# PŘIHLÁŠKA VYNÁLEZU

**zveřejněná podle § 31 zákona č. 527/1990 Sb.**


(19) ČESKÁ REPUBLIKA

ÚŘAD PRŮMYSLOVÉHO VLASTNICTVÍ

(22) Přihlášeno: **21.07.2004**

(40) Datum zveřejnění přihlášky vynálezu: **11.01.2006**
**(Věstník č. 1/2006)**

(21) Číslo dokumentu:

**2004-826**

(13) Druh dokumentu: **A3**

(51) Int. Cl.:

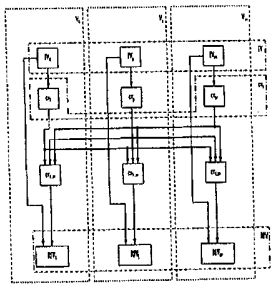
| | |
|---|---|
| ***B61L 23/16*** | (1968.09) |
| ***B61L 1/18*** | (1968.09) |
| ***B61L 29/00*** | (1968.09) |
| ***B61L 3/08*** | (1968.09) |

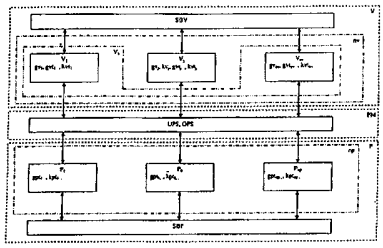


(71) Přihlašovatel:
AŽD Praha s. r. o., Praha, CZ

(72) Původce:
Klapka Štěpán RNDr. PhD, Praha, CZ
Srb Stanislav Ing. PhD, Praha, CZ
Houser Jiří Ing., Praha, CZ
Pšenička Pavel Ing., Praha, CZ
Švejda Jaromír Ing., Lysá nad Labem, CZ
Novák Vladimír Ing., Mníšek pod Brdy, CZ
Doubek Pavel Ing., Praha, CZ
Faran Pavel PhD, Praha, CZ

(74) Zástupce:
ing. Marie Smrčková, patentový zástupce, Velflíkova 8, Praha 6, 16000



(54) Název přihlášky vynálezu:

## Způsob bezpečného přenosu informací


(57) Anotace:

Způsob bezpečného přenosu informací se provádí tak, že ve vysílači (V), konfigurovaném systémem minimálního počtu (mv) větví z počtu (nv) všech možných větví vysílače (V), je rozložen postup vytvoření a kontroly rozšířené informační zprávy (RIV) tak, že využitím systému generujících polynomů ($gv_{1..nv}$) všech možných větví jsou z informační zprávy (IV) vytvořeny příslušné kontrolní části ($cv_{1..nv}$) všech možných větví a následně k ní připojeny. Po přenosu rozšířené informační zprávy (RIV) prostřednictvím přenosového média (PM) se v přijímači (P), konfigurovaném systémem minimálního počtu (mp) větví z počtu (np) všech možných větví, pomocí systému ověřovacích generujících polynomů ($gpt_{1..np,1..nv,1..fp}$) a odpovídajícího systému ověřovacích konstantních zbytků po dělení ($kpt_{1..np,1..nv,1..fp}$) po dělení příslušnými generujícími polynomy kontroluje, zda příslušné kontrolní části ($cv_{1..nv}$) všech možných větví vysílače (V) přidané do rozšířené informační zprávy (RIV) odpovídají informační zprávě (IV) vysílače (V). V případě pozitivního výsledku této kontroly je umožněno méně restriktivní využití informační zprávy (IV) v přijímači (P).



CZ 2004 - 826 A3

PV 2004-826

# Způsob bezpečného přenosu informací

## Oblast techniky

Vynález se týká způsobu bezpečného přenosu informací v železniční zabezpečovací technice, kde je při nezajištění bezpečnosti přenosu vyžadován restriktivní stav.

## Dosavadní stav techniky

V železniční zabezpečovací technice je až dosud většinou používáno při zabezpečení přenášené informační zprávy řešení, kdy je informační zpráva v každé větvi samostatně zabezpečena, nezávisle přenášena a v každé větvi po příjmu kontrolována. Komparátor s vlastní bezpečností zajišťuje restriktivní stav při nesouladu jednotlivých komparovaných informačních zpráv náležejících jednotlivým větvím například tak, že informační zpráva není použita, nebo dojde k odpojení napájecí energie výstupním obvodům vysílače, přijímače nebo celého systému. Nevýhoda tohoto řešení spočívá v problémové souvislosti mezi porovnávanými daty a datovým tokem informační zprávy na výstupu vysílače a přijímače, což v některých případech vyžaduje vysoký stupeň synchronizace jednotlivých větví a může zásadně omezovat přenosovou kapacitu.

## Podstata vynálezu

Výše uvedené nevýhody doposud známých řešení se odstraní nebo podstatně omezí způsobem bezpečného přenosu informací podle tohoto vynálezu, jehož podstata spočívá v tom, že při přenosu informační zprávy vysílače, který je konfigurován systémem minimálního počtu větví ze všech možných větví, směrem k přijímači, rozloží postup vytvoření a kontroly rozšířené informační zprávy sledované j-té větve vysílače, na první krok tak, že z informační zprávy sledované j-té větve vysílače je pomocí generujícího polynomu sledované j-té větve vysílače vytvořena kontrolní část sledované j-té větve vysílače, která je jednak poskytnuta pro druhý krok všem sousedním větvím vysílače, a zároveň je ve druhém kroku spolu s příslušnými kontrolními částmi od sousedních větví vysílače připojena k informační zprávě sledované j-té větve vysílače, čímž je vytvořena rozšířená informační zpráva sledované j-té větve vysílače, v důsledku čehož je zaručeno, že informační zpráva sledované j-té větve vysílače a příslušná kontrolní část sledované j-té větve vysílače je dělitelná generujícím polynomem sledované j-té větve vysílače s konstantním zbytkem po dělení příslušným generujícím polynomem sledované j-té větve vysílače, načež je ve třetím kroku provedena kontrola, zda kontrolní části od sousedních větví vysílače jsou přidávány do rozšířené informační zprávy sledované j-té větve vysílače a zda odpovídají informační zprávě sledované j-té větve vysílače tak, že tato kontrola je pomocí systému ověřovacích generujících polynomů sledované j-té větve vysílače a odpovídajícího systému ověřovacích konstantních zbytků po dělení příslušnými generujícími polynomy sledované j-té větve vysílače provedena v daném počtu fází ověřování vysílače umožňujících nezávislost systému ověřovacích generujících polynomů sledované j-té větve vysílače a systému generujících polynomů všech

