Univerzita Komenského
Fakulta matematiky, fyziky a informatiky
Katedra informatiky

Kontrola správnosti času autorít časových pečiatok

Diplomová práca

Autor: Marek Doršic
Vedúci diplomovej práce: Mgr. Juraj Vaško

Bratislava
Apríl 2005

Čestne prehlasujem, že som pri vypracovaní tejto práce postupoval samostatne pod vedením svojho diplomového vedúceho a na základe vedomostí, ktoré som získal počas štúdia a z uvedenej literatúry.

.....

Touto cestou by som sa chcel poďakovať vedúcemu diplomovej práce Mgr. Jurajovi Vaškovi za jeho konštruktívne rady a pripomienky, ktorými ma usmerňoval pri písaní diplomovej práce. Rovnako by som sa chcel poďakovať všetkým, ktorí mi pomáhali uskutočniť prezentované merania.

Obsah

Úvod

Elektronické dokumenty sú dnes zaužívanou formou záznamu a prenosu informácie. Ľudia, komerčné organizácie, štátne úrady ich využívajú s cieľom zjednodušiť komunikáciu, zvýšiť efektivitu alebo zrýchliť prístup k informáciám. Pokročilé informačné technológie umožňujú ukladanie veľkého množstva informácií na malom priestore a ich rýchle spracovanie.

Pojem časovej pečiatky a podmienky jej vydávania definoval zákon č. 215/2002 Z.z. o elektronickom podpise. V jeho zmysle autoritou časových pečiatok, vydávajúcou časové pečiatky, môže byť každá akreditovaná certifikačná autorita. Ale zákon a prislúchajúce vyhlášky upravujú len čiastočne podmienky prevádzky tejto služby a v súčasnosti neexistuje metodika jej kontroly. Závažným problémom je zabezpečenie dôveryhodnosti času, udávaného v časovej pečiatke. Základným kameňom tejto dôvery je dôveryhodnosť zdroja času autority časových pečiatok. Tá môže byť dosiahnutá len synchronizáciou zdroja času s dôveryhodným nadradeným zdrojom vhodnou metódou a jeho kontrolou. Rovnako závažné je určenie vzťahu zdroja času autority k Slovenskému národnému etalónu času, ktorý je pod správou Slovenského metrologického ústavu. Slovenský národný etalón času je nezávislým a oficiálnymi rozhodnutiami uznaným zdrojom času na Slovensku. V súčasnosti SMÚ neumožňuje synchronizáciu zariadení s časovým etalónom na diaľku a autority časových pečiatok sú nútené využívať iné nadradené zdroje času.

Hlavným cieľom diplomovej práce je preskúmať rôzne metódy kontroly správnosti času zdroja času autorít časových pečiatok, zhodnotiť ich kvalitu, dôveryhodnosť a náročnosť nasadenia v praxi, v podmienkach Slovenska. Práca nehľadá metódy synchronizácie so Slovenským národným etalónom času, ale na základe vykonanej analýzy určuje najvhodnejšiu metódu kontroly spomedzi skúmaných. Za týmto účelom práca prináša i základné poznatky z oblasti metrológie času a frekvencie. Pre vybranú metódu práca ďalej bližšie určí podmienky potrebné pre jej realizáciu v praxi, odhadne prevádzkové parametre a predloží analýzu jej implementácie s vysokoúrovňovým návrhom jej riešenia. Navrhnutím a implementáciou kontroly zdroja času sa má vytvoriť predpoklad pre dôveru v správnosť času vo vydaných časových pečiatkach.

Práca má slúžiť ako podklad pre rozhodovanie o implementácii infraštruktúry kontroly na strane SMÚ, a zároveň prináša úvod do problematiky merania a porovnávania času pre autority časových pečiatok.

V úvodnej kapitole práca ponúka stručný prehľad z oblasti kryptografie a informačnej bezpečnosti. Je určená pre čitateľov, ktorý sa s pojmami z tejto oblasti stretli len v menšej miere a môžu v nej nájsť popis základných technológií a riešení. Zdatnejší čitatelia môžu túto kapitolu preskočiť.

Problematiku metrológie času a frekvencie približuje druhá kapitola. Približuje základné techniky konštrukcie, charakterizácie a merania etalónov času, spôsoby ich porovnávania a šírenia časovej informácie. V závere vysvetľuje pojem nadväznosti a jeho význam pre porovnávania na lokálnej a medzinárodnej úrovni. Kapitola je určená pre čitateľov, ktorí nemajú vedomosti o tejto problematike a pre jej úplné pochopenie vyžaduje základy štatistiky.

Tretia kapitola prináša prehľad navrhovaných riešení kontroly zdroja času. Stanovuje hlavné kritéria na hľadaný systém a popisuje základnú myšlienku každej navrhovanej metódy, jej výhody a nevýhody. Po analýze určí najvhodnejšie riešenie.

Vo štvrtej kapitole sa zaoberáme opisom vybranej metódy. Prezentuje podrobný popis činnosti a spôsobu spracovania merania. Snaží sa stanoviť základné požiadavky na systém a prináša vysokoúrovňový návrh jej riešenia spolu s odhadom predpokladaných nákladov.

Kapitola 1

Kryptografia a informačná bezpečnosť

Kryptografia je pre väčšinu ľudí spojená s utajovaním správ, kedy nechceme, aby bol ich obsah známy neoprávneným osobám. Dnešná kryptografia však už nie je len o utajovaní. Poskytuje okrem utajenia ďalšie tri hlavné služby - autenticitu, integritu a neodškriepiteľnosť, pomocou ktorých je možné zachovať vybrané bezpečnostné atribúty pri spracovaní údajov. Autenticita umožňuje overiť zdroj informácie, integrita či táto nebola medzičasom náhodne alebo zámerne zmenená a neodškriepiteľnosť alebo popretie autorstva je ochrana proti odmietnutiu už vykonaného skutku, ako napríklad odopretie odoslania správy. Tieto služby zabezpečuje využitím matematických metód.

Kryptografiu využívame takmer všetci dennodenne. Začína to ráno otvorením auta s centrálnym uzamykaním na diaľkové ovládanie, pokračuje v práci prihlásením sa do svojho počítača, poobede zadaním PIN kódu pri bezhotovostnej platbe za nákup v obchode a končí večer sledovaním kódovanej televíznej stanice. To všetko sú aplikácie, v ktorých kryptografia hrá podstatnú rolu. A jej ďalšie aplikácie čakajúce na využitie elektronického podpisu alebo časovej pečiatky sú len na počiatku vývoja. Tieto budú automatizovane spracovávať veľké množstvo informácií. To si vyžaduje nasadenie počítačov a informačných technológií, ale aj spôsobov ochrany pred hrozbami. A práve tými sa zaoberá informačná bezpečnosť.

Zmysel nasledujúcej kapitoly je poskytnúť základný prehľad v kryptografii ako nástroji, ktorý pomocou matematického aparátu umožňuje definovať, navrhovať a analyzovať bezpečné spôsoby prenosu správ a informačnej bezpečnosti skúmajúcej hrozby systémov spracovávajúcich tieto správy a možnosti ochrany pred nimi. Kryptografia tvorí jednu z kľúčových komponent riešení elektronického podpisu a časových pečiatok.

1.1 Základná terminológia

Ľubovoľnú konečnú neprázdnu množinu symbolov $\Sigma = \{a_1, a_2, \ldots, a_n\}$ budeme nazývať *abeceda*. Pod *dokumentom* nad abecedou Σ budeme rozumieť ľubovoľnú, konečnú, neprázdnu postupnosť symbolov z abecedy Σ. Často, ak to nepovedie k zmäteniu a nejednoznačnosti, budeme pre skrátenie zápisu spojenie „nad abecedou“ vynechávať. Okrem toho, že dokument je postupnosť symbolov, bude predstavovať aj symbolický zápis *informácií* - faktov/dát ukrytých v dokumente. Opäť tam, kde to nepovedie k nedorozumeniu, nebudeme rozlišovať dokument, správu alebo údaj od ich informačného obsahu.

Vytváranie dokumentov je podnietené najmä prenosom informácií v nich obsiahnutých. Tento sa môže uskutočňovať v dvoch rovinách - časovej a priestorovej. Pod *prenosom dokumentu v čase* chápeme uloženie dokumentu na prenosové médium, ktoré ho bude uchovávať a v prípade potreby v budúcnosti umožní prečítať jeho obsah. Dokumentom prenášaným v čase sa hovorí aj *údaje*. K prenosu dokumentu v priestore dochádza, ak je tento prenášaný z jedného miesta na druhé. V tomto prípade sa dokumentom často hovorí aj *správy* a ich výmene/prenosu medzi dvoma entitami *komunikácia*.

Prenos správ (či už v čase alebo priestore) je uskutočňovaný cez *prenosový kanál*. Model prenosového kanála tvorí *zdroj*, *kóder*, *kanál*, *dekóder* a *príjemca*. Zdroj slúži ako generátor správy, ktorá sa má preniesť k príjemcovi. Odbremeňuje nás od skúmania pôvodu správy a špecifických vlastností jednotlivých generátorov. Správy generuje v *abecede zdroja* Σ_S a budeme predpokladať, že príjemca chce obdržať správu v rovnakej abecede. Na samotný prenos dokumentu slúži *prenosový kanál*. Tento môže byť tvorený napr. káblovou alebo satelitnou komunikačnou linkou v prípade prenosu v priestore, alebo napr. pevným diskom, DVD nosičom či elektronickou pamäťou pri prenose v čase. Každý z kanálov používa vlastnú abecedu, tzv. *kanálovú abecedu* Σ_C, ktorá najlepšie zodpovedá jeho fyzikálnym charakteristikám. Vo všeobecnosti zdrojová a kanálová abeceda môžu byť rôzne, a preto je nutná transformácia správy medzi nimi. Prevod správy zo zdrojovej abecedy Σ_S do kanálovej abecedy Σ_C a naopak zabezpečuje *kóder* resp. *dekóder*. Ak je technickými, matematickými alebo inými prostriedkami zaručená zanedbateľne malá pravdepodobnosť, že ľubovoľná neoprávnená tretia strana vstupujúca do komunikácie alebo načúvajúca komunikáciu medzi dvoma entitami nemôže porozumieť obsahu prenášanej informácie alebo meniť prenášaný dokument, hovoríme o *spoľahlivom komunikačnom kanáli*.

Dnes, keď je väčšina dokumentov a dát tvorená, prenášaná alebo spracovávaná počítačovými systémami sa takýmto dokumentom hovorí *digitálne*.

Pod týmto prívlastkom sa rozumie nič iné, ako že dokument je nad abecedou $\Sigma = \{0, 1, \ldots, n-1\}$, ktorej symboly sú prirodzené čísla. Jej podmnožina - *binárna abeceda* $\Sigma = \{0, 1\}$ je základom všetkej dnešnej výpočtovej techniky. Predstavuje tú najjednoduchšiu abecedu (častokrát však pre ľudí nie najpohodlnejšiu pre prácu), v akej môžu byť dokumenty vytvorené. Dokumenty nad binárnou abecedou budeme nazývať aj *binárnymi*.

1.2 Informačná bezpečnosť

Verejné či súkromné organizácie uchovávajú a spracovávajú dnes obrovské množstvo *elektronických dokumentov* - dokumentov spracovávaných pomocou technických prostriedkov v elektronickej, magnetickej, optickej či inej forme, teda spracovávaných výpočtovou technikou. Pod spracovaním informácie/dokumentu budeme rozumieť ľubovoľnú transformáciu $\Phi : \Sigma^+ \to \Sigma^*$ na množine dokumentov. (Spracovaním dokumentu je aj transformácia dokumentu zo zdrojovej abecedy Σ_S do kanálovej Σ_C uskutočňovaná v kódery napriek tomu, že obor a koobor tejto transformácie nie sú rovnaké. Bez ujmy na všeobecnosti totiž môžme predpokladať, že $\Sigma = \Sigma_S \cup \Sigma_C$.) Elektronický dokument, oproti jeho staršej papierovej podobe, prináša so sebou množstvo nesmiernych možností, ktoré však výrazným spôsobom komplikujú jeho ochranu. Je možné bez zanechania stôp pozmeniť jeho obsah, vytvoriť rýchlo dokonalú kópiu, či ho preniesť na veľkú vzdialenosť. Ďalej si treba uvedomiť, koľko informácií v elektronickej podobe sa zmestí do relatívne malého priestoru a v akom krátkom čase sme ich schopní pomocou výpočtovej techniky spracovať.

Častokrát je nutné dokument prenášať. Predstavme si pre zjednodušenie, že Alica chce poslať Bobovi dôvernú správu m a ich jediná komunikačná linka vedie cez verejnú sieť akou je napr. Internet. V takej situácii môže do ich komunikácie vstúpiť ľubovoľná tretia strana, napr. Eva, ktorá má rôzne záujmy. Eva sa môže usilovať zachytiť posielané správy medzi Alicou a Bobom, a tak odpočúvať ich komunikáciu. Ak sú tieto nezašifrované, alebo Eve sa podarí šifru rozlúštiť, dostane sa k dôverným informáciám, ktoré neboli ňu určené. Eva sa v tomto prípade správa pasívne, nijak nenarúša prebiehanú komunikáciu, ale ju iba pozoruje. Hovoríme, že je *pasívnym útočníkom*. Ak sa však rozhodne zdržovať tok informácií, pozmeňovať ich, či dokonca nahrádzať celé správy jej vlastnými hovoríme o Eve ako o *aktívnom útočníkovi*.

Problém však nemusí byť len tretia strana. Možné sú scenáre, keď Alica bude tvrdiť, že správu m nikdy neposlala, že obsah správy ktorú odoslala, bol iný ako ten, čo Bob obdržal alebo Bob bude tvrdiť, že správu nikdy nedostal. V takýchto prípadoch ani ochrana pred útočníkom zvonku nepomôže.

Nasadzujú sa metódy kryptografie - vedného oboru skúmajúceho matematické techniky na ochranu dokumetov. Tie majú zabezpečiť, aby prenášaná informácia nebola pozmenená, prezradená, aby bolo možné overiť identitu komunikujúcich entít a dokázať konanie každej z nich.

Ochrana informácií je však oveľa komplexnejší problém. Aby sme ho zachytili zavedieme najprv pojem *informačného systému* (IS) alebo aj *IT systému*. Pod informačným systémom budeme rozumieť systém postavený s využitím informačných technológií za konkrétnym účelom, plniaci presne definované funkcie. Pod tento pojem spadá všetok hardvér, softvér, komunikačné linky ako i obsluhujúci personál. Obklopený je *okolím informačného systému*, ktoré ho ovplyvňuje svojou legislatívou, fyzickým priestorom či vnútornými predpismi organizácie, v ktorej je inštalovaný. Vplyv okolia na informačný systém trvá počas celého jeho *životného cyklu* - od návrhu, implementácie, prevádzky až po zánik. Nutnosť s jeho detailným oboznámením je preto pre bezpečnosť IS kľúčová.

Akúkoľvek časť IS, ktorú má zmysel odlišovať z hľadiska ochrany budeme nazývať *aktívom*. Entity IS alebo jeho okolia zapríčiňujúce vykonanie operácií v IS nazývame *subjektmi* a tie časti, ktoré subjektom slúžia na vykonanie týchto operácií *objektmi*. Počas prevádzky IS sú aktíva vystavené *hrozbám*. Hrozba predstavuje možnosť pristupovať k častiam IS, ktorá nie je v súlade s popísanými pravidlami, a tak môže zapríčiniť jeho chovanie v rozpore s definovanou funkčnosťou. Subjekty, majúce možnosť realizovať hrozbu, budeme volať *nositeľmi hrozby* a výsledky realizovania hrozby *dopady*. Každý dopad na IS môže mať pre jeho prevádzkovateľa rozličnú vážnosť. Hrozbám so zdrvujúcimi dopadmi sa v rámci životného cyklu IS snažíme zabrániť. Nie však za každú cenu. Výpadok elektrického prúdu môže mať vážne dopady a ochrana voči tejto hrozbe je relatívne jednoduchá, ale výbuch sopky v neaktívnych oblastiach je nanajvýš nepravdepodobná hrozba, voči ktorej by bola ochrana ekonomicky neefektívna. Hovoríme preto o *riziku* predstavovanom hrozbou, ako o funkcii (najčastejšie súčinom) medzi pravdepodobnosťou nastatia hrozby a vážnosťou jej dopadov. *Informačná bezpečnosť* je multidisciplinárnou oblasťou zaoberajúcou sa hľadaním a rozvíjaním metód ochrany IS pred hrozbami počas jeho celého životného cyklu.

1.3 Kryptografické primitíva

Požiadavky na bezpečnosť a rýchlosť informačných systémov sú dnes častokrát natoľko široké, že je nutné kombinovať viacero kryptografických primitív na dosiahnutie vytýčeného cieľa. Kryptografické primitíva predstavujú sta-

vebné kamene pre stavbu komplexných systémov a návrh kryptografických protokolov. Každé z nich slúži inému účelu - hašovacie funkcie umožňujú vytvoriť skrátenú reprezentáciu dokumentu, autentifikačný protokol overiť identitu komunikujúcej entity, digitálne podpisy autorizovať digitálne dokumenty. Použitie kryptografického primitíva si vyžaduje dokonalú znalosť nie len jeho samotného, ale aj ostatných, ktoré ho obklopujú a s ktorými spolupracuje.

1.3.1 Kryptografia s utajeným kľúčom

Metódy kryptografie s utajeným kľúčom sú založené na spoločnom tajomstve oboch komunikujúcich entít - *kľúči*. Ich cieľom je najmä zachovanie dôvernosti prenášaných správ. Kľúč slúži ako parameter výberu šifrovacej a dešifrovacej funkcie z množiny všetkých šifrovacích resp. dešifrovacích funkcií. Pomocou šifrovacej funkcie je správa, nazývaná *otvorený text*, zašifrovaná, čím sa zmení na *šifrový text*. Ten je následne prenesený k prímateľovi, ktorý ho aplikovaním dešifrovacej funkcie opäť transformuje na otvorený text. Znamená to, že ak chcú spolu Alica a Bob bezpečne komunikovať, musia si najprv dohodnúť spoločný kľúč, ktorý bude známy len im dvom. Tieto kryptosystémy sa nazývajú aj symetrické alebo kryptosystémy s jedným kľúčom.

Formálne zadefinované: *kryptosystém* je pätica $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, pričom platí nasledovné:

1. $\mathcal{P}$ je konečná množina otvorených textov
2. $\mathcal{C}$ je konečná množina šifrových textov
3. $\mathcal{K}$ je konečná množina možných kľúčov
4. pre $\forall K \in \mathcal{K}$ existujú šifrovacia funkcia $E_K \in \mathcal{E}, E_K : \mathcal{P} \to \mathcal{C}$ a dešifrovacia funkcia $D_K \in \mathcal{D}, D_K : \mathcal{C} \to \mathcal{P}$ pre ktoré $D_K(E_K(p)) = p$ $(\forall p \in \mathcal{P})$.

Transformáciu $c = E_K(m)$ budeme nazývať *(za)šifrovaním* (správy m) a spätnú trasformáciou $m = D_K(c)$ *dešifrovaním* (správy m).

Ďalej budeme predpokladať, že otvorený text je reťazec symbolov (otvorených textov) $p = p_1 p_2 \dots p_n$ pre $n \in \mathbb{N}, n \geq 1,\ p_i \in \mathcal{P}$. Potom šifrový text $c = c_1 c_2 \dots c_n = E_K(p_1) E_K(p_2) \dots E_K(p_n)$ dostaneme zašifrovaním jednotlivých symbolov otvoreného textu. Z takejto definície plynie, že E_K musí byť injekcia, inak by dešifrovanie nebolo jednoznačné. Ak $\mathcal{P} = \mathcal{C}$ potom E_K a D_K sú permutácie a šifrovanie/dešifrovanie je len preusporiadaním jednotlivých symbolov.

Symetrické šifry rozdeľujeme na dva typy. Vyššie popísaná bola *bloková šifra*, ktorá spracúvava otvorený text po blokoch pevnej dĺžky a na zašifrovanie každého bloku použije rovnakú šifrovaciu funkciu E_K. Iným typom sú *prúdové šifry*. Prúdové šifry nepoužívajú rovnakú šifrovaciu funkciu pre každý symbol otvoreného textu, ale namiesto toho je generovaný prúd kľúčov $z = z_1 z_2 \ldots$, ktoré sa používajú na šifrovanie. Teda $y = E_{z_1}(x_1)E_{z_2}(x_2)\ldots$. Kľúče $z_i = f_i(K, p_1 p_2 \ldots p_{i-1})$ sú generované funkciou f_i v závislosti na dohodnutom kľúči K a už predtým zašifrovaného textu $p_1 p_2 \ldots p_{i-1}$. Ľahko vidieť, že blokové šifry sú špecialnym prípadom prúdových ak položíme $z_i = K = f_i(K, p_1 p_2 \ldots p_{i-1})$ pre $\forall i \geq 1$.

Využitie symetrických šifier nekončí už pri šifrovaní. Využívajú sa aj na stavbu ďalších primitív ako napr. hašovacích funkcií, alebo protokolov na autentikáciu správ (MAC). Vždy sa však vyžaduje, aby boli odolné voči všetkým známym útokom (viď kap. 1.5), a aby boli efektívne vypočítateľné. Sila šifrovania sa dá zvýšiť aj viacnásobným šifrovaním. Otvorený text je pri ňom šifrovaný viackrát za sebou, pričom najčastejšie jednotlivé šifrovacie funkcie používajú rôzne kľúče.

AES (Rijndael)

Od roku 2002 sa v USA na šifrovanie citlivých dokumentov vo federálnych úradoch a organizáciách USA požíva algoritmus AES (Advanced Encryption Standard). Nahradil predtým používaný algoritmus DES ([1], [2]), ktorý dnes pre svoju krátku dĺžku kľúča - 56 bitov umožňuje útočníkovi úspešne previesť útok úplným preberaním. AES je symetrická bloková šifra používajúca kľúče dĺžky 128, 192 alebo 256[1] na zašifrovanie blokov dokumentu. Bloky majú v prípade tejto šifry dĺžku 128 bitov. Presadil sa vďaka vysokej rýchlosti šifrovania/dešifrovania, nízkej pamäťovej náročnosti a jednoduchej implementácii v softvérovej ako i hardvérovej podobe. Presný popis algoritmu nazývaného aj Rijndael podľa jeho belgických autorov Vincenta Rijmena a Joana Deamena je uvedený v [3].

1.3.2 Kryptografia s verejným kľúčom

V roku 1976 uverejnili páni Diffie a Hellman v [4] prevratnú myšlienku. Tá viedla k vývoju kryptografických systémov s verejnými kľúčmi často nazývanými aj *asymetrické*. Ich základná idea spočíva v použití dvoch transformácií, tzv. verejnej transformácie E a súkromnej transformácie D. Ako z názvu plynie, verejná transformácia nie je tajná a slúži na šifrovanie dokumentu. Tento sa dá potom dešifrovať súkromnou transformáciou späť na otvorený text.

[1] Podľa dĺžky kľúča rozlišujeme AES-128, AES-192 resp. AES-256.

Výhodou asymetrických systémov je, že strany, ktoré chcú spolu bezpečne komunikovať, sa nemusia deliť o spoločné tajomstvo[2]. Stačí, ak ich verejné transformácie sú uvedené vo všeobecne prístupnom registri. Ak chce A poslať správu B, tak si najprv vyhľadá verejnú transformáciu B, E_B, zašifruje správu pomocou nej a odošle prijímateľovi B. Ten si správu môže prečítať po dešifrovaní jeho súkromnou transformáciou D_B. Teda nie je nutná výmena žiadnej tajnej informácie medzi A a B pred zahájením šifrovanej komunikácie. Naopak ich nevýhoda oproti klasickým systémom je malá rýchlosť šifrovania resp. dešifrovania.

Na to, aby metódy kryptografie s verejným kľúčom spoľahlivo fungovali, musia verejná a súkromná transformácia spĺňať určité podmienky. Ak označíme $\mathcal{P}$ množinu otvorených textov, $\mathcal{C}$ množinu šifrových textov, $\mathcal{R}$ množinu $\{0,1\}^*$ a definujeme funkciu $E : \mathcal{P} \times \mathcal{R} \to \mathcal{C}$ verejnou funkciou a $D : \mathcal{C} \to \mathcal{P}$ súkromnou funkciou, potom dešifrovaním textu transformáciou D zašifrovaného transformáciou E musíme dostať pôvodnú správu:

$$\forall m \in \mathcal{P}, \forall r \in \mathcal{R} : D(E(m,r)) = m \ .$$

Výber prvku $r \in \mathcal{R}$ umožňuje náhodnú voľbu pri šifrovaní. E ďalej musí byť *jednosmernou funkciou* s tzv. *zadnými dvierkami* (*trapdoor*). Funkcia E je jednosmerná, ak E je ľahko počitateľná, ale ťažko invertovateľná. A to že E má zadné dvierka znamená, že vedomosť určitej informácie robí jej invertovanie ľahkým. Táto vlastnosť umožňuje skonštruovať funkciu D, ktorá s využitím týchto informácií dovoľuje efektívne invertovanie E. Jednosmernosť E robí dešifrovanie pre kryptoanalytika ťažkým problémom, ale pre majiteľa súkromnej informácie D naopak veľmi jednoduchým. Zadnými dvierkami pre invertovanie E môže byť napríklad aj schopnosť efektívne riešiť ťažké problémy, na ktorých efektívnej neriešiteľnosti je založená bezpečnosť daného systému.

