MODELOVANIE DETEKČNÝCH VLASTNOSTÍ BEZPEČNOSTNÉHO KÓDU V MATLABE

Ing. Ján Rofár, doc. Ing. Franeková Mária, PhD.

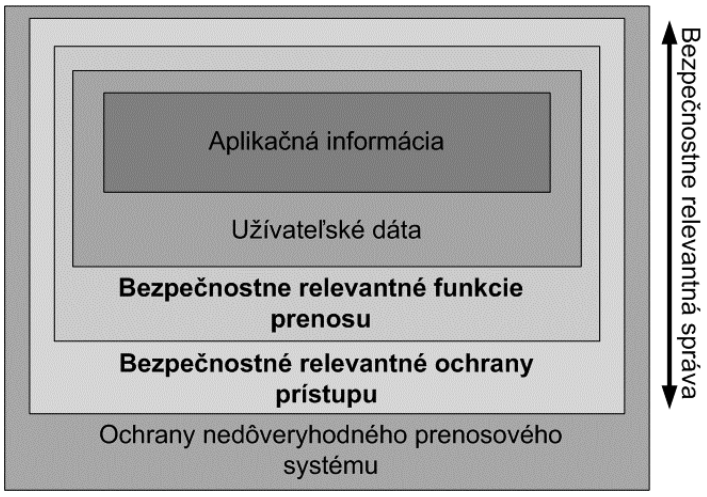
Katedra riadiacich a informačných systémov, Elektrotechnická fakulta, Žilinská univerzita v Žiline, Univerzitná 1, 010 26 Žilina, Slovensko

Príspevok je zameraný na problematiku výberu bezpečnostného kódu pre komunikačný protokol v rámci bezpečnostne relevantných aplikácií (napr. železničné riadiace systémy). Nosná časť je venovaná modelovaniu detekčných vlastností CRC-r kódu, pre rôzne dĺžky telegramov, generovanú chybovú štruktúru v komunikačnom kanáli a určeniu zvyškovej chybovosti zvoleného bezpečnostného kódu pomocou nástroja Matlab a knižnice Communication Blockset.

1 Úvod

Pre rezort železničnej dopravy v súčasnosti existuje podrobne prepracovaná metodika [1], [2], na definíciu bezpečnostných požiadaviek prenosových systémov, ktorú vo väčšej miere preberajú normy aj pre iné rezorty, napr. oblasť priemyselnej automatizácie [3].

Základnou myšlienkou bezpečnostne relevantnej komunikácie je, že bezpečnosť prenosu nesmie byť riešená pomocou prostriedkov nedôveryhodného (komerčne dostupného) prenosového systému. Na zachovanie integrity správ, narušenej v dôsledku šumových pomerov v prenosovom kanáli sa odporúča použiť vhodný bezpečnostný kód SC (Safety Code). Jeho umiestnenie je v modeli prenosu správ (obr. 1) vo vrstve ochrany prenosu.



Obr. 1: Umiestnenie bezpečnostného kódu

V otvorených prenosových systémoch sa často používajú na detekciu bitových alebo zhlukových chybových stavov prenosové kódy. Z pohľadu bezpečnosti bezpečnostne relevantný (BR) proces nesmie dôverovať týmto prenosovým kódom. Na detekciu poškodenia správy sa preto vyžaduje prídavný bezpečnostný kód, riadený BR procesom. V prípade použitia bezpečnostného kódu sa musí preukázať primeranosť schopnosti detekcie všetkých očakávaných typov chýb a hodnoty pravdepodobnosti nedetegovaných chýb. Komunikačný balík *Communication Blockset* má vo svojej knižnici silnú podporu funkčných blokov detekčných aj korekčných kanálových kódov. Podľa odporúčaní pre bezpečnostne relevantnú komunikáciu sa odporúča zamerať len na techniky detekčných kanálových kódov (tzv. ARQ techniky). V prípade výberu bezpečnostného kódu z množiny korekčných kódov (tzv. FEC techniky) je potrebné dekódovací algoritmus modifikovať alebo ukončiť procesom detekcie.

Najpoužívanejším prenosovým a bezpečnostným kódom v komunikačných protokoloch komerčných prenosových systémov a zároveň aj v bezpečnostne relevantnej vrstve je systematický cyklický kód, pracujúci na princípe CRC (Cyclic Redundancy Check). Pre vyjadrenie vlastností cyklických kódov sa používa algebra polynómov.