možných větví vysílače, přičemž pokud nenastane shoda kontroly alespoň v minimálním počtu větví zmenšených o jedna ze všech možných větví vysílače zmenšených o jedna, není rozšířená informační zpráva sledované j-té větve vysílače dále zpracovávána a ani nikam zasílána, přičemž v případě, že některá z příslušných kontrolních částí od sousedních větví vysílače neodpovídá informační zprávě sledované j-té větve vysílače, je v systému indikována chyba, případně dojde k rekonfiguraci systému vysílače, nebo pokud nebylo shodných výsledků kontrol dosaženo alespoň v minimálním počtu větví ze všech možných větví vysílače, je detekována chyba na straně celého vysílače a musí být vyvozena příslušná bezpečná reakce vedoucí k restrikci, kdežto pokud shoda kontroly nastane, je ve čtvrtém kroku rozšířená informační zpráva sledované j-té větve vysílače přenášena prostřednictvím přenosového média, které je charakterizováno jako uzavřený přenosový systém, do sledované k-té větve přijímače, který je konfigurován systémem minimálního počtu větví ze všech možných větví, načež je v pátém kroku ve sledované k-té větvi přijímače pomocí systému ověřovacích generujících polynomů sledované k-té větve přijímače a odpovídajícího systému ověřovacích konstantních zbytků po dělení příslušnými generujícími polynomy sledované k-té větve přijímače v daném počtu fází ověřování přijímače umožňujících nezávislost systému ověřovacích generujících polynomů sledované k-té větve přijímače a systému generujících polynomů všech možných větví vysílače prováděna kontrola, zda kontrolní části všech možných větví vysílače přidané do přijaté rozšířené informační zprávy sledované j-té větve vysílače odpovídají informační zprávě sledované j-té větve vysílače alespoň v minimálním počtu větví ze všech možných větví vysílače s tím, že pokud nastane shoda těchto kontrol alespoň v minimálním počtu větví ze všech možných větví přijímače, je možno použít při dalším zpracování informační zprávy vysílače méně restriktivní postupy, zatímco při potřebě přenosu informační zprávy přijímače směrem k vysílači je způsob zabezpečení proveden analogicky, pouze je použit odlišný soubor systémů generujících polynomů a jim odpovídající odlišný soubor systémů konstantních zbytků po dělení příslušnými generujícími polynomy.

Výše uvedené nevýhody jsou rovněž odstraněny tak, že pokud je zapotřebí rozšířenou informační zprávu sledované j-té větve vysílače přenášet k přijímači prostřednictvím přenosového média charakterizovaného jako otevřený přenosový systém, rozšiřuje se ve vysílači čtvrtý krok postupem s využitím blokové šifry v zřetězeném módu CBC, kdy je z informační zprávy sledované j-té větve vysílače doplněné nulami tak, aby její celková délka byla dělitelná délkou bloku první blokové šifry, pomocí prvního klíče a zřetězeného módu CBC první blokové šifry s prvním inicializačním vektorem vytvořen otisk informační zprávy sledované j-té větve vysílače, s cílem dále jej využít jako druhý inicializační vektor pro zašifrování kontrolních částí všech možných větví vysílače pomocí zřetězeného módu CBC druhé blokové šifry s druhým klíčem s tím, že před zašifrováním jsou kontrolní části všech možných větví vysílače opět doplněny nulami tak, aby jejich celková délka byla dělitelná délkou bloku druhé blokové šifry, čímž se zašifrované kontrolní části všech možných větví vysílače stávají autentizační částí sledované j-té větve vysílače, která je místo nich připojena k informační zprávě sledované j-té větve vysílače a jako autentická informační zpráva sledované j-té větve vysílače je pak přenášena přes otevřený přenosový systém do sledované k-té větve přijímače, kde je z autentické informační zprávy sledované j-té větve vysílače pomocí první blokové šifry s prvním klíčem a druhé blokové šifry s druhým klíčem dešifrována autentizační část

sledované j-té větve vysílače, čímž se zpět získá rozšířená informační zpráva sledované j-té větve vysílače složená z informační zprávy sledované j-té větve vysílače a kontrolních částí všech možných větví vysílače, která je dále v pátém kroku shodným způsobem zpracovávána a kontrolována, přičemž tato kontrola ověřuje správnost funkce šifrování ve vysílači a dešifrování v přijímači.

Hlavní výhoda způsobu bezpečného přenosu informací podle tohoto vynálezu spočívá v tom, že postup vytváření a následné kontroly informační zprávy v jednotlivých větvích je rozložen tak, že pro vlastní kontrolu neporušenosti přenesené informační zprávy není nutné znát postup vytváření kontrolní části, což zásadně snižuje pravděpodobnost vytvoření autentické zprávy při kontrole a to jak ve vysílači, tak v přijímači. Potřebná diverzita jednotlivých větví je zaručena postupem vytváření kontrolních částí ve vysílači, případně rozšířena kontrolou ve vysílači a přijímači.

Pro vytváření a ověření kontrolní části je místo systému generujících polynomů možné použít jiné vhodné metody splňující výše uvedené požadavky na nezávislost. Touto vhodnou metodou může být například systém generujících a kontrolních matic.

Kontrolu informační zprávy prováděnou ve třetím kroku ve vysílači je možné případně vypustit, protože bezpečnost přenosu je zajištěna především způsobem vytvoření rozšířené informační zprávy ve vysílači a následné kontroly neporušenosti přijaté zprávy v přijímači.

## Přehled obrázků na výkresech

Vynález je objasněn pomocí zobecněného schematického výkresu základního provedení dle obr. 1.

Na obr. 2 je zobrazen konkrétní příklad možné konfigurace vysílače a přijímače, kde vysílač je konfigurován pro minimální počet dvou větví ze tří větví všech možných větví vysílače a dvou fází ověřování, kdežto přijímač je konfigurován pro minimální počet dvou větví ze dvou větví všech možných větví přijímače a dvou fází ověřování.

Na obr. 3 je schematicky zobrazen způsob vytváření rozšířené informační zprávy.

Na obr. 4 je schematicky zobrazen způsob vytváření autentické informační zprávy.

