OPTIMALIZÁCIA VÝBERU PARAMETROV BEZPEČNOSTNÉHO KÓDU V MATLABE

Ing. Tomáš Ondrašina, Mgr. Juraj Ľupták

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

Abstrakt

Príspevok je zameraný na problematiku výberu parametrov bezpečnostného kódu pre komunikačný protokol v rámci bezpečnostne relevantných aplikácií. Nosná časť je venovaná optimalizácií výberu parametrov bezpečnostného kódu a modelovaniu detekčných vlastností CRC kódu pre rôzne správy a generačné polynómy. Generovanie chybovej štruktúry v komunikačnom kanáli a určenie zvyškovej chybovosti zvoleného bezpečnostného kódu je realizované pomocou nástroja Matlab a knižnice Communication Blockset.

1 Úvod

Bezpečnostne relevantná komunikácia 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).

Prenosové kódy sa používajú v otvorených prenosových systémoch na detekciu bitových a zhlukových chybových stavov. Na detekciu poškodenia správy v bezpečnostne relevantnom procese sa vyžaduje prídavný bezpečnostný kód. Pri použití bezpečnostného kódu sa musí preukázať primeranosť schopnosti detekcie všetkých očakávaných typov chýb a hodnoty pravdepodobnosti nedetegovaných chýb.

2 Požiadavky na bezpečnostný kód

Na dosiahnutie požadovanej integrity bezpečnosti prenosového systému treba vychádzať z nasledujúcich požiadaviek na bezpečnostný kód [1]:

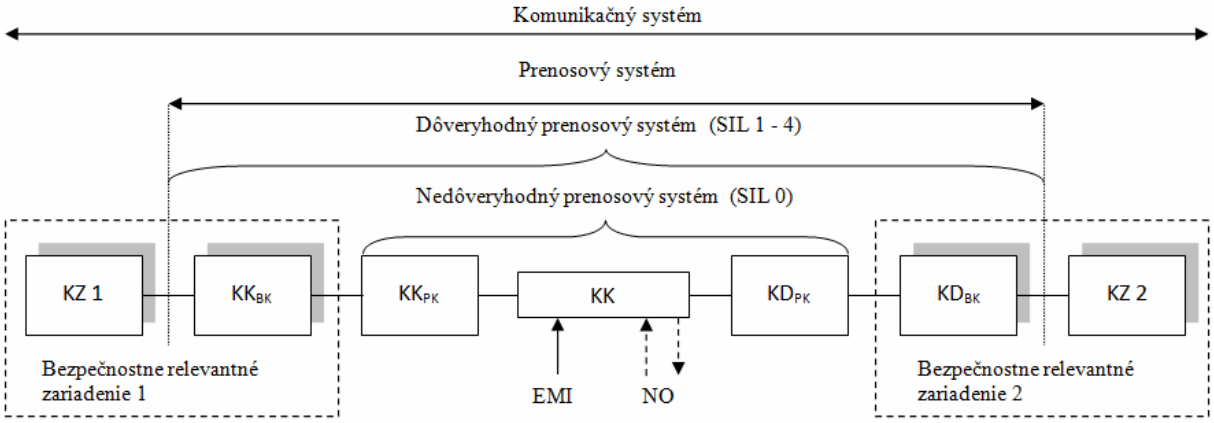
- musí byť schopný detegovať: náhodné chyby, zhluky chýb, systematické chyby (opakujúce sa vzory chýb) a kombinované chyby,
- musí byť schopný detegovať chyby typu: prerušená prenosová linka, všetky bity majú log. 1, všetky bity majú log. 0 (v prípade binárneho prenosu), inverziu správy, synchronizačný sklz (v prípade sériového prenosu),
- pravdepodobnosť nedetegovanej chyby (zvyšková chybovosť) kódu musí byť pod garantovanou hranicou,
- musí byť použitý kód s rýchlym kódovaním a dekódovacím algoritmom, lebo správa má vo väčšine prípadov časovú platnosť,
- algoritmus musí byť jednoducho prakticky realizovateľný,
- musí byť zabezpečená funkčná nezávislosť použitého kódu s prenosovým kódom.

Najčastejšie používaným bezpečnostným a prenosovým kódom v komunikačných protokoloch komerčných prenosových systémov a zároveň aj pri bezpečnostne relevantnom prenose podľa [3], [4] a [5] je systematický cyklický kód, pracujúci na princípe CRC (Cyclic Redundancy Check). Cyklické kódy patria do skupiny blokových kanálových kódov. Tieto 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. Pre vyjadrenie vlastností cyklických kódov sa používa algebra polynómov.

