BEZPEČNOSŤ PRENOSU V ŽELEZNIČNÝCH APLIKÁCIÁCH
SAFETY OF TRANSMISSION IN RAILWAY APPLICATIONS

Mária Franeková
Katedra riadiacich a informačných systémov, Elektrotechnická fakulta, Žilinská univerzita, Veľký diel, 010 26 Žilina

Abstrakt Článok je venovaný problematike bezpečnosti dát v prenosových systémoch súvisiacich s bezpečnosťou definovaných v rámci železničného dopravného procesu. Je zameraný na sumár hrozieb a protiopatrení pre uzatvorené a otvorené prenosové systémy. Podrobnejšie je rozanalyzovaná možnosť použitia kanálových kódovacích a kryptografických mechanizmov definovaných normami EN 50159. Pre zvolené bezpečnostné mechanizmy je uvedený matematický aparát na výpočet pravdepodobnosti nedetegovanej chyby kanálových dekodérov, vzťahy na určenie dešifrovacej zložitosti a pravdepodobnosti chyby kryptografického slova.

Summary The paper deals with the problems of data security in safety – related transmission systems defined within railway process. It is intent on summary of treats and security tools against them within closed and open security systems. In details is analysed possibility of using channel coding techniques and cryptography mechanisms, which are defined according to norms EN 50159. For chosen security mechanisms are deal mathematical apparatus of probability of undetected error determination for channel decoders, relations for determination decipher encoder's complexity and error probability of cryptography code word.

1. ÚVOD

Pri prenose informácie veľkých hodnôt (tzv. citlivej informácie) v rámci riadenia železničnej dopravy je nutné sa venovať otázke bezpečnosti prenosu. Informácia musí byť chránená tak, aby k nej mali prístup len oprávnené osoby, aby sa dalo zistiť, kto ju vytvoril, zmenil, alebo odstránil, aby informácia nebola prezradená a aby bola dostupná, keď je to potrebné. Komunikačné cesty predstavujú jedno z najdôležitejších a zároveň najviac zraniteľných miest zabezpečovacieho systému. Komunikačná bezpečnosť je daná zachovaním dôvernosti (k údajom majú prístup len autorizované objekty), integrity (dáta môžu byť modifikované len autorizovanými subjektami a pôvod informácie je overiteľný) a dostupnosti (dáta sú autorizovaným subjektom do určitej doby prípustné, nedôjde teda k odmietnutiu služby).

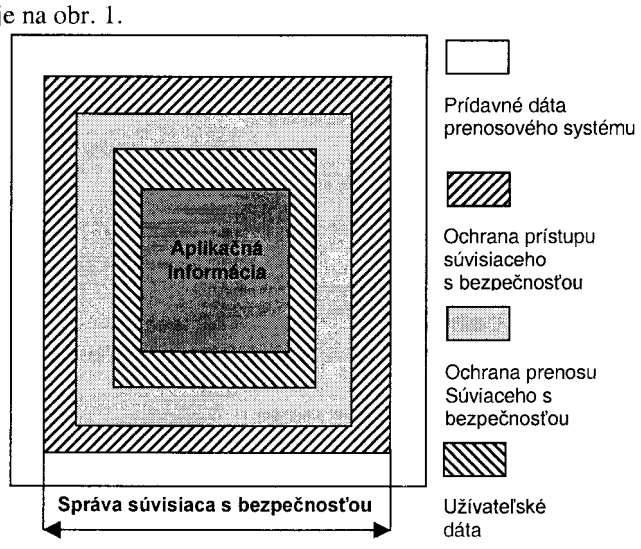
Pri prenose dát medzi zabezpečovacími systémami sú definované dve triedy systémov. Prvá trieda - uzatvorené prenosové systémy [1], zahrňuje také systémy, kde je určitá kontrola nad systémom, sú známe jeho charakteristiky a počet komunikujúcich účastníkov. Druhá trieda - otvorené prenosové systémy [2] zahrňuje také systémy, ktorých charakteristiky sú neznáme, alebo čiastočne známe a hrozí narušenie správ aj z vonkajšieho prostredia (napr. cez Internet, dátovú sieť...). Prenos definovaný v týchto normách dostáva prívlastok - prenos súvisiaci s bezpečnosťou (z ang. *safety – related transmission*).

Podľa [2] je definovaných sedem tried otvorených prenosových systémov. Závažnosť útokov v jednotlivých typoch systémov závisí od technických vlastností systému, včítane spoľahlivosti, dostupnosti systému a realizovaného prístupu do systému cez privátnu alebo verejnú sieť.