Asymetrický kryptovací systém môže tvoriť aj trieda funkcií, ktoré sú parametrizované jedným alebo viacerými kľúčmi. V takom prípade sa nehovorí o verejnej a súkromnej transformácii, ale o verejnom a súkromnom kľúči.

Ako bolo poznamenané v [5] asymetrické systémy sa dajú rozdeliť do nasledovných kategórií:

1. Systémy, ktoré boli prelomené.
2. Systémy, považujúce sa za bezpečné.
   (a) Systémy, ktorých využitie je otázne.

[2] V prípade ľubovoľných dvoch z n účastníkov, ako napr. v počítačovej sieti, by to znamenalo správu $\binom{n}{2}$ tajomstiev (kľúčov)!

(b) Systémy s praktickým využitím.

i. Systémy vhodné pre distribúciu kľúčov.

ii. Systémy vhodné pre digitálne podpisy.

iii. Systémy vhodné pre distribúciu kľúčov ako aj digitálne podpisy.

Z pohľadu čísel sa väčšina asymetrických kryptovacích systémov ukázala ako nie dostatočne bezpečná. Škoda je, že niektoré techniky použité v týchto systémoch, vykazovali vysokú priepustnosť šifrovania/dešifrovania. Takým prípadom sú napríklad systémy založené na *knapsack* probléme, ktoré sú všeobecne považované za nie bezpečné. Z ostatných systémov, ktoré neboli prelomené je veľa nepoužiteľných pre ich veľkú dĺžku kľúča alebo prílišnú expanziu dát (šifrový text je o mnoho dlhší ako otvorený text).

Iba hŕstka systémov ostala považovaných za bezpečné a prakticky použiteľné. Za bezpečný sa považuje systém, ktorého prelomenie je v zásade ekvivalentné s efektívnym riešením starého zatiaľ efektívne neriešiteľného matematického problému. Z týchto sú niektoré použiteľné len na distribúciu kľúčov ako napr. Diffie-Hellmanov protokol, alebo naopak sú použiteľné iba pre účely digitálneho podpisu ako napr. ElGamalova schéma. Jediným zatiaľ známym systémom, ktorý je bezpečný a vhodný pre zabezpečenie utajenia ako aj autentickosti je RSA (kap. 1.3.2).

Väčšina asymetrických kryptosystémov je založená na jednom z nasledujúcich matematických problémov:

- faktorizácia veľkých prirodzených čísel (napr. kryptosystém RSA)
- problém diskrétneho logaritmu pre konečné polia (kryptosystém ElGamal)
- počítanie druhých odmocním modulo n, kde n je súčin dvoch prvočísel (Rabinov kryptosystém)
- dekódovanie lineárneho kódu[3] (kryptosystém McEliece)
- počítanie súm podmnožiny[3] (Merkle-Hellman knapsack alebo Chor-Rivest knapsack)

Avšak, ako je uvedené v knihe [6, str. 102], problémy faktorizácie prirodzených čísel a počítania druhých odmocnín modulo n sú výpočtovo ekvivalentné. Rovnako ľahko vidieť, že žiadny kryptosystém s verejným kľúčom nemôže byť absolútne bezpečný. Kryptoanalytikovi by stačilo postupne generovať všetky otvorené texty a zašifrovávať ich verejnou transformáciou, ktorá

[3]problém je NP úplny

je voľne prístupná, až pokiaľ by sa nejaký nezhodoval so šifrovým textom, ktorý sa snaží prelomiť.

Kryptovací systém RSA

Kryptosystém RSA (nazvaný podľa začiatočných písmen mien jeho vynálezcov, pánov R. Rivesta, A. Shamira a L. Adlemana) je vhodným tak na digitálne podpisy ako aj distribúciu kľúčov. Jeho bezpečnosť je založená na predpoklade, že faktorizácia čísla na prvočísla je ťažkým problémom.

Princíp systému RSA je jednoduchý. Označme $\mathcal{P}$ množinu všetkých otvorených textov, $\mathcal{C}$ všetkých šifrových textov a položme $n = pq$ pre p, q dve rôzne prvočísla. Nech $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$ a definujme $\mathcal{K} = \{(n, p, q, e, d)$ pre $ed \equiv 1 \pmod{\phi(n)}$. Potom pre $x, y \in \mathbb{Z}_n, K \in \mathcal{K}, K = \{n, p, q, e, d\}$ definujme

$$E_K(x) = x^e \mod n$$

a

$$D_K(y) = y^d \mod n\ .$$

Ľahko vidieť, že verejný kľúč predstavuje dvojica (e, n) a súkromným kľúčom je číslo d. Funkcie E_K a D_K sú šifrovacia resp. dešifrovacia transformácia. Pre zabezpečenie dostatočnej bezpečnosti sa odporúča použiť dĺžku prvočísel p, q aspoň 512 bitov. Podrobnejší popis systému s poznámkami k implementácii a možnými útokmi možno nájsť napr. v [7].

1.3.3 Hašovacie funkcie

Hašovacie funkcie sa v kryptografii nasadzujú za účelom zachovať integritu správy, tj. jej nezmenenosť, v súvislosti s digitálnymi podpisovými schémami (kap. 1.3.5). Slúžia na vytvorenie otlačku správy, ktorý sa potom digitálne podpisuje.

Kryptografickou hašovacou funkciou budeme nazývať funkciu h, ktorá zo správy m konečnej potencionálne rozličnej dĺžky vyrobí reťazec pevnej dĺžky (obyčajne 64, 128, 160 alebo 256 bitov) pričom je ľahko počítateľná, jednosmerná a odolná voči kolíziám. Jej výsledok sa skrátene nazýva *haš*.

Formálne hašovaciu funkciu definujeme ako funkciu $h : \Sigma_a^i \to \Sigma_b^n, i \leq s$; $i, s, n \in \mathbb{N}$ pre ktorú platí, že

1. $\forall m \in \Sigma_a^i$ je $h(m)$ ľahko vypočítateľné
2. pre dané $x \in \Sigma_b^n$ nie je možné efektívne vypočítať $m \in \Sigma_a^i$ také, že $h(m) = x$
3. je výpočtovo neefektívne nájsť ľubovoľné dve správy m_1, m_2, $m_1 \in \Sigma_a^i$, $m_2 \in \Sigma_a^j$, $m_1 \neq m_2$, pre ktoré by platilo $h(m_1) = h(m_2)$

Parameter n je závislý od konkrétnej funkcie. V praxi sa často bez ujmy na všeobecnosti kladie $\Sigma_a = \Sigma_b = \Sigma_2$.

Ako príklady hašovacích funkcií uvedieme napr. MD4, MD5, HAVAL-128 alebo RIPEMD. Na konferencii Crypto2004 výskumníci oznámili, že objavili spôsob ako zlomiť veľkú množinu hašovacích algoritmov vrátane vyššie vymenovaných. [8]

SHA-256

Iteratívny algoritmus SHA-256 predstavuje jednosmernú funkciu na tvorbu odtlačkov (hašov) dokumentov variabilnej dĺžky menšej ako 2^{64} bitov. Jeho obdoba, SHA-1, je od roku 1994 štandardom pre výpočet hašu neklasifikovaných dokumentov vo federálnych úradoch a organizáciách USA.

Algoritmus pracuje v dvoch fázach. Najprv je dokument predspracovaný, čo zahŕňa okrem iného zarovnanie dokumentu (*padding*) na dĺžku násobku 512 a v druhej fáze je vykonávaný samotný výpočet hašu. Výpočet je séria aritmetických bitových operácií, ktorej výsledkom je haš pevnej dĺžky 256 bitov. Úplny popis algoritmu je uvedený v štandarde [9]. Nájsť v ňom možno aj popis novších verzií pripravených na podrobné testovanie, pretože algoritmus spadá do kategórie výpočtovo bezpečných.

1.3.4 Autentifikačné protokoly

Úlohou *autentifikačných protokolov* je overiť, že totožnosť, ktorá je preukazovaná je skutočne tou pravou. Proces overovania sa nazýva aj *autentifikácia*, pričom pod pojmom *identifikácia* budeme rozumieť len oznámenie svojej identity (teda nie jej overenie). Napríklad, ak chce Bob komunikovať s Alicou, pričom si chce byť istý, že komunikuje s ňou a nie s niekým iným, tak jej môže začať klásť otázky, na ktoré vie správnu odpoveď len on a Alica (začať autentifikáciu). Bob sa bude pýtať tak dlho, pokiaľ nenadobudne presvedčenie, že komunikuje s Alicou alebo naopak, že na otázky mu odpovedá niekto iný ako Alica[4]. V každodennom živote je možné nájsť nespočetne iných príkladov, kedy je potrebné elektronicky preukázať svoju identitu. Dobrým príkladom je výber z bankomatu, pri ktorom je nutné zadať štvormiestny PIN kód (obdobou je už len prosté spustenie mobilného telefónu), lebo prihlásenie sa na vzdialený počítač.

Hlavnými vlastnosťami, ktoré autentifikačný protokol musí spĺňať sú:

1. v prípade dvoch dôveryhodných strán Boba a Alice, Alica sa musí byť schopná úspešne autentifikovať u Boba

[4]V tomto prípade predpokladáme, že Alica neklame.

2. Bob nie je schopný zneužiť predošlú autentifikáciu Alice a autentifikovať sa ako Alica u Evy

3. pravdepodobnosť, že niekto, kto sa identifikuje ako Alica a Alica nie je, sa pri vykonávaní autentifikačného protokolu úspešne autentifikuje u Boba je zanedbateľne malá

4. Vyššie uvedené body ostávajú v platnosti aj keď súčasne platí, že

   Alica a Bob sa už autentifikovali (polynomiálne) veľakrát,

   Eva sa ako nepriateľ mohla zúčastniť autentifikácie či už s Alicou, Bobom alebo oboma,

   viacero inštancií protokolu, spustených napríklad aj Evou, môže bežať naraz.

V závislosti od použitej schémy, môže byť autentifikovaná buď jedna alebo aj obe entity. Niektoré schémy vyžadujú prítomnosť dôveryhodnej tretej strany. Častým je využitie techník z asymetrického šifrovania ako napríklad v modifikovanom Needham-Schroederovom protokole s verejnými kľúčmi [6] alebo Guillou-Quisquaterovom protokole [7] založenom na RSA.

Guillou-Quisquaterov protokol

Tento protokol pre autentifikáciu využíva služby dôveryhodnej autority (TA), ktorá vstupuje ako tretia strana do protokolu. TA vygeneruje prvočísla p, q a vypočíta ich súčin $n = pq$ (netreba pripomínať, že p, q sú dostatočne veľké na to, aby faktorizácia n bola ťažkým problémom). n bude verejne známe, zatiaľ čo p, q bude TA držať v tajnosti. TA ďalej zvolí prirodzené číslo b opäť dostatočne veľké, slúžiace ako verejný RSA šifrovací exponent. Nakoniec TA zvolí hašovací a šifrovací algoritmus a vypočíta certifikát pre Alicu nasledovne:

1. Priradí Alici identifikačný reťazec ID(Alica)

2. Alica zvolí $u \in \mathbb{N}$ také, že $0 \leq u \leq n-1$ a vypočíta $v = (u^{-1})^b \mod n$. Hodnotu v predá TA.

3. TA vygeneruje podpis $s = sig_{TA}(I, v)$ a predá Alici jej certifikát $C(Alica) = (ID(Alica), v, s)$

Ak Bob chce overiť Alicinu identitu, postupuje podľa nasledovného:

1. vyžiada si od Alice jej certifikát a číslo γ, kde $\gamma = k^b \mod n$ a $k \in \mathbb{N}, 0 \leq k \leq n-1$ je Alicou náhodne zvolené číslo.

2. overí podpis TA na Alicinom certifikáte
3. náhodne zvolí $r \in \mathbb{N}, 0 \leq r \leq b-1$ a pošle ho Alici
4. Alica vypočíta $y = ku^r \mod n$ a odovzdá y Bobovi
5. Bob overí či $\gamma \equiv v^r y^b \pmod{n}$

Pokiaľ je posledná podmienka splnená, Alica dokázala Bobovi svoju identitu.

1.3.5 Digitálne podpisy

Digitálne podpisy sú elektronickou analógiou bežných „ručných“ podpisov. Cieľom je, aby bolo možné jednoznačne posúdiť autenticitu a integritu elektronického dokumentu alebo správy. Ich základnými vlastnosťami sú

1. schopnosť prijímateľa overiť podpis
2. nemožnosť falšovania
3. zaručenie neodškriepiteľnosti (nepopretie autorstva).

Hlavným rozdielom medzi „ručným“ a digitálnym podpisom je, že digitálny podpis musí byť funkciou podpisovanej správy. Kým pri ručnom podpise je jedno, aká správa je podpisovaná, pretože je jej neoddeliteľnou súčasťou, digitálny podpis musí byť závislý aj od celého obsahu podpisovanej správy. Teda zmena jediného bitu musí vyvolať zmenu podpisu, čím sa zaručí, že podpísaná správa už nebude môcť byť menená. Vyplýva to z charakteru elektronického prostredia, v ktorom sa údaje ľahko kopíruju a menia. Ak by digitálny podpis nebol funkciou správy, stačilo by získať jediný podpísaný dokument a prekopírovaním podpisu by sme vedeli vierohodne podpísať ľubovoľný iný.

Pod pojmom *digitálny podpis* budeme rozumieť digitálny reťazec, ktorý sa vzťahuje k správe v digitálnej forme. Tento reťazec je v závislosti od typu schémy prenášaný paralelne ako príloha k správe, alebo je vytvorená nová dátová štruktúra obsahujúca správu a jej prislúchajúci podpis. *Schému digitálneho podpisu*, nazývanú aj *podpisová schéma*, tvorí pätica $(\mathcal{P}, \mathcal{S}, \mathcal{K}, \{sig_k \mid \forall k \in \mathcal{K}\}, \{ver_k \mid \forall k \in \mathcal{K}\})$, kde

1. $\mathcal{P}$ je neprázdna konečná množina všetkých prípustných správ
2. $\mathcal{S}$ je neprázdna konečná množina všetkých prípustných podpisov
3. $\mathcal{K}$ je neprázdna konečná množina kľúčov

4. $sig_k : \mathcal{P} \rightarrow \mathcal{S}$ je tajnou podpisovou funkciou pre kľúč k
5. $ver_k : \mathcal{P} \times \mathcal{S} \rightarrow \{true, false\}$ je verejnou overovacou funkciou pre kľúč k

Pre efektívne používanie podpisových schém je nutné, aby funkcie sig_k a ver_k mohli byť realizované pre každý kľúč k algoritmami pracujúcimi v polynomiálnom čase.

Väčšina podpisových schém je založená na kryptografických systémoch s verejnými kľúčmi za pomoci hašovacích funkcií. Použitie hašovacej funkcie umožnuje urýchliť vytváranie a overovanie podpisu, kedže asymetrické systémy sú pomalé[5] a vďaka jednosmernosti a odolnosti voči kolíziám hašovacích funkcií pridáva na bezpečnosti celej schémy.

Podpisová schéma RSA

Ako z názvu plynie, táto schéma je založená na RSA kryptografickom systéme. V tomto systéme je šifrovacia funkcia E_k verejná a dešifrovacia D_k tajná, aby ktokoľvek mohol poslať zašifrovanú správu a iba vlastník daného súkromného kľúča bol schopný si ju prečítať. V podpisovej schéme je potrebné dosiahnuť presne opačného efektu, preto je RSA systém použitý „obrátene“.

Nech $\mathcal{P} = \mathcal{S} = \mathcal{K} = \mathbb{Z}_n$, kde $n, p, q, e, d, \mathcal{P}, \mathcal{K}, E_k, D_k$ sú definované ako v 1.3.2. Pre $\forall m \in \mathcal{P}$, $\forall k \in \mathcal{K}$, $\forall s \in \mathcal{S}$ položme $sig_k(m) = D_k(m)$ a $ver_k(m, s) = true \Leftrightarrow E_k(s) = m$. Podrobnejšie informácie o tejto schéme je možné nájsť v [7].

1.4 Infraštruktúra verejného kľúča

Techniky kryptografie s verejným kľúčom, ako už bolo spomínané, umožňujú Alici a Bobovi bezpečne komunikovať bez toho, aby sa pred tým dohodli na spoločnom tajnom kľúči. Stačí ak Alica má Bobov verejný kľúč a naopak. Ako však Alica doručí svoj verejný kľúč Bobovi? Skúsme analyzovať, čo sa môže stať, ak Alica pošle svoj verejný kľúč nespoľahlivým komunikačným kanálom. Verejný kľúč, na rozdiel od kľúča používaného pri symetrických šifrách, neobsahuje nijaké tajné informácie, pomocou ktorých by bol útočník schopný dešifrovať neskoršiu komunikáciu. Pasívny útočník teda nepredstavuje v tomto prípade žiadnu hrozbu. Situácia je vážna, ak do hry vstupuje aktívny útočník - Eva. Eva totiž môže posielaný Alicin verejný kľúč modifikovať alebo dokonca nahradiť svojím vlastným verejným kľúčom. Bob túto zmenu bez ďalšej infraštruktúry nie je schopný rozpoznať. V domnení, že mu

[5] V praxi sa ukazuje, že vypočítanie hašu a jeho následné podpísanie je rýchlejšie ako iba podpísanie celého dokumentu.

bol doručený Alicin kľúč, zašifruje správu a odošle Alici. Eva ju opäť odchytí a nakoľko bola zašifrovaná jej verejným kľúčom, dešifrovaním získa dôverný obsah správy.

Jedným z modelov ako takúto situáciu riešiť je použitie tretej strany, ktorej dôverujú Alica aj Bob (Trusted Third Party - TTP). Tretia strana overí Bobovi, či prijatý verejný kľúč je skutočne Alicin. Vo svete dobre popísaná a rozšírená implementácia tohoto modelu je pomocou *certifikačných autorít* (CA). Alica požiada CA o vydanie *certifikátu* jej *verejného kľúča*. Ten obsahuje údaje jednoznačne určujúce Alicinu identitu (tá bola samozrejme predtým CA preverená) ako aj Alicin verejný kľúč. Na žiadosť Boba o Alicin verejný kľúč mu Alica zašle dva dokumenty. Jej verejný kľúč a certifikát jej verejného kľúča, ktorý dostala od CA. Bob je potom schopný overiť pravosť verejného kľúča Alice nasledovne: Skontroluje, na základe podpisu CA na certifikáte Alicinho verejného kľúča, či bol tento nezmenený. Potom za pomoci CA overí platnosť Alicinho certifikátu. Jeho platnosť mohla vypršať, alebo certifikát mohol byť predčasne odobratý. Predčasne odobraté certifikáty sú pravidelne zverejňované CA v zozname zrušených certifikátov. Ak je teda certifikát platný a nezmenený, Bob, keďže dôveruje CA, verí, že verejný kľúč patrí Alici - osobe, ktorá bola uvedená v certifikáte ako majiteľ verejného kľúča.

Certifikačné autority môžu tvoriť rôzne štruktúry podľa dôvery v ich služby. Najčastejšie sú usporiadané hierarchicky. Na vrchole sa nachádza tzv. *koreňová certifikačná autorita*, ktorá osvedčuje a kontroluje CA nižšie v hierarchii vo vykonávaní ich služieb[6]. Systém certifikačných autorít, smerníc, noriem a pravidiel pre vydávanie, používanie a odoberanie certifikátov nazývame *infraštruktúrou verejného kľúča*.

Priamy vzťah k PKI má aj autorita časových pečiatok (TSA - Time Stamp Authority). Jej úlohou je vytvárať a vydávať časové pečiatky k predloženým digitálnym dokumentom. *Časová pečiatka* je informácia pripojená alebo inak logicky spojená s elektronickým dokumentom. Požiadavky, ktoré musí časová pečiatka spĺňať, sú stanovené v §9 zákona NRSR 215/2002 Z.z. o elektronickom podpise (ZoEP). [10] Na ich základe je možné dôveryhodne identifikovať čas existencie elektronického dokumentu, ku ktorému bola časová pečiatka vystavená. Každá časová pečiatka je elektronicky podpísaná TSA. ZoEP vyžaduje použitie časovej pečiatky pri veľkom počte úkonov spojených s elektronickým podpisom a jej vydanie ustanovuje ako akreditovanú certifikačnú službu. V §9 hovorí, že vytvoriť časovú pečiatku môže len akreditovaná certifikačná autorita s použitím súkromného kľúča určeného na tento účel, čím

[6]Na Slovensku je koreňovou CA v oblasti kvalifikovaných certifikátov Národný bezpečnostný úrad (NBÚ).

jasne stotožňuje TSA s akreditovanou CA. O spôsobe jej vyhotovenia, overenia, formáte a ďalších požiadavkách hovorí vyhláška NBÚ 537/2002 Z.z. [11] Pre bližšie informácie o časových pečiatkach a autoritách časových pečiatok odporúčame čitateľa na prácu [12].

1.5 Útoky na kryptografické systémy a protokoly

Tak ako boli ľudia vynaliezaví pri vymýšľaní rôznych kryptografických systémov a protokolov, rovnako boli vynaliezaví aj pri hľadaní techník, ako tieto systémy prelomiť. Časť kryptológie zaoberajúca sa kompromitáciou kryptografických riešení sa nazýva *kryptoanalýza*. V nasledujúcej časti popíšeme ako chápeme bezpečnosť kryptosystému a niektoré základné typy útokov na kryptografiké systémy a protokoly.

1.5.1 Bezpečnosť kryptosystémov

Bezpečnosť kryptosystému (miera odolnosti voči kryptoanalýze) je posudzovaná z viacerých hľadísk a podľa toho tieto systémy rozdeľujeme do týchto základných kategórií:

Absolútne bezpečné kryptosystémy sú kryptosystémy, u ktorých je dokázateľné, že neexistuje kryptoanalytická metóda, ktorá by ich kompromitovala.

Výpočtovo bezpečné kryptosystémy sú založené na tom, že požiadavky na zdroje (výpočtový čas/výkon, pamäť, množstvo vstupných údajov a pod.), ktoré treba na kryptoanalýzu takýchto systémov prekračujú v uspokojivej miere možnosti protivníkov. Pri takýchto systémoch treba brať do úvahy technologický a teoretický pokrok. Výkon kryptoanalytických zariadení z roka na rok rastie a rovnako sa skúmajú stále nové algoritmy na riešenie kryptografických problémov. Napríklad konštruktívny dôkaz $P = NP$, ktorým sa informatika zaoberá už niekoľko desaťročí, by bol vážnym narušením bezpečnosti viacerých kryptosystémov, preto tieto systémy majú len obmedzenú dobu životnosti.

Ekonomická bezpečnosť kryptosystémov sa pozerá na bezpečnosť z pohľadu ekonomickej efektívnosti pre protivníka. Ak cena informácií chránených kryptosystémom je nižšia ako náklady spojené s jeho kryptoanalýzou hovoríme, že je ekonomicky bezpečný. Podobne ako pri výpočtovej bezpečnosti aj tu treba vziať v úvahu pokroky vo vede a výskume.

Náklady na výrobu stále výkonnejších kryptoanalytických zariadení neustále klesajú a stávajú sa tak dostupnejšími aj pre protivníka.

Relatívne bezpečné kryptosystémy predpokladajú, že poznáme možnosti protivníkov. Kryptosystém považujeme za relatívne bezpečný vtedy, ak poznáme prostriedky, aké má protivník k dispozícii, aké metódy používa, koľko času a údajov potrebuje na úspešnú kryptoanalýzu a je dokázateľné, že po dobu, v ktorej má informácia ostať chránená a za uvedených predpokladov, neexistuje metóda, ktorá by kryptosystém narušila.

Pochopiteľne prianím každého zákazníka je dostať čo možno najbezpečnejší kryptosystém. Nasadenie absolútne bezpečných systémov, aj keď takéto existujú, sa veľmi často stretáva s problémami distribúcie kľúčov, a preto sa siaha i keď z podhľadu kryptoanalytika k slabším no však prakticky jednoduchšie realizovateľným systémom.

1.5.2 Útoky na kryptografické systémy

Jednotlivé typy útokov vykonávaných na kryptosystémy sa dajú rozdeliť podľa informácie, ktorú má útočník k dispozícii.

Útok len na základe šifrového textu predpokladá znalosť iba šifrového textu. Útočník sa jeho analyzovaním snaží uhádnuť použitý kľúč resp. nájsť transformáciu, ktorá šifrový text prevedie na otvorený.

Útok na základe znalosti otvoreného textu Pri tomto útoku, predpokladáme, že útočník pozná niekoľko otvorených a k nim prislúchajúcich šifrových textov a z tejto informácie sa snaží nájsť kľúč.

Útok na základe vybraného otvoreného textu ponúka útočníkovi vybrať si/vytvoriť si vlastné otvorené texty, ktoré si nechá zašifrovať.

Útok na základe vybraného šifrového textu naopak ponúka útočníkovi možnosť vybrať si/vytvoriť si vlastný šifrový text, ktorý mu bude dešifrovaný.

Útok na základe volených otvorených textov poskytuje útočníkovi vyberať otvorené texty na zašifrovanie na základe výsledkov analýzy predtým zvolených textov.

