STU FEI

Počítačové siete 2

TESLA, bezpečné smerovanie, detekcia chýb

Martin Drozda

Formulácia problému

Šifrovanie 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)

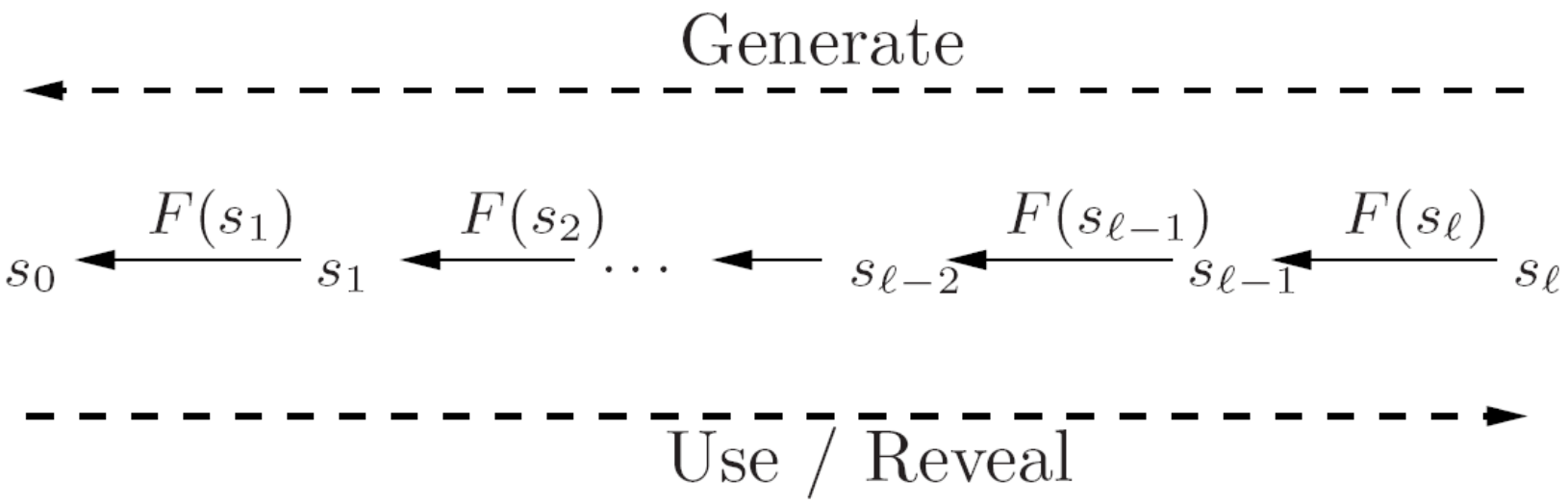
Bezpečný broadcast: 

• 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:

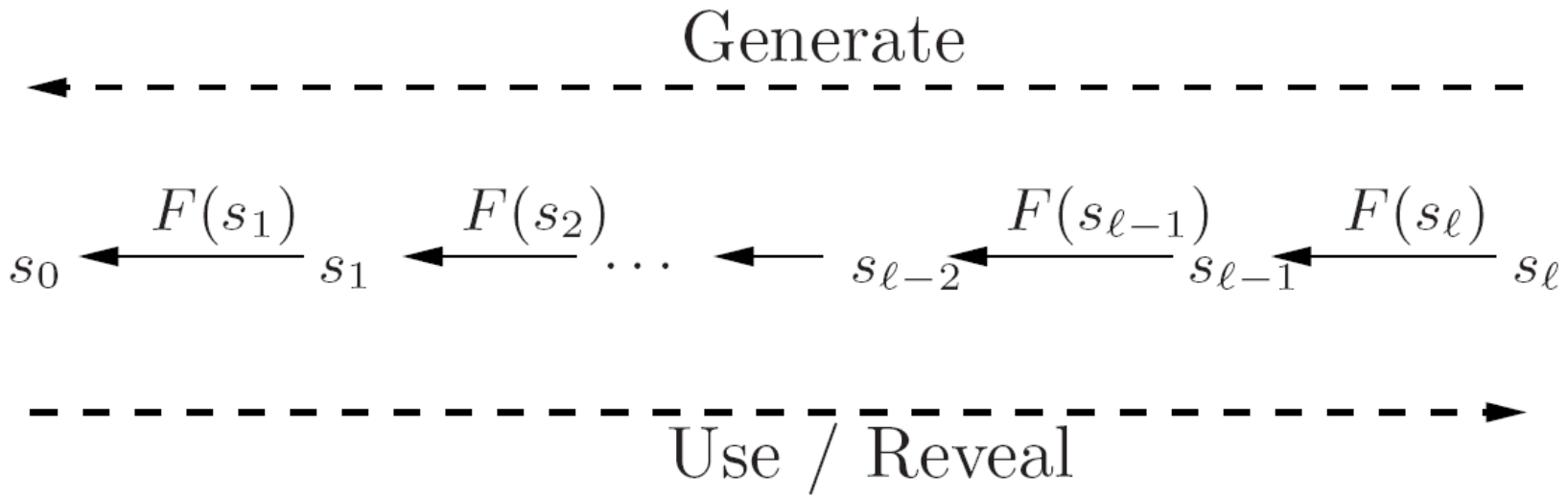
- Na generovanie jednosmernej reťazi hašov použijeme jednosmernú hašovaciu funkciu, napr. gen. náhodných čísel
- Hašovacia funkcia je použitá L-krát
- Kľúče s_i sú použité pre autentifikáciu správ (MAC = Message authetification code)