## Příklady provedení vynálezu

Způsob bezpečného přenosu informací je zřejmý ze zobecněného schématického výkresu základního provedení uvedeného na obr. 1 ze kterého je zřejmé, že při přenosu informační zprávy **IV** vysílače **V**, který je konfigurován systémem minimálního počtu **mv** větví z počtu **nv** všech možných větví vysílače **V**, směrem k přijímači **P** se rozloží postup vytvoření a kontroly rozšířené informační zprávy $\mathbf{RIV}_j$ sledované j-té větve $\mathbf{V}_j$ vysílače **V**, na první krok tak, že z informační zprávy $\mathbf{IV}_j$ sledované j-té větve $\mathbf{V}_j$ vysílače **V** je pomocí generujícího polynomu $\mathbf{gv}_j$

sledované j-té větve $V_j$ vysílače V vytvořena kontrolní část $cv_j$ sledované j-té větve $V_j$ vysílače V, která je jednak poskytnuta pro druhý krok všem sousedním větvím $V_s$ vysílače V, a zároveň je ve druhém kroku spolu s příslušnými kontrolními částmi $cv_s$ od sousedních větví $V_s$ vysílače V připojena k informační zprávě $IV_j$ sledované j-té větve $V_j$ vysílače V. Tím je vytvořena rozšířená informační zpráva $RIV_j$ sledované j-té větve $V_j$ vysílače V, v důsledku čehož je zaručeno, že informační zpráva $IV_j$ sledované j-té větve $V_j$ vysílače V a příslušná kontrolní část $cv_j$ sledované j-té větve $V_j$ vysílače V je dělitelná generujícím polynomem $gv_j$ sledované j-té větve $V_j$ vysílače V s konstantním zbytkem $kv_j$ po dělení příslušným generujícím polynomem sledované j-té větve $V_j$ vysílače V.

Ve třetím kroku je provedena kontrola, zda kontrolní části $cv_s$ od sousedních větví $V_s$ vysílače V jsou přidávány do rozšířené informační zprávy $RIV_j$ sledované j-té větve $V_j$ vysílače V a zda odpovídají informační zprávě $IV_j$ sledované j-té větve $V_j$ vysílače V tak, že tato kontrola je pomocí systému ověřovacích generujících polynomů $gvt_{j,s,1..fv}$ sledované j-té větve $V_j$ vysílače V a odpovídajícího systému ověřovacích konstantních zbytků $kvt_{j,s,1..fv}$ po dělení příslušnými generujícími polynomy sledované j-té větve $V_j$ vysílače V provedena v daném počtu fází ověřování vysílače V umožňujících nezávislost systému ověřovacích generujících polynomů $gvt_{j,s,1..fv}$ sledované j-té větve $V_j$ vysílače V a systému generujících polynomů $gv_{1..nv}$ všech možných větví vysílače V.

Pokud nenastane shoda kontroly alespoň v minimálním počtu mv větví zmenšených o jedna z počtu nv všech možných větví vysílače V zmenšených o jedna, není rozšířená informační zpráva $RIV_j$ sledované j-té větve $V_j$ vysílače V dále zpracovávána a ani nikam zasílána. V případě, že některá z příslušných kontrolních částí $cv_s$ od sousedních větví $V_s$ vysílače V neodpovídá informační zprávě $IV_j$ sledované j-té větve $V_j$ vysílače V, je v systému indikována chyba, případně dojde k rekonfiguraci systému vysílače V. Pokud nebylo shodných výsledků kontrol dosaženo alespoň v minimálním počtu mv větví z počtu nv všech možných větví vysílače V, je detekována chyba na straně celého vysílače V a musí být vyvozena příslušná bezpečná reakce vedoucí k restrikci.

Pokud shoda kontroly nastane, je ve čtvrtém kroku rozšířená informační zpráva $RIV_j$ sledované j-té větve $V_j$ vysílače V přenášena prostřednictvím přenosového média PM, které je charakterizováno jako uzavřený přenosový systém UPS, do sledované k-té větve $P_k$ přijímače P, který je konfigurován systémem minimálního počtu mp větví z počtu np všech možných větví přijímače P.

Načež je v pátém kroku ve sledované k-té větvi $P_k$ přijímače P pomocí systému ověřovacích generujících polynomů $gpt_{k,1..nv,1..fp}$ sledované k-té větve $P_k$ přijímače P a odpovídajícího systému ověřovacích konstantních zbytků $kpt_{k,1..nv,1..fp}$ po dělení příslušnými generujícími polynomy sledované k-té větve $P_k$ přijímače P v daném počtu fází ověřování přijímače P umožňujících nezávislost systému ověřovacích generujících polynomů $gpt_{k,1..nv,1..fp}$ sledované k-té větve $P_k$ přijímače P a systému generujících polynomů $gv_{1..nv}$ všech možných větví vysílače V prováděna kontrola, zda kontrolní části $cv_{1..nv}$ všech možných větví vysílače V přidané do přijaté rozšířené informační zprávy $RIV_j$ sledované j-té větve $V_j$ vysílače V odpovídají informační zprávě $IV_j$ sledované j-té větve $V_j$ vysílače V alespoň v minimálním počtu mv větví z počtu nv všech možných větví vysílače V s tím, že pokud nastane shoda

těchto kontrol alespoň v minimálním počtu **mp** větví z počtu **np** všech možných větví přijímače **P**, je možno použít při dalším zpracování informační zprávy **IV** vysílače **V** méně restriktivní postupy.

Při potřebě přenosu informační zprávy přijímače **P** směrem k vysílači **V** je způsob zabezpečení proveden analogicky, pouze je použit odlišný soubor systémů generujících polynomů $\mathbf{hv}_{1..np}$, $\mathbf{hvt}_{1..np,1..np,1..fp}$ a $\mathbf{hpt}_{1..nv,1..np,1..fv}$ a jim odpovídající odlišný soubor systémů konstantních zbytků $\mathbf{Iv}_{1..np}$, $\mathbf{Ivt}_{1..np,1..np,1..fp}$ a $\mathbf{Ipt}_{1..nv,1..np,1..fv}$ po dělení příslušnými generujícími polynomy.