3 Možnosti výberu parametrov bezpečnostného kódu v Matlabe

V rámci bezpečnostnej analýzy sa sledovali chybové stavy prenosového systému, ku ktorým mohlo dôjsť počas prenosu správ. Kontrolné mechanizmy bezpečnostného a prenosového kódu zabezpečujú správy proti rušeniu, ktoré vzniká v prenosovom kanáli. Výber generačného polynómu sa riadi chybovými štruktúrami, ktoré sa v uvažovanom dátovom spoji najčastejšie vyskytujú. Súčasťou prenosového systému je komunikačný kanál, ktorý je ovplyvňovaný elektromagnetickou interferenciou EMI (pre otvorený prenosový systém aj útokmi spôsobenými nekompetentnou osobou).

Uvažovali sme uzatvorený komunikačný systém na úrovni dvojbodového spoja, znázornený na obr. 1, ktorý pozostáva z koncových zariadení KZ_1, KZ_2 a prenosového systému. Prenosový systém obsahuje len bezpečnostne relevantné funkcie prenosu, ktoré sa fyzicky vykonávajú prostredníctvom dvojice: kanálový kóder/dekóder bezpečnostného kódu a sú nadstavbou kanálového kódera/dekódera prenosového kódu nedôveryhodného prenosového systému.

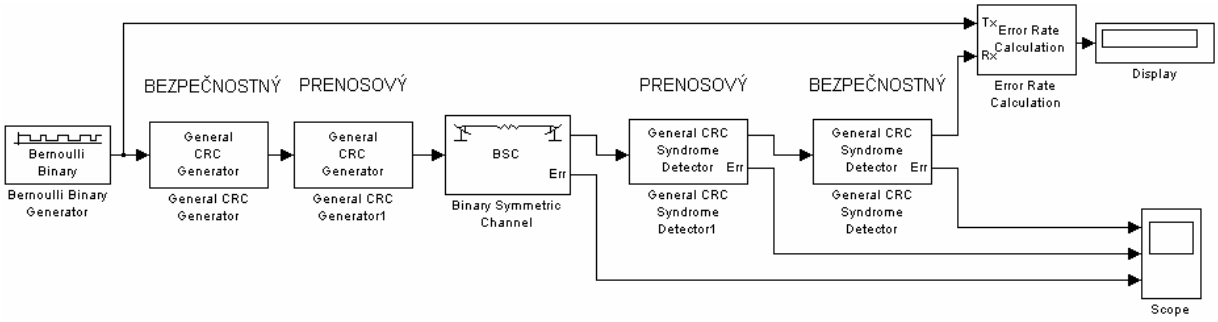


KZ	koncové zariadenie
KK_{BK}/KD_{BK}	kanálový kóder / dekodér bezpečnostného kódu
KK_{PK}/KD_{PK}	kanálový kóder / dekodér prenosového kódu
KK	komunikačný kanál
EMI	elektromagnetická interferencia
NO	nekompetentná osoba (hacker)

Obr. 1: Bezpečnostne relevantný komunikačný systém pre dvojbodové spojenie

4 Model zapojenia na testovanie CRC kódu v Simulinku

Výber parametrov bezpečnostného kódu sa realizoval podľa modelu dvojbodového zapojenia, ktorý je znázornený na obr. 2. Bol vytvorený pomocou knižníc *Communication blockset*, *Simulink*, *Signal processing blockset*. 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 [2].



Obr. 2: 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 bezpečnostného a 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 (f*rame-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 bezpečnostného a prenosového kódu je pre tento model CRC generátor (*General CRC Generator*). Ten spolu s CRC detektorom syndrómu (*General CRC Syndrome Detector*) 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.

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.

Použitím blokov CRC generátora a CRC detektora syndrómu môžeme otestovať vlastnosti ľubovoľných generačných polynómov. Nastavenia jednotlivých parametrov v týchto blokoch sú zhodne, pretože ich funkcia je inverzná. Generačné polynómy pre bezpečnostný CRC kód sú uvedené v tabuľke 1. Pre prenosový CRC kód bol použitý generačný polynóm $x^8+x^2+x^1+1$ v binárnom tvare 100000111.