Útoky sú uvedené v poradí náročnosti ich úspešného vykonania. Šifrové texty sa posielajú voľne cez verejné siete a ich úspešná kryptoanalýza patrí k najnáročnejším. Použitie asymetrického kryptosystému dáva automaticky

útočníkovi možnosť volenia si otvoreného textu, keďže šifrovacie funkcie sú verejne prístupné. Od dnešných systémov sa preto vyžaduje, aby boli odolné voči všetkým typom útokov.

1.5.3 Útoky na kryptografické protokoly

Rovnako ako na kryptografické systémy aj na kryptografické protokoly existuje množstvo typov útokov. [6] Poväčšine sú zamerané na získanie možnosti predstierať identitu inej entity. Medzi najbežnejšie patria:

Útok opakovaním kedy útočník zopakuje správu poslanú v aktuálnom alebo predchádzajúcom behu.

Útok manipuláciou správ je útok, pri ktorom útočník vyberá a kombinuje posielané správy z viacerých behov (predošlých aj práve prebiehajúcich), pričom i viaceré z týchto behov môžu byť iniciované útočníkom.

Slovníkový útok sa používa najmä pri schémach používajúcich heslá. Útočník predpokladá, že heslá sú slová, ktoré možno nájsť v nejakom dostupnom zozname slov a začne ich všetky skúšať.

Útok úplným preberaním pri ktorom útočník predpokladá, že množina všetkých možných kľúčov/hesiel je malá a snaží sa všetky vyskúšať.

Útok reflekciou pozostáva z preposielania správ v práve bežiacom protokole späť k ich odosielateľovi.

Kapitola 2

Metrológia času a frekvencie

Čas je jednou so siedmich veličín medzinárodnej sústavy jednotiek SI (Système international d'unités). V tomto systéme je to dnes veličina, ktorú sme schopní merať a generovať s najmenšou chybou. Chyba v rádoch 10^{-12} a menej nás bežne núti počítať s relativistickými efektmi. Oblasť výskumu a vedeckého skúmania zaoberajúcou sa spôsobom a technikami merania fyzikálnych veličín nazývame *metrológiou*. V súvislosti s témou práce sa v tejto vede sústredíme práve na časti týkajúce sa veličín času a frekvencie. Meranie času alebo frekvencie je dnes každodennou rutinou a tvorí základ viacerých technológií.

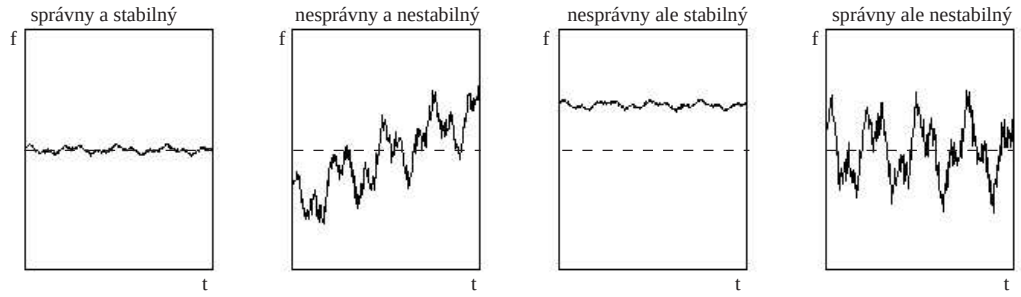
Čas, ako fyzikálna veličina, je veličina protenzívna. Veličina, ktorá sa trvale mení, a ktorú nemôžeme spätne priamo fyzikálne reprodukovať. Je to veličina, ktorá nemôže byť (práve tak ako priestor) oddelená od hmoty a pohybu. Čas zobrazuje stálu zmenu stavu predmetov a zmenu stavu hmoty. Čas a priestor sú definované ako základné formy existencie hmoty.

Etalóny času nám poskytujú 3 základné typy informácie. Prvým je dátum a čas v rámci dňa. Pomocou nich si takmer každý deň pripomíname dátumy narodenia, výročí a iných udalostí, plánujeme stretnutia a robíme svoj denný plán. Ďalším typom je časový interval - množstvo uplynulého času medzi dvoma udalosťami. Náš vek je časový interval od narodenia, sme platení za odpracovaný čas, platíme za množstvo pretelefonovaných minút. Jeho jednotkou je *sekunda*. Posledným typom je frekvencia. V sústave SI je odvodenou veličinou a predstavuje mieru, s akou sa nejaká udalosť opakuje. Denne o nej hovoríme, či už sa rozprávame o rýchlosti procesora, prenosovej linky alebo si ladíme rádio. Všetky tri typy sú spolu úzko previazané. Počítaním sekúnd vieme určiť dátum a čas a počítaním udalostí v časovom intervale, môžeme zmerať ich frekvenciu.

2.1 Základné pojmy

Najpoužívanejším zariadením v metrológii času a frekvencie ale i bežnom živote je *oscilátor*. Budeme tak hovoriť zariadeniu periodicky sa nachádzajúcemu v presne definovanom stave. Jeho výstupom je elektrický signál s frekvenciou blížiacou sa *nominálnej frekvencii* oscilátora, ktorá predstavuje ideálny stav. Termín *správnosť* (*accuracy*) hodnoty frekvencie oscilátora bude označovať tesnosť zhody tejto hodnoty s nominálnou frekvenciou.

Na chod každého oscilátora vplýva jeho okolie, ktoré spôsobuje jeho nestabilitu. Pod pojmom *frekvenčná nestabilita* (*frequency instability*) budeme rozumieť fluktuácie vo frekvencii oscilátora v okolí jeho nominálnej frekvencie zapríčinené zmenami teploty prostredia, stárnutím prístroja, šumom jeho alebo okolitých elektronických častí, šumom samotného rezonátora v oscilátore a inými zmenami. Udáva sa ako pomer veľkosti fluktuácií k nominálkej frekvencii za určité obdobie. Vo všeobecnosti rozlišujeme *krátkodobú* ($\leq$ 100 s) a *dlhodobú* ($\geq$ 100 s) nestabilitu hodnoty frekvencie. Veľakrát budeme hovoriť o nestabilite oscilátora. Budeme mať pritom na mysli nestabilitu hodnoty jeho frekvencie. Pri čítaní ďalšej literatúry sa čitateľ môže stretnúť aj s označením frekvenčná stabilita namiesto nestabilita. Napriek tomu, že to nie je úplne správne, je to tolerované.[16] Vzťah medzi správnosťou a nestabilitou je ilustrovaný na obrázku 2.1



Obr. 2.1: *Vzťah medzi správnosťou a nestabilitou oscilátora.*

Aby metrológia mohla merať a porovnávať jednotlivé veličiny, musí mať definovaný *etalón* (*standard*) - zhmotnenú mieru, referenčný materiál alebo merací systém určený na definovanie, realizovanie či uchovávanie tej ktorej jednotky. Etalóny, majúce na určenom mieste vo všeobecnosti najvyššiu metrologickú kvalitu a od ktorých sa odvodzujú tam vykonané merania, budeme nazývať *referenčné*. Etalón, uznaný oficiálnym rozhodnutím aby slúžil v štáte ako základ na odovzdávanie hodnôt iným etalónom príslušnej veličiny, nazývame *štátny (národný) etalón*. Častokrát ak to nepovedie k nedorozumeniam, nebudeme rozlišovať medzi oscilátorom a etalónom.

Oscilátory slúžia ako generátory elektrického periodického signálu. Najčastejšie sa s nimi budeme stretávať vo forme *frekvenčných etalónov*. Ich hlavnou úlohou je produkovať čo možno najvernejší sínusový alebo impulzný výstupný signál o určenej nominálnej frekvencii. Číselné označenie jednotlivých periód sa deje až v *hodinách* (*clock*) očíslovaním sekundových značiek nazývaných aj *pulzy*. Snaha je, aby hodiny bežali nepretržite, a takto generovali *časovú stupnicu* (*time scale*). Ak je oscilátor súčasťou hodín, jeho frekvenčná nestabilita vedie k fluktuáciám časovej stupnice, ktorú produkuje, oproti ideálnej časovej stupnici konštruovanej na základe jeho nominálnej frekvencie. Toto sa označuje *časovou nestabilitou*. Ak v ďalšom budeme hovoriť o nestabilite a nebude povedané inak, budeme mať na mysli frekvenčnú nestabilitu.

Nestabilita (frekvenčná alebo časová) môže byť náhodná alebo deterministická. V druhom prípade predpokladáme, že je funkciou externých parametrov (teplota prostredia, vek oscilátora a pod.), a tak je možnosť ju odmerať a redukovať. Vlastnosti nestability sa dajú charakterizovať v *časovej* alebo *frekvenčnej doméne*. V časovej doméne sa sledujú vzorky priemernej frekvencie za rôzne časové intervaly. Vo frekvenčnej doméne sú využívané vlastnosti Furiérovej transformácie funkcie reprezentujúcej zmeny vo frekvencii alebo čase. V ďalšom sa budeme zaoberať iba časovou doménou pre jej ľahšiu aplikovateľnosť vo výpočtovej technike.

Náhodné frekvenčné fluktuácie rozdeľujeme do piatich kategórií:

- biely frekvenčný šum (*white frequency noise*)
- biely fázový šum (*white phase noise*)
- blikavý frekvenčný šum (*flicker frequency noise*)
- blikavý fázový šum (*flicker phase noise*)
- náhodný šum (*random walk noise*)

Metódou ako určiť prevládajúcu zložku šumu oscilátora sa budeme zaoberať v kapitole 2.3.2. Dôležité však bude zistiť, kedy v oscilátore prevláda biely frekvenčný šum, ktorý má zo štatistického pohľadu normálne rozdelenie s priemernou hodnotou $\mu = 0$ a dovoľuje klasickým aparátom štatistiky určiť výsledok merania. Najnižšiu dosiahnuteľnú hodnotu fluktuácií frekvencie oscilátora nazývame jeho *spodnou hranicou šumu* (*noise floor*).

Pri vyhodnocovaní merania budeme rozlišovať medzi jeho chybou a neistotou. Rozdiel výsledku merania a skutočnej (pravej) hodnoty veličiny predstavuje *chybu merania* (*measurement error*). *Neistota merania* (*measurement uncertainty*) je parameter priradený k výsledku merania, ktorý charakterizuje rozptyl hodnôt, ktoré sa môžu zdôvodnene priraďovať k meranej veličine.

Takýmto parametrom môže byť smerodajná odchýlka alebo šírka intervalu spoľahlivosti. Okrem týchto nás bude ešte zaujímať *odchýlka* (*offset, deviation*), pod ktorou budeme rozumieť rozdiel hodnoty a referenčnej hodnoty.

Napriek tomu, že budeme hovoriť o čase, nedefinovali sme nikde jeho presnosť. Je to tým, že Slovenská technická norma [13] takýto termín nepozná. Pod presnosťou sa rozumie neistota alebo správnosť. Ak máme hodiny s "presným" časom, v súlade s STN hovoríme o ich správnom čase (o tesnosti zhody času hodín a skutočného (referenčného) času). Posúdiť „presnosť“ hodín môžeme len do takej miery, akú nám to dovolí metóda jej merania, pričom každá metóda vykazuje určitú neistotu merania.

Nato aby sme boli schopní vzájomne porovnávať dva vzdialené etalóny bude potrebný prenos signálu z jedného etalónu k druhému. Pri opise možných spôsobov realizácie prenosu sa budeme stretávať s pojmom *prenosové oneskorenie*. Predstavuje časový interval potrebný na prenesenie signálu/informácie z jedného miesta na druhé. Jeho zrejmou príčinou je konečná rýchlosť šírenia signálu. Prenos časovej informácie medzi hodinami nám umožní spustiť proces nastavenia dvoch alebo viacerých hodín na rovnaký čas - ich *synchronizáciu*.

2.2 História merania času

2.2.1 Kalendár

Zmeny v prírode, nočná obloha, striedanie dní a nocí boli v pozornosti ľudstva už od počiatku. S rozvojom astronomického pozorovania však nastala potreba, zaznamenávať čas, aby bolo možné popísať dráhu nebeských telies a robiť predpovede. Vznikali prvé kalendáre rozdeľujúce čas do väčších úsekov s využitím prírodných javov. Najkratší prirodzený časový úsek bol deň alebo mesiac. Známe a dodnes používané kalendáre sú islamský, židovský či Gregoriánsky. Práve posledne menovaný je používaný aj na Slovensku. Do platnosti vstúpil roku 1582 reformou pápeža Gregora XIII[1]. Delenie dní na hodiny, minúty a sekundy sme zdedili bo Babylóňanoch.

Tento komplexný systém, v ktorom jednotky nemajú voči sebe konštantný vzťah, kde rok môže mať 365 alebo 366 dní a deň, normálne trvajúci 86 400 sekúnd, od roku 1971 niekedy o jednu menej či viac, sa ukázal nevhodný pre astronómov. Za účelom zjednodušenia práce bol zavedený *Juliánsky dátum* (*Julian Date* - JD). Je založený na kontinuálnom počte dní od roku 4713 p.n.l., pričom deň začína o dvanástej hodine na poludnie. Rozširuje sa

[1]Je natoľko správny, že medzi rokom 1582 a 3200 sa pridá zhruba jeden deň oproti tropickému kalendáru (založenom na tropickom roku - dobe medzi dvoma nasledujúcimi prechodmi slnka stredným jarným bodom).

pridaním desatinnej časti dňa. V metrologickej praxi, pri výskume rotácie Zeme alebo vesmírnych skúmaniach sa však častejšie používa *Modifikovaný juliánsky dátum* (*Modified Julian Date* - MJD) definovaný ako

$$\mathrm{MJD} = \mathrm{JD} - 2\,400\,000,5\ . \tag{2.1}$$

Jeho výhodou je kratší zápis a presunutie začiatku dňa na polnoc[2].

2.2.2 Meranie času na báze striedania dňa a noci

Tento spôsob merania času má svoj pôvod v delení dňa a noci od východu slnka po západ resp. naopak na 12 hodín. Je zrejmé, že dĺžka trvania jednej hodiny počas dňa je iná ako počas noci, je závislá na ročnom období (od toho aj jeho názov - *sezónny čas*) a polohe pozorovateľa, ale astronómovia ho používali až do 15. storočia. Zlepšenie prišlo s *pravým slnečným časom*, ktorý definuje hodinu ako 15° slnečného uhla v mieste pozorovateľa. Ani tento čas však nebol uniformný. Nerovnomernosti zapríčinené eliptickou dráhou zeme a kývaním sa zemskej osi, a ktorých amplitúda dosahovala až 30 minút v priebehu roka, boli odstránené zavedením *stredného slnečného času* (*mean solar time*). [14]

S nástupom železníc v druhej polovici 19 stor. prišla požiadavka na jednotnú definíciu hodiny aspoň na národnej úrovni, keďže interval jednej hodiny stredného slnečného času je stále závislý od poludníka, na ktorom sa slnko pozoruje. Vo veľkom počte krajín sa zaviedol stredný slnečný čas poludníka, ktorý prechádzal hlavným mestom zvýšený o 12 hodín[3]. V štátoch s veľkými rozdielmi v zemepisnej dĺžke však aj takéto riešenie bolo nepraktické. V roku 1870 prišiel Ch. Dowd v USA s myšlienkou časových pásiem - rozdelením územia na pásma líšiace sa o jednu celú hodinu, tak aby slnečné poludnie nastalo približne o 12 h. [15] Tento koncept bol najprv prijatý kanadskými železnicami.

Dohoda o medzinárodnom ujednotení času a vzniku *univerzálneho času* (*Universal Time* - UT)[4] prišla až v roku 1884. Vybraný bol stredný slnečný čas na greenwichskom poludníku (*Greenwich Mean Time* - GMT), kedže už bol dlho používaný ako počiatok zemepisných dĺžok na námorných mapách. Rovnako sa prijalo, že univerzálny deň začína o polnoci na greenwichskom poludníku[5]. Krása tejto jednoty bola narušená v roku 1916. Francúzsko, ne-

[2]Napríklad 1. januára 2000 00:00 odpovedá 51 544,0 MJD.

[3]Astronomické časy vždy začínali o dvanástej hodine na poludnie.

[4]Neskôr bol definovaný aj čas UT1 - UT čas korigovaný o pohyb zemského pólu a čas UT2 ako čas UT1 opravený o sezónne variácie v rotácii Zeme.

[5]Je treba pripomenúť časté nesprávne použitie skratky GMT namiesto UT. Stupnica GMT je totiž posunutá o 12 hodín a začína na poludnie.

skôr nasledované ďalšími krajinami medzi inými aj Československom, zaviedlo zimný a letný čas.

Až do roku 1970 sa mechanické či iné hodiny používali ako okamžitá aproximácia UT času v reálnom čase. Po každom astronomickom pozorovaní boli vyrátané ich nové korekcie, aby ich časová stupnica vykazovala čo najmenšie odchýlky od UT. Rozvoj vedy a techniky najmä v oblasti šírenia elektromagnetických vĺn však prinášal ďalšie potiaže. Keď rádiové vlny boli schopné prekonať Atlantik okolo roku 1910, vedci zistili, že technická realizácia univerzálneho času napriek jeho jednoznačnej definícii je značne zložitá. Merania ukázali odchýlky jednej až dvoch sekúnd. Rok 1919 dal preto vzniku BIH (Bureau international de l'heure). Jeho hlavným cieľom bolo poskytnúť jedinú aproximáciu univerzálneho času - *definitívny čas*. Tento úrad sa v roku 1988 rozpadol na BIPM (Bureau international des poids et mesures), ktorý má na starosti meranie atómového času a IERS (International Earth Rotation Service) zastávajúci aktivity v oblasti astronómie a geodézie.

Do roku 1960 bola jedna sekunda chápala ako trvanie 1/86 400 slnečného dňa. Táto definícia však nebola nikdy oficiálne prijatá.

2.2.3 Čas založený na dynamike slnečného systému

Iným spôsobom merania času bolo pozorovanie orbitálnych pohybov vesmírnych telies. Dogma pretrvávajúca z antického Grécka, že rotácia zeme je uniformná sa začala rozpadať až s príchodom Keplera. V 1825 Laplace napísal, že od roku asi 125 p.n.l. sa dĺžka dňa nezmenila o viac ako 0,00864 (dnešných) sekúnd. [16] Presvedčivý dôkaz priniesol až rok 1927, po ktorom bolo jasné, že rotácia zeme nie je dobrým oscilátorom.

Efemeridový čas bol definovaný v roku 1952 na základe pohybov slnka analyzovaných od roku 1900. Jeho prínosom bola značne komplikovaná definícia sekundy v rokoch 1960 až 1967 ako 1/31556925,9747 tropického roku pre 0. január 1900 o 12:00 efemeridového času. Prednosťou efemeridnej časovej stupnice sú jej z dlhodobého hľadiska malé odchýlky v stabilite. Nevýhodou je jeho zlá kvalita odčítavania, ktorá sa pohybuje v rádoch 0,1 s. Používa sa už len v astronómii.

2.2.4 Atómové meranie času

Ku koncu 19. storočia vedci dávno akceptovali, že látky sa skladajú z molekúl zložených z atómov. Podarilo sa nájsť vzťah medzi štruktúrou vyžarovaného spektra látky zloženej z molekúl a atómov excitovaných plynov. Už v 1873-om Maxwell a neskôr v 1879-om roku Kelvin navrhli použiť vlnovú dĺžku spektrálnej čiary a periódu prislúchajúceho žiarenia na definíciu metra resp.

sekundy. Tieto návrhy boli vskutku nadčasové, ak si uvedomíme, že takáto definícia metra bola prijatá až v roku 1960. K vzniku prvých atómových hodín bolo treba vybádať veľa poznatkov z oblasti elektromagnetizmu, kvantovej fyziky a spektroskopie, ku ktorým prispeli najmä Planck, Einstein, Bohr, Hertz, De Broglie s Heisenbergom a Schrödingerom, Stern a ďalší. Na konci 2. svetovej vojny boli vedci schopní vyrobiť rádiové vlny o kmitočte 30 GHz a zmerať ich frekvenciu.

Odtiaľ bol len kúsok k skonštruovaniu prvých atómových hodín roku 1948 v USA v laboratóriu dnešného NIST-u (National Institute of Standards and Technology). Ako referencia bola použitá absorpčná čiara molekúl amónia v oblasti frekvencií okolo 24 GHz. Molekulárna rezonancia riadila frekvenciu kryštálového oscilátora, ktorý generoval časové značky. Prechod medzi dvoma veľmi jemnými úrovňami základného stavu atómu cézia 133 bol známy už v roku 1940 a možnosti využitia magnetickej rezonancie diskutované od roku 1939. Avšak spoľahlivých céziových atómových hodín sa svet dočkal až v roku 1955, kedy ich prvýkrát postavili páni Essen a Perry vo Veľkej Británii. [17] Ďalším skúmaným princípom pre konštrukciu hodín bolo mikrovlnné zosilňovanie, pracujúce na základe vzbudenej emisie žiarenia atómov - maser (Microwave Amplification by Stimulated Emission of Radiation). Skúmaný bol v rovnakom čase ako v USA, tak i v ZSSR. Prvé amoniakové masery sa objavili v roku 1955. Vodík ako základný prvok pre maser sa začal využívať o päť rokov neskôr.

Relatívne odchýlky vo frekvencii prvých céziových hodín dosahovali hodnoty 10^{-9} (maserov 10^{-10}). Určenie presnej frekvencie prechodu medzi dvoma úrovňami základného stavu atómu v céziových hodínách bolo vykonané až v roku 1958. Essen a Parry používali v čase vývoja sekundu odvodenú od stredného slnečného času, ktorá bola dostupná v reálnom čase. Efemeridná sekunda už bola v tom čase definovaná (aj keď nie medzinárodne prijatá ako SI jednotka), ale jej realizácia si vyžadovala dlhotrvajúcu analýzu. Tú previedol Markowitz a stanovil frekvenciu prechodu na $9\,192\,631\,770 \pm 20$ Hz. Jednotka Hz teda bola závislá na efemeridnej sekunde a neistota ± 20 Hz skoro celá zapríčinená chybou jej realizácie. Samozrejme, že vedecká obec zaoberajúca sa skúmaním atómových frekvenčných etalónov si priala jednoznačnú hodnotu. Keď relatívne frekvenčné odchýlky týchto etalónov dosiahli 10^{-12} v roku 1967, astronomicky definovaná sekunda bola predefinovaná kvantovou definíciou ako *trvanie 9 192 631 770 period žiarenia prislúchajúcemu prechodu medzi dvoma veľmi jemnými úrovňami základného stavu atómu cézia 133*. Čo najvernejšie sa tak priblížila k pôvodnej definícii. Od tých čias sa relatívna nestabilita najlepších céziových etalónov posunula k hodnotám 10^{-16}/deň. Problémy s realizáciou atómového času, keď rôzne laboratória udržujú rôzne časové stupnice, sú rovnaké ako pri UT stupnici a aj rieše-

nie bolo rovnaké. Definovaná bola časová stupnica TAI (Temps atomique international) ako časová referenčná súradnica ustanovená medzinárodným ústredím pre čas - BIH[6] na základe meraní atómových hodín prevádzkovaných v rozličných ustanovizniach v súlade s definíciou sekundy, jednotkou času v systéme SI.

2.2.5 Koordinovaný univerzálny čas - UTC

Vznik časovej stupnice UTC bol podnietený úsilím koordinovať vysielanie rádiových časových signálov (vysielaný bol UT čas). S príchodom atómových hodín a predefinovaním sekundy s využitím efemeridovej časovej stupnice prišli vedci k zisteniu, že atómové časové stupnice bežia rýchlejšie oproti UT. Nastala potreba zavedenia relatívnej frekvenčnej korekcie y_U. UTC bol matematicky presne definovaný v roku 1965 BIH rovnicou

$$UTC - TAI = y_U(TAI - TAI_0) + B \ , \tag{2.2}$$

kde TAI_0 je ľubovolne zvolený počiatok a B konštanta menená v skokoch, aby platila nerovnosť

$$\mid UTC - UT2 \mid \leq \varepsilon. \tag{2.3}$$

Korekcia y_U na rádiových vysielačoch času však častokrát musela byť riešená dolaďovaním oscilátorov. Dôvod nevysielania času TAI namiesto UT predstavovalo námorníctvo využívajúce tieto služby. Navigácia bola stále založená na pohybe nebeských telies, a tak by vznikla potreba zadávať korekciu pri každom určovaní polohy, čo sa zdalo ako príliš riskantné. Spor sa vyriešil až v roku 1970, kedy sa stanovilo, že UTC bude definované s $y_U = 0$ a B rovným celému násobku sekúnd, takým aby nerovnosť (2.3) platila najskôr pre $\varepsilon = 0,7$ s a od roku 1974 $\varepsilon = 0,9$ s.

Prestupná sekunda sa pridáva alebo odoberá na konci mesiaca prednostne decembra alebo júna, inak na konci septembra či marca. Ak sa sekunda pridáva, jej začiatok bol dohodou stanovený na 23 h 59 m 60 s a koniec na 0 h 0 m 0 s nasledujúceho dňa. Pri takomto spôsobe nenastane nejednoznačnosť v označovaní udalostí v čase. Bohužiaľ to však spôsobuje nejednoznačnosť v iných systémoch, napríklad používajúcich zlomky dňa. Dátum N,000 005 79 môže znamenať deň (N-1) o 23 h 59 m 60,5 s alebo aj deň N o 0 h 0 m 0,5 s. Nejednoznačnosť nenastáva ak sa má sekunda odobrať. Avšak pravdepodobnosť tejto potreby je takmer nulová.