Pri oboch typoch systémov (uzatvorený, otvorený) je správa jedným z hlavných subjektov celkovej analýzy bezpečnosti pri prenose. Útoky na správy, ktoré sú zasielané cez komunikačné linky sa môžu prejaviť následnou poruchou v komunikačnom zariadení. Tok správ, ktorý je aktuálne prijatý sa môže líšiť od vyslaného toku správ z nasledujúcich dôvodov :

- Viac prijatých správ, ako sa očakáva: jedna alebo viac správ je zopakovaných alebo vsunutých do komunikačnej linky (*repeated, inserted message*).
- Menej prijatých správ, ako sa očakáva: jedna alebo viac správ je vymazaných (*deleted message*).
- Zhodný počet prijatých a očakávaných správ, ale:
  - všetky správy v toku sú korektné v obsahu a v čase prenosu, ale sekvencia vplyvom zmeny poradia prvkov je chybná (*resequenced message*),
  - tok správy je prijatý v prijímači s oneskorením (*deleyed message*),
  - správa je modifikovaná (*corrupted mess*age),
  - prijímateľ si myslí, že odosielateľ správy je iný, ako v skutočnosti je, lebo sa modifikovala adresa odosielateľa (*resequenced, delayed, corrupted, masqueraded message).*

Model reprezentácie správy súvisiacej s bezpečnosťou je na obr. 1.



Obr. 1. Štruktúra modelu reprezentácie správy súvisiacej s bezpečnosťou

Na obmedzenie rizika súvisiaceho s ohrozeniami sa musia podľa [2] uvažovať a poskytnúť nasledujúce bezpečnostné služby: autentickosť správy, integrita správy, aktuálnosť správy, poradie správy.

Integrita správy môže byť narušená neúmyselne, vplyvom šumového prostredia prenosového kanála, (podľa ISO/OSI 7498-2 [3] ide o tzv. slabú integritu). Pri návrhu prenosového systému sa tento prípad najčastejšie rieši pomocou dostupných kódovacích a dekódovacích kanálových techník. Bezpečnostné požiadavky na kanálové kódovacie techniky sú definované v [1].

Integrita dát však môže byť narušená aj úmyselné, vplyvom nekompetentnej osoby, ktorá môže správu modifikovať. Podľa [3] ide o tzv. silnú integritu, kedy je nutné použiť silnejšie ochranné mechanizmy, pracujúce hlavne na báze kryptografických techník. Požiadavky na kryptografický a hašovací kód sú definované v [2] .

2. VÝBER KANÁLOVÝCH KÓDOVACÍCH TECHNÍK PRE PRENOSOVÉ SYSTÉMY SÚVISIACE S BEZPEČNOSŤOU

V uzatvorených aj otvorených prenosových systémov je podľa [1] a [2] odporúčané na zabezpečenie prenosu proti vplyvu šumového prostredia použiť kódy len s detekčnými vlastnosťami. Pri výbere vhodného bezpečnostného kódu (v teórii kódovania sa označuje pojmom kanálový kód - *Channel Coding*), treba vychádzať z požiadaviek:

- na schopnosť kódu detegovať systematické a náhodné chyby,
- na pravdepodobnosť nedetegovanej chyby (má byť pod garantovanou hranicou),
- na rýchlosť kódovacieho a dekódovacieho algoritmu (správa je platná len určitý čas, cyklický charakter prenosu),
- na praktickú realizáciu algoritmu.

Umiestnenie bezpečnostného kódu pre prenos dát súvisiaceho bezpečnosťou je v na obr. 1 v rámci vrstvy ochrana prenosu.

Najviac používaným detekčným kódom v tejto oblasti je blokový systematický cyklický kód, ktorý pracuje na princípe CRC-r (*Cyclic Redundancy Check*). Dokáže detegovať jednoduché chyby a náhodné zhluky chýb dĺžky r, kde r je stupeň generujúceho polynómu $g(x)$ kódu.

V teórií kanálového kódovania však existuje množstvo efektívnych kódovacích a dekódovacích techník, ktoré síce patria do množiny samopravných kódov (tzv. techniky FEC *Forward Error Control*), ale pri dekódovaní sa dá jednoznačne vyčleniť časť súvisiaca s detekciou, čo by umožnilo použiť FEC techniky v aplikáciách definovaných podľa [1] a [2]. Na druhej strane však treba skonštatovať, že niektoré techniky samoopravných kódov, nemajú (bez zásahu do algoritmu) jasne oddeliteľnú časť detekcie a korekcie. Ide o techniky konvolučných kódovacích štruktúr, pracujúce na princípe maximálne pravdepodobnostného dekódovania [4], [5]. Spomínaná vlastnosť sa dá jednoducho realizovať len pri množine blokových, systematických kódov, používajúcich syndrómové techniky dekódovania. Na základe hodnoty syndrómu sa určí, či pri prenose v danom kódovom slove došlo resp. nedošlo k narušeniu správy.

V prípade polynomiálnych kódov (kód, ktorého charakteristiky sa dajú vyjadriť pomocou algebry mnohočlenov) existujú tri typy syndrómov [6]. Syndróm $s(x)$ definovaný vzťahom (1), čo je prípad binárnych cyklických kódov:

$$s(x) = c'(x) \bmod g(x). \tag{1}$$

$c'(x)$ je tu prijaté kódové slovo kódu, definovaného generačným polynómom $g(x)$.

Pretože všetky kódové slová sú deliteľné generačným polynómom $g(x)$, syndróm $s(x)$ nezávisí od vyslaného kódového slova, ale len od chýb, ktoré vznikli pri prenose.