Tab. 1: GENERAČNÉ POLYNÓMY V CRC BLOKOCH

CRC metóda	*Binárny tvar*	*Generačný polynóm*	*Počet bitov*
CRC-8	100101111	$x^8+x^5+x^3+x^2+x^1+1$	8
CRC-8	100010011	$x^8+x^4+x^1+1$	8
CRC-8	100011001	$x^8+x^4+x^3+1$	8
CRC-8	100110001	$x^8+x^5+x^4+1$	8
CRC-8	101000011	$x^8+x^6+x^1+1$	8
CRC-8	110000101	$x^8+x^7+x^2+1$	8
CRC-8	110010001	$x^8+x^7+x^4+1$	8
CRC-8	111000001	$x^8+x^7+x^6+1$	8
CRC-8	101011101	$x^8+x^6+x^4+x^3+x^2+1$	8
CRC-8	101110101	$x^8+x^6+x^5+x^4+x^2+1$	8
CRC-8	110011011	$x^8+x^7+x^4+x^3+x^1+1$	8
CRC-8	110100111	$x^8+x^7+x^5+x^2+x^1+1$	8
CRC-8	110110011	$x^8+x^7+x^5+x^4+x^1+1$	8
CRC-8	111001011	$x^8+x^7+x^6+x^3+x^1+1$	8
CRC-8	111101001	$x^8+x^7+x^6+x^5+x^3+1$	8
CRC-8	101111111	$x^8+x^6+x^5+x^4+x^3+x^2+x^1+1$	8
CRC-8	111111101	$x^8+x^7+x^6+x^5+x^4+x^3+x^2+1$	8

Testovanie prebiehalo pre 3 rôzne správy. Pri každom meraní sa posielalo 100 správ.

Správa č.1 mala tvar: 1

Správa č.2 mala tvar: 0

Správa č.3 mala tvar: 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

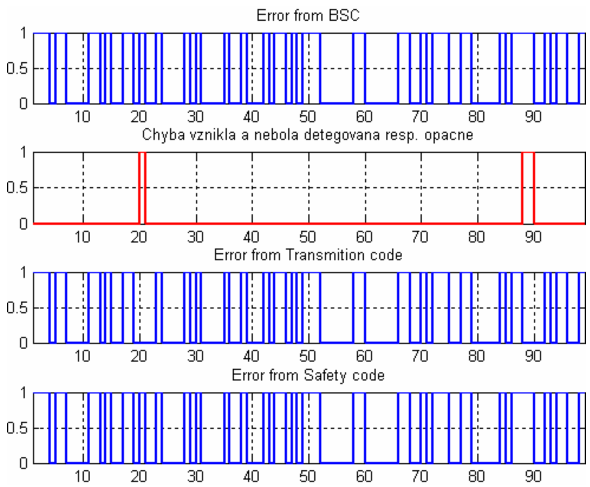
Výsledky z jednotlivých meraní sa nachádzajú v tabuľke 2. Vyhodnocovala sa chyba bezpečnostného kódu, chyba prenosového kódu, počet detegovaných chýb a počet kolízií.

Tab. 2: DETEKČNÉ SCHOPNOSTI GENERAČNÉHO POLYNÓMU

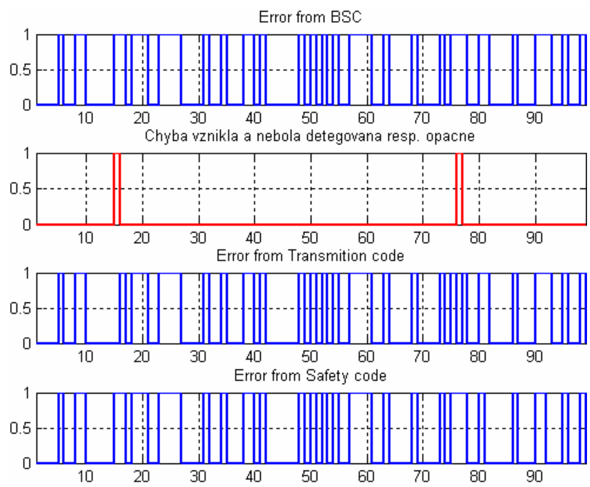
Číslo merania	*Binárny tvar*	*Správa č.1*				*Správa č.2*				*Správa č.3*			
		Chyba BK	*Chyba PK*	*Počet deteg. chýb*	*Počet kolízií*	*Chyba BK*	*Chyba PK*	*Počet deteg. chýb*	*Počet kolízií*	*Chyba BK*	*Chyba PK*	*Počet deteg. chýb*	*Počet kolízií*
1.	100101111	41	44	44	0	52	54	56	2	41	43	44	1
2.	100010011	45	46	46	0	49	51	53	2	40	40	42	2
3.	100011001	41	40	44	4	37	37	39	2	44	41	45	4
4.	100110001	51	47	51	4	51	52	53	1	45	44	48	4
5.	101000011	43	43	45	2	46	45	47	2	52	53	54	1
6.	110000101	47	47	51	4	44	43	44	1	44	42	45	3
7.	110010001	45	48	50	2	47	45	49	4	48	47	49	2
8.	111000001	55	56	57	1	48	48	51	3	41	36	41	5
9.	101011101	44	43	45	2	44	44	47	3	40	41	42	1
10.	101110101	46	46	47	1	44	42	45	3	54	53	57	4
11.	110011011	51	49	53	4	43	43	45	2	50	49	52	3
12.	110100111	43	40	43	3	44	45	46	1	39	36	40	4
13.	110110011	44	44	47	3	38	39	40	1	51	50	51	1
14.	111001011	42	42	47	5	47	47	49	2	53	54	55	1
15.	111101001	47	46	48	2	52	49	54	5	42	44	46	2
16.	101111111	49	47	49	2	44	42	44	2	40	39	42	3
17.	111111101	44	46	48	2	43	46	48	2	42	41	43	2