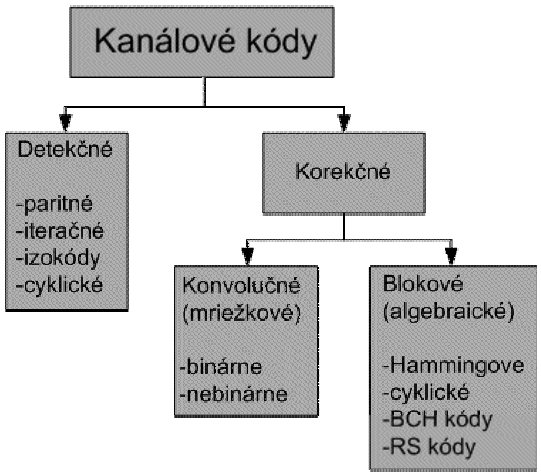
V praxi sa často stretávame s požiadavkou súvisiacou s modelovaním bezpečnostných vlastností komunikačného systému z dôvodu preukázania bezpečnostných vlastností nového produktu. Ide o preukázanie dostatočnej odolnosti komunikačného systému proti útokom na prenášané správy, kedy treba vypočítať pravdepodobnosť resp. intenzitu nedetegovateľného narušenia prenášanej správy na základe teoretických úvah (odhad bitovej chybovosti komunikačného kanála, výpočet

zvyškovej chybovosti použitých kódov). V tomto prípade možno použiť vhodné kombinácie modelovacích nástrojov, medzi ktoré možno zaradiť aj, *Matlab - Communications blockset* a *Communication toolbox*.

2 Výber bezpečnostného kódu

V súčasnej dobe existujú dve významné skupiny kanálových kódov (blokové a konvolučné). Blokové kódy pridávajú k informačnej časti, pozostávajúcej z *k* symbolov *r* redundantných symbolov čím vznikne kódové slovo dĺžky *n*, a preto sa im hovorí (*n,k*) kódy. Vyznačujú sa tým, že kodér a dekodér je zariadenie bez pamäte, t. j. k výpočtu nového kódového slova nie je potrebné si pamätať informačné symboly z predchádzajúceho kódového slova (kódové slová kódu sú na sebe nezávislé). Dekódovanie u blokových kódov využíva matematické vlastnosti lineárnej algebry a Galoissových konečných polí. Algoritmy sú viac vhodné pre HW realizáciu, z dôvodu rýchlosti dekódovania, aj keď v súčasnosti existujú aj rýchle SW realizácie.

U konvolučných kódov, na rozdiel od blokových, je tvorba kódových slov na sebe závislá a preto sa im hovorí aj kódy s pamäťou. K výpočtu redundancie je potrebné si pamätať určitý počet informačných symbolov, o veľkosti tzv. kódovacieho záberu (*contraint lenght*) dĺžky *m*, preto ich označujeme (*n,k,m*) kódy. Kódovací pomer u oboch typov kódov sa označuje ako pomer vstupných a výstupných symbolov *k/n.* Dekódovanie konvolučných kódov je vo väčšine aplikácií založené na maximálnom pravdepodobnostnom dekódovaní podľa Viterbiho algoritmu. Základné členenie kanálových kódov je znázornené na obr. 2.



Obr. 2 : Základné členenie kanálových kódov

Najviac používaným detekčným kódom v bezpečnostne kritických aplikáciách je blokový systematický cyklický kód, ktorý pracuje na princípe CRC-r.

3 Konštrukcia cyklických kódov CRC

Konštrukcia a realizácia lineárneho blokového kódu sa stáva pre dlhšie kódové slová nepraktická. Tu nachádza široké uplatnenie podmnožina lineárných blokových kódov – cyklické kódy, u ktorých okrem podmienky linearity sa požaduje, aby cyklickým posunom kódového slova bolo opäť kódové slovo. CRC je jedným z najpoužívanejších spôsobov zabezpečenia správ proti rušeniu vplyvom šumu, ktoré vniká v prenosovom kanále. Vlastnosť lineárity umožňuje jednoduchú konštrukciu kodéra a dekodéra založenú na posuvných registroch so spätnou väzbou. Pre opis cyklických kódov sa používa algebra polynómov [4]. Kódové slovo C je reprezentované polynómom *C(x)* stupňa *(n-1)*, ktorého koeficienty c_i sú symboly kódového slova :

$$C(x)=c_1x^{n-1}+c_2x^{n-2}+\ldots+c_{n-1}x+c_nx^0 \qquad (1)$$

Mocniny premennej *x* vyjadrujú poradie symbolov v kódovom slove a preto súčin *x*c(x)* znamená posunutie všetkých symbolov o jedno miesto.