Dátumy zavedenia prestupnej sekundy stanovuje IERS a sú oznamované najmenej 8 týždňov vopred. K februáru 2004 je rozdiel TAI-UTC +32 sekúnd a zatiaľ nie je známy dátum pridania ďalšej.

[6] dnešné BIPM

Pretože na realizácii UTC sa podieľajú metrologické ústavy všetkých vyspelých krajín sveta, možno ho považovať za medzinárodný etalón času a frekvencie.

2.3 Nestabilita času a frekvencie

Každý dej v prírode je ovplyvňovaný podmienkami prostredia, v ktorom prebieha. Taktiež oscilátory sú nimi zasiahnuté a pod zmenami prostredia sa mení aj ich perióda kmitania a stávajú sa tak nestabilnými. Preto si priblížime základné metódy merania a vyhodnocovania ich nestability.

2.3.1 Spôsoby merania nestability

Každé meranie v metrológii spočíva na porovnávaní s etalónovou alebo konvenčne skutočnou hodnotou. Meranie nestability si vyžaduje aspoň dva oscilátory. Jednak je to oscilátor, ktorý chceme zmerať a jednak referenčný etalón, ktorý musí mať aspoň takú kvalitu ako oscilátor podliehajúci meraniu. V meraní sa porovnávajú metrologické kvality týchto dvoch oscilátorov. V prípade, že referenčný etalón má lepšiu stabilitu, nameraná nestabilita sa celá chápe ako nestabilita meraného oscilátora. Ak sú oscilátory rovnakej kvality, príspevky jednotlivých oscilátorov k nestabilite sa dajú prijateľným spôsobom rozdeliť pomocou metódy trojrohého klobúka, za použitia tretieho oscilátora rovnakej kvality. [16]

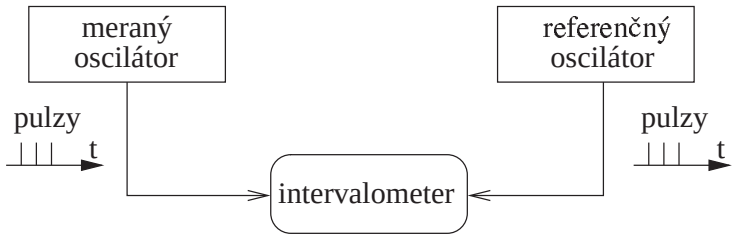
Meranie nestability času v časovej doméne

Schematické znázornenie zapojenia aparatúry je naznačené na obrázku 2.2. Referenčný oscilátor je pripojený na prvý vstup intervalometru a meraný na druhý. *Intervalometer* spustí meranie časového intervalu s príchodom pulzu na prvom vstupe a zastaví s príchodom pulzu na vstupe druhom. Výsledkom je množina hodnôt x_i meraných v rovnakých časových rozostupoch τ. Tieto hodnoty sú ovplyvnené oneskoreniami zapríčinenými dobou prechodu pulzu z oscilátora do intervalometru. Pokiaľ je toto oneskorenie konštantné, potom nemá vplyv pri štatistickom určovaní nestability.

Bežnými intervalometrami, ako napr. HP 53132A používaným v Slovenskom metrologickom ústave (SMÚ) na tieto účely, sa dajú merať intervaly už od 150 ps. [18]

2.3.2 Allanova odchýlka

Allanova odchýlka (*Allan deviation*) je štatistický ukazovateľ (podobne ako smerodajná odchýlka) vyrátavaný z dát získaných meraním v časovej do-



Obr. 2.2: *Schematické znázornenie merania nestability času.*

méne. Pre väčšinu iných meraní možno s úspechom použiť odhad smerodajnej odchýlky definovaný ako

$$s = \sqrt{\frac{1}{N-1}\sum_{i=1}^{N}(x_i - \bar{x})^2} \,, \tag{2.4}$$

kde $N \geq 2$ je počet vzoriek a

$$\bar{x} = \frac{1}{N}\sum_{i=1}^{N} x_i \,, \tag{2.5}$$

ich priemerná hodnota. [19] Odhad smerodajnej odchýlky je však funkciou množstva vzoriek N a navyše ak sú v oscilácii oscilátora prítomné aj iné typy šumu ako biely frekvenčný, nevykazuje požadované správanie[7].

Spomínané nedostatky odstraňuje Allanova odchýlka prijatá aj ako IEEE štandard pre špecifikáciu stability v časovej doméne. [20] Ak označíme namerané časové intervaly intervalometrom (viď kap. 2.3.1) ako $x_i, 1 \leq i \leq M+1$ a

$$y_i = \frac{x_{i+1} - x_i}{\tau} \,, \tag{2.6}$$

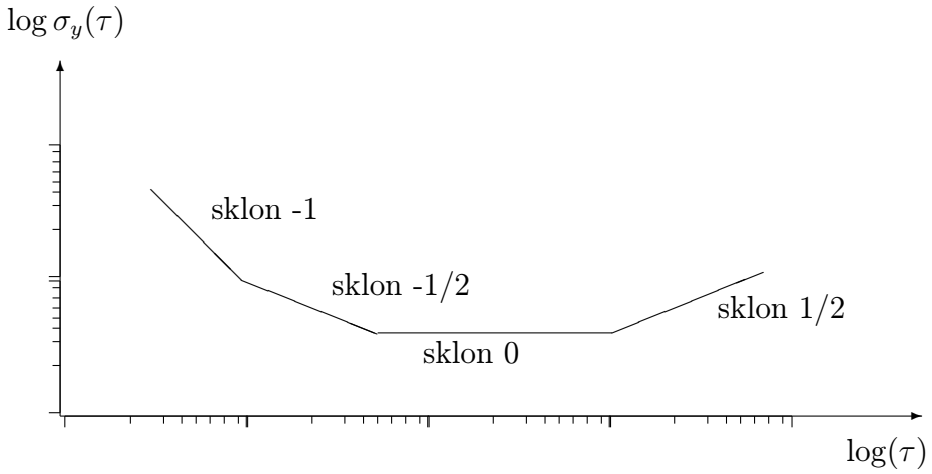
kde τ je časový interval medzi dvoma po sebe nasledujúcimi meraniami (typicky 1 s), potom Allanova odchýlka je definovaná rovnicou

$$\sigma_y(\tau) = \sqrt{\frac{1}{2(M-1)}\sum_{i=1}^{M-1}(y_{i+1} - y_i)^2} \,. \tag{2.7}$$

Zaujímavé je ako sa Allanova odchýlka správa pre rôzne intervaly τ. Ak predpokladáme, že odchýlky oscilátorov sme merali intervalometrom v intervaloch τ_0, potom jednoduchou iteratívnou metódou môžeme dostať hodnotu $\sigma_y(\tau)$ pre celočíselné násobky τ_0. Stačí ak definujeme y_i ako

$$y_i = \frac{1}{k\tau_0}(x_{ki+1} - x_{k(i-1)+1}) \tag{2.8}$$

[7]Napríklad pre modely signálu s blikajúcim frekvenčným šumom so vzrastajúcim počtom vzoriek odhad smerodajnej odchýlky monotónne neohraničene rastie.



Obr. 2.3: *Typický priebeh závislosti Allanovej odchýlky $\sigma_y(\tau)$ od τ.*

Sklon	Typ šumu
-1	biely alebo blikajúci fázový šum
-1/2	biely frekvenčný šum
0	blikajúci frekvenčný šum
+1/2	náhodný frekvenčný šum

Tabuľka 2.1: *Vzťah medzi sklonom grafu $\sigma_y(\tau)$ a prevládajúcim typom šumu.*

a dosadíme ich do (2.7).

Iným spôsobom je pre výpočet $\sigma_y(\tau)$ použiť vzťah

$$\sigma_y(\tau) = \sqrt{\frac{1}{2(M-2k+1)(k\tau_0)^2} \sum_{i=1}^{M-2k+1} (x_{i+2k} - 2x_{i+k} + x_i)^2}\ , \qquad (2.9)$$

ktorý lepšie využíva namerané hodnoty a dosahuje tak menšiu neistotu (kým za použitia (2.8) vstupovalo do sumy (2.7) $\lfloor \frac{M}{k} \rfloor - 1$ sčítancov, pri použití (2.9) je to $M - 2k + 1$). [16]

Podstatné na Allanovej odchýlke je, že dokáže vypovedať aká forma šumu prevláda počas danej priemerovacej periódy τ. Za týmto účelom je závislosť $\sigma_y(\tau)$ na τ vynesená do grafu pre rôzne hodnoty τ s logaritmickými stupnicami na oboch osiach (obr. 2.3). Predtým je ale nutné z nameraných hodnôt odstrániť systematické chyby (napr. lineárnu závislosť a pod.). Určiť prevládajúci typ šumu možno potom podľa sklonu grafu na základe tabuľky 2.1.

V oblasti intervalu τ s prevládajúcim bielym frekvenčným šumom sa dá, ako bolo už spomínané vyššie, s úspechom použiť Gaussova štatistika. Pre

obojstranný interval spoľahlivosti skutočnej priemernej hodnoty μ na hladine významnosti α (obyčajne 95% alebo 99%, tj. $\alpha = 0,05$ resp. $\alpha = 0,01$) platí

$$\mu = \bar{x} \pm t_{1-\frac{\alpha}{2}}(\frac{s}{\sqrt{N}}) \ , \tag{2.10}$$

kde $t_{1-\frac{\alpha}{2}}$ je kvantyl Studentovho rozdelenia a s spolu s $\bar{x}$ vypočítame z rovníc (2.4) a (2.5). Interval spoľahlivosti bude teda tým užší, čím väčšie bude N.

Allanova odchýlka sa dá využiť aj pri určovaní synchronizačného intervalu dvoch hodín. Najprv intervalometrom odmeriame časové odchýlky voľne bežiacich hodín voči referenčnému etalónu (viď kap. 2.3.1), odstránime systematické chyby a zakreslíme výslednú $\sigma_y(\tau)$ do grafu. Ak má Allanova odchýlka na grafe sklon -1, prevládajúci typ šumu je biely alebo blikajúci fázový, čo nám napovedá, že šum v nameraných dátach je viac spôsobený samotným procesom merania ako fluktuáciami frekvencie meraných hodín. Bolo by chybou tieto namerané hodnoty použiť pre poopravenie času hodín, pretože stabilita frekvenčného oscilátora hodín je lepšia ako pozorované fluktuácie.

Pre predikciu frekvenčných fluktuácií je najvhodnejší biely frekvenčný šum. Vtedy existuje priemerná hodnota relatívnej odchýlky frekvencie $y_i = \frac{x_{i+1}-x_i}{\tau}$. y_i sa k tejto priemernej hodnote blíži s predlžovaním priemerovacieho intervalu τ. Biely frekvenčný šum nastáva pri sklone grafu -1/2. Predlžovaním priemerovacieho intervalu τ až po ďalší zlom v grafe sa teda lepší odhad správania oscilátora hodín v budúcnosti a tým znižuje neistota. Ďalším predlžovaním priemerovacieho intervalu až do oblastí τ, kedy začína prevládať blikajúci frekvenčný a náhodný šum (teda za hodnotu τ, pri ktorej sa dosahuje spodná hranicu šumu), sa neistota odhadu bude len horšiť. Interval synchronizácie preto treba vybrať z intervalu hodnôt τ, kedy v meraní prevláda biely frekvenčný šum a sklon grafu Allanovej odchýlky $\sigma_y(\tau)$ v závislosti od τ je -1/2. Podrobnejší rozpis predchádzajúcich myšlienok možno nájsť napr. v [21].

2.4 Etalóny frekvencie

Pri hľadaní stabilných etalónov pre použitie je rozhodujúcim faktorom ich *kvalita*. Kvalita Q oscilátora je podiel jeho prirodzenej rezonančnej frekvencie a jej rezonančnej šírky[8]. Rezonančná šírka je rozsah hodnôt prirodzenej

[8]V kapitole 2.1 sme definovali nominálnu frekvenciu oscilátora. V tejto kapitole sa zaoberáme vnútornou stavbou oscilátora, v ktorom je vždy použitá nejaká sústava schopná periodickej zmeny stavu (napr. atómy cézia) s prirodzenou rezonančnou frekvenciou (pre cézium 9,192 631 770 GHz). Na výstupe oscilátora (ako elektronického zariadenia) sa však objavuje v ideálnom prípade nominálna frekvencia (typicky 10 alebo 5 MHz).

rezonančnej frekvencie, na ktorých bude oscilátor oscilovať. Vo všeobecnosti teda platí, že čím vyššia je kvalita oscilátora tým bude menšia nestabilita.

Typ oscilátora	Kremíkový		Rubídiový	Céziový lúč	Vodíkový maser
	TCXO	OCXO			
Q	10^4 až 10^6	$3,2 \times 10^6$	10^7	10^8	10^9
Rezonančná f.	rôzna	rôzna	6,834 GHz	9,192 GHz	1,420 GHz
Stabilita $\sigma_y(\tau), \tau = 1s$	$1 - 0,1 \times 10^{-8}$	1×10^{-12}	$5 - 0,5 \times 10^{-11}$	$5 - 0,5 \times 10^{-11}$	1×10^{-12}
Hranica šumu, $\sigma_y(\tau)$	1×10^{-9}	1×10^{-12}	1×10^{-12}	1×10^{-14}	1×10^{-15}
pre τ = [sek]	1 až 10^2	1 až 10^2	10^3 až 10^5	10^5 až 10^7	10^3 až 10^5
Starnutie/rok	5×10^{-7}	5×10^{-9}	1×10^{-10}	žiadne	$\simeq 1 \times 10^{-13}$
Chyba frekvencie po zahriatí	1×10^{-6}	1×10^{-8} až 1×10^{-10}	5×10^{-10} až 1×10^{-12}	5×10^{-12} až 1×10^{-14}	1×10^{-12} až 1×10^{-13}
Doba zahrievania	< 10 sek	< 5 min	< 5 min	30 min	24 hod

Tabuľka 2.2: *Prehľad rôznych typov oscilátorov.*

Dnes sa v praxi využívajú 4 typy. Kryštálové oscilátory dosahujú najvyššej kvality spomedzi všetkých mechanických. Vodíkové masery spolu s rubídiovými a céziovými etalónmi sú založené na dejoch na atomárnej úrovni. Ich kvalita je rádovo vyššia ako mechanických oscilátorov. Prehľad ďalej popisovaných typov je v tabuľke 2.4.

2.4.1 Etalóny s kryštálom kremíka

Oscilátory na báze kryštálu kremíka (*quartz crystal oscillators*) patria k najbežnejšiemu typu. Ročne sa ich vyrobí niekoľko miliárd a nájdeme ich takmer v každých náramkových hodinách či iných elektronických obvodoch. Dokonca sú základom aj ostatných ďalej popisovaných atómových oscilátorov.

Kremíkový kryštál (pre ich masové nasadenie najčastejšie syntetický) v oscilátore je rezonátorom, ktorý sa privedením napätia vratne deformuje (zväčší alebo zmenší). Jeho rezonančná frekvencia je závislá od veľkosti, rezu, veku, ako i stavu okolitého prostredia, najmä teploty a vibrácií. Preto boli vyvinuté rôzne technológie ako túto závislosť kompenzovať. OCXO (Oven controlled crystal oscillator) kryštálové oscilátory majú kryštál umiestnený v tepelne regulovanej komore. Pri jeho zapnutí je potrebný čas na zahriatie, pokiaľ sa teplota kryštálu nestabilizuje. Iným typom sú TCXO (Temperature-compensated crystal oscillator) oscilátory. V nich sú umiestnené snímače teploty kryštálu, ktoré generujú príslušné korekcie.

Oscilátory s kremíkovým kryštálom dosahujú vynikajúcu krátkodobu stabilitu (až $10 \times 10^{-12}/sec$ pre OCXO) . Dlhodobá stabilita je limitovaná najmä stárnutím kryštálu, kedy sa vekom mení jeho rezonančná frekvencia.

Tieto typy oscilátorov sú základom hodín používaných v dnešných počítačoch. Ich dlhodobá stabilita sa pohybuje na úrovni 10^{-4} a pri použití špecializovaných rozširujúcich kariet s TCXO oscilátormi okolo 10^{-6}/deň.

2.4.2 Rubídiové etalóny

Prirodzená rezonančná frekvencia 6 834 682 608 Hz atómu rubídia ^{87}Rb kontroluje kremíkový kryštálový oscilátor. Mikrovlnné žiarenie, ktorého frekvencia je odvodená z kryštálového oscilátora, udržuje atómy rubídiovej pary v stave s určitou energiou. Cez túto paru je vyslaný optický lúč generovaný rubídiovou lampou a fotobunkou sa meria množstvo pohlteného žiarenia, ktoré slúži na doladenie frekvencie kryštálového oscilátora, tak aby množstvo pohlteného žiarenia bolo maximálne. Nominálna frekvencia etalónu je teda odvodená od kryštálového oscilátora (ako aj v ostatných typoch). Posuny rezonančnej frekvencie sú spôsobené najmä znečistením rubídiovej pary atómami iných prvkov.

Výhodou rubídiových etalónov je ich lepšia krátkodobá stabilita ako kryštálových oscilátorov, menšie rozmery a cena oproti céziovým. Z triedy atómových oscilátorov patria k najkompaktnejším.

2.4.3 Céziové etalóny

Céziové oscilátory sú primárnymi etalónmi (v zmysle [13]), odkedy bola SI sekunda definovaná na základe rezonančnej frekvencie atómu cézia 133, ktorá je 9 192 631 770 Hz. Dnes sú známe dva návrhy ako využiť ich rezonanciu - céziový lúč a céziová fontána.

Oscilátory na báze céziového lúča (*caesium beam*) pracujú podobne ako rubídiové. Atómy cézia 133 sú najprv zahrievané a potom ako plyn vstupujú do vákuovej trubice v úzkom lúči. Tento je vystavený mikrovlnnému žiareniu, odvodeného od frekvencie kryštálového oscilátora, ktoré mení stav atómov. Počet atómov, ktorým mikrovlnné žiarenie zmenilo stav sa snažime maximalizovať doladťovaním frekvencie kryštálového oscilátora.

Dĺžka vákuovej trubice je okolo 50 cm v bežne dostupných etalónoch a rýchlosť céziového lúča väčšia ako 100 m/s. To ohraničuje čas pozorovania na stovky milisekúnd a výslednú rezonančnú šírku na pár sto herzov.

Spomaliť atómy cézia, a tak zmenšiť rezonančnú šírku sa snaží návrh céziovej fontány (*caesium fontain*). Pri tejto konštrukcii je plyn z atómov cézia vypúšťaný do vákuovej komory. Tam sú sústavou laserov atómy podchladené na teplotu pár stotín nad absolútnou nulou a stlačené do malého priestoru. Ďalšie lasery ich potom vytláčajú do výšky asi jedného metra, odkiaľ po ich vypnutí padajú pôsobením gravitačnej sily a sú vystavené mikrovlnnému žiareniu. Tie, ktoré zmenili svoj stav pod vplyvom mikrovlnného žiarenia, po ožiarení laserom emitujú fotón. Ich počet sa opäť snažime maximalizovať doladením kryštálového oscilátora, od ktorého je odvodená frekvencia mikrovlnného žiarenia.

Kvalita etalónov na báze céziovej fontány je asi sto násobne vyššia a pohybuje sa v rádoch 10^{10}. Stabilita oboch typov je však lepšia ako 1×10^{-12} za deň.

2.4.4 Vodíkové masery

Vodíkové masery pracujú na rezonančnej frekvencii vodíka 1 420 405 752 Hz. Princíp ich činnosti je založený na vysielaní plynu vodíka cez magnetické pole, ktoré vytriedi atómy s určitým stavom. Tie vstupujú do banky, v ktorej niektoré prejdú do stavu s nižšou energiou a vyžiaria fotóny mikrovlnného žiarenia. Tieto fotóny spôsobia prechod iných atómov, a takto je v banke tvorené mikrovlnné žiarenie. Výsledný mikrovlnný signál sa používa na riadenie kremíkového kryštálového oscilátora.

Napriek tomu, že rezonančná frekvencia vodíku je nižšia ako cézia, rezonančná šírka je obyčajne iba niekoľko herzov. Preto kvalita týchto oscilátorov je rádovo 10^9. Ich krátkodobá stabilita je rovnako lepšia ako pri céziových (typicky $< 1 \times 10^{-12}$/s), ale pri meraniach dlhších ako pár dní alebo týždňov sú céziové oscilátory stabilnejšie.

2.5 Spôsoby porovnávania času

Pre vytvorenie nadväznosti (viď kap. 2.8) je nutné podľa definície vytvoriť neprerušený reťazec porovnaní. Iba málo prípadov je však takých, že etalón s vyššou metrologickou kvalitou sa nachádza na tom istom mieste ako ten, s ktorým ho chceme porovnať. Preto si teraz priblížime rôzne spôsoby ako vzdialené etalóny porovnať.

2.5.1 Transport hodín

Transport hodín najstarším spôsobom porovnávania a patrí medzi nižšie popísanú Common view metódu. Keďže u vysokokvalitných etalónov je nemysliteľným narúšať akýmkoľvek spôsobom ich pracovné prostredie z dôvodu degradácie stability, používali sa na tento účel prenosné porovnávacie etalóny. Ak je treba porovnať dva etalóny, jeden v mieste A a druhý v mieste B, prenosné hodiny sa najprv zosynchronizovali s etalónom v bode A a určil sa rozdiel hodnôt výstupných frekvencií medzi nimi. Následne sa fyzicky transportovali do bodu B, kde sa porovnali s miestnym etalónom. Nakoniec sa opäť previezli do bodu A, kde bolo uskutočnené kontrolné meranie voči miestnemu etalónu. Výhodou tohto spôsobu je malá chyba (1 ns v čase, a 10^{-14} pre frekvenciu [22]) merania a nízke nároky na zdroje. Ničmenej pre rôzne administratívne prekážky (napr. bezpečnostné pravidlá leteckej prepravy) a

dostupnosť iných porovnateľne výkonných spôsobov sa dnes už takmer nepoužíva.

2.5.2 Jednosmerný prenos elektromagnetických signálov

Pri jednosmernom prenose signálov je časový signál jedného z porovnávaných etalónov vysielaný v podobe elektromagnetických signálov jednosmerným komunikačným kanálom. Kritickým v tejto súvislosti je určiť prenosové oneskorenie signálu, spôsobené konečnou a variabilnou rýchlosťou šírenia sa časovej informácie v komunikačnom kanále. V ideálnom prípade sa táto šíri konštantnou rýchlosťou, pričom najvyššia možná je rýchlosť svetla. Pri tejto rýchlosti odpovedá na 1 kilometer prenosové oneskorenie 3,336 μs.

Najčastejšie sa na vysielanie časového signálu používajú rádiostanice (DCF77, WWWV a iné) alebo satelity (GPS, Glonass). V minulosti bola často používaná aj známa Československá televízna metóda ([23]). Pri použití rádiových alebo satelitných signálov tento prestupuje premenlivým prostredím - atmosférou a rýchlosť šírenia závisí od jeho stavu pozdĺž trajektórie (napr. teploty, tlaku vzduchu, vlhkosti, stavu ionosféry a pod.). Celkové oneskorenie je teda viac výsledkom výpočtov nad matematickým modelom ako skutočným meraním. Zlepšenie odhadu oneskorenia poskytuje vysielanie na dvoch odlišných nosných frekvenciách, kedže rýchlosť šírenia elektromagnetického vlnenia v atmosfére je závislá aj na jeho vlnovej dĺžke.

Pri väčšine systémov platí, že ak je už raz vysielač uvedený do činnosti časovú informáciu je schopný doručiť neobmedzenému množstvu prijímačov, čo je nespornou výhodou. Pripomína to klient-server model, kde však zaťaženosť servera nestúpa s množstvom obsluhovaných klientov.

Metóda "Common view"

Ak dvoje hodiny, ktoré majú byť porovnané, nie sú v priamej viditeľnosti, tj. vysielaný signál z hodín A nie je možné zachytiť na mieste hodín B a naopak, možno na ich porovnanie použiť signál vysielaný z hodín S viditeľný oboma hodinami A i B. V rovnakom čase sa uskutoční porovnanie hodín A voči S a hodín B voči S. Pri kombinácii týchto meraní sa vplyvy hodín S na meranie vyrušia. V prípade, že hodiny S sú dostatočne stabilné, nemusia tieto porovnania prebehnúť v rovnakom čase. Ak signál hodín S prestupuje atmosférou nehodno zabúdať na jej vplyv a zmenu atmosferických podmienok, ktoré sa môžu za tú dobu zmeniť. Pre dosiahnutie čo najlepších výsledkov je nutné dbať na to, aby vzdialenosť medzi A - S a B - S bola rovnaká a tým aj prislúchajúce oneskorenia.

Common View metóda však nemusí byť viazaná len na umelé zdroje signálu. V aplikáciách VLBI (Very Long Baseline Interferometry) sa pri štúdiu pohybov Zeme používajú kvazary. V laboratóriách vzdialených od seba 100 až niekoľko tisíc km sa atómovými hodinami merajú rozdiely v čase prijatia náhodného signálu z týchto hviezd.