BK bezpečnostný kód
PK prenosový kód

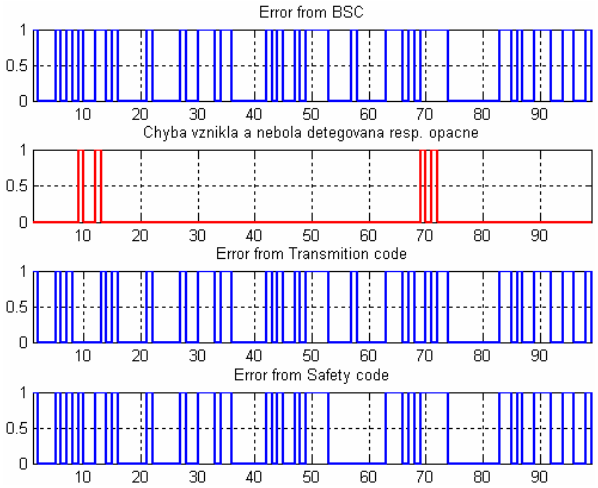
Na obr. 3, 4 a 5 sú zobrazené vybrané priebehy signálov z tabuľky 2 potrebných na overenie detekčnej schopnosti daného kódu. Sú to priebehy, pri ktorých počet detegovaných chýb bol najnižší. Priebehy spojené s detekciou narušenej správy zobrazujú jednotlivé bitové chyby pri bitovej chybovosti p_b=0,005. Ak má signál hodnotu 1, narušená správa bola detegovaná. Ak má signál hodnotu 0, správa detegovaná nebola.



Obr. 3: Správa č.1 - priebehy pri 12.meraní



Obr. 4: Správa č.2 - priebehy pri 3.meraní



Obr. 5: Správa č.3 - priebehy pri 12.meraní

5 Záver

CRC kód 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. Určenie jeho detekčných vlastností je potrebné pri zisťovaní celkovej úrovne bezpečnosti komunikačného systému.

Tento článok vznikol v rámci projektu VEGA-1/0040/08 "*Matematicko-grafické modelovanie bezpečnostných vlastností bezpečnostne kritických riadiacich systémov.*"

Literatúra

[1] Franeková, M., Kállay, F., Peniak, P., Vestenický, P.: *Komunikačná bezpečnosť priemyselných sietí.* EDIS, ŽU 2007, ISBN 978-80-8070-715-6
[2] Franeková, M.: *Modelovanie komunikačných systémov v prostredí Matlab, Simulink a Communications Toolbox.* ŽU 2003, ISBN 80-8070-027-3
[3] ČSN EN 50159-1: *Drážní zařízení – Sdělovací a zabezpečovací systémy a systémy zpracovaní dat. Část 1: Komunikace v uzavřených přenosových zabezpečovacích systémech.* ČTN, 2002.
[4] ČSN EN 50159-2: *Drážní zařízení – Sdělovací a zabezpečovací systémy a systémy zpracovaní dat. Část 2: Komunikace v otvořených přenosových zabezpečovacích systémech.* ČTN, 2002.
[5] IEC 61784-3: *Digital data communications for measurement and control. Part 3: Profiles for functional safety communications in industrial networks.* Draft 2006
[6] www.mathworks.com

Ing. Tomáš Ondrašina
Žilinská univerzita v Žiline, Elektrotechnická fakulta, Katedra riadiacich a informačných systémov
Univerzitná 1, 010 26 Žilina
tel.: +421 41 513 3306
e-mail: tomas.ondrasina@fel.uniza.sk

Mgr. Juraj Ľupták
Žilinská univerzita v Žiline, Elektrotechnická fakulta, Katedra riadiacich a informačných systémov
Univerzitná 1, 010 26 Žilina
tel.: +421 41 513 3306
e-mail: juraj.luptak@fel.uniza.sk