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

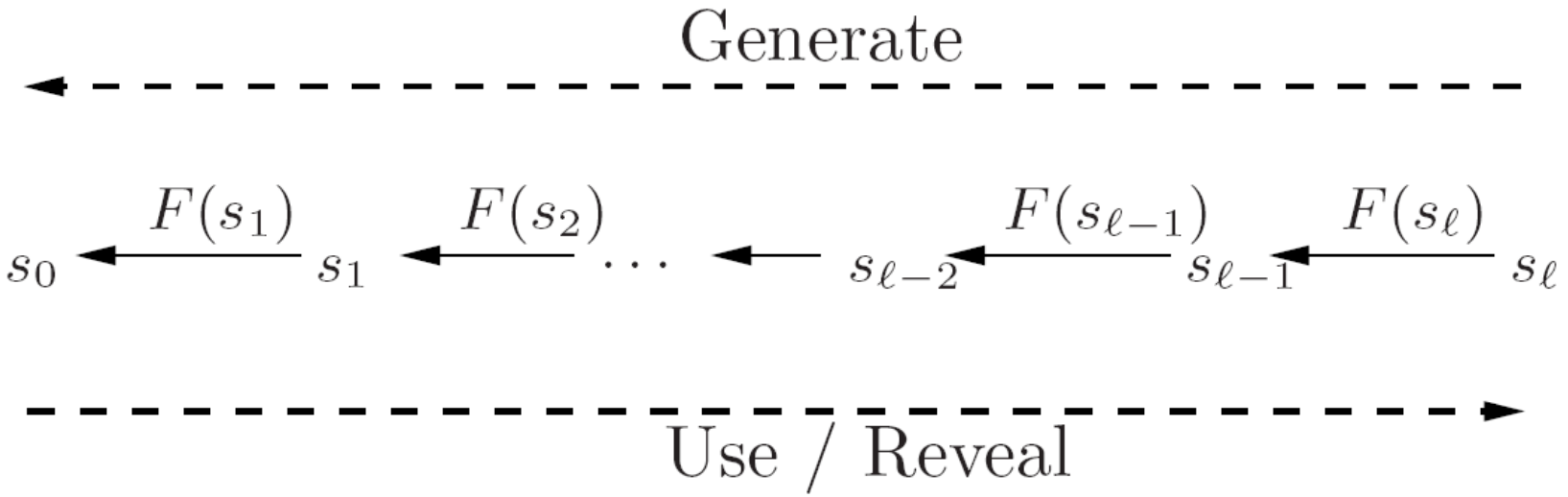
Timed efficient stream loss-tolerant authentication (TESLA)

- 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)



Približná synchronizácia času

Synchronizácia odosielateľa S a prijímateľa R

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

Horné ohraničenie času odosieľatela: $t - t_R + t_S = RTT + t_S$

Nonce je náhodný bit-string s dĺžkou h

t = čas teraz; t_S = čas odosielateľa; t_R = čas prijímateľa
RTT = round trip time

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

RBS (Reference-Broadcast Synchronization)

ARIADNE

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

ARIADNE: RREQ/RREP formát

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 RREQ/RREP

ARIADNE

• Cieľový uzol overí, že hašovacia reťaz je rovná:

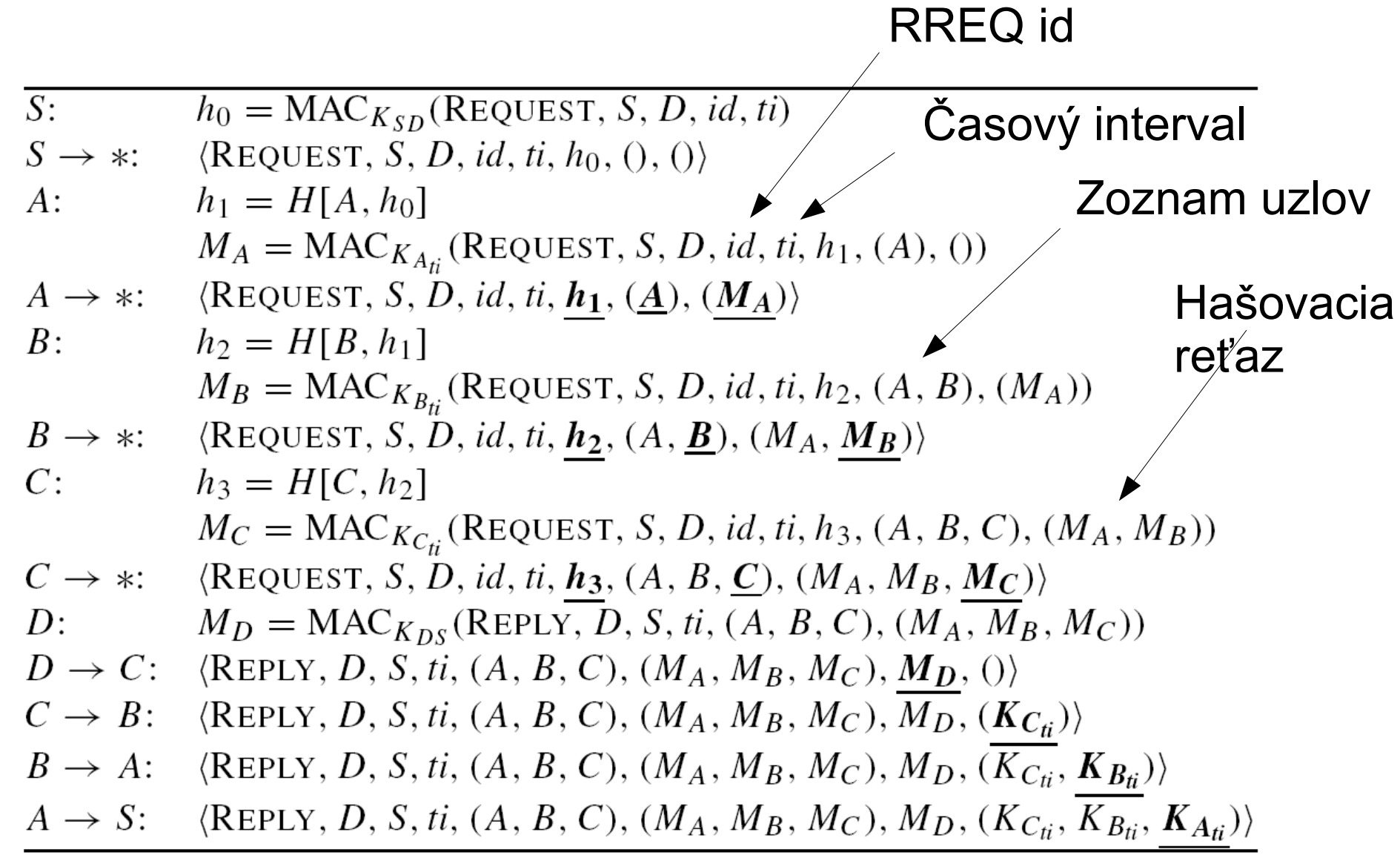
$H[\eta_n, H[\eta_{n-1}, H[..., H[\eta_1, MAC_{KSD}(\text{initiator, target, id, time interval})]\ldots]]]$