Způsob bezpečného přenosu informací je realizován také tak, že pokud je zapotřebí rozšířenou informační zprávu $\mathbf{RIV}_j$ sledované j-té větve $\mathbf{V}_j$ vysílače **V** přenášet k přijímači **P** prostřednictvím přenosového média **PM** charakterizovaného jako otevřený přenosový systém **OPS**, rozšiřuje se ve vysílači **V** čtvrtý krok postupem s využitím blokové šifry v zřetězeném módu CBC, kdy je z informační zprávy $\mathbf{IV}_j$ sledované j-té větve $\mathbf{V}_j$ vysílače **V** doplněné nulami tak, aby její celková délka byla dělitelná délkou bloku první blokové šifry **BS1**, pomocí prvního klíče **BK1** a zřetězeného módu CBC první blokové šifry **BS1** s prvním inicializačním vektorem **BV1** vytvořen otisk $\mathbf{OIV}_j$ informační zprávy sledované j-té větve $\mathbf{V}_j$ vysílače **V**, s cílem dále jej využít jako druhý inicializační vektor **BV2** pro zašifrování kontrolních částí $\mathbf{cv}_{1..nv}$ všech možných větví vysílače **V** pomocí zřetězeného módu CBC druhé blokové šifry **BS2** s druhým klíčem **BK2** s tím, že před zašifrováním jsou kontrolní části $\mathbf{cv}_{1..nv}$ všech možných větví vysílače **V** doplněny nulami tak, aby jejich celková délka byla dělitelná délkou bloku druhé blokové šifry **BS2.** Tím se zašifrované kontrolní části $\mathbf{cv}_{1..nv}$ všech možných větví vysílače **V** stávají autentizační částí $\mathbf{av}_j$ sledované j-té větve $\mathbf{V}_j$ vysílače **V**, která je místo nich připojena k informační zprávě $\mathbf{IV}_j$ sledované j-té větve $\mathbf{V}_j$ vysílače **V** a jako autentická informační zpráva $\mathbf{AIV}_j$ sledované j-té větve $\mathbf{V}_j$ vysílače **V** je pak přenášena přes otevřený přenosový systém **OPS** do sledované k-té větve $\mathbf{P}_k$ přijímače **P**, kde je z autentické informační zprávy $\mathbf{AIV}_j$ sledované j-té větve $\mathbf{V}_j$ vysílače **V** pomocí první blokové šifry **BS1** s prvním klíčem **BK1** a druhé blokové šifry **BS2** s druhým klíčem **BK2** dešifrována autentizační část $\mathbf{av}_j$ sledované j-té větve $\mathbf{V}_j$ vysílače **V**. Tak se zpět získá rozšířená informační zpráva $\mathbf{RIV}_j$ sledované j-té větve $\mathbf{V}_j$ vysílače **V** složená z informační zprávy $\mathbf{IV}_j$ sledované j-té větve $\mathbf{V}_j$ vysílače **V** a kontrolních částí $\mathbf{cv}_{1..nv}$ všech možných větví vysílače **V**, která je dále v pátém kroku shodným způsobem zpracovávána a kontrolována, přičemž tato kontrola ověřuje správnost funkce šifrování ve vysílači **V** a dešifrování v přijímači **P**.

Ze základního provedení uvedeného na obr. 1 vyplývá, že ve vysílači **V** je obecně znázorněna první větev $\mathbf{V}_1$, sledovaná j-tá větev $\mathbf{V}_j$, a poslední větev $\mathbf{V}_{nv}$ ze všech možných větví, přičemž je u každé větve uveden příslušný generující polynom **gv** pro vytváření kontrolní části **cv** a systém ověřovacích generujících polynomů **gvt** a ověřovacích zbytků **kvt** po dělení příslušnými generujícími polynomy, přičemž je znázorněn počet **nv** všech možných větví vysílače **V** a je naznačena množina sousedních větví $\mathbf{V}_s$, zatímco sběrnicí vysílače **SBV** je umožněn oboustranný vzájemný přenos dat mezi všemi větvemi vysílače **V.** Po vytvoření rozšířené informační zprávy **RIV** dochází k jejímu přenosu prostřednictvím přenosového média **PM** do přijímače **P**, v němž je znázorněna první větev $\mathbf{P}_1$, sledovaná k-tá větev $\mathbf{P}_k$ a poslední větev $\mathbf{P}_{np}$ ze všech možných větví, přičemž je u každé větve uveden příslušný systém ověřovacích generujících polynomů **gpt** a ověřovacích zbytků **kpt**

po dělení příslušnými generujícími polynomy použitých pro ověření rozšířené informační zprávy **RIV**, přičemž je znázorněn počet **np** všech možných větví přijímače **P**, zatímco sběrnicí **SBP** přijímače **P** je umožněn oboustranný vzájemný přenos informačních dat mezi všemi větvemi přijímače **P**.

Z příkladu provedení dle obr. 2 je zřejmá realizace vynálezu pro častý případ konfigurace vysílače **V** a přijímače **P**, kdy je ve vysílači **V** provedena konfigurace pro minimální počet dvou větví ze tří větví všech možných větví vysílače **V** a dvou fází ověřování, kdežto přijímač **P** je konfigurován pro minimální počet dvou větví ze dvou větví všech možných větví přijímače **P** a dvou fází ověřování. V uvedeném příkladu provedení je vzájemná komunikace mezi jednotlivými větvemi znázorněna oboustrannými šipkami, z čehož plyne, že se jedná o obousměrný přenos informací mezi jednotlivými větvemi a že se rovněž jedná o oboustranný přenos informací od vysílače **V** k přijímači **P** a naopak. Proto je na uvedeném příkladu provedení použito označení jednotlivých komponent formou zlomku, kdy v čitateli je uveden symbol pro komponentu sloužící pro jeden směr přenosu informací, kdežto ve jmenovateli pro směr opačný.

Ze schematicky zobrazeného způsobu vytváření rozšířené informační zprávy **RIV** uvedeného na obr. 3 vyplývá, že z informační zprávy **IV** jsou v každé větvi vysílače **V** vytvořeny příslušné kontrolní části $\mathbf{cv}_{1..nv}$ všech možných větví vysílače **V** a po výměně mezi větvemi k této informační zprávě **IV** připojeny.

Ze schematicky zobrazeného způsobu vytváření autentické informační zprávy **AIV** uvedeného na obr. 4 vyplývá, že postup vytváření rozšířené informační zprávy **RIV** je rozšířen postupem s využitím blokové šifry, kdy je z informační zprávy **IV** a její kontrolní části $\mathbf{cv}_{1..nv}$ všech možných větví vysílače **V** vytvořena autentizační část, po jejímž připojení k informační zprávě **IV** vznikne autentická informační zpráva **AIV.**

Vytváření kontrolních částí $\mathbf{cv}_{1..nv}$ a jejich následnou kontrolu ve vysílači **V** a přijímači **P** pomocí systému generujících polynomů $\mathbf{gv}_{1..nv}$, systémů ověřovacích generujících polynomů $\mathbf{gvt}_{1..nv,1..nv,1..fv}$ a $\mathbf{gpt}_{1..np,1..nv,1..fp}$ a odpovídajících systémů ověřovacích konstantních zbytků $\mathbf{kvt}_{1..nv,1..nv,1..fv}$ a $\mathbf{kpt}_{1..np,1..nv,1..fp}$ po dělení příslušnými generujícími polynomy je možné nahradit jinou vhodnou metodou, která bude zaručovat požadavek na nezávislost, kdy pro vlastní kontrolu neporušenosti přenesené informační zprávy **IV** není nutné znát postup vytváření kontrolních částí $\mathbf{cv}_{1..nv}$, což zásadně snižuje pravděpodobnost vytvoření autentické zprávy při kontrole a to jak ve vysílači **V** tak v přijímači **P**. Touto vhodnou metodou může být například systém generujících a kontrolních matic.