Druhý typ syndrómov možno matematicky vyjadriť, ak generačný polynóm $g(x)$ je súčinom viacerých ireducibilných polynómov $g_1(x)$, $g_2(x)$,..., $g_j(x)$ (2),

$$g(x) = g_1(x)g_2(x)...g_j(x), \tag{2}$$

potom sa syndrómy počítajú podľa (3):

$$\begin{aligned} s_1(x) &= c'(x) \bmod g_1(x), \\ s_2(x) &= c'(x) \bmod g_2(x), \\ &\dots \\ s_j(x) &= c'(x) \bmod g_j(x). \end{aligned} \tag{3}$$

Tento spôsob výpočtu syndrómov používa množina zovšeobecnených Hammingových kódov - Bose Chaudhuri Hocquenghových - BCH kódov, ktoré patria k významnej skupine kanálových korekčných techník.

Tretia schéma definovania syndrómov spočíva v zavedení syndrómov vo vektorovom tvare S_1, S_2, ..., S_j. Potom sa syndrómy počítajú podľa (4), kde α_j je koreňom generujúceho polynómu $g(x)$:

$$\begin{aligned} S_1 &= c'(\alpha_1), \\ S_2 &= c'(\alpha_2), \\ &\dots \\ S_j &= c'(\alpha_j). \end{aligned} \tag{4}$$

Ide o prípad výpočtu syndrómu pre skupinu znakových Reedových - Solomonových (ďalej RS) kódov, ktoré v porovnaní s binárnymi kódmi sa vyznačujú vyššou rýchlosťou kódovania a dekódovania (závisí od konkrétnej implementácie) a dobre prepracovanými dekódovacími technikami [6]. Vlastnosti RS kódov sú založené na aritmetike konečných Galoisových polí GF (*Galois field*) GF(q), kde q je počet prvkov poľa, a v porovnaní s binárnymi Hammingovými kódmi

(vhodných pre korekciu jednej chyby v kódovom slove) sú schopné korekcie zhlukov chýb $t = (n\text{-}k)/2$ znakov.
Proces dekódovania RS kódov možno zhrnúť do nasledujúcich bodov:

1. výpočet syndrómov S_k,
2. nájdenie polynómov lokátorov chýb $\sigma(x)$,
3. nájdenie koreňov lokátorov $\sigma(x)$ – lokátory X_i,
4. výpočet hodnôt Y_i a následná korekcia chyby.

Ak by sme z dekódovacieho algoritmu vyčlenili len časť zodpovedajúcu detekcii chyby, z uvedeného postupu stačí vypočítať len prvý krok – syndrómy S_k, čím sa originálny dekódovací algoritmus značne urýchli. Použitie RS kódov v železničných aplikáciách závisí od viacerých okolností. Pokiaľ by sme ich chceli použiť ako korekčné kódy (zatiaľ to normy nepovoľujú) treba dokázať, že pravdepodobnosť nekorigovanej chyby je v súlade s bezpečnostnými požiadavkami, definovanými v [1] a [2]. Ak predpokladáme, že prijaté kódové slovo $c'(x)$ je súčtom vysланého a chybového slova $c(x)+e(x)$ syndrómy pre jednotlivé generujúce korene z možno vypočítať podľa:

$$S_k = c'(z^k) = c(z^k) + e(z^k), \tag{5}$$

pre $k = 0,1,\ldots,2t\text{-}1$, kde t je počet korigovaných znakov.

2. 1. VÝPOČET PRAVDEPODOBNOSTI CHYBY KANÁLOVÝCH DEKÓDOVACÍCH TECHNÍK

Pre zvolený blokový (n,k,t) kód je podľa [1], [2] potrebné vypočítať, aká je pravdepodobnosť chyby dekódovacieho algoritmu. Ide o prípad, keď syndróm je síce rovný nule, ale pri prenose kódového slova došlo ku chybe. Matematicky sa dá tento prípad vyjadriť pravdepodobnosťou chyby kódového slova p_e v závislosti od bitovej chybovosti p_b používaného kanála. Pri výpočte možno použiť štatistické hodnoty pravdepodobnosti chyby elementárneho symbolu (bitu) niektorých typických komunikačných kanálov. Binárny symetrický kanál (BSC) alebo kanál s gausovským aditívnym šumom AWGN sú veľmi často používané matematické modely kanálov, pri matematickom vyjadrení pravdepodobnosti nedetegovanej (nekorigovanej) chyby [7]. V literatúre existujú vzťahy na výpočet pravdepodobnosť chyby p_e, ktoré sú všeobecne platné pre celú množinu blokových (n,k,t) kódov, prípadne presnejšie vzťahy, platné len pre konkrétny typ kódu.

Pri niektorých postupoch výpočtu pravdepodobnosti chyby je potrebné poznať všetky kódové slová kódu. Potom pravdepodobnosť nedetegovanej chyby kódového slova p_{e1} pre BSC možno vypočítať podľa :

$$p_{e1} = \sum_{i=\left\|\frac{d_{min}+1}{2}\right\|}^{n} A_i p_b{}^i (1 - p_b)^{n-i}, \tag{6}$$

kde

d_{min} je minimálna Hammingova vzdialenosť kódu,
A_i je celkový počet kódových slov s váhou i,
p_b je bitová chybovosť kanála.