U cyklických kódov požadujeme, aby cyklickým posuvom kódového slova bolo opäť iné kódové slovo a pre polynómy cyklických kódov musí platiť $x^rC_i(x)=C_j(x)$ (kde *r* je celé kladné číslo). Táto požiadavky je splnená, ak polynóm každého nenulového kódového slova možno rozložiť do súčinu polynómov, z ktorých jeden, označený ako *g(x)*, je spoločný pre všetky nenulové slová je stupňa *r* a má tvar:

$$g(x)=x^r+g_1x^{r-1}+\ldots+g_{r-1}x+1 \qquad (2)$$

Potom $g(x)$ nazývame generujúci polynóm, lebo polynóm ľubovoľného kódového slova z neho vypočítame $C_i(x)=g(x)a_i(x)$, kde $a_i(x)$ sú polynómy stupňa najviac $(k-1)$. Počet rôznych polynómov $a_i(x)$ je teda 2^k, čo je počet všetkých kódových slov. Nie každý polynóm cyklického kódu (n,k). Aby ním bol musí platiť, že generujúci polynóm delí výraz x^n-1 bezo zvyšku:

$$(x^n-1)/g(x)=h(x)=x^k+h_1x^{k-1}+...+h_{k-1}x+1, \quad (3)$$

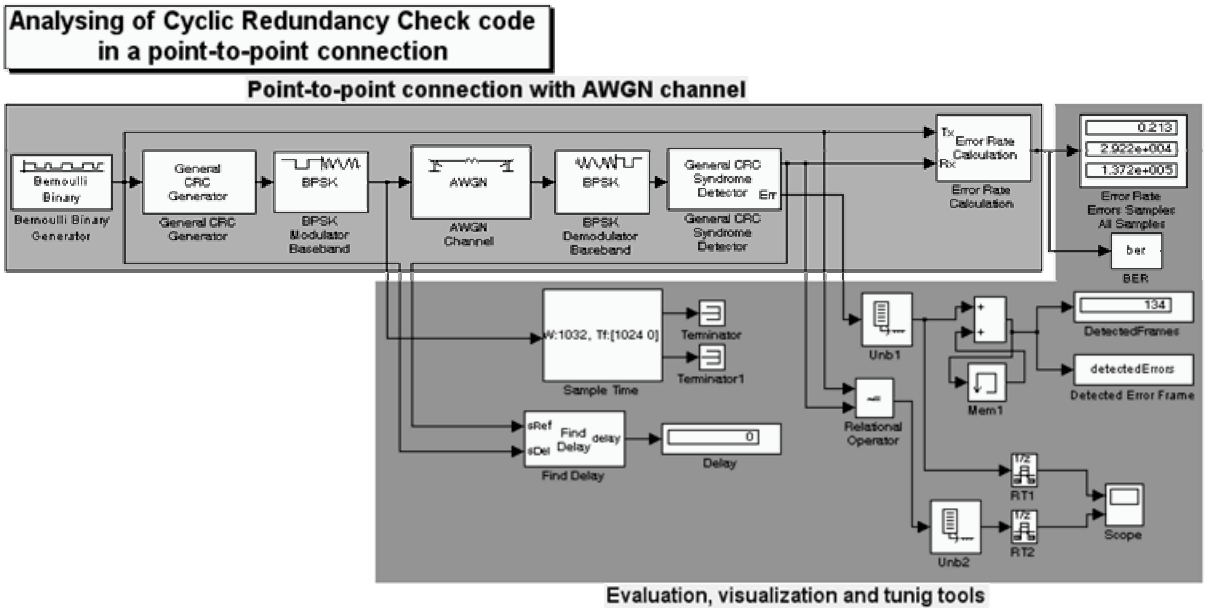
kde $h(x)$ je polynóm stupňa k nazývame ho kontrolný polynóm, pretože jeho súčin s polynómom kódového slova je nulový:

$$h(x)C_i(x)=((x^n-1)/g(x))g(x)a_i(x)=x^na_i(x)-a_i(x)=a_i(x)-a_i(x)=0 \quad (4)$$