η_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

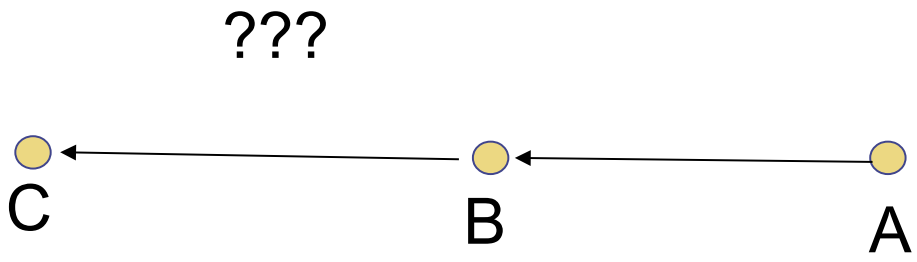


S:	$h_0 = \mathrm{MAC}_{K_{SD}}(\textsc{Request}, S, D, id, ti)$
$S \rightarrow *$:	$\langle \textsc{Request}, S, D, id, ti, h_0, (), () \rangle$
A:	$h_1 = H[A, h_0]$
	$M_A = \mathrm{MAC}_{K_{A_{ti}}}(\textsc{Request}, S, D, id, ti, h_1, (A), ())$
$A \rightarrow *$:	$\langle \textsc{Request}, S, D, id, ti, \underline{\boldsymbol{h_1}}, (\underline{\boldsymbol{A}}), (\underline{\boldsymbol{M_A}}) \rangle$
B:	$h_2 = H[B, h_1]$
	$M_B = \mathrm{MAC}_{K_{B_{ti}}}(\textsc{Request}, S, D, id, ti, h_2, (A, B), (M_A))$
$B \rightarrow *$:	$\langle \textsc{Request}, S, D, id, ti, \underline{\boldsymbol{h_2}}, (A, \underline{\boldsymbol{B}}), (M_A, \underline{\boldsymbol{M_B}}) \rangle$
C:	$h_3 = H[C, h_2]$
	$M_C = \mathrm{MAC}_{K_{C_{ti}}}(\textsc{Request}, S, D, id, ti, h_3, (A, B, C), (M_A, M_B))$
$C \rightarrow *$:	$\langle \textsc{Request}, S, D, id, ti, \underline{\boldsymbol{h_3}}, (A, B, \underline{\boldsymbol{C}}), (M_A, M_B, \underline{\boldsymbol{M_C}}) \rangle$
D:	$M_D = \mathrm{MAC}_{K_{DS}}(\textsc{Reply}, D, S, ti, (A, B, C), (M_A, M_B, M_C))$
$D \rightarrow C$:	$\langle \textsc{Reply}, D, S, ti, (A, B, C), (M_A, M_B, M_C), \underline{\boldsymbol{M_D}}, () \rangle$
$C \rightarrow B$:	$\langle \textsc{Reply}, D, S, ti, (A, B, C), (M_A, M_B, M_C), M_D, (\underline{\boldsymbol{K_{C_{ti}}}}) \rangle$
$B \rightarrow A$:	$\langle \textsc{Reply}, D, S, ti, (A, B, C), (M_A, M_B, M_C), M_D, (K_{C_{ti}}, \underline{\boldsymbol{K_{B_{ti}}}}) \rangle$
$A \rightarrow S$:	$\langle \textsc{Reply}, D, S, ti, (A, B, C), (M_A, M_B, M_C), M_D, (K_{C_{ti}}, K_{B_{ti}}, \underline{\boldsymbol{K_{A_{ti}}}}) \rangle$

K_{SD} = symetrický kľúč; K_{Ati} = kľúč uzla A zverejnený v čase t_i;
H = jednosmerná hašovacia funkcia

Watchdog

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



Detekcia chýb v distribuovanom systéme

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

Challenge #1

Klasifikácia s

a) vysokým počtom falošných poplachov (simple)

b) nízkym počtom falošných poplachov (complex)

Challenge #2

Klasifikácia, ktorá je

a) energeticky neúsporná (simple)

b) energeticky úsporná (complex)