Pri výpočte podľa vzťahu (6) predpokladáme, že chyby v kanále sú nezávislé a vyskytujú sa s bitovou chybovosťou p_b a ich výskyt možno aproximovať hustotou rozdelenia pravdepodobnosti podľa binomického rozloženia.

Hammingove perfektné (n,k) kódy sú jedny z mála skupín kódov, u ktorých je známa kompletná funkcia váhová funkcia $A(x)$

$$A(x) = \sum_{i=0}^{n} A_i x^i, \tag{7}$$

kde

A_i je počet kódových slov s váhou i,
x predstavuje polynomické vyjadrenie váhovej funkcie,
x^i mocninou i určuje hodnotu váhy.

Váhová funkcia pre Hammingove kódy s $d_{min}=3$ a dĺžkou kódového slova $n = 2^r\text{-}1$ (r je počet redundantných bitov) je podľa [8]:

$$A(x) = \frac{1}{n+1}\left[(1+x)^n + n(1+x)^{(n-1)/2}(1-x)^{(n+1)/2}\right]. \tag{8}$$

Pre kódové slová s väčšou dĺžkou n môže byť výpočet p_{e1} komplikovaný. Veľkou výhodou je, že hodnoty funkcie $A(x)$ sú symetrické pozdĺž $(n\text{-}1)/2$, čo môže výpočet zjednodušiť. Hammingove kódy s $d_{min}=3$ sa dajú ľahko prekonvertovať na Hammingove kódy s $d_{min}=4$ pridaním jedného paritného bitu (predpokladáme párnu paritu). To spôsobí, že všetky kódové slová s váhou i (pre nepárnu váhu) sa stanú kódovými slovami s váhou $i+1$. Výsledky pravdepodobnosti nedetegovanej chyby kódového slova pre rozšírený Hammingov kód sú uvedené v [9]. Tento typ kódov, aj keď má dobre prepracovaný aparát na detekciu chýb a výpočet pravdepodobnosti chyby pri dekódovaní, možno v železničných aplikáciách definovaných podľa [1] a [2] použiť len v obmedzenom prípade, v slabo zašumených prenosových kanáloch (pri výskyte nezávislých chýb). Výhodnejšie je vybrať kód z techník FEC, akými sú už spomínané znakové RS kódy, pomocou ktorých sa dajú vytvoriť veľmi efektívne binárne kódy. Výhodou týchto kódov z pohľadu výpočtu pravdepodobnosti chyby je, že váhová štruktúra týchto kódov A_j je tiež známa [8]. Je definovaná nasledujúcimi vzťahmi:

$$A_0 = 1, A_j = 0 \; pre \; (1 \le j \le n-k), \tag{9}$$

$$A_j = \binom{n}{j} \sum_{h=0}^{j-1-(n-k)} (-1)^h \binom{j}{h} \left[q^{j-h-(n-k)} - 1\right]$$

$$pre \; (n-k+1) \le j \le n.$$

Pre všetky zabezpečené blokové kódy nie je jednoduché generovať váhovú funkciu kódových slov. Napr. pre BCH kódy nie je všeobecný vzťah váhovej funkcie, platný pre všetky (n,k) dvojice známy [8]. Potom pravdepodobnosť nedetegovanej chyby

kódového slova možno počítať úpravou vzťahu (6) tak, že hodnotu A_i aproximujeme pomocou

$$A_i \cong \frac{1}{2^{n-k}}\binom{n}{i}. \tag{10}$$

Pravdepodobnosť nedetegovanej chyby kódového slova p_{e2} potom je

$$p_{e2} \cong \frac{1}{2^{n-k}} \sum_{i=d_{\min}}^{n} \binom{n}{i} p_b{}^i (1-p_b)^{n-i}. \tag{11}$$

Ak súčin $n\ p_b$ je omnoho menší ako jedna ($n\ p_b << 1$) môže byť suma v uvedenom vzťahu (11) aproximovaná prvým členom sumy, čím získame p_{e3}

$$p_{e3} \cong \frac{1}{2^{n-k}}\binom{n}{d_{\min}} p_b{}^{d_{\min}} (1-p_b)^{n-d_{\min}}. \tag{12}$$

Je evidentné, že vo vzťahu (12) je potrebné poznať okrem parametrov (n,k) aj minimálnu Hammingovu vzdialenosť kódu d_{min} kódových slov. Ak je jej hodnota neznáma, na výpočet d_{min} možno použiť pre párne kódové slová tzv. Gilbertovu nerovnosť (13) a pre nepárne kódové slová vzťah (14).

$$2^k \sum_{i=0}^{(d_{min}-1)\ 2} \binom{n}{i} \le 2^n, \tag{13}$$

$$2^k \sum_{i=0}^{(d_{\min}-2)/2} \binom{n-1}{i} \le 2^{n-1}. \tag{14}$$

Pre RS kódy v GF(2^m) možno určiť odhad pravdepodobnosti chyby symbolu p_s pre prenose cez BSC kanál podľa:

$$p_S = \frac{1}{2^{m-1}} \sum_{j=t+1}^{2^{m-1}} j \binom{2^m-1}{j} p_b{}^j (1-p_b)^{2^m-1-j}, \tag{15}$$

Kde:

m	predstavuje počet bitov na znak,
t	počet korigovaných znakov,
p_b	bitová chybovosť kanála.