Ak pri rozklade polynómu $g(x)$ medzi činiteľmi nie je žiadny polynóm stupňa $(n-k)$, potom cyklický kód s danou kombináciou neexistuje. Naopak môžeme zistiť viac polynómov požadovaného stupňa. Rozklady polynómu x^n-1 pre menšie hodnoty kódového slova a sú tabelované. Binárne koeficienty polynómov rozkladu sú vyjadrené oktávovými číslami. Napr. rozklad polynómu x^7-1 je označený v oktávovej forme $3.13.15$, čo v binárnom tvare znamená $011.001011.001101$ a v tvare polynómov ide o súčin polynómov $(x+1)$, (x^3+x+1) a (x^3+x^2+1). Z toho je zrejmé, že pre dĺžku kódového slova $n=7$ existujú dva ireducibilné polynómy 3.rádu (x^3+x^2+1) a $(x^3+x+1$ [5].

4 Model dvojbodového spojenia na testovanie CRC kódu

Model na overenie detekčných vlastností CRC kódu bol vytvorený pomocou knižníc *Communication blockset*, *Simulink*, *Signal processing blockset* [6]. Z dôvodu jednoduchšej manipulácie a spracovania výstupných údajov bol naprogramovaný aj pomocný program, ktorý je uložený v *m-file* súbore. Na overenie detekčných vlastností cyklického kódu CRC je použité jednoduché dvojbodové zapojenie zdroj-prijímač (obr. 3).



Obr. 3: Model dvojbodového zapojenia na testovanie vlastností prenosového kódu

Ako zdroj bol použitý blok bernoulliho generátor binomických čísel (*Bernoulli binary generator*). Zdroj umožňuje generovať binomické čísla dátového typu *double*, ktorý je podporovaný pri práci s komunikačnými knižnicami *Communication toolbox* a *Communication blockset*. Z tohto dôvodu nie je nutná konverzia dátového typu. Pri testovaní vlastností prenosového kódu sú potrebné dátové typy ako *boolean* a *double*. Pomocou *bernoulliho generátora binomických čísel* je možné výstupný signál odosielať ako postupnosti jednotlivých vzoriek, bitov (*sample-based signal*), alebo ako postupnosti rámcov (*frame-based signal*). Jeden rámec je tvorený niekoľkých vzorkami, ktoré sú

vysielané cyklicky ako jeden celok. Pomocou tejto vlastnosti generátora je možné simulovať tvorbu náhodných správ, ktoré sa následne zakódujú v bloku určenom pre tvorbu prenosového kódu.

Blok tvorby prenosového kódu je pre tento model CRC generátor. Ten spolu s CRC detektorom syndrómu je najdôležitejšou, testovanou časťou celého zapojenia. CRC generátor pridáva na základe istých pravidiel ku každej vysielanej správe extra bity slúžiace na zabezpečenie danej správy. Redundantné bity sa nazývajú syndróm (*checksum*). Po prijatí správy na strane prijímača, generátor CRC kódu pomocou tých istých pravidiel vypočíta zvyšok z daného reťazca. Ak sa tento výsledok nerovná 0, počas prenosu nastala chyba.

V knižnici *Communication blockset* sa nachádzajú štyri bloky určené pre prácu s CRC kódom.

1. CRC generátor (*general CRC generator*).
2. CRC detektor syndrómu (*general CRC syndrom detector*).
3. CRC-N generátor (*CRC-N generator*).
4. CRC-N detektor syndrómu (*CRC-N syndrom detector*.

V prvých dvoch sú generačné polynómy (ich tvar aj dĺžka) určené užívateľom. V druhých dvoch si užívateľ môže vybrať z ponúkaných možnosti vopred definovaných generačných polynómov, kde *N* je stupeň rádu a nadobúda hodnoty rovne 4, 8, 16, 24 alebo 32 (tab.1).

