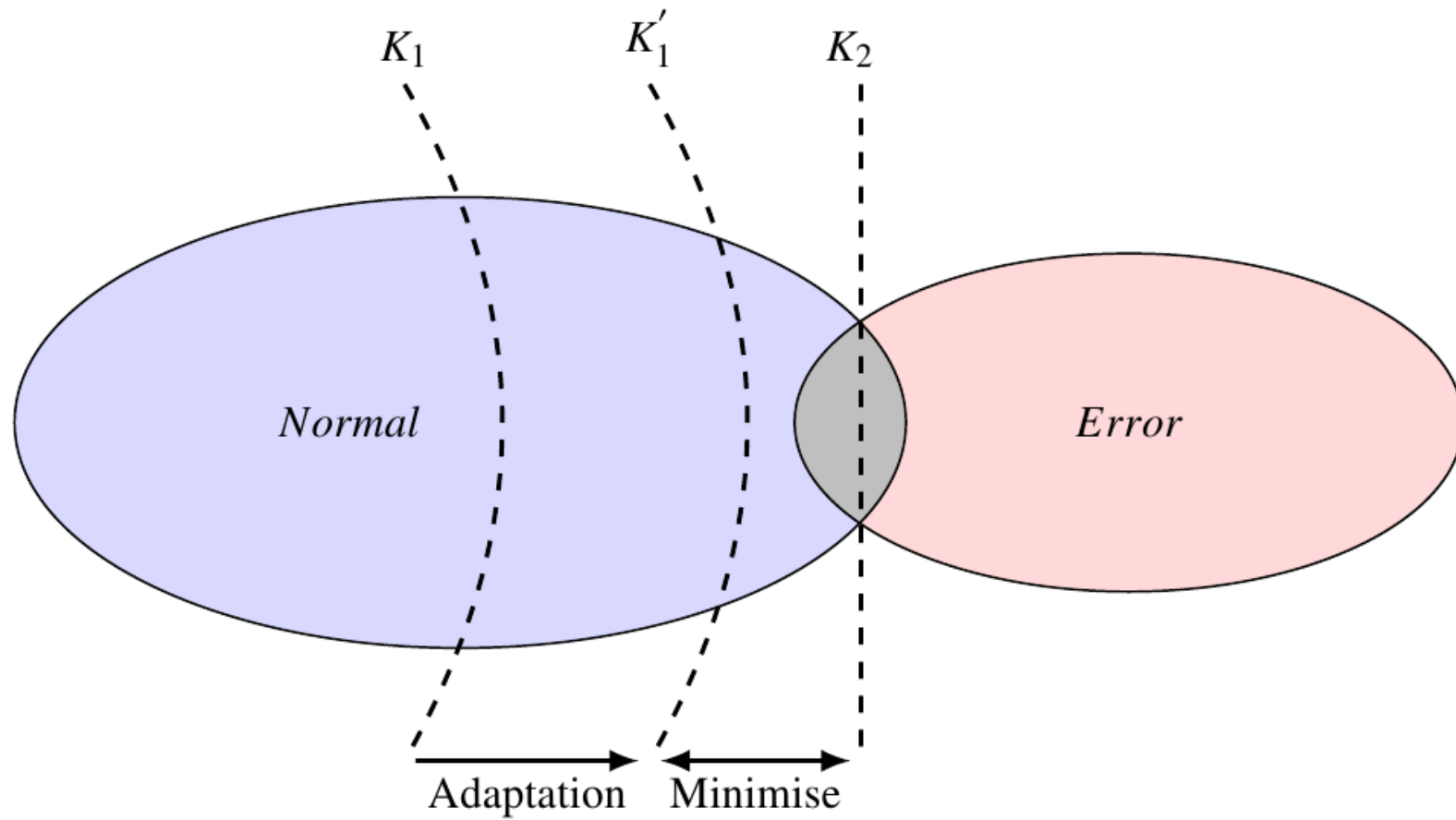
Ak K2 nesprávne deteguje objekt, potom je možné, že sa túto nesprávnu detekciu naučí aj K1