3. VÝBER KRYPTOGRAFICKÝCH TECHNÍK PRE PRENOSOVÉ SYSTÉMY SÚVISIACE S BEZPEČNOSŤOU

Kryptografické techniky sa môžu podľa [2], použiť, keď nie je možné alebo je ťažko realizovateľné zvládnuť úmyselné útoky na správy v rámci otvoreného prenosového systému. Vo väčšine prípadov sa dá v komunikačnom systéme určiť, či sa môže vylúčiť neoprávnený prístup k nemu alebo nie. V prípade možnosti neoprávneného prístupu je nutné použiť samostatnú vrstvu ochrany prístupu (viď obr. 1) používajúcu hlavne kryptografické mechanizmy. Kryptografické techniky je nutné implementovať do prenosových systémov využívajúcich služby verejnej siete, siete s rádiovým prenosom, verejnej dátovej siete alebo Internetu. Tieto techniky je možné kombinovať s bezpečným mechanizmom kódovania alebo sa môžu používať samostatne.

Treba si uvedomiť, že na rozdiel od techník kanálového kódovania, kryptografické mechanizmy zahŕňajú použitie nielen algoritmov, ale aj metód na generovanie, prenos a archiváciu kľúčov. Vývoj kryptografie je omnoho dynamickejší ako techník kanálového kódovania. Ak sa šifra stane štandardom, tento je prijímaný na dobu maximálne 5 -10 rokov a sila jeho algoritmu musí byť pravidelne prehodnocovaná. Pre prenosové systémy súvisiace s bezpečnosťou treba vziať do úvahy pri výbere kryptografických mechanizmov aj túto skutočnosť a vychádzať z najmodernejších, odbornou verejnosťou posúdených algoritmov.

V súčastnej dobe existuje množstvo kryptografických techník na báze symetrického, asymetrického alebo kombinovaného spôsobu šifrovania [10].

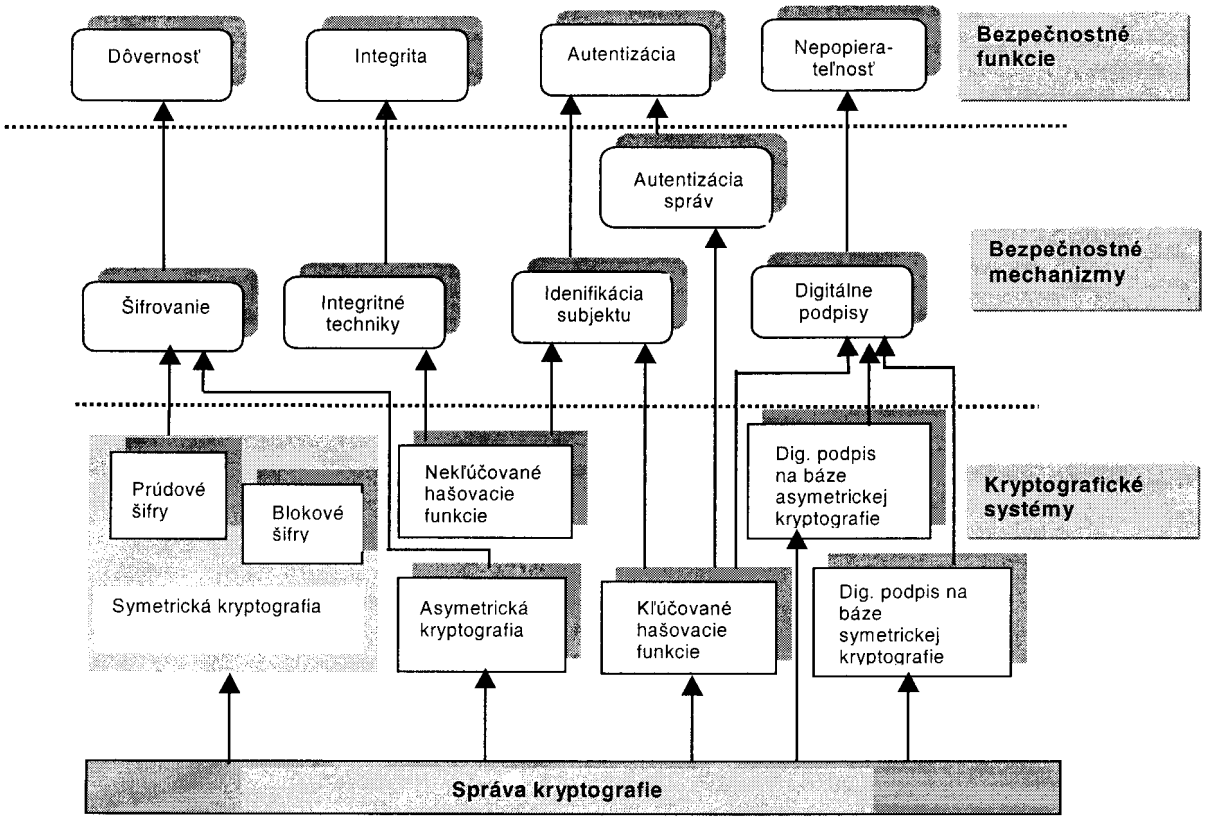
Na obr. 2 vidno prepojenie kryptografického systému s bezpečnostnými funkciami, ktoré zabezpečuje pomocou bezpečnostných mechanizmov, pričom kľúčový management (správa kryptografie) tvorí základ celého systému.