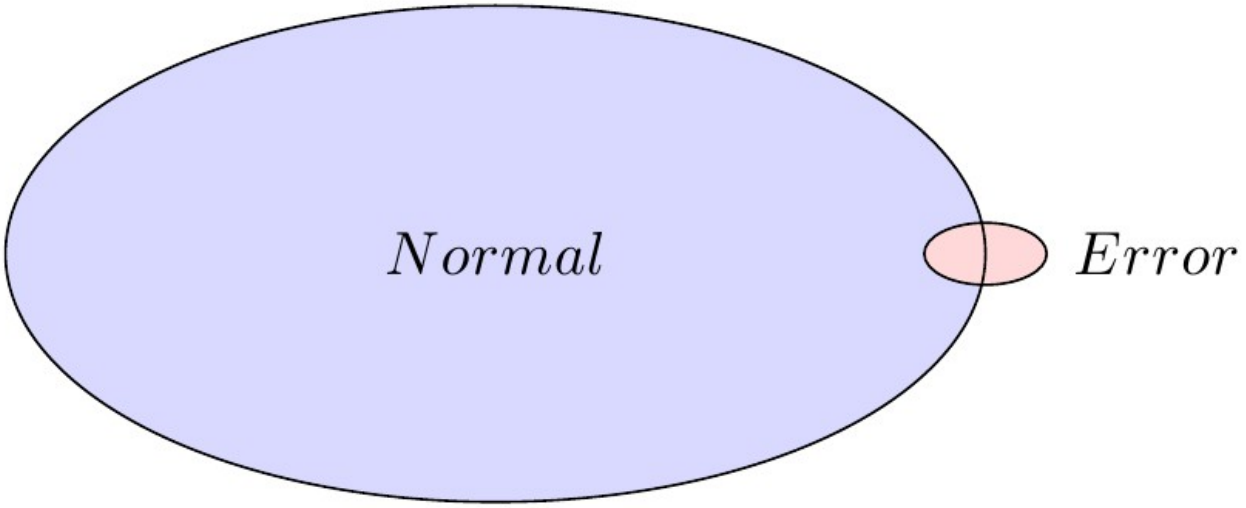
Zložitosť riešenia

simple + simple = maybe simple

complex + complex = complex

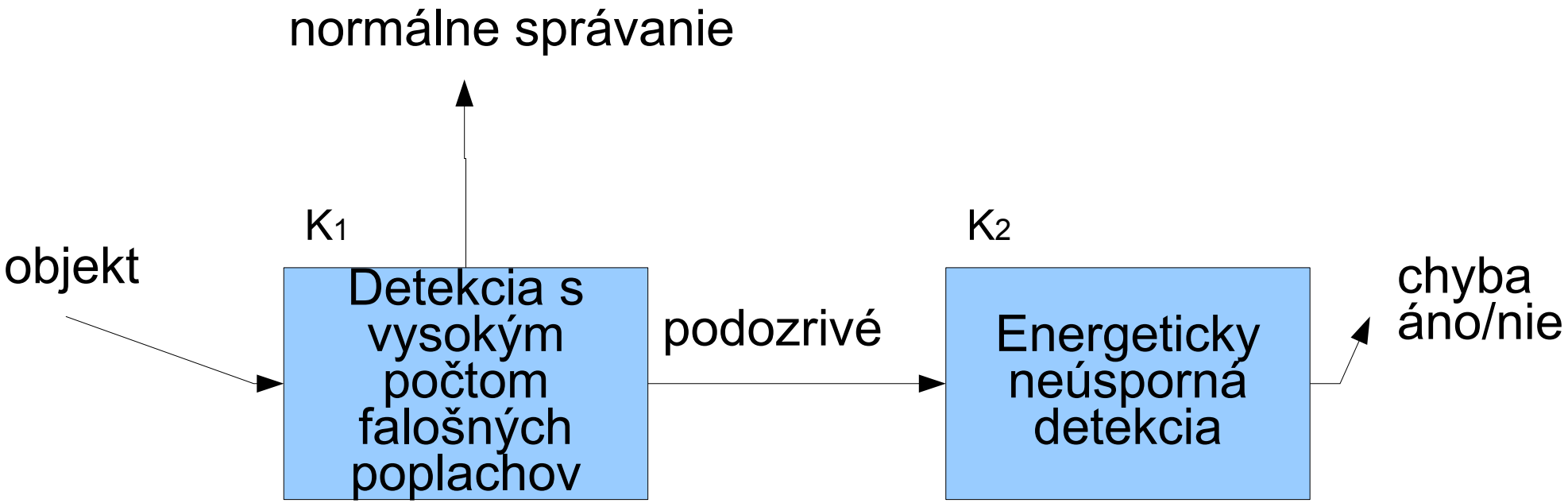
simple + complex = complex

Normálne správanie vs chyby



Normálne správanie je dominantné v správne navrhnutých systémoch

Architektúra: simple + simple



Energeticky úsporná detekcia chýb

Dve možnosti:

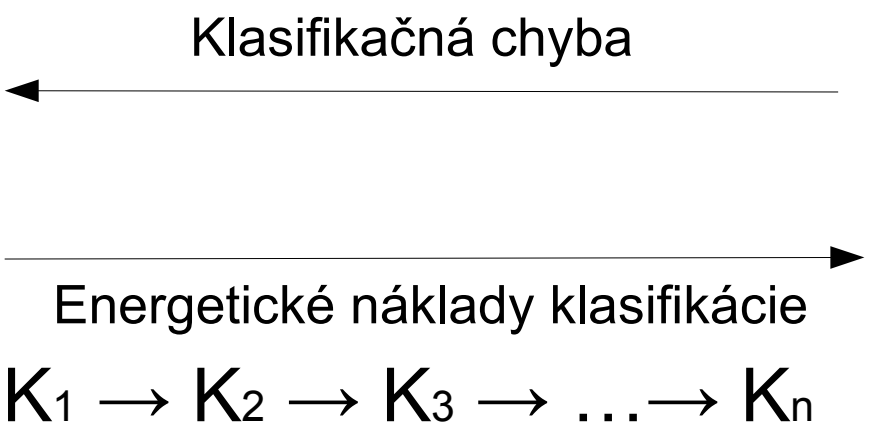
- Vývoj detekčného systému, ktorý je energeticky úsporný

- 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)



$K_1 \rightarrow K_2 \rightarrow K_3 \rightarrow \ldots \rightarrow K_n$

Watchdog je neúsporný?

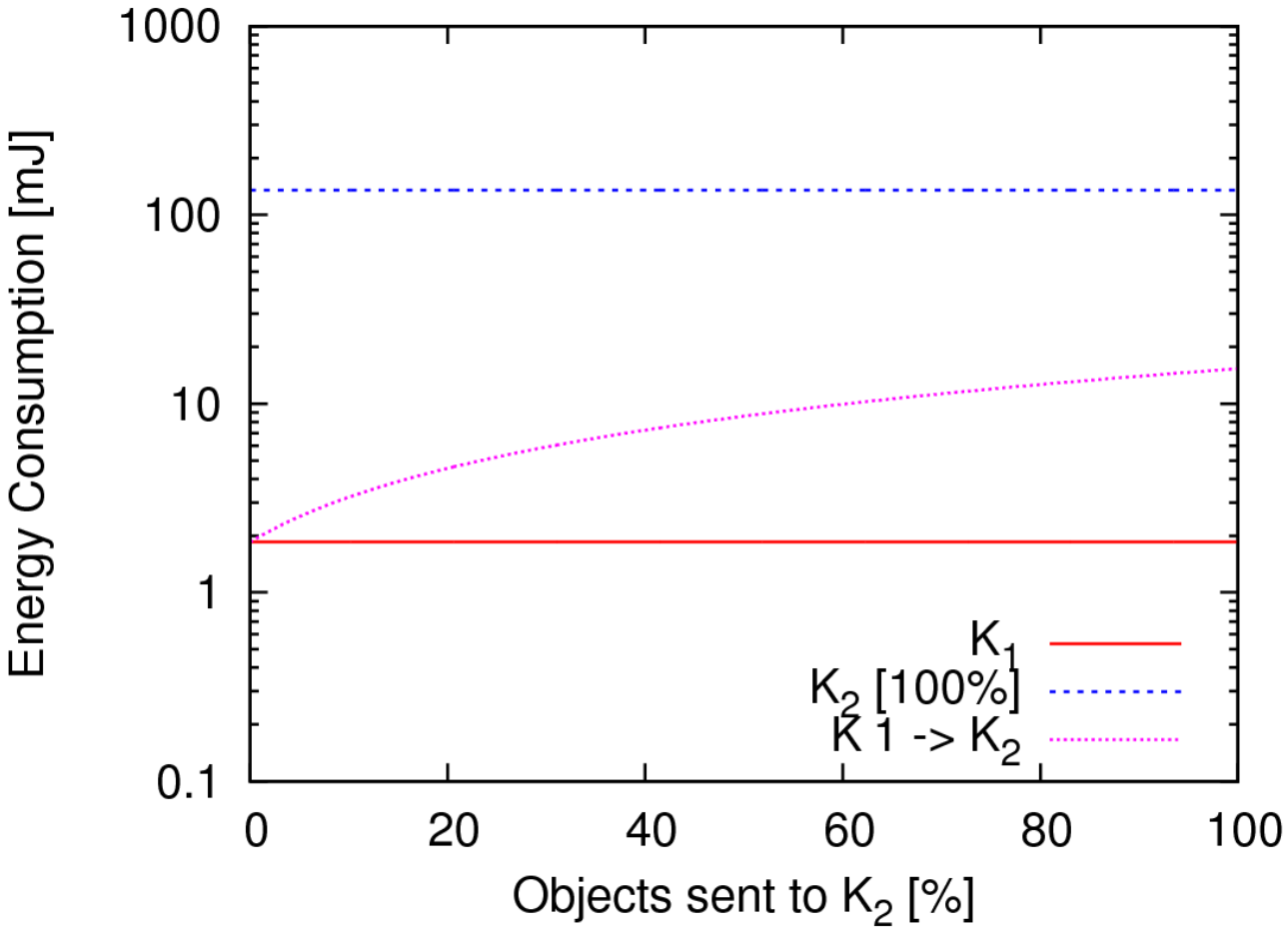
Watchdog je energeticky neúsporný

Watchdog = ACK zo vzdialenosti 2 (od suseda suseda)