TAB.1 PREDDEFINOVANÉ GENERAČNÉ POLYNÓMY V CRC-N BLOKOCH

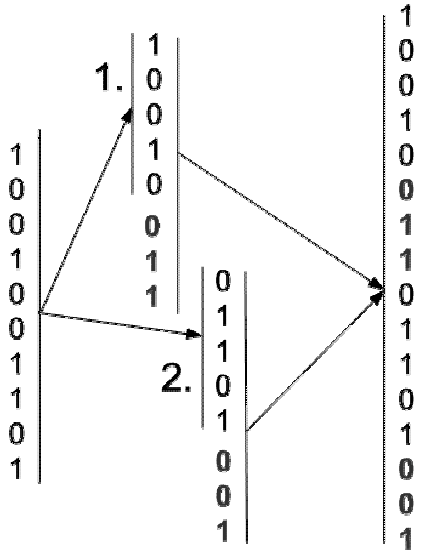
CRC metóda	Generický polynóm	Počet bitov
CRC-32	$x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^2+x+1$	32
CRC-24	$x^{24}+x^{23}+x^{14}+x^{12}+x^8+1$	24
CRC-16	$x^{16}+x^{15}+x^2+1$	16
Reversed CRC-16	$x^{16}+x^{14}+x+1$	16
CRC-8	$x^8+x^7+x^6+x^4+x^2+1$	8
CRC-4	$x^4+x^3+x^2+x+1$	4

Dôležitým atribútom vo všetkých CRC blokoch je počet syndrómov. Jeho dĺžka je zhodná z dĺžkou generačného polynómu. Počet jeho opakovaní je však voliteľný. Na nasledujúcom príklade je vysvetlené pridanie viacnásobného syndrómu.

Predpokladaná dĺžka vysielaného rámca je 10 bitov. Stupeň generačného polynómu je 3, a počet opakovaní syndrómu na jeden rámec je 2. Blok CRC generátora rozdelí vstupný rámec na dva podrámce s 5 bitmi a na obidve bude aplikovaný generačný polynóm tretieho radu. Obidve 3-bitové syndrómy sa potom pridajú k vysielanému rámcu. Celé kódové slovo teraz bude mať 16 bitov . Príklad je názorne zobrazený na obr.4.

Nastavenia jednotlivých parametrov v blokoch CRC generátor a CRC detektor syndrómu sú zhodné. Ich funkcia je inverzná. Ak detektor vyhodnotí, že zvyšok po danom algoritme sa nerovná 0 prenesená správa bola chybná a bola narušená jej integrita. CRC kód sa vo väčšine praktických aplikácií používa ako detekčný kód. Ak CRC detektor syndrómu vyhodnotí, že prijatá správa je narušená, vyšle signál zdroju správy o jej opätovné vyslanie. CRC detektor syndrómu v knižnici *Communication blockset* obsahuje výstupný vektor chýb. V prípade nenarušenej správy je na výstupe 0, v prípade chybnej správy 1. CRC kód dokáže detegovať chybnú správu nie však chybný bit. Z tohto dôvodu je porovnávacím kritériom počet detegovaných správ ku počtu všetkých prenesených správ.

V zostrojenom modeli sú použité bloky CRC generátor a CRC detektor syndrómu. Ich použitím je možné otestovať vlastnosti ľubovoľných generačných



Obr. 4: Kódové slovo (pridanie syndrómu k informačnej časti)

polynómov. Tie sú do modelu načítavané z programu uloženého v m-file súbore (CRCstart.m). Tento program generuje všetky primitívne generačné polynómy v danom ráde a dáva ich výstupy (počet detegovaných narušených správ) k vzájomnému porovnaniu. Z dôvodu veľkého množstva kombinácii pri polynómoch vyšších radov (pre polynóm CRC 32 je počet kombinácii 2^{30}), ale aj z dôvodu otestovania polynómov použitých v jednotlivých aplikáciách je program naprogramovaný tak, aby bolo možné zadať aj požadovaný generačný polynóm. Program umožňuje nastaviť aj ďalšie parametre CRC kódu, ako je napr. počet pridávaných syndrómov. Výstupom programu je počet detegovaných narušených správ, ktoré boli zabezpečené jednotlivými generačnými polynómami.

Ďalšou časťou modelu sú bloky určené na vytvorenie virtuálnych prenosových vlastností kanála. Za účelom hodnotenia vlastností prenosového kódu je najjednoduchšou voľbou použitie binárneho symetrického kanála (*Binnary Symetric Channel*). Binárny symetrický kanál prenáša binárnu informáciu, pričom vznik chyby je daný pravdepodobnosťou jej výskytu p_b. Tento model prenosového kanála však nedostatočne opisuje fyzikálne charakteristiky reálneho zapojenia. Z tohto dôvodu je odporúčane použiť iný z dostupných modelov prenosového kanála. Na opis vlastnosti káblového vedenia je vhodné použitie AWGN kanál s prídavným gaussovským šumom (*Additive White Gaussian noise* kanál). AWGN kanál má v celom svojom frekvenčnom pásme rovnomerne rozložený gaussovský šum. Blok AWGN kanála ponúka viacero možných nastavení.