Najlepšie je realizovať kompletné bezpečnostné služby pomocou kryptografického modulu (či už v podobe HW alebo SW), ktorý možno umiestniť na vstupných bodoch otvoreného prenosového systému. Model správy s použitím kryptografického a nekryptografického kódu je definovaný v [2] pomocou módov, označovaných ako mód B0 a B1.

Pri výbere kryptografickej techniky pre uvedené módy treba vziať do úvahy špecifikácie prenosu v rámci otvoreného systému, čo vyžaduje splnenie požiadaviek na:

- rýchlosť algoritmu,
- bezpečnosť algoritmu,
- praktickú realizovateľnosť algoritmu.

V prípade módu B0 je odporúčaný nekryptografický bezpečnostný kód, pomocou ktorého sa zakódujú užívateľské aj prídavné dáta bezpečného prenosového systému. Medzi nekryptografické bezpečnostné kódy možno zaradiť nekľúčované, lineárne, hašovacie, blokové kódy, ktoré možno porovnať s technikami na zabezpečenie integrity údajov. Tieto techniky slúžia na zachovanie autenticity správy. Hašovacie funkcie musia spĺňať požiadavky jednocestnosti (*one-way function*). Ich úlohou je vytvorenie tzv. otlačku správy (*message digest*) pevnej dĺžky. Ak by sme v správe zmenili jeden bit, na výstupe by sme dostali celkom rozdielny otlačok. Medzi najvýznamnejšie hašovacie funkcie, ktoré možno použiť za týmto účelom funkcie typu MD (MD4, MD5), SHA (SHA-1, SHA-256, SHA-384, SHA-512 alebo RIPEMD (RIPEMD-160). Okrem nekľúčovaných hašovacích funkcií možno na zachovanie autenticity použiť aj



Obr.2 Kryptografia, bezpečnostné mechanizmy a bezpečnostné funkcie

kľúčované hašovacie kódy, akým je napr. MAC (*Message Authentication Code*) kód.

Model správy v prenosovom systéme podľa módu B1 okrem nekryptografického kódu odporúča použiť aj kryptografický kód na zachovanie dôvernosti správ. Požiadavku dôvernosti správy z dôvodu vyššej rýchlosti lepšie spĺňajú šifrovacie algoritmy pracujúce na báze systému s tajným kľúčom, v porovnaní so systémom s verejným kľúčom. V súčasnosti existuje množstvo symetrických šifrovacích algoritmov, ktoré sú uznávané odbornou verejnosťou. V norme [2] je za týmto účelom odporúčaný etalón symetrickej kryptografie - algoritmus DES, ktorý je celosvetovou normou viac ako 20 rokov. Jeho výhody sú:

- rýchlosť šifrovania/dešifrovania,
- cyklický charakter algoritmu (viac vhodné pre HW realizáciu),
- jeden algoritmus pre šifrovanie aj dešifrovanie.

Algoritmus DES v súčasnej dobe však už nepatrí medzi výpočtovo bezpečné šifry. O bezpečnosti algoritmu DES stručne pojednáva kapitola 3.1.

Uvedené výhody algoritmu sa väčšinou stali základom algoritmov, ktoré postupne nahradzujú DES. Perspektívne treba počítať s voľbou niektorého z nich. Odbornou verejnosťou bol za štandard tohto tisícročia v súťaži s pracovným názvom AES (*Advanced Enryption Standard*) vybraný algoritmus Rijndael. Autormi algoritmu sú Belgičania dr. Joan Daemen a dr. Vincent Rijmen [11]. Je to iteračná bloková šifra, ktorá používa opakujúce sa kolá s variabilnou dĺžkou bloku a variabilnou dĺžkou kľúča. Dĺžka vstupného a výstupného bloku je definovaná 128 bitmi, ale šifra môže podporovať aj bloky väčších dĺžok. Dĺžka kľúča je voliteľná 128, 192 alebo 256 bitov. Základom algoritmu sú operácie v rôznych algebraických štruktúrach. Pracuje s prvkami $GF(2^8)$ a s polynómami, ktorých prvky sú z $GF(2^8)$. Príslušné operácie s nimi možno prevádzať tabuľkovo (vhodné pre softwarovú implementáciu) alebo priamo výpočtom (vhodné pre hardwarovú implementáciu). Rijndael bol implementovaný na rozličných procesoroch s veľmi malými nárokmi na pamäť aj veľkosť kódu, napr. na čipových kartách a špecializovanom hardvéri. Je vhodný aj pre paralelné spracovanie. Z hľadiska bezpečnosti je Rijndael kryptosystém, u ktorého z pohľadu kryptoanalýzy neexistuje žiaden efektívny algoritmus na jeho prelomenie. Pri návrhu algoritmu boli vzaté do úvahy známe útoky a samotný algoritmus bol navrhnutý tak, aby týmto útokom čo najefektívnejšie odolával. Rijndael bol testovaný na existenciu slabých kľúčov DES-ovského typu, slabých kľúčov typu IDEA, na odolnosť voči diferenciálnej a lineárnej kryptoanalýze, *Truncated Differentials Attack*, *Square Attack*, interpolačnému útoku a útoku pomocou príbuzných kľúčov. Na Rijndael s redukovaným počtom kôl možno zaútočiť efektívnejšie, Rijndael s plným počtom kôl sa ukázal byť dostatočne odolný voči známym kryptoanalytickým útokom. Operácie použité v