## Průmyslová využitelnost

Jak plyne z uvedeného popisu, lze způsob bezpečného přenosu informací podle tohoto vynálezu použít jak při nové výstavbě železničních zabezpečovacích zařízení, tak při inovacích stávajících železničních zabezpečovacích zařízení, zejména využitím předmětných bezpečnostně relevantních skutečností. V neposlední

řadě lze vynálezu využít všude tam, kde se vyžaduje zabezpečený přenos informací, jako například v bankovnictví, jaderné energetice a podobně.

PV 2004 - 826

# PATENTOVÉ NÁROKY

1. Způsob bezpečného přenosu informací, **vyznačující se tím**, že

při přenosu informační zprávy (IV) vysílače (V), konfigurovaného systémem minimálního počtu (mv) větví z počtu (nv) všech možných větví vysílače (V), směrem k přijímači (P), se rozloží postup vytvoření a kontroly rozšířené informační zprávy ($RIV_j$) sledované j-té větve ($V_j$) vysílače (V) na první krok tak, že z informační zprávy ($IV_j$) sledované j-té větve ($V_j$) vysílače (V) se pomocí generujícího polynomu ($gv_j$) sledované j-té větve ($V_j$) vysílače (V) vytvoří kontrolní část ($cv_j$) sledované j-té větve ($V_j$) vysílače (V),

kontrolní část ($cv_j$) sledované j-té větve ($V_j$) vysílače (V) se jednak poskytuje pro druhý krok všem sousedním větvím ($V_s$) vysílače (V), a zároveň se ve druhém kroku spolu s příslušnými kontrolními částmi ($cv_s$) od sousedních větví ($V_s$) vysílače (V) připojí k informační zprávě ($IV_j$) sledované j-té větve ($V_j$) vysílače (V), čímž se vytvoří rozšířená informační zpráva ($RIV_j$) sledované j-té větve ($V_j$) vysílače (V), v důsledku čehož je zaručeno, že informační zpráva ($IV_j$) sledované j-té větve ($V_j$) vysílače (V) a příslušná kontrolní část ($cv_j$) sledované j-té větve ($V_j$) vysílače (V) je dělitelná generujícím polynomem ($gv_j$) sledované j-té větve ($V_j$) vysílače (V) s konstantním zbytkem ($kv_j$) po dělení příslušným generujícím polynomem sledované j-té větve ($V_j$) vysílače (V),

načež se ve třetím kroku provádí kontrola, zda kontrolní části ($cv_s$) od sousedních větví ($V_s$) vysílače (V) jsou přidávány do rozšířené informační zprávy ($RIV_j$) sledované j-té větve ($V_j$) vysílače (V) a zda odpovídají informační zprávě ($IV_j$) sledované j-té větve ($V_j$) vysílače (V) tak, že tato kontrola se pomocí systému ověřovacích generujících polynomů ($gvt_{j,s,1..fv}$) sledované j-té větve ($V_j$) vysílače (V) a odpovídajícího systému ověřovacích konstantních zbytků ($kvt_{j,s,1..fv}$) po dělení příslušnými generujícími polynomy sledované j-té větve ($V_j$) vysílače (V) provádí v daném počtu fází ověřování vysílače (V) umožňujících nezávislost systému ověřovacích generujících polynomů ($gvt_{j,s,1..fv}$) sledované j-té větve ($V_j$) vysílače (V) a systému generujících polynomů ($gv_{1..nv}$) všech možných větví vysílače (V), přičemž pokud nenastává shoda kontroly alespoň v minimálním počtu (mv) větví zmenšených o jedna z počtu (nv) všech možných větví vysílače (V) zmenšených o jedna, rozšířená informační zpráva ($RIV_j$) sledované j-té větve ($V_j$) vysílače (V) se dále nezpracovává a ani nikam nezasílá, přičemž v případě, že některá z příslušných kontrolních částí ($cv_s$) od sousedních větví ($V_s$) vysílače (V) neodpovídá informační zprávě ($IV_j$) sledované j-té větve ($V_j$) vysílače (V), v systému se indikuje chyba, případně dojde k rekonfiguraci systému vysílače (V), nebo pokud nebylo shodných výsledků kontrol dosaženo alespoň v minimálním počtu (mv) větví z počtu (nv) všech možných větví vysílače (V), se detekuje chyba na straně celého vysílače (V) a musí se vyvodit příslušná bezpečná reakce vedoucí k restrikci, kdežto