1. *Eb/No* , pomer bitovej energie Eb ku spektrálnej výkonovej hustote bieleho šumu,
2. *Es/No*, pomer signálovej energie ku spektrálnej výkonovej hustote bieleho šumu,
3. *SNR*, pomer výkonu užitočného signálu k výkonu šumu.

Vzájomné vzťahy medzi nimi sú definované ako :

$$Es/N_0 = (T_{sym}/T_{samp}).\ SNR, \tag{5}$$

kde T_{sym} je parameter periódy symbolov (v tomto prípade rámcov) a T_{samp} je vzorkovací čas bloku v sekundách.

$$Es/N_0 = Eb/N_0 + 10log10(k), \tag{6}$$

kde k je pomer informačných bitov (vzoriek) ku počtu symbolov (rámcov).

Na to aby mohol byť použitý AWGN kanál je potrebne binárny (digitálny) signál namodulovať. Pre tento model bola vybraná binárna fázová modulácia BPSK (*binary phase shift keying*), a to z dôvodu jej schopnosti modulovať binárny signál vysielaný v rámcoch. Ak je vstupný bit 0 resp. 1 potom je modulovaný signál $exp(j\theta)$, resp. $-exp(j\theta)$, kde θ je parameter fázového posuvu.

Posledným blokom prenosového systému, ktorý má funkciu komunikačného prijímača je blok výpočtu chybovosti (*error rate calculation*). Blok dáva do pomeru počet chybne prijatých bitov k počtu všetkých prijatých bitov a výsledkom je bitová chybovosť. Ukazovateľ bitovej chybovosti patri medzi jeden zo základných kritérií pri hodnotení prenosových vlastností systému.

Na obr. 3 môžete vidieť aj ďalšie bloky použite v modelovom zapojení. Plnia funkciu čiastkových výpočtov, vizualizácie a ladenia modelu.

5 Výber generačného polynómu pre rôzne štruktúry chýb v prenosovom kanáli

Výber generačného mnohočlena, by sa mal riadiť chybovými štruktúrami, ktoré sa v uvažovanom dátovom spoji najčastejšie vyskytujú. Existuje niekoľko typických chýb (jednoduché chyby, dvojnásobné chyby, zhluky chýb atď.), pred ktorými by sa dáta mali ochrániť. Pravdepodobnosť zabezpečenie proti jednotlivým typom chýb je v tabuľke 2.

Posledné dva prípady vykazujú rovnakú pravdepodobnosť pre akúkoľvek chybovú štruktúru. Polynomické kódy všeobecne umožňujú dosiahnuť vysokého stupňa zabezpečenia. Porovnanie schopnosti detekcie narušených správ generačných polynómov rádu *r=2* až *12* je zobrazené v tabuľke 3. Bola overená detekčná schopnosť všetkých kombinácií generačných polynómov uvedeného rádu.