Rijndaeli sú typu, ktorý sa dá najľahšie ochraňovať proti tzv. *Power a Timing attacks* (v prvom prípade ide o útoky založené na zvyšovaní napájacieho napätia a skúmaní správania systému, v druhom o útoky založené na časovej analýze výpočtu a odvodzovania možných hodnôt parametrov z dĺžky trvania vykonávaných výpočtov/operácií.) Použitie maskovacích techník na ochranu Rijndaelu proti týmto útokom nespôsobuje výraznejšie zhoršenie výkonu, ani podstatné zvýšenie nárokov na pamäť.

Algoritmus Rijndael sa môže použiť ako symetrická blokovú šifra, ale je možné jeho použitie aj pre iné aplikácie:

- ako bloková šifra v CBC-MAC (*Cipher Block Chaining*) algoritme,
- ako iteračná hašovacia funkcia, pričom samotný algoritmus slúži ako kolová funkcia,
- pomocou OFB (*Output Feedback*) módu možno Rijndael použiť ako synchrónnu prúdovú šifru, resp. v CFB (*Cipher Feedback*) móde ako samosynchronizujúcu prúdovú šifru,
- pomocou algoritmu Rijndael možno vytvoriť generátor pseudonáhodných čísel.

Na zachovanie neporušiteľnosti správy možno v rámci módu B1 použiť z kryptografických mechanizmov digitálny podpis, ktorý sa najčastejšie realizuje na báze asymetrickej kryptografie v kombinácií s hašovacími funkciami. Z asymetrických šifrovacích algoritmov sa stále za výpočtovo bezpečnú šifru považuje algoritmus RSA (*Rivest-Shamir-Adelman*). Asymetrická kryptografia je nutná aj pri bezpečnom prenose kľúča symetrickej šifry.

3.1. BEZPEČNOŤ KRYPTOGRAFICKÝCH MECHANIZMOV

Úroveň bezpečnosti kryptografických mechanizmov sa kvantifikuje pomocou niekoľkých modelov bezpečnosti [12], z ktorých sa v praxi najviac používa pojem výpočtovej bezpečnosti, ktorá je založená na výpočte šifrovacej a dešifrovacej zložitosti šifry. Za výpočtovo bezpečné šifry sa pokladajú také šifry, ktorá sú pre kryptoanalytika nerozlomiteľné útokom hrubou silou (*brute force attack*), ani inými známymi metódami kryptoanalýzy. V súčasnosti sa pokladajú za výpočtovo bezpečné šifry s exponenciálnou zložitosťou. Okrem útoku hrubou silou dnes existujú iné efektívne kryptoanalytické útoky, založené hlavne na lineárnej a diferenciálnej kryptoanalýze.

Blokové symetrické šifry odporúčané podľa [2] sú šifry s digitálnou substitúciou, preto sú zraniteľné klasickou frekvenčnou analýzou blokov. Pre bezpečnosť blokových šifier sa vyžaduje použitie veľkých blokov otvoreného textu. Kľúč musí byť utajený a počas celej doby používania odolný proti kryptoanalytickým útokom (čo vedie na veľký počet bitov kľúča).

Ako príklad, už výpočtovo nie bezpečnej šifry, uveďme blokovú šifru DES.
Hlavné bezpečnostné slabiny algoritmu DES sú:

- **kľúč**

Algoritmus DES so svojim 56-bitovým kľúčom poskytuje 2^{56} (približne 10^{17}) možností, na rozlomenie útokom hrubou silou. Z tejto množiny kľúčov, treba vylúčiť tzv. slabé, poloslabé a potenciálne slabé kľúče (podrobnejšie v [12]). Mnoho kryptografov už v počiatkoch vzniku DES odporúčalo dlhší kľúč minimálne 112 bitov. Od roku 1990 sú vyvíjané rôzne lúštiteľské počítače na rozlomenie algoritmu DES. V r. 1993 M. Wiener navrhol počítač, ktorý metódou hrubej sily by DES rozlomil za 3,5 hodiny. V súčasnej dobe existujú aj iné metódy rozlomenia DES založené na diferenčnej a lineárnej kryptoanalýze.

- **počet rúnd**

DES algoritmus používa dve dôležité črty „dobrej šifry" – *diffusion* (rozptýlenie) a *confusion* (chaos). Jadro algoritmu je nemenné a opakuje sa v 16 rundách (kolách), z dôvodu získania slabej korelácie medzi otvoreným a zašifrovaných textom. Algoritmus s menším počtom rúnd je možné rozlúštiť omnoho účinnejšou metódou lúštenia pomocou otvoreného textu, než útokom hrubou silou. Algoritmus s väčším počtom rúnd ako 16, by bol z tohoto pohľadu ešte účinnejší.