V súčinnosti so systémom GPS (Global Positioning System) je dnes Common View najpoužívanejšou metódou pri porovnávaní etalónov medzi jednotlivými národnými laboratóriami. S jej nasadením sa dosahujú neistoty merania v priemere okolo 20 ns pri vzdialenostiach nad 1000 km.

2.5.3 Obojsmerný prenos elektromagnetických signálov

Obojsmerný prenos sa snaží odstrániť potrebu modelovania prenosového kanálu a odhadovania oneskorenia. Prenosové oneskorenie je priamo odmerané vyslaním signálu z jedného miesta na druhé, kde je okamžite preposlaný spätnou linkou naspäť. Jednosmerné oneskorenie sa potom určí ako polovica celkového. Preto je dôležité, aby bol prenosový kanál čo najsymetrickejší.

Rozlišujeme tri základné spôsoby realizácie obojsmernej linky:

Pri *časovom multiplexovaní* sa striedavo menení tok prenosu dát na jednej linke. Táto sa javí ako obojsmerná, ale v skutočnosti sa informácia v každom okamihu šíri iba jedným smerom. Takúto linku nazývame half-duplexnou. Miera nesymetrickosti kanála je úmerná veľkosti fluktuácií oneskorenia v jednotlivých smeroch.

Frekvenčné multiplexovanie moduluje signál pre každý smer na inú frekvenciu, čím umožňuje simultánnu komunikáciu v oboch smeroch na danej linke. Takúto linku budeme nazývať full-duplexnou. Nesymetrickosť prenosového kanála je mierou rozdielu rýchlosti šírenia signálu s rôznou frekvenciou. Typickým príkladom sú satelitné komunikačné linky, či telefónne modemy.

Tretím spôsobom je vytvoriť pre každý komunikačný smer samostatnú prenosovú linku. Dáta sú tak prenášané po dvoch úplne nezávislých, nominálne identických jednosmerných kanáloch. Nesymetrickosť je daná iba schopnosťou vybalancovať tieto dve linky a mierou závislosti fluktuácií medzi nimi. Príkladom sú napr. telekomunikačné linky na stredné vzdialenosti realizované optickými vláknami.

2.5.4 Systémy na prenos času

V histórii nájdeme len málo systémov, ktoré boli primárne postavené za účelom porovnávania metrologických vlastností hodín. Častejšie sú využívané systémy navrhnuté pre zabezpečenie iných služieb ako napr. navigačných či komunikačných. V predchádzajúcej časti popísané spôsoby preto úzko súvisia so systémami, ktoré sú v dnešnom čase k dispozícii. Zosumarizovanie výkonnosti predstavovaných systémov uvádza tabuľka 2.3.

Typ prenosu	**Predpoklady, tech. vybavenie**	**Neistota času, priemer za 1 deň**	**Neistota frekvencie, priemer za 1 deň**
Zvukové časové signály	telefón/rádio	< 1 ms	-
Časová služba cez telefón	telefónna prípojka, modem, počítač, softvér	< 5 ms	-
Časová služba cez Internet	počítač, softvér, internetové pripojenie	< 100 ms	-
Rozhlasové vysielanie	rozhlasový prijímač s RDS (87 - 108 MHz)	< 100 ms	1×10^{-5} (a) $< 1 \times 10^{-10}$ (b)
Rádiové časové signály	NF prijímač (20 - 80 kHz)	$< 500\,\mu$s	10^{-5} až 10^{-8}
	VF prijímač (2 - 15 MHz)	< 500 ns	10^{-10} až 10^{-12}
Analógové televízne vysielanie	televízny prijímač	100 ms	1×10^{-5}(a) $< 1 \times 10^{-10}$(b)
CDMA mobilná sieť	CDMA mobilná sieť, prijímač	1 až 10 μs	1×10^{-12}
GPS	GPS prijímač	10 až 100 ns	10^{-11} až 10^{-13}
TWSTFT	prijímač a vysielač	< 5 ns	$< 1 \times 10^{-13}$

Tabuľka 2.3: *Prehľad systémov na prenos časovej informácie a ich typickej výkonnosti. (a) výkonnosť plynúca zo zákona a prislúchajúcich predpisov (b) potencionálna výkonnosť*

Zvukové časové signály

"Oznam o presnom čase" je označenie zvukových signálov vysielaných v programe rozhlasu. Okrem toho, že je to informácia pre poslucháčov, využíva sa aj na zabezpečenie nadväznosti jednotlivých programov, ktoré môžu byť preberané z inej rozhlasovej stanice. Slovenský rozhlas ich zaraďuje do vysielania od roku 1926.

Informácia o čase je sprostredkovaná hlásateľom ústne pred alebo po odvysielaní časového signálu. Ten pozostáva zo šiestich pulzov o frekvencii 1 kHz. Prvých päť má dĺžku 100 ms (medzera 900 ms) a šiesty, začínajúci v čase oznámenom hlásateľom, je dlhý 500 ms (medzera 500 ms).

Identické je vysielanie zvukovej časovej informácie po telefóne.

Neistota v čase v priemere za 1 deň sa pohybuje okolo 1 ms. Spôsobená je zmenou prenosového oneskorenia rozhlasového resp. telefónneho signálu.

Časová služba cez telefón

S rozširovaním výpočtovej techniky vznikala potreba synchronizácie času jednotlivých počítačov/serverov. Existujúca telefónna sieť sa zdala ako vhodným prenosovým kanálom. Časovú službu cez telefón zabezpečuje na strane jej poskytovateľa server synchronizovaný s referenčným etalónom (často s národným etalónom). Telefonické spojenie je realizované štandardnými modemami dnes používanými napr. na Dial-Up pripojenie do Internetu. Používateľ, ktorý chce svoj čas na počítači s pripojeným modemom synchronizovať, vytočí s využitím určeného softvéru telefónne číslo poskytovateľa. Po spojení server začne vysielať v sekundových intervaloch informáciu o správnom čase. Formát správy by sa mal riadiť odporúčaním Medzinárodnej telekomunikačnej únie ITU-R TF583.4. Prijatý čas zo servera je vysielaný v predstihu. Správnym je v okamihu príjmu presne definovaného znaku v tejto správe.

Neistota v čase pri jednodennom priemerovaní sa pohybuje v rádoch milisekúnd a je ovplyvnená variáciou prenosového oneskorenia a oneskorením spracovania.

Časová služba cez Internet

NTP (Network Time Protocol) je najpoužívanejším zo série protokolov pre synchronizáciu času pomocou siete Internet. Poskytuje momentálne najlepšie algoritmy na minimalizáciu chýb spôsobených asymetrickým a nestálym prenosovým kanálom akým Internet je. Dnes je dostupný už v štvrtej verzii, avšak štandardom je zatiaľ len tretia. [24]

Servery poskytujúce časovú informáciu tvoria hierarchiu podľa toho k akému zdroju času sa synchronizujú. Jednotlivé úrovne tejto hierarchie sa nazývajú *stratum*. Najvyššie sú stratum 1 servery, ktoré sa synchronizujú k vonkajšiemu zdroju času (referenčný etalón, GPS prijímač...). Servery na úrovni stratum n sú synchronizované so servermi úrovne $n-1$. Stratum 1 servery synchronizované často i k národným etalónom majú svoje služby zväčša voľne prístupné.

Klient žiadajúci o synchronizáciu vysiela v pravidelných intervaloch žiadosť o synchronizáciu na viaceré prednastavené servery. Zabudovaný algoritmus sa snaží z pomedzi nich vybrať ten najvhodnejší - taký, ku ktorému prenos správy od klienta na server a späť trvá čo najkratší časový interval a jednotlivé rozdiely v týchto intervaloch sú čo najmenšie. Krátke prenosové oneskorenie správy dáva totiž predpoklad, že v spojení medzi klientom a serverom je len málo smerovačov, prepínačov, opakovačov a iných sieťových prvkov spôsobujúcich oneskorenia a nepravidelnosti intervalu potrebného na prenos správy. Získa sa tak lepší odhad prenosového oneskorenia.

Neistota v čase v jednodennom priemere sa pohybuje od desiatok po

stovky milisekúnd a je silne závislá najmä od vyťaženia spojenia medzi serverom a klientom, jeho asymetrickosti a oneskorením plynúcim zo spracovania.

Rozhlasové a televízne vysielanie

Každá rozhlasová a televízna stanica musí podľa zákona udržať stabilitu svojej nosnej frekvencie na úrovni 10^{-5}, aby bolo zaručené, že sa jednotlivé stanice nebudú rušiť. Táto nosná frekvencia sa dá využiť ako referencia pre jednoduchú kalibráciu a iné nenáročné aplikácie. Ak by však boli na vysielačoch použité atómové oscilátory, dajú sa dosiahnuť rádovo lepšie výsledky.

FM rozhlasové prijímače môžu získať časovú informáciou z RDS (Radio Data System) správ, ktoré vysiela väčšina rozhlasových staníc. Aj keď časová informácia nepatrí k povinným, ktoré by mali byť vysielané a jej vysielanie nemá slúžiť čo najlepšej synchronizácii, dosiahnutá neistota v čase je obyčajne menšia ako 100 ms. Časová správa obsahuje MJD dátum, UTC hodinu a minútu a posun miestneho času voči UTC. Je vysielaná každú minútu.

Podobne je informácia o správnom čase vysielaná v televíznom vysielaní pomocou teletextu.

Rádiové časové signály

Vysielanie časových signálov na rádiových vlnách patrí medzi najstaršie spôsoby prenosu časovej informácie. Od roku 1957 do 1996 bol v prevádzke aj Československý vysielač v Libliciach OMA vysielajúci na frekvencii 50 kHz. [25]

Signály sú vysielané na nosných frekvenciách od 20 kHz do 20 MHz. Časová informácia je nepretržite vysielaná rýchlosťou 1 bit/s s použitím modulácie šírky pulzu. Krátky pulz (100 ms u DCF77) reprezentuje bit 0 a dlhý pulz (200 ms u DCF77) bit 1. [26] Prenos kompletnej správy trvá 1 minútu.

Pri použití tohto spôsobu prenosu času, je nutné poznať vzdialenosť prijímača od vysielača, aby bolo možné výsledky merania korigovať o prenosové oneskorenie. Pre nízkofrekvenčné vysielače (20-80 kHz) neistota dosahuje v priemere za 1 deň niekoľko sto μs v čase a 10^{-5} až 10^{-8} vo frekvencii odvodenej od nosnej frekvencie.

CDMA mobilné siete

Prenos CDMA mobilnou sieťou je najmladším spôsobom prenosu časovej informácie a frekvencie. Samotná skratka CDMA (Code Division Multiple Access) označuje spôsob, akým môže komunikovať viacero zariadení na spoločnej prenosovej linke. Vysielané signály zariadení sú voči sebe ortogonálne,

a tak sú ľahko rozlíšiteľné. Tento spôsob využívajú niektoré mobilné siete (bohužiaľ nie na Slovensku).

Na zabezpečenie ich bezchybnej prevádzky je nutná dobrá synchronizácia času základových staníc a stabilita nosnej frekvencie. Štandard IS-95 pre CDMA mobilné siete vyžaduje chybu 10 μs pre čas a nestabilitu frekvencie lepšiu ako 5×10^{-8}. Najľahším a najjednoduchším spôsobom ako to dosiahnuť je použitie GPS disciplinovaného oscilátora na každej základovej stanici.

Neistota v čase je opäť závislá na vzdialenosti od základovej stanice. Tá je obyčajne tým menšia, čím hustejšie je osídlené okolie. V zastavaných oblastiach možno rátať s neistotou spôsobenou prenosovým oneskorením na úrovni 5 μs. V nezastavaných to môže byť až 100 μs, avšak tam kde je možné telefonovať s využitím danej siete, je neistota obyčajne menšia ako 25 μs. [27]

GPS

GPS je opäť príkladom systému, podobne ako väčšina predchádzajúcich, primárne navrhovaného pre iný účel. Americká armáda v spolupráci s NASA ho vystavali pre potreby určovania zemepisnej polohy kdekoľvek na Zemi. Avšak poskytovať správny čas je pre jeho funkčnosť kritické, pretože poloha prijímača sa vypočítava zo vzdialenosti k jednotlivým satelitom. Tie sa určujú z prenosového oneskorenia signálov vysielaných satelitmi. Na jednotlivých satelitoch sa preto nachádzajú až troje atómové hodiny (najčastejšie kombinácia céziových a rubídiových). Všetky satelity vysielajú na rovnakých frekvenciách L1 = 1575,42 MHz a L2 = 1227,6 MHz s vyžitím CDMA technológie. [28]

Neistoty $10 - 100$ ns v čase a 10^{-11} až 10^{-13} vo frekvencii sú tak malé, že tento spôsob prenosu je vhodný takmer pre každú aplikáciu. Ovplyvnené sú najmä stavom ionosféry, ktorá má najväčší efekt na zmeny prenosového oneskorenia.

TWSTFT

TWSTFT (TWSTFT - Two-Way Satellite Time and Frequency Transfer) spojenie je priame prepojenie dvoch koncových staníc satelitnou linkou, pomocou ktorého sa posielajú časové signály jednej stanice k druhej a naopak. Predstavuje najlepší spôsob prenosu času a frekvencie na veľké vzdialenosti. Neistoty sú menšie ako 5 ns v čase a 1×10^{-13} vo frekvencii pri jednodennom priemerovaní.

2.6 Realizácia TAI a UTC

Ako sme spomínali v kapitole 2.2.5 čas UTC nie je ničím iným ako časom TAI poopraveným o celý násobok (prestupných) sekúnd tak, aby približne sledoval čas UT2. Preto sa v ďalšom zameriame len na realizáciu času TAI.

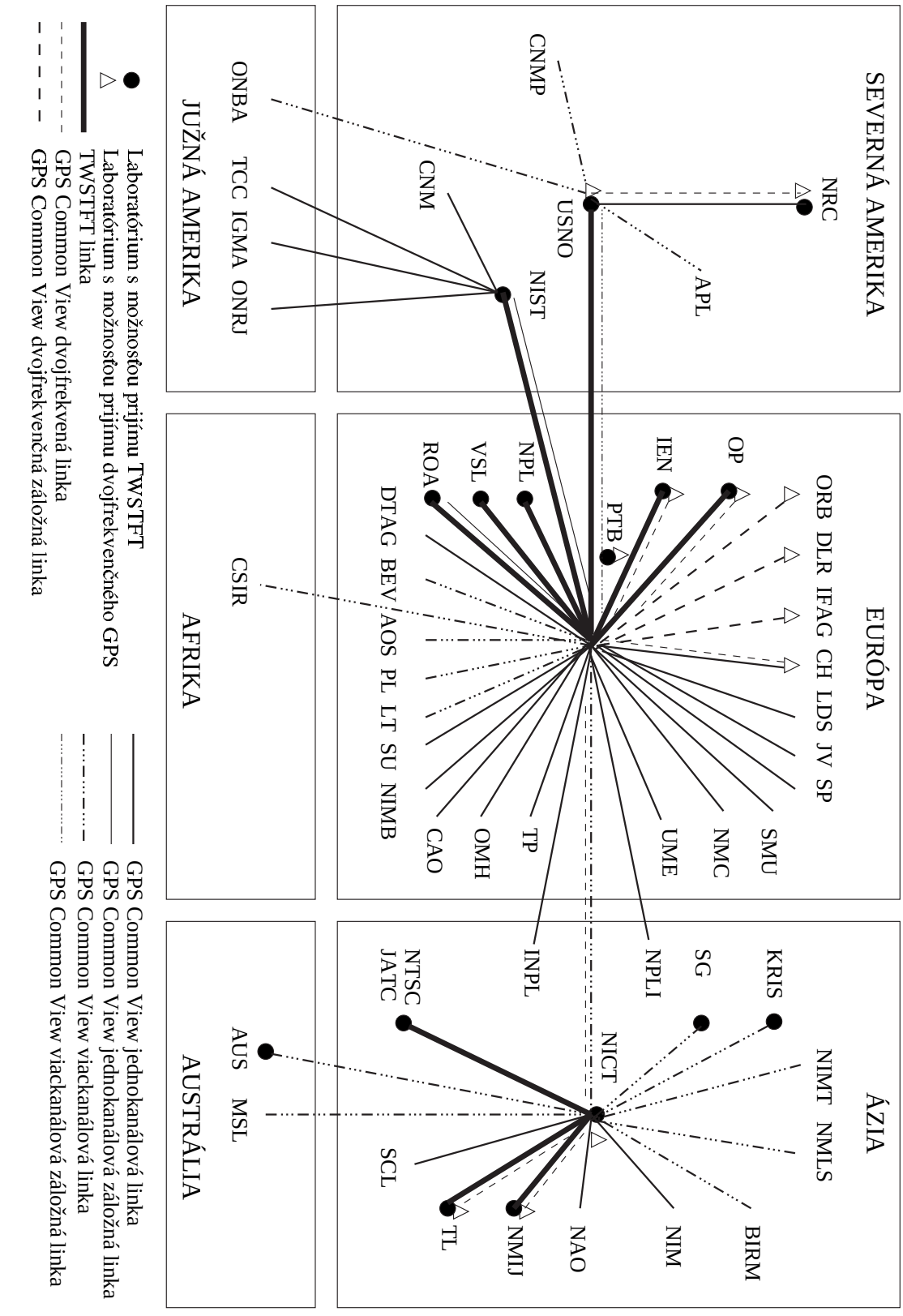
Čas TAI je získavaný kombináciou dát z asi 230 atómových hodín v približne 65 laboratóriách po celom svete. [29] Dáta sú pravidelne odosielané do BIPM asi 50-timi časovými centrami (medzi inými aj SMÚ), ktoré udržiavajú lokálnu časovú stupnicu UTC(k), kde k je označenie laboratória (viď Dodatok A). Odosielané sú vo forme časových rozdielov [UTC(k) - Clock] a vyhodnocované v 5 dňových intervaloch o 0 h UTC pre dni končiace 4 alebo 9 v zápise MJD. Týmto dátumom sa hovorí aj *štandardné dátumy.*

TAI je tvorený tak, aby poskytoval dlhodobú frekvenčnú stabilitu (po dobu jedného až dvoch mesiacov) a frekvenčnú správnosť. Keďže je to „papierová“ stupnica vyrátavaná spätne, medzičasom rozdiel medzi lokálnym časom a TAI môže byť extrapolovaný, čím získame aproximáciu TAI v reálnom čase.

Vypočítavanie TAI sa robí v dvoch krokoch. Najprv je iteračným algoritmom Algos vypočítaná voľne bežiaca atómová stupnica EAL (Echelle Atomique Libre), ktorej stabilita je optimálna pre dané časové obdobie pozorovania. Založená je na váhovom priemere hodnôt jednotlivých hodín vstupujúcich do výpočtu. Algoritmus počíta rozdiel EAL-UTC(k) v štandardných dátumoch v mesačných balíkoch počas ktorých sa váha hodín nemení. Aby sa zamedzilo prílišnej závislosti EAL na kontréktnych hodinách, bola stanovená horná hranica pre jednotlivé váhy tak, aby žiadne hodiny nedostali váhu prevyšujúcu o viac ako 0,7% celkovú váhu. V ďalšom kroku sa zavedie korekcia frekvenčnej chyby EAL v ráde 10^{-15}, aby bola zaručená stabilita stupnice v periódach oveľa dlhších ako mesiac.

Po týchto korekciách je čas TAI známy z rozdielu TAI-UTC(k) v štandardných dátumoch. Rozdiely jednotlivých laboratórií od UTC (teda poopraveného TAI o príslušný počet prestupných sekúnd) sú mesačne publikované v *Circular T* ako rozdiely UTC-UTC(k).

Neistota pri určovaní TAI v lokálnom laboratóriu z hodnôt v Circular T je približne rovná neistote v porovnávaniach v lokálnom laboratóriu pri formovaní TAI. Pri používaní signálov GPS táto odhaduje na asi 20 ns.



Obr. 2.4: *Organizácia medzinárodných časových liniek.*

2.7 UTC(SMU)

Zákon NRSR 142/2000 Z.z. o metrológii (ZoM) [30] v §3 ustanovuje za zákonnú meraciu jednotku času sekundu, definovanú v zmysle jej definície v Medzinárodnej sústave jednotiek SI. Realizovaná je Národným etalónom času a frekvencie v Slovenskom metrologickom ústave. Časová stupnica odvodená od tohto etalónu má medzinárodné označenie UTC(SMU) a zároveň je realizáciou stupnice UTC na Slovensku.

Národným etalónom času a frekvencie je primárny céziový frekvenčný etalón typu HP 5071A. Tento typ patrí dnes medzi špičku céziových etalónov. Vyše 170 etalónov z celkového počtu asi 260 zahrnutých v roku 2003 do výpočtu TAI bolo práve tohoto typu. Jeho nestabilita sa podľa špecifikácie pohybuje na úrovni $\leq 3,0 \times 10^{-14}$ za deň. [31]

SMÚ sa podieľa aj na tvorbe stupnice UTC. Metódou Common View GPS je etalón porovnávaný s ostatnými európskymi národnými etalónmi (viď obr. 2.4) a výsledky 13 minútových meraní sú odosielané na spracovanie do francúzskeho BIPM. Zároveň sa tak napĺňa §6 ZoM, podľa ktorého musia byť národné etalóny „medzinárodne porovnávané alebo nadviazané na medzinárodné etalóny alebo na národné etalóny iných štátov tak, aby sa zabezpečila porovnateľnosť meraní vykonaných v Slovenskej republike s meraniami v zahraničí“. V algoritme Algos pri výpočte TAI v mesiaci február 2004 mal pridelenú váhu 0,026 z celkovej váhy 1,0. [32] Táto hodnota je však ovplyvnená snahami SMÚ stabilizovať časovú stupnicu prebiehajúcimi v poslednom období a dosiahnúť tak tesnejšiu zhodu medzi UTC(SMU) a UTC. Odchýlka časovej stupnice UTC(SMU) od UTC bola v mesiaci február menšia ako 100 ns. [32]

2.8 Nadväznosť času a frekvencie

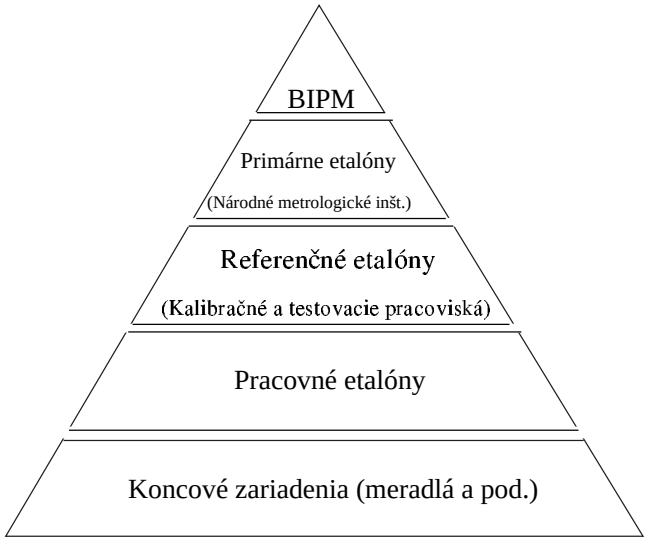
Infraštruktúra verejného kľúča nám umožňuje overiť pravosť verejného kľúča vydaného ľubovoľnou zúčastnenou certifikačnou autoritou pomocou väzieb dôvery medzi nimi. Ak máme verejný kľúč koreňovej certifikačnej autority, na základe hierarchie medzi ostatnými CA overíme podpis CA, ktorá vydala overovaný verejný kľúč. Inak povedané overiť pravosť verejného kľúča znamená nájsť neprerušenú linku dôvery medzi koreňovou CA a overovaným verejným kľúčom. Avšak ako získať dôveru v správnosť času v časovej pečiatke?

Túto otázku sa snaží riešiť vyhláška NBÚ 537/2002 Z.z.[11] V §8 pre poskytovateľov časovej pečiatky ustanovuje, že „zdroj časových údajov je synchronizovaný s referenčným zdrojom času s deklarovanou presnosťou“.

Parafrázované slovníkom metrológie, žiadame aby TSA preukázala *nadväznosť* zdroja času na referenčný etalón.

Nadväznosť (traceability) v metrológii predstavuje vlastnosť výsledku merania alebo hodnoty etalónu, ktorá má vzťah k určeným referenčným etalónom, všeobecne k štátnym (národným) alebo medzinárodným etalónom prostredníctvom neprerušeného reťazca porovnaní s určenými neistotami.

Podobný systém ako PKI existuje vďaka nadväznosti aj v metrológii. Jednotlivé laboratóriá tvoria hierarchiu, ktorej vrcholom je BIPM. Spravuje medzinárodnú sústavu jednotiek SI teda aj jednotku času - sekundu. Priamo na BIPM sú nadviazané národné metrologické ústavy udržujúce nadväznosť (na Slovensku zo ZoM) svojich primárnych etalónov na medzinárodnú sústavu. Takto je zabezpečená nadväznosť na medzinárodnej úrovni. V rámci jedného štátu sú referenčné etalóny v kalibračných a testovacích strediskách porovnávané s národným etalónom. Referenčné etalóny slúžia účelu kalibrácie pracovných etalónov a úplne na spodku sú koncové zariadenia určené ku každodennej práci ako napríklad parkovacie hodiny alebo policajné radary. Táto klasická pyramída je znázornená na obrázku 2.5.