TAB.2 STUPEŇ ZABEZPEČENIA VZHĽADOM NA CHYBOVÚ ŠTRUKTÚRU KANÁLA

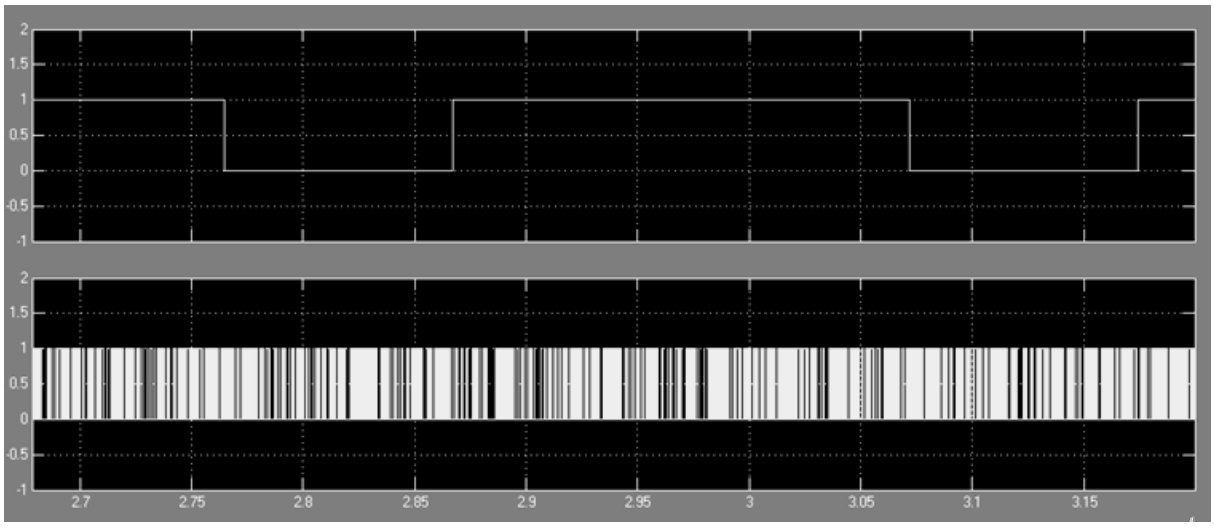
Typ chybovej štruktúry	Stupeň zabezpečenia
Jednotlivé chybné bity	100% zabezpečenie
Dva chybné bity (oddelené, či neoddelené)	100% zabezpečenie
Nepárny počet chybných bitov	100% zabezpečenie
Zhluk kratší ako (r+1) bitov	100% zabezpečenie
Zhluk chýb dĺžky (r+1) bitov	$p_{det}= 1-(1/2)^{(r-1)}$
Zhluk chýb dlhší ako (r+1) bitov	$p_{det}= 1-(1/2)^{r}$
Pozn.: p_{det} je pravdepodobnosť detekcie zhluku r je stupeň rádu generačného polynómu	

V tabuľke sa nachádzajú výsledky v podobe - najvyšší a najnižší počet detegovaných správ pre daný stupeň generačného polynómu. Je zrejmé, že detekčné schopnosti so zvýšeným stupňom generačného polynómu narastajú.

TAB. 3 DETEKČNÉ SCHOPNOSTI GENERAČNÉHO POLYNÓMU V ZÁVISLOSTI OD RÁDU

Rád polynómu r	Najviac detegovaných správ	Najmenej detegovaných správ	Bitová chybovosť v prenosovom kanály	Počet chybných bitov
2	492	492	0.2133	218451
4	899	868	0.2134	218522
5	949	920	0,2140	219174
6	980	958	0,2142	219388
7	990	974	0.2144	219512
8	997	986	0.2141	219249
9	998	991	0.2146	219758
10	1000	995	0.2141	219231
12	1000	997	0.2143	219431
Dĺžka správy N=1024 bitov, počet prenesených správ S=1000,			pomer signál šum Eb/No = -5, počet syndrómov na správu Checksum=1.	

Na obr. 5 sú zobrazené priebehy signálov potrebných pri overení detekčnej schopnosti daného kódu. Horný priebeh zobrazuje signál detekcie narušenej správy. Ak má signál hodnotu 1 narušená správa bola detegovaná. Ak má signál hodnotu 0 správa detegovaná nebola. Spodný priebeh zobrazuje jednotlivé bitové chyby pri bitovej chybovosti p_b=0,21711. Ako generačný polynóm bol použitý (x^3+x^2+1).



Obr. 5 Priebehy spojené s detekciou narušenej správy

Zabezpečenie typu CRC-r je vhodné pre detekciu chýb v železničných aplikáciách, lebo spĺňa požiadavky na bezpečnostný kód definovaný v [1]. Tento fakt vyplynul aj z navrhovaného riešenia komunikácie koncepcie JAZZ (*jednotná architektúra zabezpečovacieho zariadenia*) pre podnik AŽD,

spol. s.r.o., Praha [7]. Zabezpečenie typu CRC-r sa tu navrhuje použiť v systémoch zálohovanej komunikácie (systémy 2 z 2 alebo 2 z 3), kde komunikácia je zabezpečená rôznymi CRC-r v pozdĺžnom (cez prenosový kanál) a v priečnom smere (prenos medzi jednotlivými jednotkami jadra). Z dôvodu zabezpečenia nezávislosti bezpečnostného kódu používaného v protokole nedôveryhodného prenosového systému a kódu v komunikačnom systéme súvisiacom s bezpečnosťou je potrebné nevoliť štandardné typy CRC-r. Zabezpečenie typu CRC-r je používane takisto v systémoch od spoločnosti Sheidt&Bachman. Pri otestovaní niektorých generačných polynómov používaných v týchto aplikáciách boli detegované všetky narušené správy. Výsledky testu sú zhrnuté v tabuľke 4.