- **S-boxy**

NSA (*National Security Agency*) bola obvinená z modifikácie vnútornej štruktúry S-boxov. Odborná verejnosť venovala hodne pozornosti analýze S-boxov a podrobuje ich skúškam. Boli v nich nájdené aj také štruktúry, ktoré môžu odolnosť lúštenia šifry znížiť, napr. slabá nelinearita.

Ak by sme chceli matematicky vyjadriť pravdepodobnosť zlyhania dešifrovacieho algoritmu blokovej šifry, treba vychádzať z úvahy, že kódové slovo je definované ako skupina bitov. Ak predpokladáme, že sú použité korekčné kódy a chyby na výstupe prijímača sú nezávislé, je pravdepodobnosť chyby kódového slova p_w daná

$$p_w = 1-(1-p_b)^k, \tag{16}$$

kde

k je počet bitov na jedno kódové slovo,

P_b je pravdepodobnosť chybného bitu.

Ak je na výstupe prijímača šifrovaný text, označme pravdepodobnosť chyby na výstupe dešifrátora p_{cw}. Pre synchrónnu šifru je $p_w=p_{cw}$. Pre blokové šifry spôsobí šírenie chýb zvýšenie p_{cw} oproti p_w. V konvenčných blokových šifrách je obvykle otvorený text s n - bitmi komprimovaný na celý počet k - bitových slov. Na základe uvedených úvah možno priemernú pravdepodobnosť chyby kryptografického slova pre blokovú šifru podľa [13] aproximovať :

$$\overline{p}_{cw} \approx (1-2^{-n})^{-1}(1-2^{-k})\left[1-(1-p_b)^n\right]. \tag{17}$$

Čo po rozvoji do Taylorovho radu dáva výsledok

$$\overline{p}_{cw} \approx (1-2^{-n})^{-1}(1-2^{-k})np_b. \tag{18}$$

Presnosť vzťahu (17) je vyhovujúca, ak :

$$p_b << 2(n-1)^{-1}. \quad (18)$$

Priemerná súborová pravdepodobnosť chyby bitu pre blokovú šifru vo vzťahoch (17), (18) sa získa dosadením za k=1. Aby sa dosiahla ochrana proti frekvenčnej analýze vzoriek blokov sa obvykle vyžaduje, aby n≥k (odporúča sa voliť n≥4k).

5. ZÁVER

Cieľom tohto príspevku bola bezpečnostná analýza mechanizmov vhodných na ochranu dôvernosti, integrity a nepopierateľnosti správ prenášaných v rámci uzatvorených a otvorených prenosových systémov medzi železničnými zabezpečovacími zariadeniami.

Sú naznačené nekonvenčné spôsoby použitia kanálových kódovacích techník z množiny samoopravných FEC kódov, z ktorých sa, vzhľadom na špecifikum prenosu, ako perspektívne javia RS kódy. Bol zosumarizovaný matematický aparát na výpočet pravdepodobnosti chyby dekódovacích, syndrómových techník blokových, lineárnych, systematických kódov.

Pre prenosové systémy súvisiace s bezpečnosťou sú naznačené možnosti výberu kryprografického a hašovacieho kódu so zameraním na výpočtovo bezpečné algoritmy.

Pre železničné aplikácie, vzhľadom na špecifikáciu prenosu, sú vhodné rýchle algoritmy symetrických bokových šifier v kombinácií s blokovými hašovacími funkciami, pričom je nutné venovať pozornosť problematike kľúčového hospodárstva a výpočtu pravdepodobnosti chyby kryptografického slova v dešifrátore.

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, april 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, máj 2002

[3] Hanáček, P., Staudek, J.: Bezpečnost informačních systému, metodická príručka, Úřad pro státní informační systém, 2000

[4] Franeková, M.: Konvolučné kódovacie štruktúry, dizertačná práca, Žilina, 1995

[5] Muzikářová L., Franeková M. : Konvolučné kódy s použitím Viterbiho algoritmu, Medzinárodná vedecká konferencia VŠDS *Elektro 95*, Žilina. str.77-83

[6] Farkaš, P.: Kódovanie a modulácie, STU, Bratislava, 1993

[7] Hrdina, Z.,Vejražka, F.: Digitální radiová komunikace, ČVUT, Praha, 1994

[8] Clark, G., Cain, B.: Error-Correction Coding for digital Communications, Olenum Press, New York, 1988

[9] Franeková, M., Bubeníková, E.: The calculation of the probability of undetected sequence error for ARQ systems, MOSIS 2000, Rožnov pod Radhoštem, ČR, s. 203-208

[10] Menezes, A., van Oorschot, Vastone,S.:Handbook for Applied Cryptography, CRC Press, 1996

[11] Daemen, J., Rijmen, V.: AES Proposal: Rijndael, Leuven, Belgicko, 2002

[12] Přibyl, J., Kodl, J.: Ochrana dat v informatice, ČVUT, Praha, 1996

[13] Bagnall,P.,Briscoe,A.Poppitt: Axonomy of communications requirements for large-scale multicast applications, Internet Draft, IETF, 2002