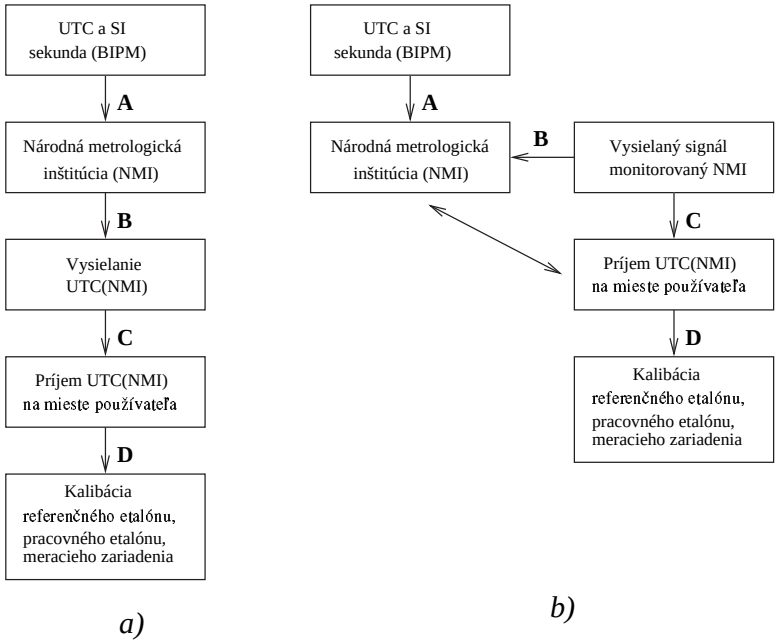


Obr. 2.5: *Pyramída nadväznosti.*

V niektorých odboroch metrológie je nadväznosť realizovaná iba v periodických intervaloch, nakoľko metódy porovnania etalónov si vyžadujú ich transport. Typickým príkladom je metrológia hmotnosti. Našťastie na prenos času a frekvencie bolo vyvinutých veľa metód, akými sa dá realizovať nadväznosť na národný etalón kontinuálne a v reálnom čase (viď 2.5).

2.8.1 Vytváranie nadväznosti

Obrázok 2.6 zobrazuje dva možné spôsoby ako vytvoriť nadväznosť na národný etalón času a frekvencie.



Obr. 2.6: *Reťazce nadväznosti. a) pre signály kontrolované NMI b) pre signály monitorované NMI*

V prvom prípade národná metrologická inštitúcia (NMI)[9] poskytuje službu koncovým používateľom a vysiela časové signály priamo odvodené od UTC(NMI). Tento signál je tak priamo kontrolovaný NMI. V praxi je šírenie časovej informácie realizované rádiovými vysielačmi (napr. DCF77, WWWV, MSF...), vysielaním po telefónnej sieti alebo internetom s využitím protokolu NTP. Spojenie **A** spojuje BIPM s národným metrologickým úradom. Neistota linky **A** sa dá iba spätne zistiť z Circular T pravidelne vydávaného BIPM. Spojenie **B** prepája NMI s vysielacím strediskom a jeho neistota je uverejňovaná NMI. Najväčšiu neistotu väčšinou predstavuje spojenie **C**. Vplývajú na ňu podmienky šírenia signálu prostredím medzi vysielačom a prijímačom. Nakoniec spojenie **D** prepája prijímač s prijímateľovým referenčným etalónom, ktorý môže byť použitý napríklad na kalibráciu pracovných etalónov či koncových zariadení. Podľa definície je nadväznosť výsledok merania, a preto všetko čo zabezpečuje meranie prispieva aj k neistote spojenia **D** vrátane prijímačov, antén, softvéru alebo ľudských chýb. Očividne neistoty spojení

[9]Národná metrologická inštitúcia je všeobecné označenie inštitúcie (ústavu) majúcej na starosti udržiavanie národných etalónov v jednotlivých krajinách. Na Slovensku NMI je Slovenský metrologický ústav.

A a **B** sú ďaleko menšie ako neistoty liniek **C** a **D** a pri väčšine meraní sa môžu zanedbať.

U nás sa s takýmto modelom nadväznosti môžeme stretnúť najmä pri využití nemeckého rádiového vysielača DCF77 umiestneného v Mainflingene pri Frankfurte nad Mohanom. Vysielač časovej informácie vysiela na frekvencii 77,5 kHz s výkonom 50 kW a jeho signál sa dá zachytiť do vzdialenosti asi 2000 km. Na synchronizáciu ho používa Slovenský rozhlas, Dopravný podnik mesta Bratislavy ale i niektoré autority časových pečiatok. Jeho príjmom tak vzniká nadväznosť na čas UTC(PTB), nie však UTC(SMU).

Spôsob *b)* dovoľuje nadväznosť na UTC(NMI), za predpokladu, že NMI monitoruje systém, ktorý nepodlieha priamo jeho kontrole. Je takmer identický prvému, ibaže spojenie **B** je v tomto prípade len monitorovacie. Aby sa nenarušila nadväznosť, miestny NMI musí monitorovať vysielaný signál nepretržite, bez prerušenia. Typickým príkladom takéhoto modelu je satelitný navigačný systém GPS. Takmer každý NMI vo svete (vrátane SMÚ) dnes neustále monitoruje časový signál vysielaný družicami GPS.

Na dokreslenie uvedieme modelový príklad, v ktorom vytvoríme nadväznosť časovej stupnice, ktorú tvorí zdroj času TSA, označme ju UTC(TSA), na UTC. Podľa definície je treba vytvoriť neprerušený reťazec porovnaní s určenými neistotami.

Predpokladajme, že TSA svoj zdroj času synchronizuje pomocou prijímača GPS. Na vytvorenie nadväznosti UTC(TSA) na GPS samotný fakt synchronizácie nestačí. Je nutné určiť priemernú odchýlku časovej stupnice UTC(TSA) od GPS a jej neistotu, čím vytvoríme spojenie **C** a **D** z obrázku 2.6. Túto službu bežne poskytuje NMI alebo iné kalibračné centrum.

Ďalšie merania už nie sú potrebné. Nadväznosť UTC(TSA) na UTC sa získa kombináciou meraní UTC(TSA) voči GPS, GPS voči UTC(NMI) (spojenie **B**; realizované nepretržite NMI, výsledky sú publikované NMI) a UTC(NMI) voči UTC (spojenie **A**; realizované nepretržite NMI, výsledky sú publikované BIPM v Circular T). Až príde sporná situácia a TSA bude musieť preukázať odchýlku svojej časovej stupnice od UTC, z výsledkov týchto 3 meraní sa vypočíta konečná odchýlka a neistota časovej stupnice UTC(TSA), realizovanej zdrojom času TSA, od stupnice UTC.

2.8.2 Počítanie s neistotami

Metodika ako kombinovať jednotlivé výsledky meraní a určiť výslednú neistotu pochádza zo štatistiky. Zhrnutá je napríklad v [33] alebo [34]. Základné

princípy pritom vychádzajú z nasledovného. Veličina ktorú meriame, je veličina, ktorej hodnoty presne nepoznáme, a preto je považovaná za náhodnú veličinu. Pre náhodné veličiny sa používa ako miera rozptýlenia hodnôt rozptyl ich rozdelenia, alebo jeho kladná druhá odmocnina - smerodajná odchýlka. Neistota merania x, označovaná ako $u(x)$, je smerodajnou odchýlkou meranej veličiny X.

Pre konkrétne meranie je odhadom meranej veličiny výberový priemer počítaný podľa rovnice (2.5) z nameraných hodnôt x_i (predpokladáme, že namerané hodnoty sú nezávislé a s normálnym rozdelením). Odhad rozptylu rozdelenia je druhá mocnina výberovej smerodajnej odchýlky s definovanej rovnicou (2.4). Výsledok je potom prezentovaný ako $\bar{x} \pm u(x) = \bar{x} \pm ks$, kde k je závislé od zvolenej hladiny významnosti a počtu nameraných hodnôt veličiny.

Pre rozptyl platí

$$D(X + Y) = D(X) + D(Y) \,, \tag{2.11}$$

preto ak je treba kombinovať výsledky viacerých meraní $X_1, X_2, \ldots, X_n$ veličiny X s neistotami $u(x_1), u(x_2), \ldots, u(x_n)$ potom pre výslednú neistotu $u(x)$ platí

$$u(x) = \sqrt{u(x_1)^2 + u(x_2)^2 + \ldots + u(x_n)^2} \,. \tag{2.12}$$

Uvedené demonštrujeme na krátkom príklade. Predpokladajme, že národný etalón času má odchýlku od UTC -100 ns pričom túto hodnotu poznáme s neistotou $\pm$ 20 ns. Ďalej nech zdroj času TSA má ochýlku od UTC 800 ± 90 ns. Potom odchýlka TSA od národného etalónu času je

$$-100 + 800 \pm \sqrt{20^2 + 90^2} = 700 \pm 92 \text{ ns} \,.$$

Kapitola 3

Systémy kontroly

Od využitia časovej pečiatky v praxi sa očakáva, že poskytne dôkaz o existencii dokumentu v určenom čase, podporu pri dokazovaní doručenia dokumentu adresátovi a podporu dlhodobého uloženia elektronicky podpísaných dokumentov. Všetky aplikácie si od zúčastnených vyžadujú dôveru v správnosť času uvedeného v časových pečiatkach. Ako základný kameň tejto dôvery považujeme dôveru v správnosť zdroja času TSA voči dôveryhodnému referenčnému etalónu času, ktorá vznikne nadväznosťou zdroja času TSA na referenčný etalón. Vyhláška NBÚ 537/2002 Z.z v požiadavkách na zdroj časových údajov pre časovú pečiatku požaduje, aby bol tento synchronizovaný s deklarovanou presnosťou k referenčnému zdroju, a aby kalibrácia zdroja času bola udržiavaná tak, aby bolo zaručené, že nenastane odchýlka nad rámec deklarovanej presnosti. Žiaľ neustanovuje bližšie čo rozumie pod referenčným zdrojom, ani ako spomínané požiadavky kontrolovať.

V predošlej časti sme popísali viacero mechanizmov, ako synchronizovať dvoje hodiny a vytvoriť nadväznosť. Sú to väčšinou systémy bežne používané v metrológii a ich metrologická kvalita je známa. Možno predpokladať, že každá TSA používa jeden z nich. Avšak všetky bežne dostupné systémy štandardne neposkytujú autentifikáciu a zabezpečenie spoľahlivého prenosu časovej informácie. Nie je teda zaručené, že referenčný etalón, ku ktorému sa synchronizujeme, je skutočne ten, ktorý deklarujeme, alebo že signál nie je po ceste spomaľovaný. Riešiť tieto problémy sa snaží napr. NTP protokol vo svojej štvrtej verzii (NTPv4), ktorý na zabezpečenie komunikačného kanála ponúka možnosti kryptografie s verejným kľúčom. Rovnako systém GPS, nakoľko sa jedná o vojenský systém, obsahuje podporu zabezpečenia autentickosti signálu, avšak táto nie je dostupná pre civilné potreby.

V ďalšom preto predstavíme niekoľko rôznych návrhov systému, ktorý umožňuje kontrolu správnosti času zdroja času TSA, na základe ktorej je

možné dôverovať v správnosť času v časovej pečiatke. Hlavným cieľom takéhoto systému nebude umožniť synchronizáciu alebo dosiahnúť čo najmenšej neistoty porovnania etalónov, ale dosiahnuť čo možno najvyšší stupeň dôvery v nameraný výsledok pri udržaní neistoty v rozumných hraniciach. Jeho používateľom je úrad vykonávajúci kontrolu nad TSA.

3.1 Základné predpoklady a požiadavky na systém

V nasledujúcom za *zdroj času* považujeme zariadenie, z ktorého TSA získava časové údaje vkladané do časových pečiatok. Pre jednoduchosť ďalej predpokladajme pravdivosť tvrdenia: *Čas zdroja času TSA je správny práve vtedy a len vtedy, ak je správny čas v časovej pečiatke vystavenej TSA.* Navrhované systémy majú za cieľ overiť metrologické kvality zdroja času TSA, ktoré sú deklarované v politike časových pečiatok TSA. V tomto dokumente sa pod termínom presnosť uvádza neistota času voči UTC. Pod pojmom *systém* budeme rozumieť všetky časti, hardvérové, softvérové a iné, podieľajúce sa na a zabezpečujúce kontrolu zdroja času.

3.1.1 Predpoklady

Pri návrhu jednotlivých systémov sme vychádzali z nasledovných predpokladov:

1. *Referenčný zdroj TSA je nadviazaný na UTC.*

2. *Za referenčný etalón systému v ďalšom považujeme Národný etalón času a frekvencie umiestnený v SMÚ*, ktorý realizuje sekundu v zmysle definície SI a oficiálnym rozhodnutím slúži ako základ na odovzdávanie hodnôt iným etalónom času a frekvencie[1]. Navyše je tento etalón nadviazaný na medzinárodnú časovú stupnicu UTC, čo umožňuje overiť tvrdenia v politike časových pečiatok TSA o neistote synchronizácie k referenčnému zdroju TSA. Miesto „referenčný etalón systému“ budeme častokrát používať iba skrátené spojenie „referenčný etalón“.

3. *Prevádzku navrhovaného systému predpokladáme v SMÚ* aj napriek tomu, že dozorným orgánom nad TSA je NBÚ. Dôvodom je jeho priame napojenie na Národný etalón času a frekvencie, a preto nebude potrebné budovať ďalší systém správy a nadväznosti referenčného etalónu

[1] V súčasnosti žiadny predpis konkrétne nedefinuje referenčný etalón, resp. referenčné pracovisko poskytujúce referenčný čas v zmysle vyhlášky NBÚ 537/2002 Z.z.

umiestneného v NBÚ. Okrem toho je SMÚ odborným garantom výsledkov merania. Preto ak budeme hovoriť o kontrolnom orgáne, máme na mysli SMÚ.

4. *Okrem referenčného etalónu, jednokanálového Common View GPS prijímača a emailu nepredpokladáme žiadne, pre systém využiteľné, existujúce zdroje v kontrolnom orgáne.* Na referenčný etalón je v súčasnosti napojený len jediný systém. Zabezpečuje nadväznosť na UTC pomocou porovnávaní Common View GPS metódou. Z jeho infraštruktúry je však možné využiť len vyššie menované časti.

5. *TSA má jeden zdroj času.* Vo všeobecnosti existujú modely IT systému TSA, v ktorých používa TSA viacero zdrojov času. Motívom môže byť zvýšiť priepustnosť služby a vydať viac časových pečiatok za jednotku času. V našich úvahách sa obmedzíme len na model s jedným zdrojom času, ktorý je používaný TSA na Slovensku.

6. *Navrhovaný systém sa skladá z dvoch častí, ktoré budú medzi sebou komunikovať, pričom každá časť je napojená na jeden z porovnávaných etalónov.* Tento predpoklad je prirodzený nakoľko sa porovnávajú etalóny vo všeobecnosti umiestnené v rôznych lokalitách.

7. *Obsah prenášanej správy nie je nutné utajovať.* Rôzne časti systému si budú medzi sebou vymieňať informáciu o čase, alebo vedúcu k jeho určeniu a túto nepovažujeme za dôvernú.

8. *Výsledok merania je vyhodnocovaný kontrolným orgánom.*

3.1.2 Požiadavky

Od systému vyžadujeme, aby v čo najväčšej miere eliminoval riziko podvodu zo strany TSA ako i tretej strany, ktorá by chcela poškodiť/polepšiť TSA a umožnil overiť tvrdenia z politiky časových pečiatok TSA. Za týmto účelom budeme požadovať nasledovné:

1. *Výsledkom merania systému je odchýlka časovej stupnice realizovanej zdrojom času TSA od referenčného etalónu s deklarovanou neistotou plynúcou z merania.* Tento výsledok nám spôsobom uvedeným v kap. 4.4 umožní overiť či zdroj času TSA spĺňa požiadavky na neistotu času uvedené v politike časových pečiatok TSA.

2. *Neistota výsledku merania odchýlky je lepšia ako* ± 30 *ms.* Požadovaná neistota výsledku, ktorú má systém poskytnúť, musí byť dostatočná na to, aby overila pravdivosť tvrdení v politike časových pečiatok TSA.

Zároveň je treba vychádzať aj z reálnych požiadaviek na neistotu času v časových pečiatkach a ich predpokladu do budúcnosti.

Malá neistota odchýlky zdroja času TSA voči jej referenčnému etalónu kladie zvýšené nároky na IT systém TSA. Na to, aby sa TSA rozhodla udržovať svoj zdroj času takto synchronizovaný, je v trhovom hospodárstve prirodzene nutný dopyt po službe, ktorú by táto skutočnosť umožnila. Časová pečiatka je dôkazom o existencii elektronického dokumentu v určenom čase. Z tohto pohľadu preto nemá zmysel uvažovať o veľmi malej neistote. Dnes TSA na Slovensku deklarujú v politike časových pečiatok neistotu od ±100 do ±500 ms. Neistota merania ±30 ms tak poskytuje dostatočnú rezervu a je v súlade i s napríklad [35].

3. *Prevádzka systému musí umožniť odhaliť všetky abnormálie časovej stupnice zdroja času TSA.* Túto požiadavku demonštrujeme na jednoduchom príklade. Predstavme si, že priebeh časovej stupnice kolíše voči referenčnej stupnici s amplitúdou 1 s a periódou 1 deň. Ak budeme robiť meranie zdroja času každý deň v tú istú hodinu, tak počas viacerých dní zistíme, že odchýlka týchto stupníc je relatívne konštantná a neodhalíme jej kolísanie.

4. *Systém musí umožniť kontrolu zdroja času TSA aspoň jedenkrát denne, pričom iniciátorom kontroly je kontrolný orgán.*

5. *Prenos správy sa musí uskutočniť cez spoľahlivý komunikačný kanál, aby sa zabezpečila integrita správy a musí byť zaručený pôvod tejto správy - autenticita.* Od systému nebudeme požadovať utajený prenos správy, nakoľko sa predpokladá, že správa nebude obsahovať dôverné informácie.

6. *Systém musí byť v čo najväčšej rozumnej miere chránený voči manipulácii s výsledkami a zabezpečiť autentickosť výsledku.*

7. *Inštalácia a prevádzka systému si musí vyžadovať čo najmenší zásah do IT systému TSA, aby tak nebola ovplyvnená jeho spoľahlivá prevádzka, funkčnosť, výkonnosť a bezpečnosť.*

8. *Systém musí byť transparentný*, aby si získal dôveru ako kontrolného úradu tak i TSA.

9. *Obmedzenia kladené na IT systém TSA systémom a náklady spojené s jeho zavedením musia byť adekvátne výkonnosti systému.* Zavedenie a prevádzka systému si bude vyžadovať ďalšie s ním spojené zdroje

(hardvérové, ľudské, finančné...) na strane TSA i kontrolného orgánu, ktoré musia byť úmerné dosiahnutému výsledku. Všeobecne sa dá predpokladať, že TSA bude len s neochotou investovať veľké prostriedky do niečoho, čo ju kontroluje a nevytvára žiaden zisk.

3.2 Poskytovanie času zdrojom času

V každom riešení, ktoré má porovnať čas zdroja času TSA, je nutné časovú informáciu z tohto zdroja získať. V niektorých prípadoch budeme dokonca vyžadovať synchronizáciu času časti systému v TSA k zdroju času TSA. V tejto súvislosti v krátkosti popíšeme akým spôsobom nám môže zdroj času poskytnúť informáciu o jeho aktuálnom čase v danom okamihu.

PPS signál+číslicový výstup PPS (Pulse Per Second) signály[2] spolu s digitálnou informáciou o čase predstavujú najsprávnejšiu formu výstupu času. Pomocou definovaného komunikačného protokolu je možné z číslicového výstupu zdroja získať čas v digitálnej podobe s rozlíšením 1 sekundy (počet sekúnd, minút, hodín od začiatku dňa a dátum). Tieto hodnoty sú platné práve v okamihu príchodu PPS impulzu.

V prípade, keď zdroj času PPS výstup priamo neposkytuje je možné ho nahradiť rozširujúcou kartou (PCI, VME, ISA,...). Táto karta obsahuje oscilátor častokrát stabilnejší a poskytuje PPS a dátový vstup/výstup. Inštalovanie rozširujúcej karty vyžaduje zásah do hardvéru.

Programový interface Každý zdroj času poskytuje sadu funkcií (interface), ktoré môžu byť volané inými softvérovými aplikáciami a umožňuje tak začleniť zdroj času k ostatnému IT systému TSA. Pre získanie informácie o aktuálnom čase zdroja bude volaná príslušná funkcia z tejto sady.

V najhoršom je jediná cesta ako získať aktuálny čas zdroja času vytvorenie časovej pečiatky. V takomto prípade, ak je nutné zistiť čas zdroja, zašleme žiadosť o časovú pečiatku a z odpovede získame požadovanú informáciu.

Network Time Protocol Veľa zdrojov času TSA je už dnes synchronizovaných pomocou NTP protokolu k referenčnému zdroju (NTP serveru). Prirodzené je teda použiť zdroj času TSA ako referenčný pre ďalšieho NTP klienta. Ak sú NTP server a klient na tej istej lokálnej sieti je odchýlka časových stupníc $\leq$0.2 ms. [36] Klient už môže byť časťou

[2]Na PPS výstupe zariadenia sa generuje pravidelne na začiatku každej sekundy elektrický impulz.

systému a porovnávať svoj čas s referenčným etalónom. Pre použitie zdroja času ako NTP servera je nutná rekonfiguráciu NTP softvéru zdroja času.

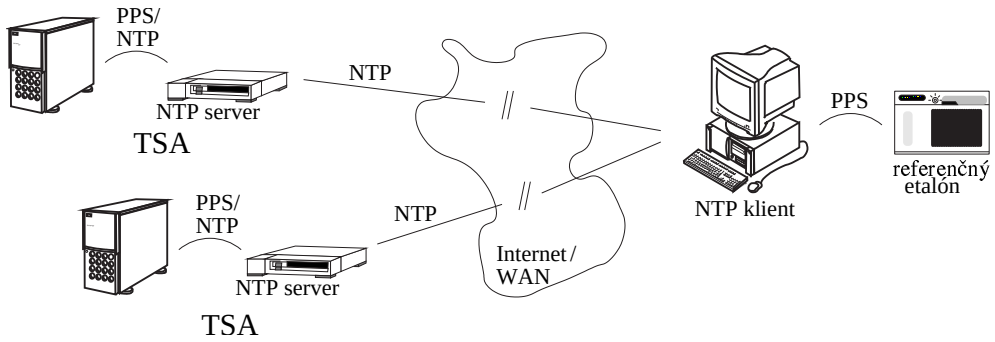
3.3 Navrhované riešenia

V predošlom sme stanovili základné predpoklady a požiadavky, ktoré budeme klásť na systém. Na ich základe sme navrhli niekoľko riešení, ktoré sa im snažia čo najlepšie priblížiť. Bližšie ich prestavujeme v tejto kapitole.

3.3.1 Využitie NTP

Protokol NTP bol navrhnutý pre synchronizáciu hodín počítača. Ich základom je kremíkový kryštálový oscilátor a počítadlo pulzov. To počíta počet pulzov z oscilátora a vytvára časovú stupnicu. K hodinám v počítači operačný systém poskytuje súbor funkcií, umožňujúcich bežiacim programom prácu s hodinami (získať časovú informáciu, nastaviť čas...). NTP sa snaží porovnať časovú stupnicu tvorenú lokálnymi hodinami, so stupnicou iného (referenčného) počítača a doladiť (softvérovo) frekvenciu oscilátora, tak aby sa výsledné dve časové stupnice čo najmenej odchyľovali.

Protokol NTP využijeme na prenos časovej informácie a odmeranie odchýlky medzi zdrojom času TSA a referenčným etalónom, pričom predpokladáme, že tieto sú spojené počítačovou sieťou (Internetom, prenajatou linkou a pod.).



Obr. 3.1: *Schematické znázornenie NTP systému.*

Systém pozostáva z dvoch častí. Na mieste zdroja času TSA je umiestnený NTP server synchronizovaný k zdroju času TSA. Ten je počítačovou sieťou prepojený s NTP klientom v kontrolnom orgáne. Klient sa synchronizuje na referenčný etalón. Hodiny klienta (ako počítača) preto realizujú

Server	Prenos. oneskorenie	Odchýlka	Neistota
ntp.metas.ch	53 ms	$+0,86$ ms	$\pm 22,4$ ms
ptbtim1.ptb.de	55 ms	$+0,14$ ms	$\pm 25,5$ ms
ntp1.ien.it	91 ms	$+7,60$ ms	$\pm 28,9$ ms
time-a.nist.gov	130 ms	$-2,69$ ms	$\pm 25,4$ ms

Tabuľka 3.1: *Výsledky pozorovania stratum-1 NTP serverov.*

s danou odchýlkou a neistotou časovú stupnicu referenčného etalónu. Rovnako hodiny servera sú synchronizované so zdrojom času a realizujú časovú stupnicu zdroja času. Meranie prebieha tak, že klient vysiela v periodických intervaloch žiadosti o synchronizáciu na server v TSA. Po odpovedi servera na žiadosť je zistená odchýlka časovej stupnice servera od klienta (podrobnosti v [24]). Táto je zaznamenaná pre konečné spracovanie výsledku, avšak samotná synchronizácia nenastáva, pretože klient musí ostať synchronizovaný k referenčnému etalónu. Takéto nastavenie umožnuje voľba `-noselect` pri konfigurácii klienta zo štandardného balíka NTPv4 stiahnuteľného z *http://www.ntp.org*. Získané odchýlky sú spracované rovnakým spôsobom ako v kap. 4.3. Do konečného výsledku je však nutné započítať i neistoty synchronizácie hodín oboch počítačov k referenčným etalónom.