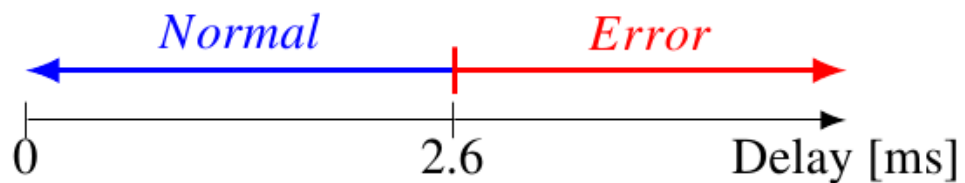


# Rôznorodosť K1

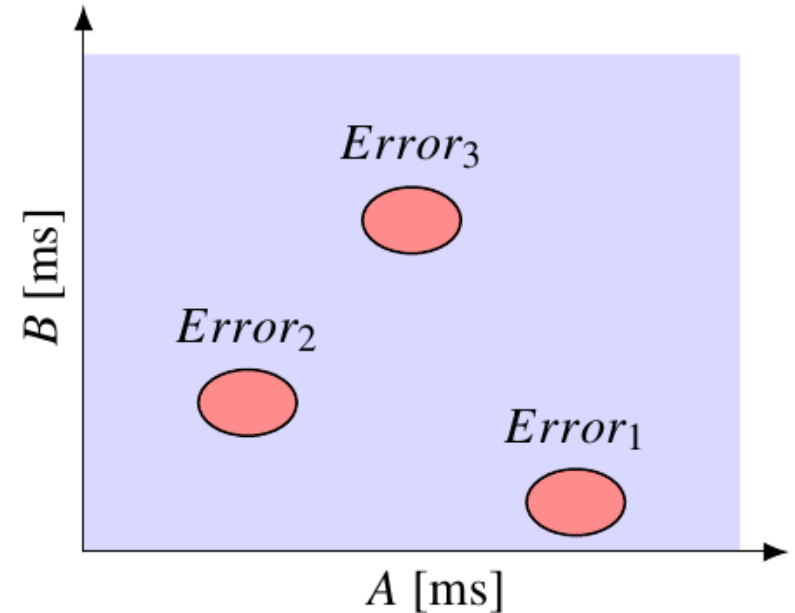


# Adaptivita



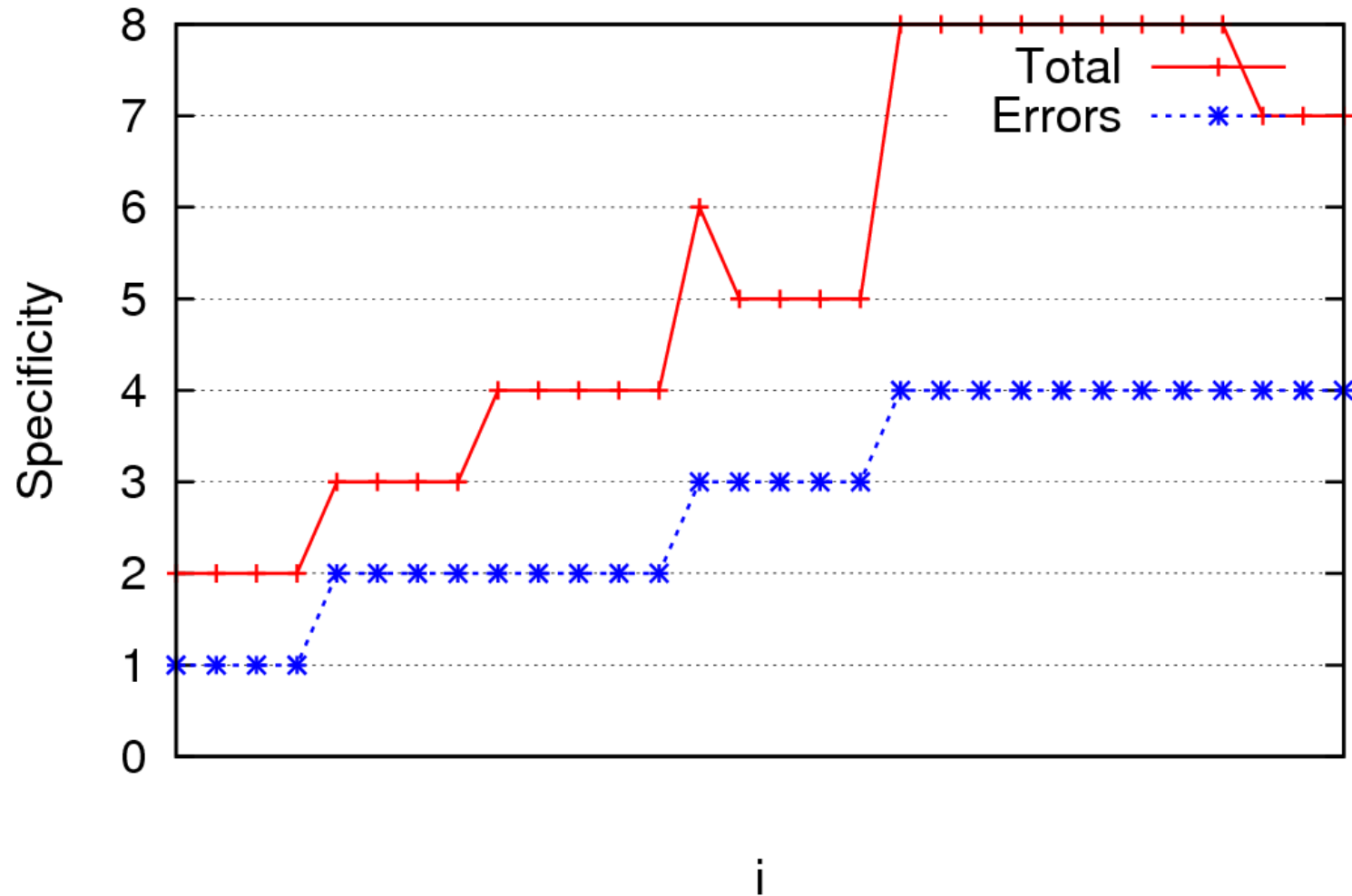


**K2:** jediná  
používateľom  
stanovená prahová  
hodnota



**K1:** naučené  
rozoznávanie 3 druhov  
chýb

## Detekcia špecifických chýb: experiment

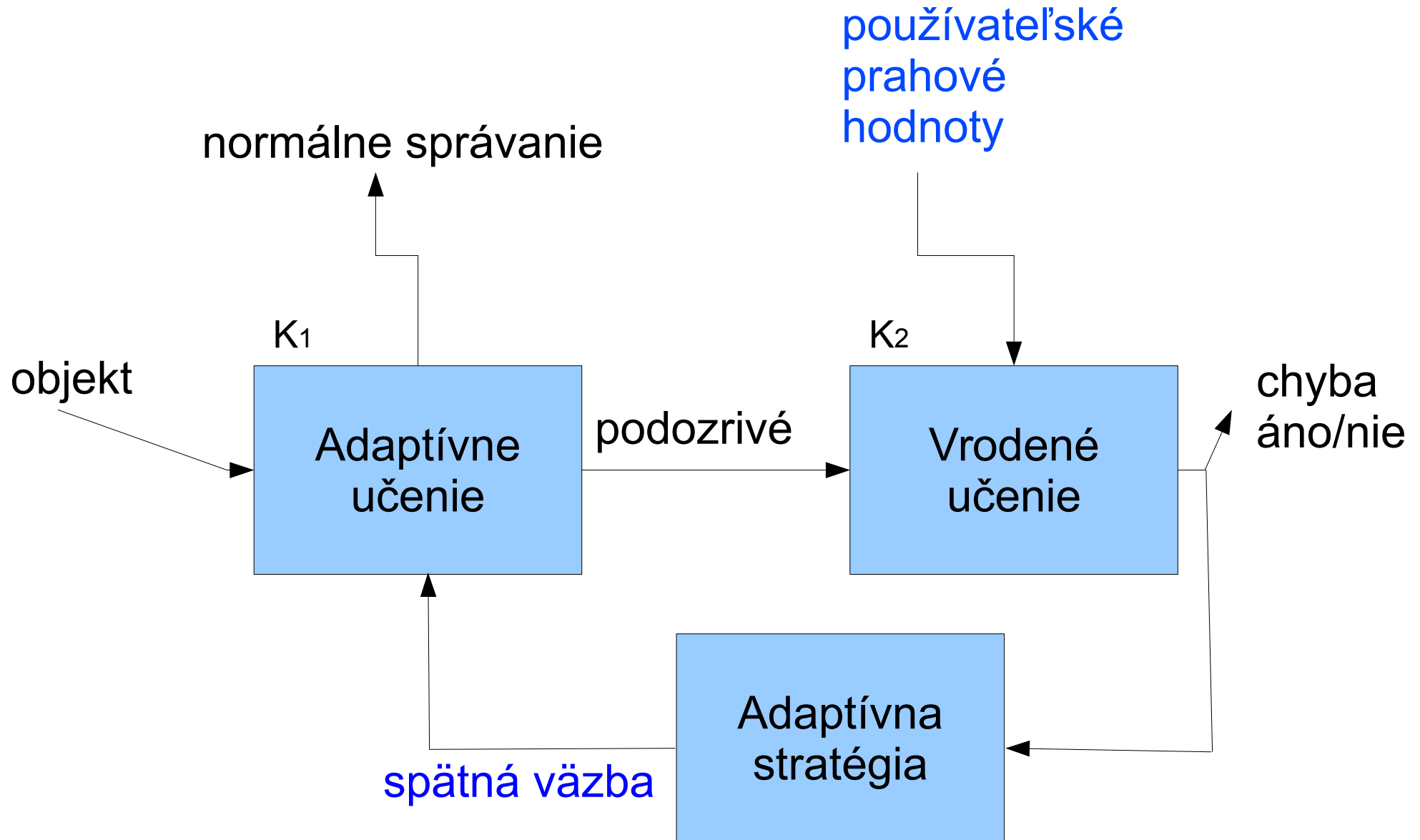


# Vakcinácia: Jenner, 1796



Podanie očkovacej látky (vakcíny) do organizmu, ktorý si následne vytvorí ochranné protilátky proti antigénom obsiahnutým vo vakcíne

## Vakcinácia: off-line výpočet K1



Perrig, A. and Canetti, R. and Tygar, JD and Song, D. The TESLA Broadcast Authentication Protocol, RSA CryptoBytes, 2002.

Hu, Y.C., Perrig, A. and Johnson, D.B. Ariadne: A secure on-demand routing protocol for ad hoc networks. Wireless networks, 11(1-2), pp.21-38, 2005.

Rokicki, M. and Drozda, M. Evaluating trade-offs in energy-efficient error detection. International Journal of Communication Systems, Wiley, 2017.