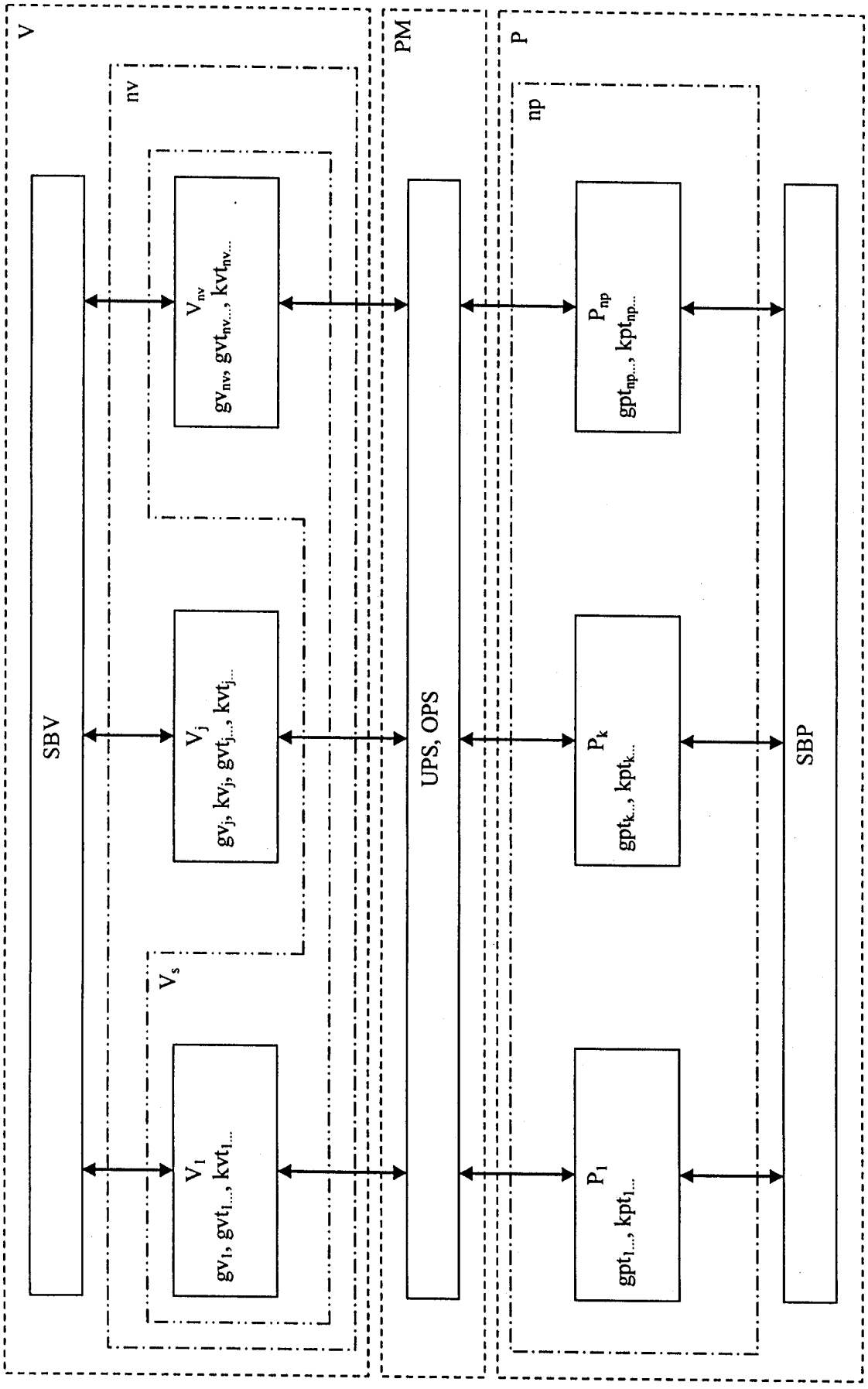
pokud shoda kontroly nastane, ve čtvrtém kroku se rozšířená informační zpráva ($RIV_j$) sledované j-té větve ($V_j$) vysílače (V) přenáší prostřednictvím přenosového média (PM), charakterizovaného jako uzavřený přenosový systém (UPS), do sledované k-té větve ($P_k$) přijímače (P), konfigurovaného systémem minimálního počtu (mp) větví z počtu (np) všech možných větví,

načež v pátém kroku ve sledované k-té větvi ($P_k$) přijímače (P) pomocí systému ověřovacích generujících polynomů ($gpt_{k,1..nv,1..fp}$) sledované k-té větve ($P_k$) přijímače (P) a odpovídajícího systému ověřovacích konstantních zbytků ($kpt_{k,1..nv,1..fp}$) po dělení příslušnými generujícími polynomy sledované k-té větve ($P_k$) přijímače (P) v daném počtu fází ověřování přijímače (P) umožňujících nezávislost systému ověřovacích generujících polynomů ($gpt_{k,1..nv,1..fp}$) sledované k-té větve ($P_k$) přijímače (P) a systému generujících polynomů ($gv_{1..nv}$) všech možných větví vysílače (V) [redacted] provádí kontrola, zda kontrolní části ($cv_{1..nv}$) všech možných větví vysílače (V) přidané do přijaté rozšířené informační zprávy ($RIV_j$) sledované j-té větve ($V_j$) vysílače (V) odpovídají informační zprávě ($IV_j$) sledované j-té větve ($V_j$) vysílače (V) alespoň v minimálním počtu (mv) větví z počtu (nv) všech možných větví vysílače (V) s tím, že pokud nastane shoda těchto kontrol alespoň v minimálním počtu (mp) větví z počtu (np) všech možných větví přijímače (P), je možno použít při dalším zpracování informační zprávy (IV) vysílače (V) méně restriktivní postupy, zatímco při potřebě přenosu informační zprávy přijímače (P) směrem k vysílači (V) se způsob zabezpečení provádí analogicky, pouze se používá odlišný soubor systémů generujících polynomů ($hv_{1..np}$), ($hvt_{1..np,1..np,1..fp}$) a ($hpt_{1..nv,1..np,1..fv}$) a jim odpovídající odlišný soubor systémů konstantních zbytků ($lv_{1..np}$), ($lvt_{1..np,1..np,1..fp}$) a ($lpt_{1..nv,1..np,1..fv}$) po dělení příslušnými generujícími polynomy.

2. Způsob bezpečného přenosu informací podle nároku 1, **vyznačující se tím**, že
pokud je zapotřebí rozšířenou informační zprávu ($RIV_j$) sledované j-té větve ($V_j$) vysílače (V) přenášet k přijímači (P) prostřednictvím přenosového média (PM), charakterizovaného jako otevřený přenosový systém (OPS),
rozšiřuje se ve vysílači (V) čtvrtý krok postupem s využitím blokové šifry v zřetězeném módu CBC, kdy se vytvoří z informační zprávy ($IV_j$) sledované j-té větve ($V_j$) vysílače (V) doplněné nulami tak, aby její celková délka byla dělitelná délkou bloku první blokové šifry (BS1), pomocí prvního klíče (BK1) a zřetězeného módu CBC první blokové šifry (BS1) s prvním inicializačním vektorem (BV1) otisk informační zprávy ($OIV_j$) sledované j-té větve ($V_j$) vysílače (V), s cílem dále jej využít jako druhý inicializační vektor (BV2) pro zašifrování kontrolních částí ($cv_{1..nv}$) všech možných větví vysílače (V) pomocí zřetězeného módu CBC u druhé blokové šifry (BS2) s druhým klíčem (BK2) s tím, že před zašifrováním se kontrolní části ($cv_{1..nv}$) všech možných větví vysílače (V) doplní nulami tak, aby jejich celková délka byla dělitelná délkou bloku druhé blokové šifry (BS2), čímž se zašifrované kontrolní části ($cv_{1..nv}$) všech možných větví vysílače (V) stávají autentizační částí ($av_j$) sledované j-té větve ($V_j$) vysílače (V), která se místo nich připojí k informační zprávě ($IV_j$) sledované j-té větve ($V_j$) vysílače (V) a jako autentická informační zpráva ($AIV_j$) sledované j-té větve ($V_j$) vysílače (V) se pak přenáší přes otevřený přenosový systém (OPS) do sledované k-té větve ($P_k$) přijímače (P), kde se z autentické informační zprávy ($AIV_j$) sledované j-té větve ($V_j$) vysílače (V) pomocí první blokové šifry (BS1) s prvním klíčem (BK1) a druhé blokové šifry (BS2) s druhým klíčem (BK2) dešifruje autentizační část ($av_j$) sledované j-té větve ($V_j$) vysílače (V), čímž se zpět získá rozšířená informační zpráva ($RIV_j$) sledované j-té větve ($V_j$) vysílače (V), složená z informační zprávy ($IV_j$) sledované j-té větve ($V_j$) vysílače (V) a kontrolních částí ($cv_{1..nv}$) všech možných větví vysílače (V),