TAB. 4 DETEKČNÉ SCHOPNOSTI GEN. POL. POUŽITÝCH V BEZPEČNOSTNÝCH APLIKÁCIÁCH

Aplikácia	Gen. polynóm	Počet detegovaných správ	Bitová chybovosť
JAZZ – prepojenie riadiacich jednotiek	$x^{32}+x^{29}+x^{27}+x^{25}+x^{24}+x^{22}+x^{19}+$ $x^{18}+x^{16}+x^{15}+x^{12}+x^{11}+x^{10}+x^4+x^2+1$	1000	0,2171
JAZZ – prepojenie riadiacich jednotiek	$x^{32}+x^{31}+x^{29}+x^{25}+x^{23}+x^{22}+x^{21}+x^{19}+x^{13}+$ $x^9+x^7+x^3+1$	1000	0,217
JAZZ – prepojenie riadiacich jednotiek	$x^{32}+x^{30}+x^{25}+x^{21}+x^{18}+x^{17}+x^{13}+x^{10}+x^9+x$ $^7+x^5+x^4+ x^3+x^{2+}1$	1000	0,217
Scheidt&Bachman	$x^{32}+x^{31}+x^{30}+x^{29}+x^{27}+x^{26}+x^{25}+$ $x^{22}+x^{20}+x^{19}+x^{17}+x^{16}+x^{14}+x^9+x^7+$ $x^6+x^5+x^4+x^3+x^2+1$	1000	0,2176
Dĺžka správy N=1024 bitov, počet prenesených správ S=1000, celková dĺžka prenášanej správy 1 024 000 bitov		pomer signál šum Eb/No = -5, počet syndrómov na správu Checksum=1.	

6 Záver

Použitie systematického cyklického CRC kódu patrí v súčasnosti medzi najrozšírenejšie ochrany proti narušeniu integrity prenášanej správy. Je súčasťou štandardného prenosového kódu, ale aj prídavných bezpečnostných kódov používaných v bezpečnostne kritických aplikáciách. Vyčíslenie ukazovateľov jeho detekčných schopnosti je potrebnou súčasťou pri určovaní úrovne bezpečnosti celého prenosového, resp. komunikačného systému vzhľadom ku [1]. Jedným z možných riešení je vytvorenie spoľahlivého modelu plniaceho funkciu overovania bezpečnostného kódu, ale aj iných funkcií pri prenose bezpečnostne relevantnej správy. Takýto model sa môže stať dôležitou súčasťou metodiky na hodnotenie bezpečnostne relevantných komunikačných systémov.

Acknowledgment

Tento článok vznikol v rámci projektu KEGA K-057-06-00 "*Inovácia metodiky laboratórnej výučby na báze modelovania a simulácie v programovom prostredí Matlab v kombinácii s výukovými modelmi prostredníctvom e-learningu.*"

Literatúra

[1] ČSN EN 50159-1: *Drážní zařízení – Sdělovací a zabezpečovací systémy a systémy zpracovaní dat. Část 1: Komunikace v uzavřených přenosových zabezpečovacích systémech.* ČTN, 2002.
[2] ČSN EN 50159-2: *Drážní zařízení – Sdělovací a zabezpečovací systémy a systémy zpracovaní dat. Část 2: Komunikace v otvořených přenosových zabezpečovacích systémech.* ČTN, 2002.
[3] IEC 61784-3: *Digital data communications for measurement and control. Part 3: Profiles for functional safety communications in industrial networks.* Draft 2006
[4] Adámek, J.: *Kódovaní*, *Matematika pro vysoké školy technické*, SNTL, Praha 1989.

[5] Franeková, M.: *Modelovanie komunikačných systémov v prostredí Matlab, Simulink a Communications Toolbox*. ŽU 2003, ISSN 80-8070-027-3
[6] www.mathworks.com
[7] Rastočný,K., Záhradník, J., Franeková, M. Mikuláš, M.: *Verifikácia JAZZ (Jednotní architektúra zabezpečovacích zařízení)*, Objednávatel: AŽD spol. s.r.o. Praha, EF/9/2003.

Ing. Ján Rofár
Tel.: +421 41 513 3337
E-mail: jan.rofar@fel.uniza.sk

doc. Ing. Mária Franková, PhD.,
Tel.: +421 41 513 3346
E-mail: maria.franekova@fel.uniza.sk