Kumulatívne ACK-2 je úsporné:

- ACK pre niekoľko paketov naraz

K1, K2: experiment

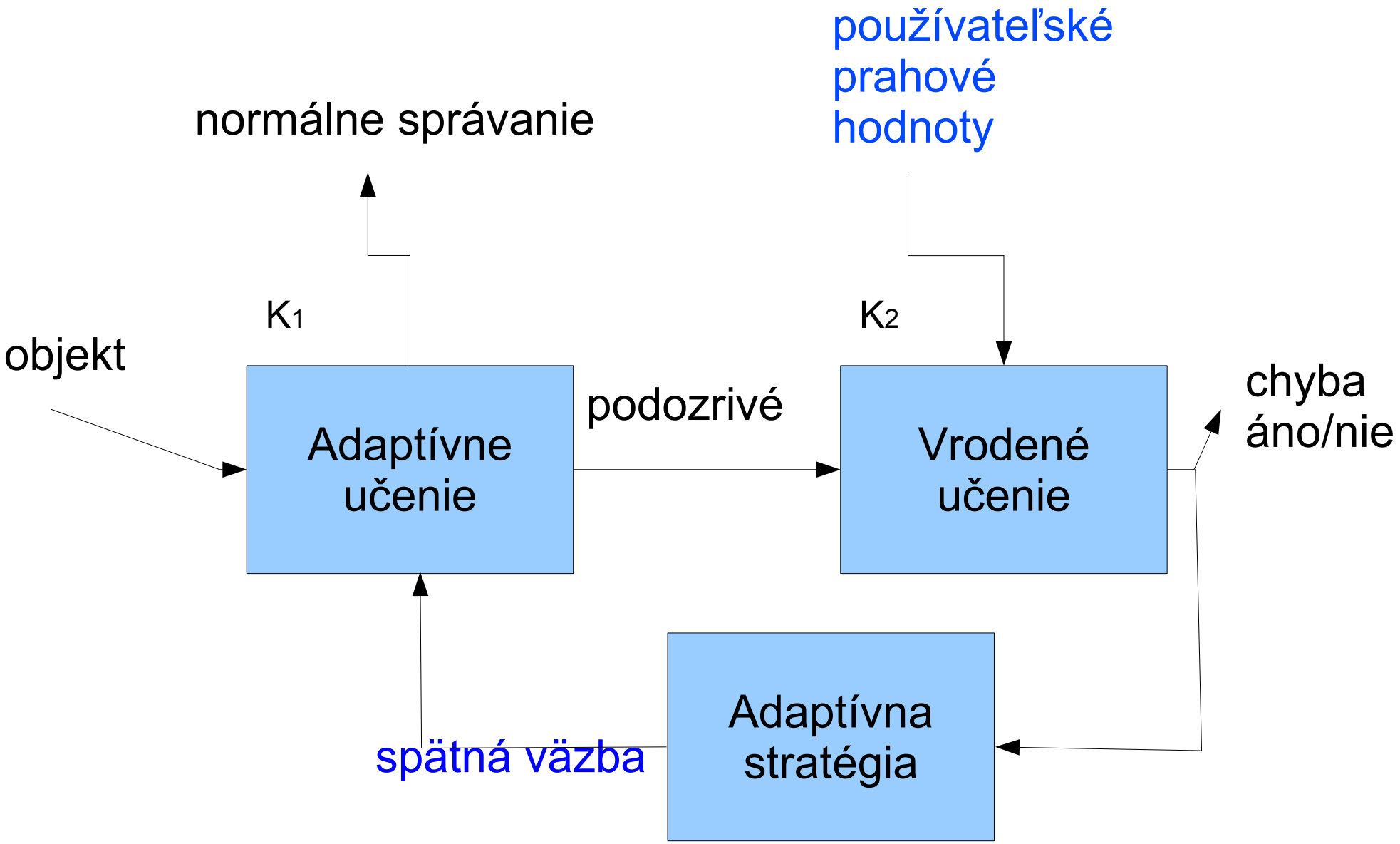


Falošný poplach?

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

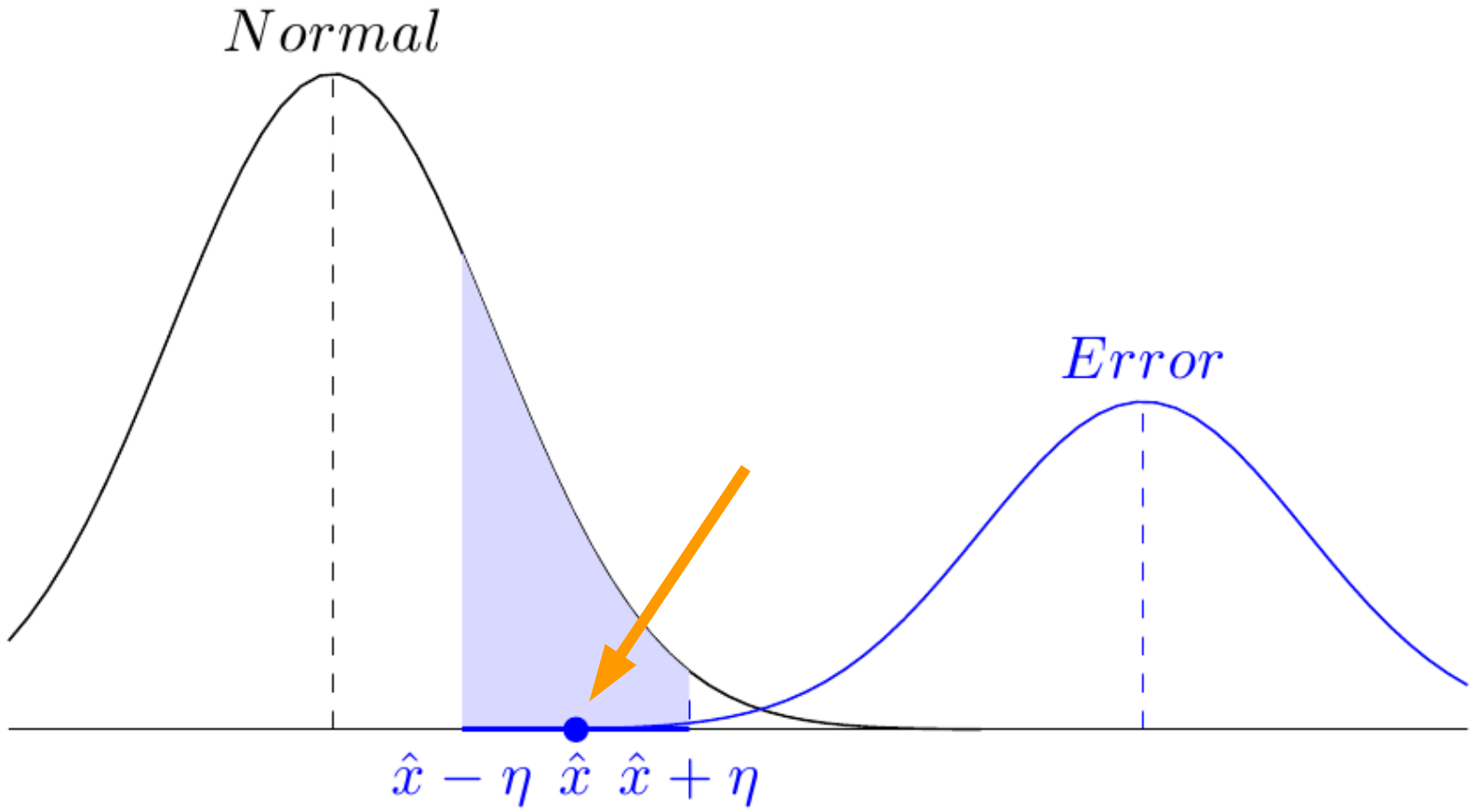
- Potvrdené experimentálnymi výsledkami
- Objekty, ktoré K2 nevie správne klasifikovať sú správne klasifikované K1