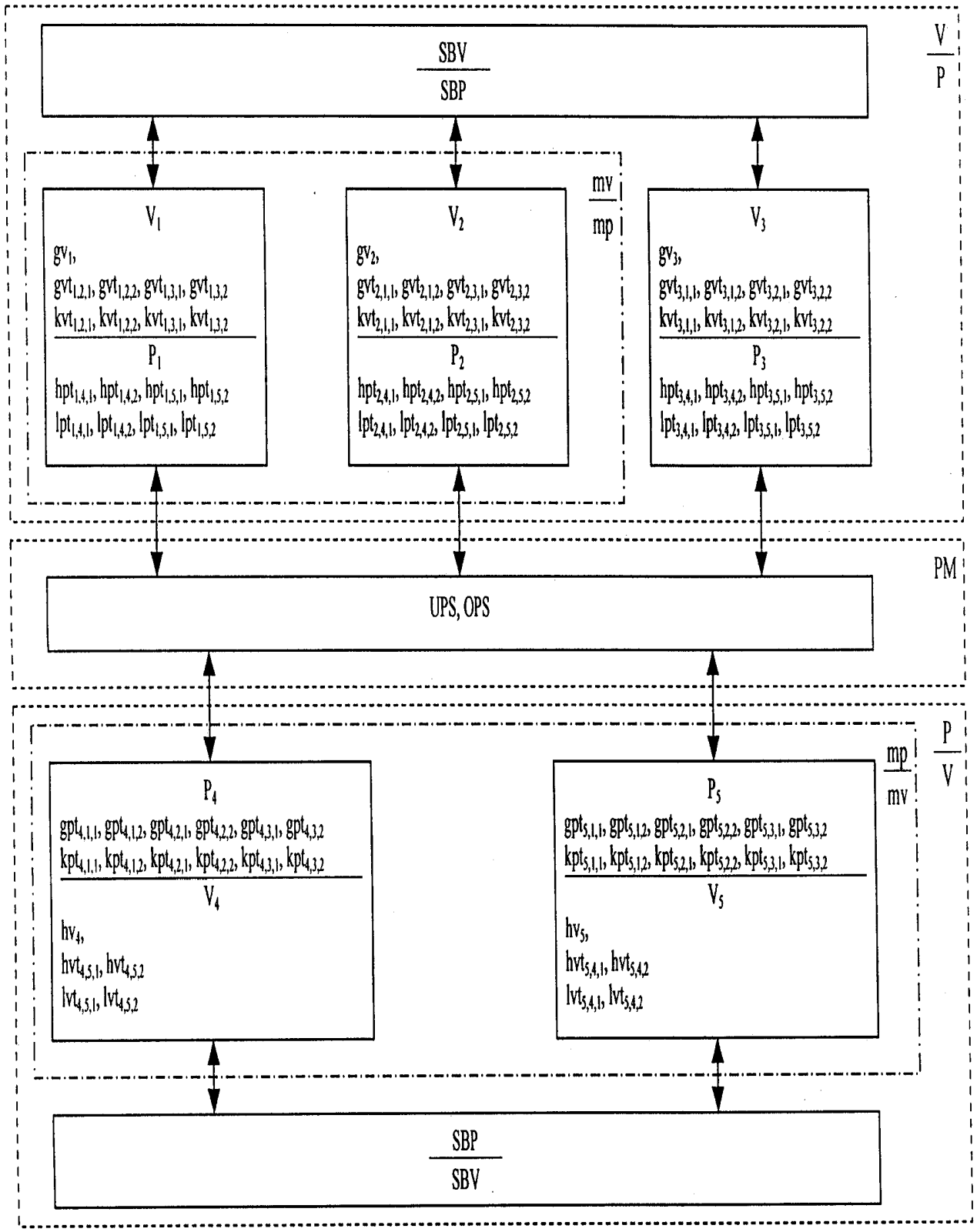
↳ která se dále v pátém kroku shodným způsobem zpracovává a kontroluje, přičemž tato kontrola ověřuje správnost funkce šifrování ve vysílači (V) a dešifrování v přijímači (P).