Odchýlka merania by nemala prekročiť požadovaných ±30 ms. Na jej odhad sme pripravili experiment, v ktorom bol NTP klient počas 60 dní pripojený pomocou ADSL pripojenia do Internetu. Zbieral odchýlky časovej stupnice od prednastavených NTP serverov synchronizovaných k národným etalónom, pričom bol sám synchronizovaný na automaticky zvolený jeden z nich. Neboli použité žiadne kryptografické nástroje na zabezpečenie spojenia. Spracované výsledky sú zostavené v tabuľke 3.1. Pozoruhodné je, že ani pri transatlantickom serveri *time-a.nist.gov*, kde prenosové oneskorenie bolo nad 120 ms, dosiahnutá neistota ostala porovnateľná s európskymi servermi.

V štandardnom programovom balíku NTPv4 autenticitu a integritu prenášaných správ zabezpečujú mechanizmy založené na RSA digitálnych podpisoch a MD5 hašovaní. Ich detailný popis možno nájsť v [37]. NTPv4 umožňuje použiť automaticky generované kľúče a ich výmenu (za pomoci modifikovaného Schnorrovho, Guillou-Quisquaterovho či Mu-Varadharajanovho algoritmu) alebo vlastné. V druhom prípade je súkromný kľúč uložený v súbore na pevnom disku počítača. Preto ak budeme požadovať jeho maximálnu ochranu, je nutné NTP softvér upraviť tak, aby na podpisovanie využíval špeciálne zariadenie na tento účel.

Medzi kritické body riešenia patrí i zabezpečenie spoľahlivej synchronizácie NTP servera uloženého v prostredí TSA k zdroju času TSA. Namerané

výsledky totiž hovoria o vlastnostiach NTP servera a nie priamo zdroja času. Fyzickými, softvérovými a organizačnými prostriedkami je nutné v čo najväčšej miere zabrániť hrozbe, pri ktorej by sa NTP server synchronizoval k inej referencii ako k zdroju času TSA. Najspoľahlivejším riešením je zlúčenie funkcií zdroja času a NTP servera systému, ak to zdroj času TSA umožňuje. S týmto problémom sa však budeme stretávať i vo väčšine ostatných riešení.

Nevýhody súvisia i s ďalšími otázkami bezpečnosti. Uloženie kľúčov pre podpisovanie NTP správ vymieňaných medzi NTP klientom a serverom je nutné riešiť spôsobom, aby sa v čo najväčšej miere zamedzilo ich kompromitácii. Umiestnenie kľúča do hardvérového bezpečnostného modulu je finančne náročné riešenie, a naopak ich uloženie na trvalom pamäťovom médiu NTP servera/klienta nie dostatočne bezpečné, nakoľko NTP server sa nachádza v prostredí kontrolovanom TSA. Riešením by mohlo byť vkladanie požadovaných kľúčov autorizovanými osobami pri štarte systému. Pravda takýto spôsob si vyžaduje návštevu TSA autorizovanými osobami pri každom spustení.

Výhodou použitia NTP je relatívne jednoduchá infraštruktúra. Ak neuvažujeme použitie hardvérového bezpečnostného modulu na ochranu kľúčov, ale budeme zadávať kľúče pri každom spustení, na strane TSA i kontrolného orgánu si implementácia vyžaduje nákup a zabezpečenie spoľahlivej prevádzky jedného počítača a zabezpečenie bezpečného pripojenia do Internetu. Veľa komerčných riešení pre IT systém TSA už využíva NTP na synchronizáciu zdroja času a zdroj času by tak mohol slúžiť i ako NTP server pre klienta v kontrolnom orgáne. Kontrolný orgán navyše potrebuje zabezpečiť vývoj aplikácie spracovávajúcej výsledky merania a upraviť štandardný balík NTP, aby sa kľúče nemuseli ukladať na disk. Rovnako doporučujeme použitie rozširujúcej karty nahrádzajúcej hodiny klienta, kvôli čo najlepšej synchronizácii s referenčným etalónom. Ďalším pozitívom je, že systém umožnuje nastavenie, pri ktorom je zdroj času TSA synchronizovaný na referenčný etalón. Rovnako ku kladom počítame schopnosť systému nepretržite kontrolovať zdroj času ako i skutočnosť, že časť systému na strane kontrolného orgánu sa dá používať pre kontrolu všetkých TSA. NTP klient v kontrolnom orgáne môže byť nastavený tak, aby monitoroval ľubovolný počet NTP serverov.

3.3.2 Zabezpečený telefónny prenos

Systém používajúci telefónne spojenie na prenos časovej informácie je podobný systému využívajúceho NTP. Na strane TSA sa nachádza počítač (server) synchronizovaný so zdrojom času a pripojený k telefónnej sieti pomocou modemu. Podobne na strane kontrolného orgánu sa nachádza klient synchronizovaný s referenčným etalónom a napojený na telefónnu sieť modemom.

Meranie sa začína vytočením telefónneho čísla serveru klientom. Po úspešnom spojení server niekoľkokrát vyšle špeciálny znak, ktorý bude klientom ihneď reflektovaný späť. Táto procedúra umožní stanoviť prenosové oneskorenie medzi klientom a serverom, o ktorom predpokladáme, že sa počas merania nebude meniť. Následne začne server posielať na začiatku každej sekundy správu o jeho čase. Klient si zaznamenáva čas príjmu (prvého znaku) každej správy. Po potrebnom počte meraní je spojenie prerušené a výsledky štatisticky spracované.

Podobné systémy využívajú NMI vo svete pre poskytovanie služby synchronizácie času počítačov širokej verejnosti. Z ich skúsenosti sa odporúča použiť prenosovú rýchlosť 1200 baud. [38, 39] Taktiež pre formát prenášanej správy existuje vypracované odporúčanie Medzinárodnej telekomunikačnej únie ITU-R TF583.4. Výňatok z neho možno nájsť v [40].

Najväčším zdrojom neistoty výsledku je neistota prenosového oneskorenia. Na jej odhad sme opäť zostavili experiment. Vytvorili sme medzi dvoma počítačmi telefónne spojenie a pomocou neho bol z jedného počítača posielaný znak smerom k druhému, ktorý ho okamžite preposielal naspäť. Merali sme pritom časový interval medzi odoslaním a príjmom znaku. Pri prvom pokuse sme spojili počítače napojené na telefónne prípojky v Bratislave. V druhom sme skúmali spojenie na vzdialenosť asi 200 km. V oboch prípadoch sa po odfiltrovaní zjavne zlých meraní (viď (4.4)), ktorých bolo menej ako 5%, neistota nameraného prenosového oneskorenia pohybovala okolo ± 10 ms.

Obyčajne telefónne spojenia nie sú nijak chránené a telefónna linka neposkytuje spoľahlivý prenosový kanál. Aby sme získali dôveryhodný výsledok o zdroji času, musíme zabezpečiť, že správy ktoré prijímame sú autentické a nezmenené. Uvedené sa dá zabezpečiť ako symetrickým šifrovaním, tak i asymetrickým. Jedným z možných spôsobov je použiť tajný kľúč alebo jednorázové kľúče a pre každé nové spojenie na ochranu prenášaných správ použiť nový kľúč z preddefinovanej sady. Pre nesporné nevýhody so správou kľúčov navrhujeme použiť šifrovanie s verejným kľúčom. Každá správa posielaná serverom bude digitálne podpísaná jeho podpisom určeným len na tento účel.

Problémy, s ktorými sa potýkame pri ochrane kľúčov ako i zabezpečenia synchronizácie serveru so zdrojom času TSA, sú identické ako pri prvom riešení využívajúcom NTP. Rovnako v „opačnom“ nasadení (server v SMÚ a klient v TSA) môže slúžiť pre synchronizáciu času TSA s referenčným etalónom. Systém postavený na telefónnom prenose nie je myslený pre nepretržité monitorovanie zdroja času TSA (aj keď to nevylučuje), ale umožňuje kontrolnému orgánu voliť ľubovoľný čas kontroly.

Implementácia systému si v každej TSA a kontrolnom orgáne vyžaduje zabezpečenie spoľahlivej prevádzky jedného počítača s telefónnym modemom a telefónnu prípojku. I pri tomto systéme doporučujeme použitie rozširujúcej karty nahrádzajúcej hodiny počítača v kontrolnom orgáne. Navyše kontrolný orgán musí zabezpečiť vývoj aplikácií umožňujúcich meranie a spracovanie výsledkov.

3.3.3 Analýza časových pečiatok

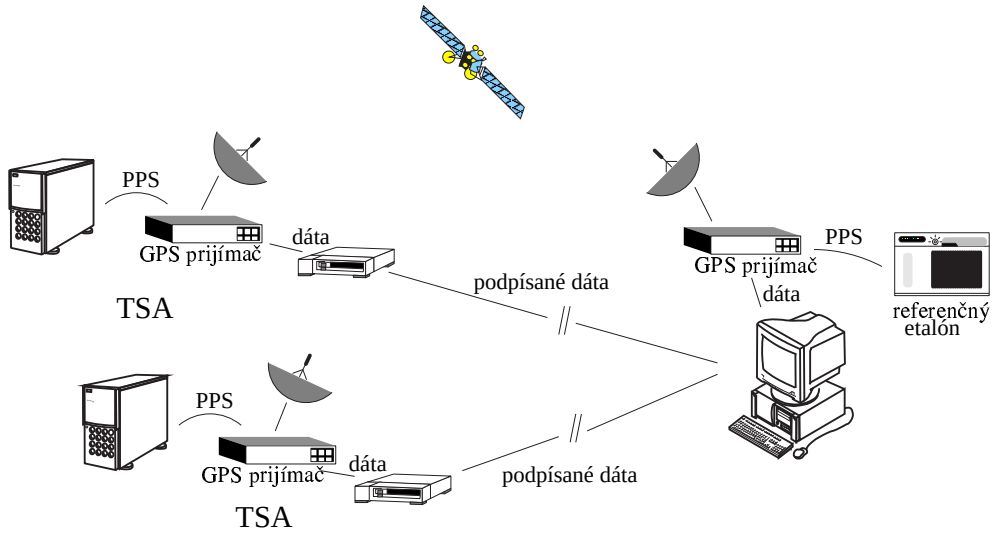
Systém analýzy časových pečiatok je založený na nie zložitej idei merania. Meranie sa vykonáva zasielaním žiadostí o časovú pečiatku TSA z kontrolného orgánu a porovnaním času v nej uvedeného s referenčným. Počítač posielajúci žiadosti je synchronizovaný s referenčným etalónom a zaznamenáva si čas odoslania a čas príjmu odpovede každej z nich. Čas uvádzaný v časovej pečiatke je porovnaný s časom odoslania žiadosti zväčšeným o prenosové oneskorenie získané odčítaním času odoslania od času príjmu a vydelením dvoma. Bezpečnosť prenosu časovej pečiatky, autenticita a integrita, je zaručená jej elektronickým podpisom. Oceniť treba i fakt, že výsledok merania sa zakladá na rovnakom konečnom produkte, aký dostáva zákazník.

Nevýhodou riešenia sú nároky na TSA a vyťažovanie služby poskytovania časových pečiatok systémom. TSA musí poskytovať svoje služby on-line, vybavovať žiadosti bezodkladne a udávať milisekundové rozlíšenie. Všetky tieto predpoklady sú nutné pre dosiahnutie požadovanej neistoty. Opäť experimentom sa nám podarilo overiť, že môže byť menšia ako ± 30 ms (viď kap. 4.5). Naopak medzi výhody patrí transparentnosť. Pre TSA sa kontrolný orgán javí ako radový klient využívajúci jej služby. Na strane TSA nie je nutné budovať žiadne časti systému, a teda systém nevyžaduje ani žiaden zásah do IT systému TSA, čo ho značne zjednodušuje. Kontrolný orgán potrebuje zabezpečiť počítač spolu so softvérom vykonávajúcim a spracovávajúcim merania jeho bezpečnú a spoľahlivú prevádzku a bezpečné pripojenie do Internetu.

3.3.4 Common View GPS

Na porovnávanie etalónov v metrológii sa dnes najčastejšie používa metóda Common View GPS. Predstavuje najvýkonnejšie riešenie, schopné overiť takmer akékoľvek tvrdenie o neistote zdroja času TSA.

Systém je založený na americkom vojenskom systéme GPS, ktorý umožňuje určiť polohu prijímača kdekoľvek na Zemi. Neistota porovnávaní pritom dosahuje nanosekundové hodnoty. Aby sme boli schopní využiť celý potenciál metódy Common View GPS, požadujeme od zdroja času PPS a dátový



Obr. 3.2: *Schematické znázornenie Common View GPS porovnávania.*

výstup poskytujúci plnú informáciu o čase. Signál zo zdroja času je privedený priamo do prijímača GPS konštruovaného pre porovnávanie Common View metódou. Prijímač porovnáva signál na vstupe so signálom vybranej družice. Také isté meranie prebieha v kontrolnom orgáne, kde sa referenčný etalón porovnáva voči tej istej družici. Výsledky merania zdroja času sú nakoniec zaslané do kontrolného orgánu, kde sú spracovávané a vyhodnocované. Schematické znázornenie systému je zachytené na obrázku 3.2.

Pre dosiahnutie čo najlepších výsledkov je zapotreby, aby sa referenčný etalón a zdroj času porovnával voči tej istej družici v tom istom čase. To si vyžaduje pripraviť rozvrh porovnávaní. Pri jeho zostavovaní sa snažíme o to, aby bol vybraný satelit v danom čase čo najvyššie nad obzorom (pri pozorovaní z oboch lokalít). Minimalizuje sa tak dráha signálu zo satelitu cez ionosféru a tým aj neistota. Ďalej je nutné poznať zemepisnú polohu prijímacích antén s neistotou na niekoľko desiatok centimetrov[3]. Znalosť polohy dovoľuje GPS prijímaču vypočítať prenosové oneskorenie signálu z družice.

Vzhľadom na malú rozlohu Slovenska, nie je problém zostaviť jeden rozvrh, ktorým by sa riadili všetky TSA. Dobré výsledky by boli dosiahnuté aj použitím rozvrhu pripraveného BIPM, podľa ktorého sa riadi porovnanie národných etalónov v celej Európe. V takomto prípade nie je nutné na strane referenčného etalónu inštalovať ďalší GPS prijímač a môžu sa použiť výsledky zbierané za účelom medzinárodnej nadväznosti.

[3]GPS prijímač síce častokrát umožňuje zistiť polohu antény, ale nie s požadovanou neistotou.

Aby sme zaručili dôveru nameraných výsledkov, je nutné zaistiť hodnovernosť výsledkov posielaných TSA do kontrolného orgánu. Pre tento účel sa dá použiť vybudovaná PKI infraštruktúra. Dokument s porovnaním GPS voči zdroju času je digitálne podpísaný a môže sa odostať i nezabezpečeným kanálom (emailom a pod.). Nutné je pri tom postarať sa o to, aby nebolo možné manipulovať s výsledkami medzitým ako sú načítané z GPS prijímača a ich digitálnym podpísaním, ako i bezpečnosť privátnych kľúčov.

Napriek tomu, že GPS neposkytuje zabezpečený signál, jeho rušenie by sme ľahko odhalili. Rušiť GPS nie je technicky náročný problém nakoľko satelity vysielajú len malý výkon (20 W) na frekvencii asi 1,5 GHz. Signál na Zemi sa dá preto ľahko prebiť vlastným. Na výpadok signálu družice prijímač ihneď upozorňuje.

Iná situácia nastáva ak je útočník schopný injektovať falošný signál GPS prijímaču TSA. V takom prípade oba GPS prijímače robia dve úplne nezávislé porovnania a o kvalite zdroja času TSA voči referenčnému etalónu nie je možné vysloviť žiadne tvrdenie. Avšak s určitosťou nastane zhoršenie kvality zdroja času TSA vo výsledkoch, ak zdroj času útočníka vysielajúceho falošné GPS signály je horšej kvality ako zdroj TSA. Postaviť systém simulujúci GPS považujeme za pomerne technicky, odborne i finančne náročné.

Pripomenúť treba skutočnosť, že GPS je systém budovaný a prevádzkovaný USA a podlieha plne ich kontrole. Z minulosti sú známe prípady zámerného rušenia jeho signálu, zavedením tzv. Selective Availability. Ale ani v tomto období neistota meraní nedosahovala hodnoty nad sto nanosekúnd. Úplné vypnutie GPS pre civilný sektor je dnes pre veľké množstvo aplikácií, ktoré sú na ňom závislé už takmer nepredstaviteľné. V takomto prípade sa ponúka použitie obdobného ruského systému Glonass, či pripravovaného európskeho systému Galileo. Rovnako je nutné brať na zreteľ, že výsledky merania sú známe až po doručení výsledkov pozorovania TSA kontrolnému orgánu a ich spracovaní. Výsledok preto nepoznáme ihneď, ale vypovedá o správaní zdroja času spätne v čase.

Najväčšie výhody riešenia sú kontinuálny monitoring zdroja času a veľmi nízka neistota výsledku. Tá sa javí až neadekvátne nízka pre daný účel systému, a preto môžeme spochybniť vynaloženie nemalých vstupných nákladov na implementáciu. Tie si vyžadujú Common View GPS prijímač, ktorých cena sa pohybuje okolo 500 tis. Sk a počítač s aplikáciou zbierajúcou, podpisujúcou a odosielajúcou výsledky kontrolnému orgánu v každej TSA. Kontrolný orgán môže využiť svoj prijímač používaný pre porovnanie referenčného etalónu s inými národnými etalónmi. Ďalej musí kontrolný orgán zabezpečiť vývoj aplikácie príjmajúcej a spracovávajúcej výsledky meraní spolu s potrebným harvérom.

3.4 Porovnanie riešení

V predošlom sme opísali štyri systémy, všetky slúžiace pre porovnanie času zdroja času TSA s referenčným etalónom resp. UTC. Všetky spĺňajú požadované kritérium na neistotu výsledku menšiu ako ±30 ms. Preto hlavným kritériom pri výbere jedného konkrétneho riešenia bude bezpečnosť a jednoduchosť jeho realizácie.

Každý zo systémov, okrem systému založeného na analýze časových pečiatok, pozostáva z dvoch častí, pričom jedna z nich je umiestnená v prostredí TSA. Aby tieto mohli medzi sebou spoľahlivo komunikovať, využívajú digitálne podpisy na zabezpečenie autenticity a integrity správ. Ak chceme systém chrániť aj proti útokom TSA, musí byť schopný sám vytvárať podpisy a svoje súkromné kľúče dostatočne chrániť. Ako sme naznačili pri systéme využívajúcom NTP, ochrana kľúčov si vyžaduje nemalé nároky na zdroje. Takisto spoľahlivá synchronizácia časti systému so zdrojom času TSA môže byť netriviálna, nakoľko u každej TSA musíme predpokladať iný IT systém poskytujúci rôzne možnosti. Common View GPS požaduje od zdroja času PPS výstup, aby sa využil celý potenciál metódy. Nie každý zdroj času poskytuje PPS signály a ich zabezpečenie ani nemusí byť vždy možné. Pre použitie systému využívajúceho NTP je najlepšie, aby zdroj času mohol vystupovať i ako NTP server systému.

Oba tieto problémy obchádzajú systém analýzy časových pečiatok. Jeho realizácia nevyžaduje žiadnu časť systému umiestnenú v TSA, a preto nemusíme nič predpokladať o možnostiach IT systému TSA a robiť doň zásahy. Celý systém je realizovaný v kontrolnom orgáne a využíva služieb TSA. Bezpečnosť je založená na už existujúcich mechanizmoch používaných TSA na zabezpečenie dôvery vydaných časových pečiatok. Pre zavedenie a prevádzku požaduje minimálne zdroje TSA. Taktiež treba vyzdvihnúť, že systém analyzuje kvalitu konečného produktu, naprotičomu ostatné tri riešenia sa snažia kontorolovať predpoklady jeho kvalitnej výroby. V reálnom svete platí že, ak zdroj času má správny čas, môžeme len predpokladať, že správny čas bude vložený aj do časovej pečiatky a naopak. Preto systém analýzy časových pečiatok považujeme za vhodnejší pre dosiahnutie konečného cieľa zaručenia správnosti času v časových pečiatkach. Zaručenie správnosti času zdroja času je len medzistupňom k tomuto cieľu. Vedľajším produktom je i schopnosť overiť, či TSA danú službu v požadovaný okamih vôbec poskytuje. Obmedzením systému analýzy časových pečiatok, ako vidno i z tabuľky 3.2, sú požiadavky, ktoré musí každá TSA spĺňať. Pre jeho použitie musí každá TSA poskytovať služby on-line, uvádzať milisekundové rozlíšenie v časových pečiatkach a vybavovať žiadosti o časovú pečiatku bezodkladne.

Tieto skutočnosti zatienia aj také výhody ostatných systémov ako ne-

	Využitie NTP	**Telefónny prenos**	**Analýza č. pečiatok**	**C.V. GPS**
Neistota výsledku	< 30 ms	< 30 ms	< 30 ms	< 100 ns
Náklady na implement.	stredné	stredné	nízke	vysoké
Nutnosť ochrany súkromného kľúča	áno	áno	nie	áno
Ľubovoľný čas kontroly	áno	áno	áno	nie
Nepretržitý monitoring	áno	možný	obmedzene možný	áno
Časť systému v TSA	áno	áno	nie	áno
Zasahuje do IS TSA	áno	áno	nie	áno
Možnosť synchronizácie TSA na ref. etalón	áno	áno	nie	nie
Predpokl. o službách TSA	nie	nie	áno	nie
Spol. časť systému v kon. orgáne pre všetky TSA	áno	áno	áno	áno

Tabuľka 3.2: *Porovnanie navrhnutých systémov.*

pretržitý monitoring zdroja času, či možnosť ich použitia i na synchronizáciu s referenčným etalónom. Systém analýzy časových pečiatok považujeme za najvhodnejšie riešenie.

Kapitola 4

Systém analýzy časových pečiatok

V predchádzajúcej kapitole sme analyzovali rôzne spôsoby, ako porovnať čas zdroja času TSA s referenčným etalónom, ktorý je nadviazaný na časovú stupnicu UTC. Na jej základe sme vybrali podľa nás najvhodnejší systém hodiaci sa pre tento účel. Nasledovná kapitola prináša jeho podrobný popis.

4.1 Popis činnosti

Hlavnú myšlienku činnosti systému sme predstavili v kap. 3.3.3. Systém využíva základných služieb TSA, pre ktoré pôvodne vznikli.

Predpokladajme, že kontrolný orgán chce overiť správnosť času zdroja času TSA resp. správnosť času udávaného v časových pečiatkach TSA. Za týmto účelom si vygeneruje sadu náhodných dokumentov a žiadostí na ich opečiatkovanie. Postupne bude žiadosti zasielať TSA, pričom si systém zaznamenáva nasledovné údaje, ktoré použije neskôr pri vyhodnocovaní konečného výsledku merania:

- dokument m, ktorý má byť opečiatkovaný
- $h(m)$ – haš dokumentu m, ktorý má byť opečiatkovaný
- t_m^s– čas odoslania žiadosti na opečiatkovanie dokumentu m TSA
- t_m^r – čas prijatia časovej pečiatky dokumentu m z TSA
- t_m^c – čas uvedený v časovej pečiatke dokumentu m vystavenej TSA

Po opečiatkovaní celej sady môžeme pristúpiť k spracovaniu nameraných výsledkov. Predovšetkým overíme podpis TSA na všetkých časových pečiatkách, a či bol opečiatkovaný dokument, ktorý sme žiadali. Predpokladáme,

že už máme k dispozícii verejný kľúč kontrolovanej TSA. Pokiaľ sú časové pečiatky podpísané iným podpisom ako TSA, alebo časová pečiatka patrí inému dokumentu, ako sme žiadali, je zrejmé, že komunikácia medzi TSA a kontrolným orgánom bola narušená. V takomto prípade opakujeme celé meranie, alebo je upozornená určená osoba.

Po overení integrity a autentickosti časových pečiatok môžeme začať analyzovať namerané údaje. Časové intervaly od zaregistrovania žiadosti v TSA po jej opečiatkovanie a od opečiatkovania po odoslanie považujeme za časy prenosu a budeme ich rátať do prenosového oneskorenia. O prenosovom kanále predpokladáme, že je symetrický a prenosové oneskorenie správy posielanej z kontrolného orgánu do TSA je rovnaké ako opačným smerom. Prenosové oneskorenie d_m pri časovom opečiatkovávaní dokumentu m vypočítame zo vzťahu

$$d_m = \frac{(t_m^r - \tau) - t_m^s}{2} , \tag{4.1}$$

kde τ je konštanta kompenzujúca čas potrebný na podpísanie časovej pečiatky. Podpisové zariadenie TSA dokáže podpísať len približne 50 až 400 časových pečiatok za sekundu. Na podpísanie jednej časovej pečiatky je preto potrebný čas 2,5 až 20 ms v závislosti od konkrétneho podpisového zariadenia.