So spätnou väzbou



Priming bias: zaujatosť pri učení

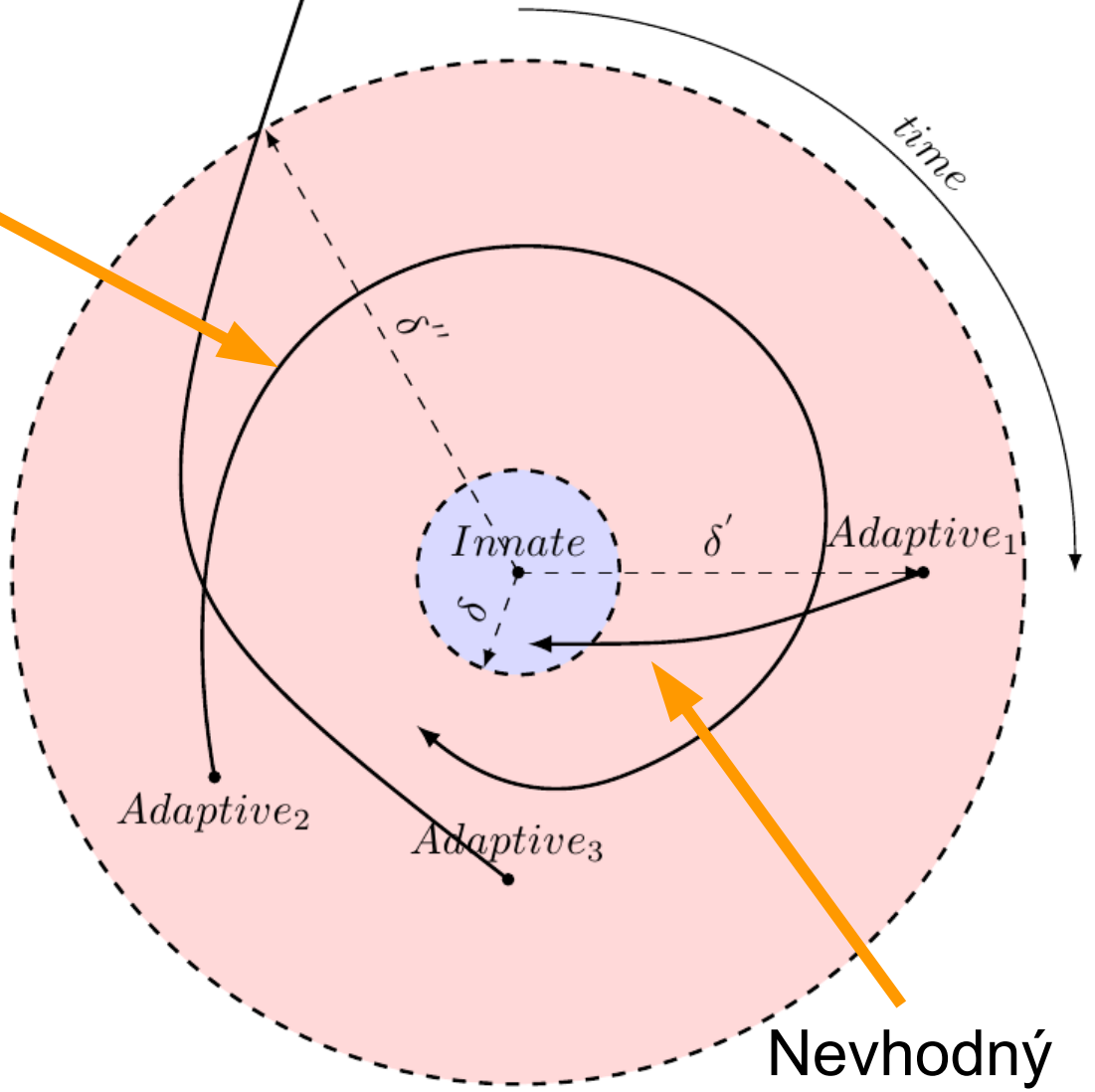
Ak K2 nesprávne deteguje objekt, potom je možné, že sa túto nesprávnu detekciu naučí aj K1