PV 2004 - 826



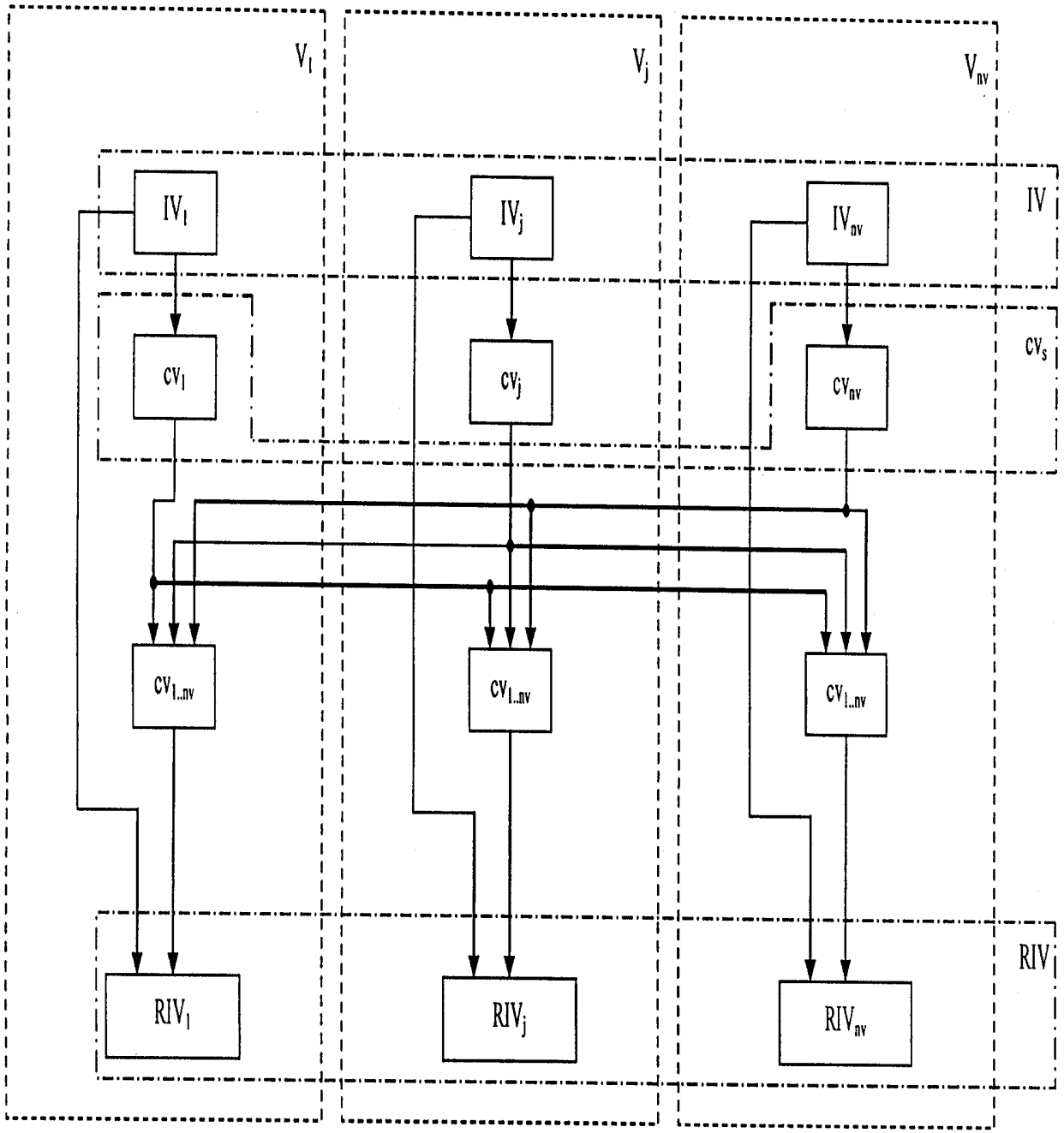

Obr.1

PV 2004 – 826



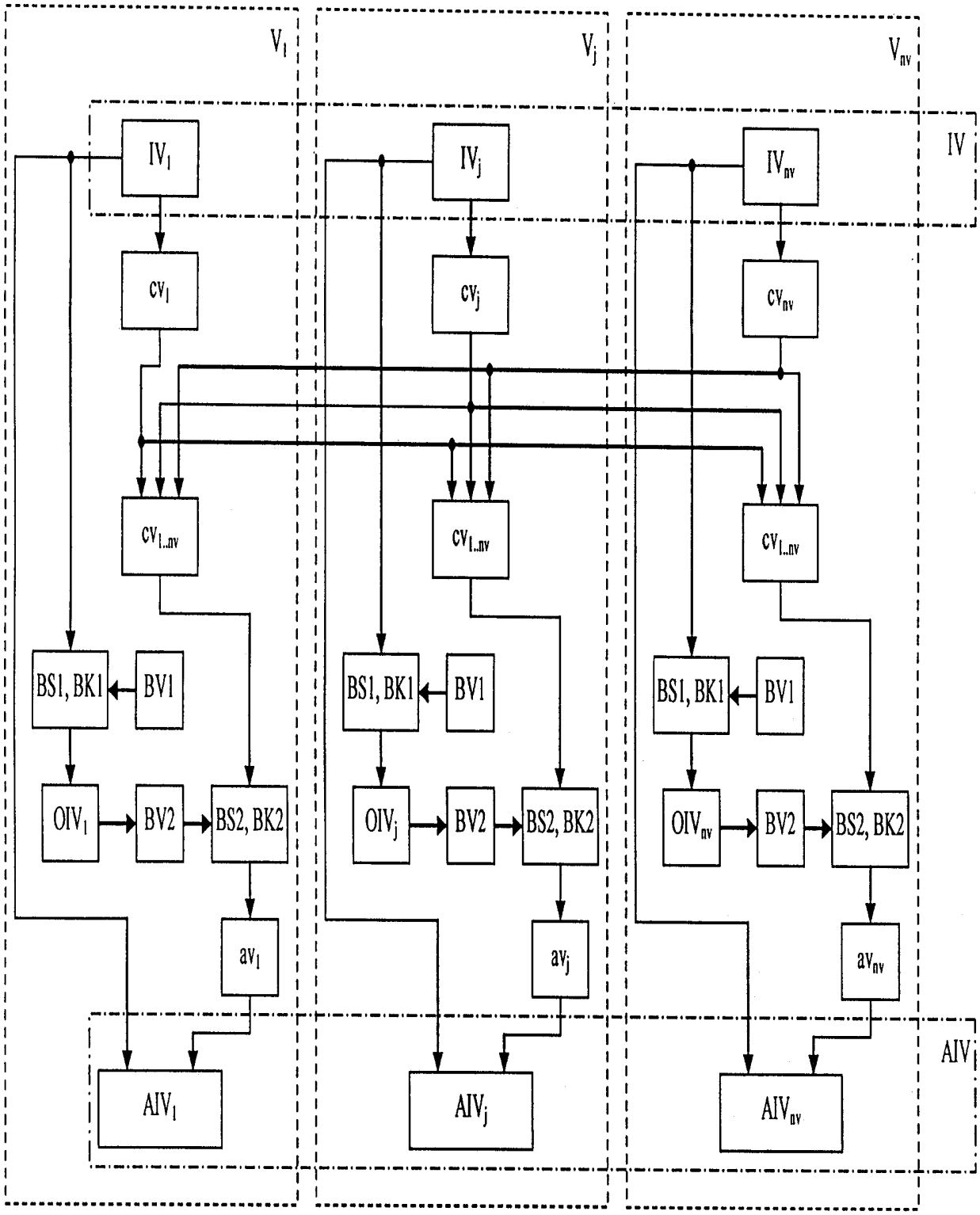

Obr.2

PV2004-826




Ob.3

PV2004-826




Obr.4