Rôznorodosť K1

Nevhodný divergujúci klasifikátor

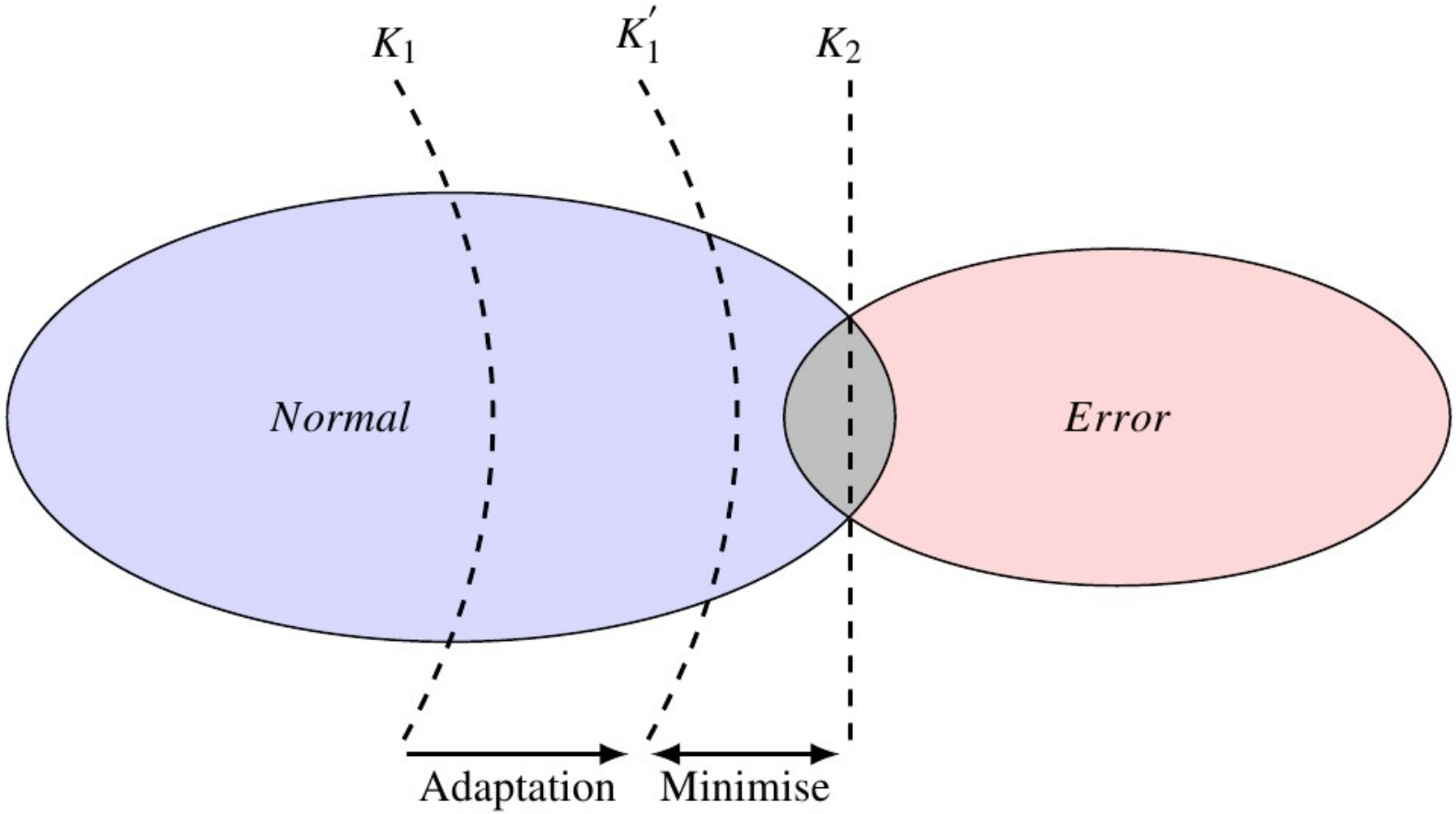
Vhodný klasifikátor je nepresný



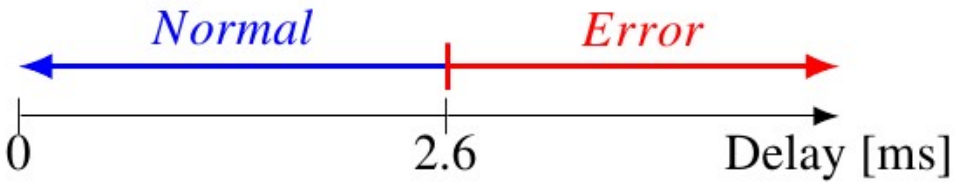
Vhodnosť K1 podľa rozdielnej klasifikačnej chyby v porovnaní s K2

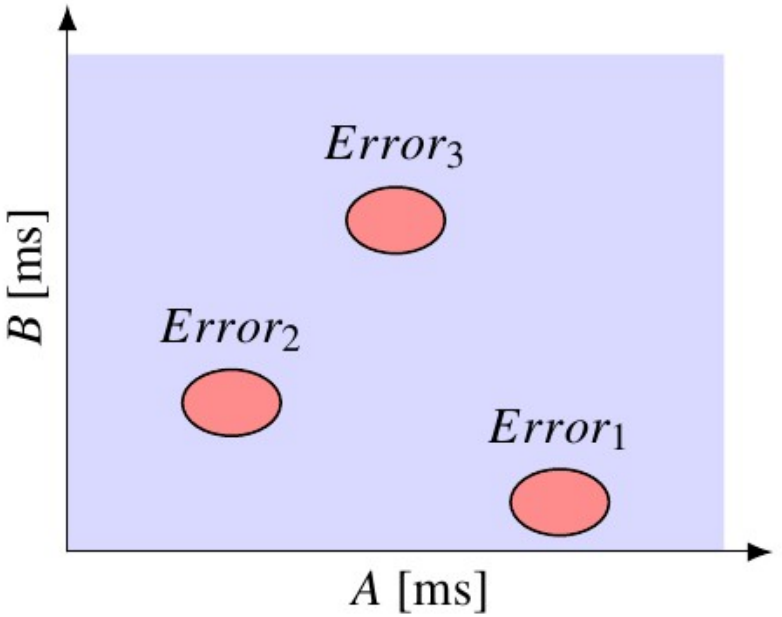
Nevhodný konvergujúci klasifikátor

Adaptivita



Špecifickosť

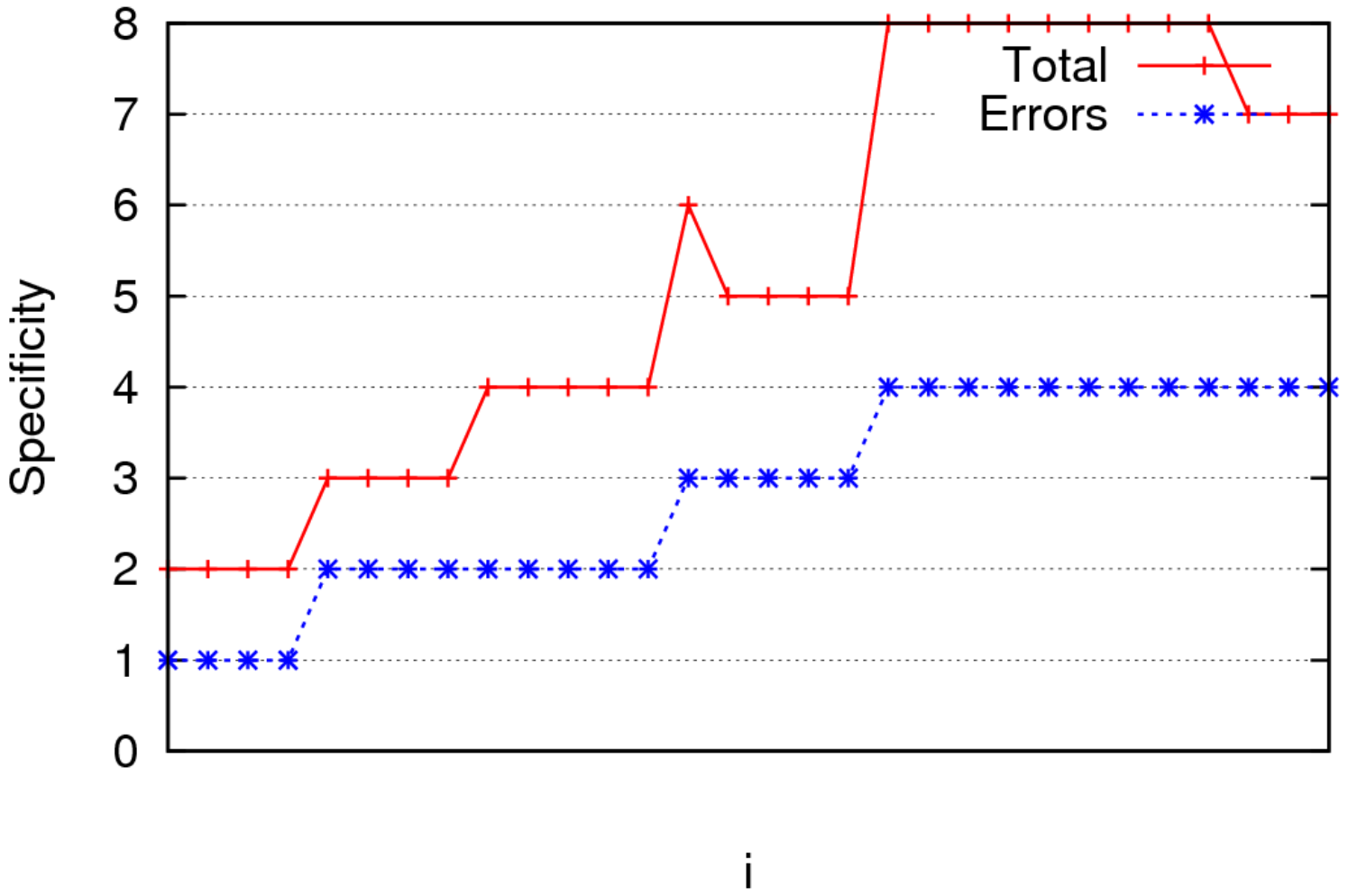




K2: jediná používateľom stanovená prahová hodnota

K1: naučené rozoznávanie 3 druhov chýb

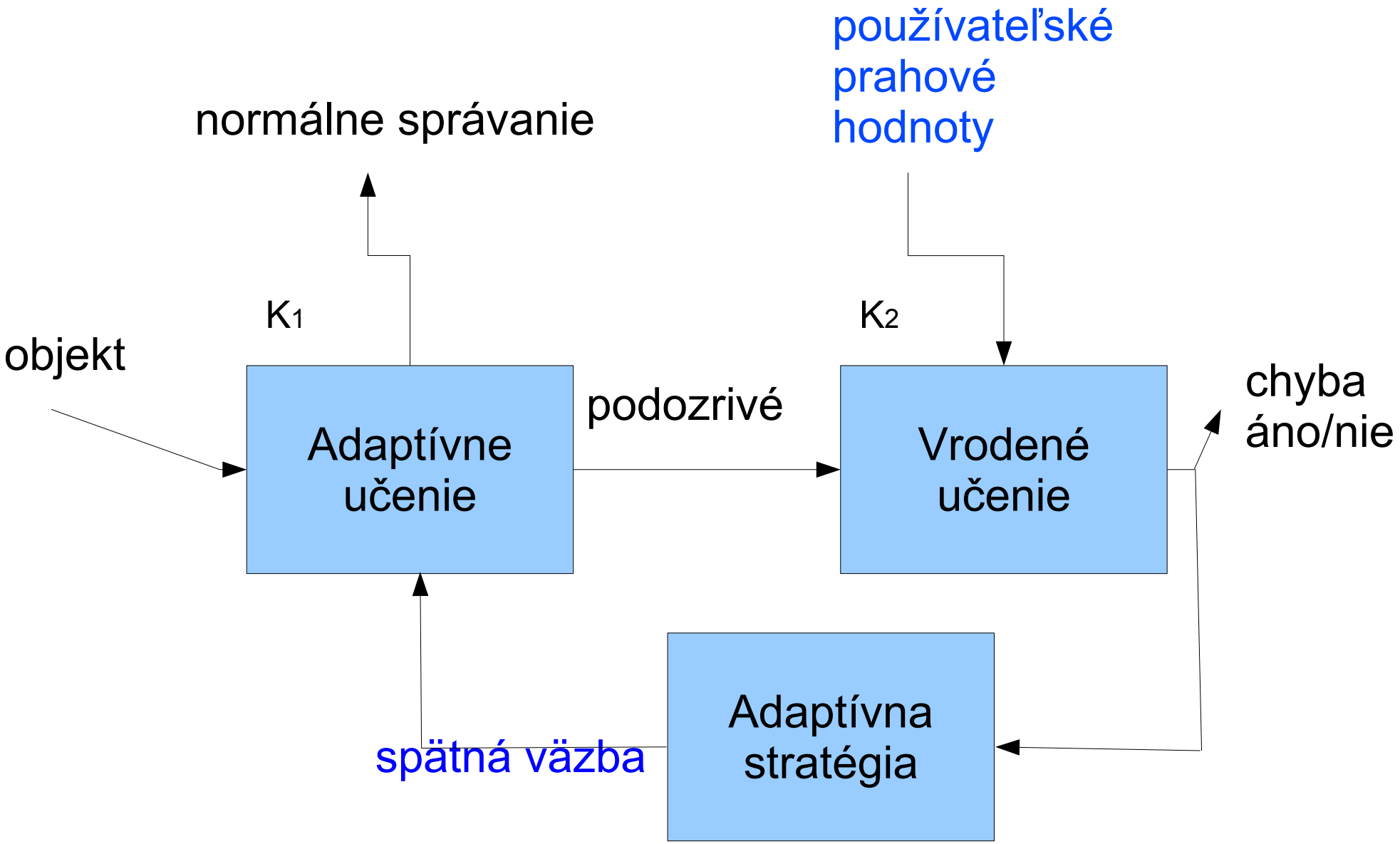
Detekcia špecifických chýb: experiment



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



Literatúra

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.