Je zrejmé, že prenosové oneskorenie bude pre každý dokument m iné, nakoľko stav prenosového kanála bude iný. Aby sme zmeny stavu prenosového kanála minimalizovali, budeme žiadosti o časovú pečiatku zasielať ihneď po sebe, v čo najkratších časových intervaloch.

Pre odchýlku časových stupníc zistenú za pomoci časovej pečiatky dokumentu m platí

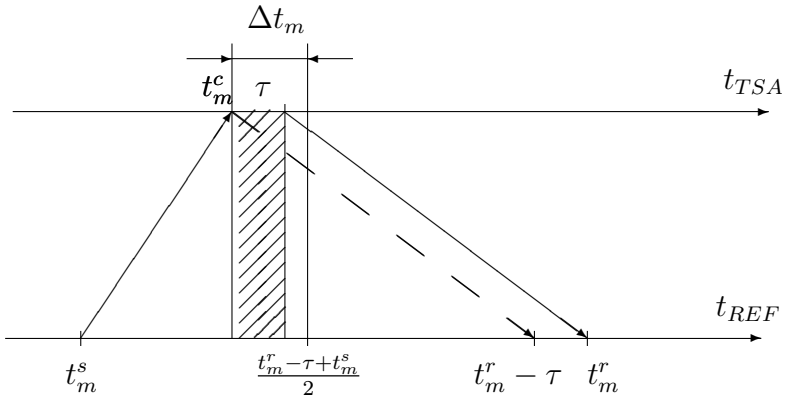
$$\Delta t_m = t_m^c - (t_m^s + d_m) \tag{4.2}$$

a dosadením rovnice (4.1) do (4.2) dostávame výsledný vzťah

$$\Delta t_m = t_m^c - \frac{t_m^s + t_m^r - \tau}{2} . \tag{4.3}$$

Odchýlka časových stupníc je rozdielom času udávaného v časovej pečiatke dokumentu a priemerným časom medzi odoslaním žiadosti o časovú pečiatku dokumentu a prijatím odpovede. Výslednú odchýlku časových stupníc referenčného etalónu od zdroja času TSA a neistou merania dostaneme štatistickým spracovaním odchyliek Δt_m každého dokumentu a zarátaním odchyliek časových stupníc počítača vykonávajúceho meranie od referenčného etalónu a referenčného etalónu od UTC.

Otázkou ostáva, koľko žiadostí je nutné zaslať na dosiahnutie reprezentatívneho výsledku o odchýlke časových stupníc. V tomto smere je nutné nájsť



Obr. 4.1: *Znázornenie udalostí pri vydávaní časovej pečiatky v jednotlivých časových stupniciach.*

kompromis. Zaslanie malého počtu žiadostí by nám prinieslo iba hrubý odhad o odchýlke, ktorý nemusí odpovedať skutočnosti. Naopak posielaním veľkého počtu žiadostí by sme mohli zbytočne preťažovať službu TSA a spôsobovať jej ďalšie náklady spojené s vydávaním časových pečiatok. Pritom nie je zaručená adekvátne lepšia hodnota výsledku. Na základe vykonaného merania (viď kap. 4.5) navrhujeme zaslať zakaždým približne 100 žiadostí o časovú pečiatku, avšak stanovenie presných hodnôt si vyžaduje dlhšie pozorovania a analýzu.

4.2 Predpoklady systému o TSA

Pretože systém nemá žiadne časti inštalované v TSA, aby mohol vykonávať svoju činnosť, kladie na TSA predpoklady, ktoré musí spĺňať.

TSA ponúka služby aj on-line. Ponuka on-line služieb v portfóliu TSA je základným predpokladom pre získanie kvalitných dát. On-line prevádzka minimalizuje dobu medzi odoslaním žiadosti a jej doručením do TSA, ako i čas prijatia odpovede a umožňuje zasielanie väčšieho počtu žiadostí v krátkom časovom intervale.

TSA spracováva žiadosti o časovú pečiatku aj bezodkladne. Na spracovanie žiadosti si TSA môže stanoviť určitý čas (hodinu, deň, týždeň...), pričom sa zaručí, že do jeho uplynutia bude žiadosť spracovaná a odoslaná odpoveď. Napríklad ak predpokladáme, že TSA spracováva naše žiadosti do hodiny, potom na základe prvej žiadosti môže vystaviť časovú pečiatku už po minúte od doručenia, avšak odpoveď odoslať až po 30 minútach. Pri nasledujúcej žiadosti môže byť časová pečiatka vystavená po 50 minútach a ihneď odoslaná i odpoveď. Je zrejmé, že

v takejto situácii nie je možné získať neistotu merania lepšiu ako 30 minút, pretože prenosový kanál by bol silne asymetrický vzhľadom na prenosové oneskorenie, ak doň zarátame intervaly medzi doručením žiadosti a vystavením časovej pečiatky a odoslaním odpovede. Preto je dôležité, aby TSA spracovávala žiadosti o časovú pečiatku bezodkladne. V ideálnom prípade TSA nielenže spracováva žiadosti bezodkladne, ale i umožňuje priradiť žiadostiam prioritu dovoľujúcu uprednostniť spracovanie jednotlivých žiadostí pred ostatnými, skôr zaregistrovanými. Avšak s takouto možnosťou zatiaľ žiadny štandard alebo odporúčanie pre TSA nepočíta.

TSA vydáva časové pečiatky aj s milisekundovým rozlíšením. Pre výslednú neistotu merania je dôležité uvedenie informácie o čase v časovej pečiatke s milisekundovým rozlíšením. Ak žiadame dosiahnute neistoty merania v rádoch jednej až desiatok milisekúnd je rozlíšenie desiatok milisekúnd nevhodné, nakoľko rozdiely v nameraných odchylkách $\Delta t_m$by boli príliš veľké.

4.3 Spracovanie výsledkov merania

Pri spracovávaní výsledkov merania považujeme frekvenciu zdroja času TSA za stabilnú a správnu po celú dobu merania. Ak by sa odchýlka časových stupníc zdroja času TSA a referenčného etalónu systematicky zväčšovala vplyvom rozdielnych frekvencií oscilátorov, budeme tento efekt v rámci jedného merania zanedbávať, nakoľko o meraní predpokladáme, že je dostatočne krátke nato, aby sa vplyv mohol výraznejšie prejaviť v konečnom výsledku.

Na spracovanie výsledkov použijeme metód Gaussovej štatistiky. V tejto súvislosti je dobré si uvedomiť nasledovné fakty. Odchýlka časových stupníc je náhodnou veličinou a o základnom súbore náhodnej veličiny predpokladáme, že má normálne rozdelenie pravdepodobnosti s neznámymi parametrami μ, σ. Namerané odchýlky časových stupníc Δt_{m_i}, vypočítané podľa rovnice (4.3), tvoria výber zo základného súboru. Výsledok merania $\overline{\Delta t}$ je výberová priemerná hodnota, ktorá je odhadom priemernej hodnoty μ základného súboru ($\overline{\Delta t}$) spolu s neistotou $u_{\overline{\Delta t}}$. Metrologickou konvenciou je na hladine významnosti 95% neistota merania určená ako dvojnásobok odhadu s smerodajnej odchýlky základného súboru. [33]

Predpokladajme, že máme súbor meraní Δt_{m_i} pre $2 \leq i \leq N$ odchyliek časových stupníc tvoriaci výber zo základného súboru. Predovšetkým je nutné zo súboru odfiltrovať tie merania, ktoré sa očividne vymykajú z priemeru. Pri každom meraní môžeme namerať niekoľko hodnôt zjavne iných ako všetky ostatné. Tieto považujeme za chybné a vylúčime ich zo súboru. Ako

formálne kritérium pre chybné meranie zavedieme

$$\Delta t_{m_i} \notin (\overline{\Delta t} - 3s; \overline{\Delta t} + 3s) \ . \tag{4.4}$$

Pri náhodnej veličine s normálnym rozdelením môžeme s 99,7% pravdepodobnosťou predpokladať, že jej hodnota padne do intervalu $(\overline{\Delta t}-3s; \overline{\Delta t}+3s)$. [41] Ak by sme takto odstránili viac ako 5% hodnôt z celého súboru meraní, považujeme celý súbor za zlý a budeme vyžadovať nové meranie.

Z upraveného súboru meraní opäť vypočítame priemernú hodnotu $\overline{\Delta t}$ a odhad smerodajnej odchýlky základného súboru - s. Ak sa s nebude príliš vymykať z dlhodobého normálu, výsledok $\overline{\Delta t} \pm u_{\overline{\Delta t}}$ pre $u_{\overline{\Delta t}} = 2s$ môžeme považovať za odchýlku časových stupníc počítača vykonávajúceho meranie a zdroja času TSA. Pre konečnú odchýlku Δt zdroja času od UTC k získanej odchýlke pripočítame odchýlku dt_{ref} počítača od referenčného etalónu a odchýlku dt_{utc} referenčného etalónu od UTC a ich neistoty.

$$\Delta t = \overline{\Delta t} + dt_{ref} + dt_{utc} \pm \sqrt{u^2_{\overline{\Delta t}} + u^2_{dt_{ref}} + u^2_{dt_{utc}}} \tag{4.5}$$

Hodnoty dt_{ref}, dt_{utc} a ich neistoty získava kontrolný orgán vlastnými meraniami. Ale pre konečný výsledok sú len málo významné (dt_{ref} očakávame v rádoch mikrosekúnd a dt_{utc} je niekoľko desiatok nanosekúnd (viď kap. 2.7)), a preto ich môžeme zanedbať.

Vyššie uvedené zhrnieme do nasledovného algoritmu:

Vstup: $\tau, t^s_{m_i}, t^r_{m_i}, t^c_{m_i}$ pre $2 \leq i \leq N$

Výstup: $\overline{\Delta t} \pm u_{\overline{\Delta t}}$

1. Vypočítaj $\Delta t_{m_i} = t^c_{m_i} - \dfrac{t^s_{m_i} + t^r_{m_i} - \tau}{2}$.
2. Vypočítaj $\overline{\Delta t} = \dfrac{1}{N} \sum\limits_{i=1}^{N} \Delta t_{m_i}$.
3. Vypočítaj $s = \sqrt{\dfrac{1}{N-1} \sum\limits_{i=1}^{N} \left(\Delta t_{m_i} - \overline{\Delta t}\right)^2}$.
4. Odstráň tie Δt_{m_i}, pre ktoré platí $\Delta t_{m_i} \notin (\overline{\Delta t}-3s; \overline{\Delta t}+3s)$ a preindexuj výslednú množinu Δt_{m_i}.
5. Nech M je počet zvyšných Δt_{m_i}. Ak $M/N \geq 0.95$ opakuj kroky 2 a 3 pre $N = M$, inak požaduj nový vstupný súbor meraní.
6. Ak sa s príliš neodchyľuje od dlhodobého priemeru stanov výsledok merania ako $\overline{\Delta t} \pm 2s$, inak požaduj nový vstupný súbor meraní.

4.4 Interpretácia výsledku merania

Z popísaného modelu výpočtu odchýlky časových stupníc plynie niekoľko dôsledkov. Predovšetkým daný model nerozlišuje medzi asymetrickosťou prenosového kanála a odchýlkou zdroja času. Ak je prenosové oneskorenie prenosu správy smerom do TSA menšie ako prenosu z TSA, potom rozdiel týchto prenosových oneskorení, miera asymetrickosti, sa prejaví ako odchýlka časovej stupnice zdroja času.

Ďalším faktom je, že rozdielna veľkosť prenosového oneskorenia pri posielaní jednotlivých žiadostí o časovú pečiatku a ich odpovedí nemá vplyv na výsledok merania, ak prenosový kanál ostáva stále symetrický. Predpokladajme, že žiadosť o časovú pečiatku dokumentu m_1 a odpoveď na ňu sa posielala cez kanál c_1 a žiadosť o časovú pečiatku dokumentu m_2 a odpoveď sa posielala cez kanál c_2. Tento prípad v sieti Internet nemusí byť ničím výnimočným. Ak sú oba kanály c_1, c_2 symetrické, potom rozdiel ich prenosových oneskorení sa na konečnom výsledku merania neprejaví.

Iný prípad by nastal ak by sme člen d_m v rovnici (4.2) nahradili priemernou hodnotou prenosového oneskorenia $\bar{d}$. V takejto situácii by výsledok merania ovplyvnila i stabilita prenosového oneskorenia počas celého merania. Ak by sa menila veľkosť prenosového oneskorenia pre jednotlivé dokumenty (pre posielanie žiadostí a odpovedí by sa napríklad využívalo niekoľko kanálov), pričom kanál by ostával stále symetrický, zväčšila by sa neistota nameraného výsledku.

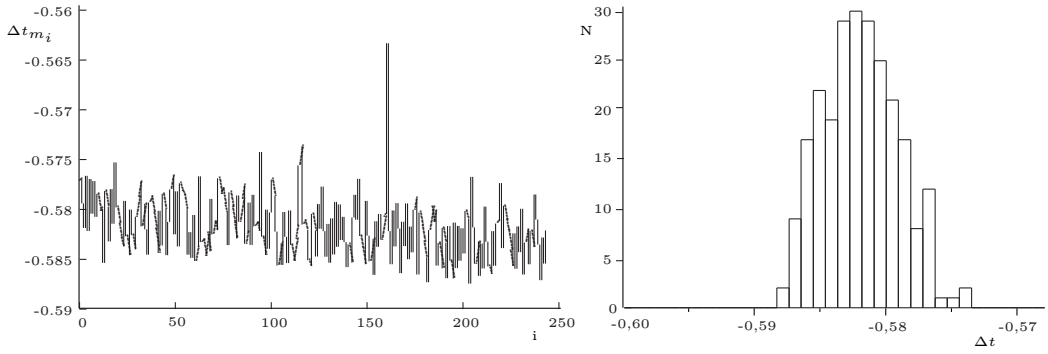
Pre stanovenie výsledného verdiktu, či zdroj času TSA spĺňa kritérium uvedené v politike časových pečiatok si pripomeňme, čo hovorí. V politike časových pečiatok sa deklaruje neistota u_c odchýlky časovej stupnice zdroja od UTC, pričom sa predpokladá, že samotná odchýlka je nulová. Preto ak zanedbáme odchýlky a neistoty časovej stupnice počítača vykonávajúceho meranie od UTC, pre zdroj času bude platiť tvrdenie uvedené v politike časových pečiatok práve vtedy, ak interval $(\overline{\Delta t} - u_{\overline{\Delta t}}; \overline{\Delta t} + u_{\overline{\Delta t}})$ je podintervalom intervalu $(-u_c; +u_c)$.

4.5 Neistota výsledku

Rovnako ako pri ostatných systémoch uvažovaných v kapitole 3, aj pre systém analýzy časových pečiatok sme zostavili experiment, ktorý by overil, že dosiahnutá neistota merania bude menšia ako ± 30 milisekúnd.

Na výslednú neistotu sme predpokladali, že bude vplývať asymetrickosť prenosového kanála, ako i rozdielne časy spracovania žiadosti o časovú pečiatku TSA. Na rozdiel od predchádzajúcich experimentov, pri tomto už

boli použité kryptografické nástroje a časové pečiatky boli podpisované TSA. Experiment spočíval v zaslaní a analýze 250 žiadostí o časovú pečiatku v čo najkratšom čase spoločnosti *Viasec, s.r.o.* Server spoločnosti akceptoval žiadosti po vytvorení socket spojenia, pričom oba počítače sa nachádzali v Bratislave. Zber dát prebiehal identicky ako je popísané v kapitole 4.1 a výsledky boli spracované postupom uvedeným v kapitole 4.3.



Obr. 4.2: *Graf a histogram nameraných odchyliek časových stupníc.*

Graf nameraných odchyliek a ich histogram ukazuje obr. 4.2. Z týchto dát bolo už odstránených podľa kritéria (4.4) 5 zjavne zlých hodnôt. Odchýlky sa v týchto prípadoch pohybovali okolo $-1,8$ s. 5 z 250 predstavuje 2% preto sme zvyšný súbor pokladali za reprezentatívny. Prenosové oneskorenie v priemere dosahovalo hodnotu 44,2 ms. Vypočítaná priemerná odchýlka časovej stupnice počítača robiaceho meranie voči zdroju času TSA bola

$$\overline{\Delta t} = -582 \pm 6,0 \text{ ms}.$$

Odchýlku 0,5 sekundy pripisujeme zlej synchronizácii času počítača vykonávajúceho meranie voči UTC. Experiment však potvrdil, že systém analýzy časových pečiatok je schopný priniesť dostatočne kvalitné výsledky v súlade s tým, čo sa požaduje.

4.6 Požiadavky na systém

Hlavným cieľom systému je kontrola správnosti času v časových pečiatkach, ktorá nám umožní overiť pravdivosť tvrdení v politike časových pečiatok. Tomuto cieľu sú podrobené aj požiadavky kladené na systém. Snažia sa zabezpečiť, aby systém vykonával činnosť, pre ktorú bol zamýšľaný, aby jeho používanie bolo spoľahlivé, a aby systém bol do určitej miery univerzálny a dal sa použiť na kontrolu činnosti viacerých TSA.

Funkčné požiadavky

1. *Systém musí byť schopný kontroly času v časových pečiatkách voči referenčnému etalónu s požadovanou neistotou* ±30 *ms.* Jedná sa o hlavnú funkčnosť systému. Na jej zabezpečenie je potrebné, aby systém vedel realizovať meranie spôsobom opísaným v kapitole 4.1 a 4.3. To znamená, že systém musí byť schopný zaslať žiadosť o časovú pečiatku a prijať odpoveď, pričom si zaznamenáva časy týchto udalostí. Systém musí vedieť získať čas uvedený v časovej pečiatke a overiť, či časová pečiatka patrí dokumentu, ktorý mal byť opečiatkovaný, overiť podpis TSA a vypočítať konečný výsledok.

2. *Systém musí byť schopný kontrolovať správnosť času v časových pečiatkách viacerých TSA.* Nie je účelom stavať pre každú TSA samostatný systém. Od navrhovaného systému preto žiadame, aby bol univerzálne použiteľný pre každú TSA.

3. *Systém musí umožniť voľbu času kontroly TSA a automatické vykonávanie kontrol podľa rozvrhu.* Požiadavka umožní vykonať kontrolu v zvolenom čase a automatizovať činnosť systému.

4. *Systém musí byť rozšíriteľný a umožniť jednoduchým spôsobom pridať kontrolu ďalšej TSA.* V momente návrhu systému nie je možné predvídať koľko, a ktoré TSA bude mať systém kontrolovať. Preto by mal systém ponúkať jednoduchý spôsob zaradenia kontroly času v časových pečiatkach novej TSA.

5. *Systém musí vedieť uchovať výsledky merania po určenú dobu.* Požiadavka umožnuje spätne sa vracať k výsledkom meraní, umožňuje robiť dlhodobejšie analýzy správnosti času TSA a detekovať prípadné zmeny a chyby. ZoEP nariaďuje TSA uchovávať údaje v archíve najmenej 10 rokov. Doporučujeme preto rovnaké obdobie.

6. *Systém musí upozorňovať na neštandardné situácie, výsledky merania a nepredvídané udalosti na to zvoleným spôsobom určené osoby.* Jedná sa o schopnosť systému upozorniť sa situácie, ktoré nevie sám riešiť, s ktorými sa pri jeho detailnom návrhu nepočítalo, alebo ktoré si vyžadujú zásah človeka. Upozornenie môže byť riešené zaslaním emailu, SMS správy, zvukovým alebo svetelným signálom a pod.

7. *Systém musí robiť auditné záznamy.* Zaznamenávanie všetkých bezpečnostne a inak významných udalostí a aktivít uľahčuje riešenie vzniknutých problémov.

Bezpečnostné ciele

Jedinou potenciálne dôvernou informáciou v systéme sú výsledky merania. Ich prezradením sa však základná činnosť TSA nijak neovplyvní a dopady považujeme za malé. Preto bezpečnostné požiadavky systému budú zamerané hlavne na zaistenie jeho spoľahlivej prevádzky a výsledkov. Mali by v čo najväčšej miere zabezpečiť nasledovné bezpečnostné ciele:

1. *Umožnenie manipulácie so systémom len autorizovaným osobám.* Zabraňuje zneužitiu systému inými osobami. Napríklad pri každej operácii systém vyžaduje identifikáciu a autentifikáciu používateľa.

2. *Identifikovať neoprávnenú manipuláciu so systémom a narušenie integrity.* Dovoľuje zistiť zneužitie alebo napadnutie systému. Jedná sa napríklad o zaplombovanie káblov v systéme a pod.

3. *Od systému požadujeme spoľahlivú prevádzku, nie však nepretržitú.* Krátky výpadok činnosti systému nepovažujeme za kritický a nevyžadujeme, aby bol napríklad v prevádzke 24 hodín denne 7 dní v týždni. Avšak návrh a prevádzka systému musí v rozumnej miere minimalizovať riziko jeho výpadku.

4. *Prenos dát mimo systém je umožnený len v nevyhnutnej miere.* Zabraňuje narušeniu dôvernosti dát v systéme, narušeniu ich integrity.

4.7 Architektúra systému

Logická architektúra

Logická architektúra rozdeľuje jednotlivé časti systému podľa ich logických činností. Pre činnosť systému potrebujeme nasledovné moduly:

- *modul pre komunikáciu s TSA* - Modul zabezpečuje odosielanie žiadostí do TSA a prijímanie odpovedí.

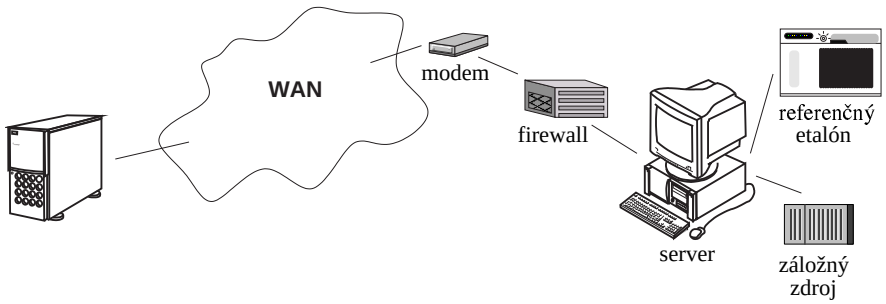
- *modul pre štatistické spracovanie výsledkov* - Obstaráva výpočty nad nameranými dátami a stanovenie výsledku.

- *modul plánovania* - Modul zaisťuje vytváranie plánov kontrol a ich sledovanie (spúšťanie kontroly TSA v požadovanom čase).

- *databáza* - Uchováva výsledky meraní, verejné kľúče komunikačné protokoly a iné potrebné informácie o jednotlivých TSA a nastaveniach systému.

- *modul pre notifikáciu* - Upozorňuje určené osoby na neštandardné výsledky alebo správanie systému, nepredvídané a iné dôležité udalosti.
- *modul pre logovanie* - Zaznamenáva všetky dôležité a nepredvídané udalosti v behu systému.

Fyzická architektúra



Obr. 4.3: *Fyzická architektúra systému.*

Pre zabezpečenie prevádzky systému potrebujeme tieto časti:

- *referenčný etalón času* - Zariadenie poskytujúce správny čas. Voči referenčnému etalónu bude čas v časových pečiatkach porovnávaný. Referenčným etalónom je už v SMÚ prevádzkovaný Národný etalón času a frekvencie.
- *server* - Aplikácie bežiace na serveri nevykonávajú žiadne výpočtovo náročné operácie, ani neukladajú veľké množstvá dát. Kritéria výberu servera by mali byť orientované na jeho spoľahlivú prevádzku a nie výkon.
- *rozširujúca karta s hodinami pre server* - Zabezpečuje synchronizáciu času servera s referenčným etalónom na hardvérovej úrovni. Etalón času a frekvencie neposkytuje priamo dotazovacie funkcie umožňujúce zistiť jeho aktuálny čas s požadovanou presnosťou pri odoslaní žiadosti a príjme odpovede z TSA serverom. Etalón poskytuje len výstup PPS signálov a čas v digitálnej forme s rozlíšením jednej sekundy. Preto časová stupnica servera zabezpečujúceho komunikáciu s TSA musí byť nadviazaná na referenčný etalón a neistota odchyliek týchto dvoch časových stupníc musí byť v ráde milisekúnd a menej.

  Rozširujúca karta sa inštaluje do zbernice servera. Obsahuje nové hodiny, ktorých základom je kvalitnejší oscilátor (najčastejšie TCXO alebo OCXO kryštálový oscilátor), ako oscilátor bežne sa nachádzajúci v serveri a predovšetkým rozširujúca karta poskytuje PPS vstup pre jeho

riadenie. Riadenie sa uskutočňuje PPS impulzmi posielanými z etalónu do oscilátora hodín, pomocou ktorých elektronika obklopujúca oscilátor neustále porovnáva a dolaďuje jeho frekvenciu.

Alternatívne sa problém synchronizácie dá riešiť použitím NTP protokolu. NTP dokáže riadiť hodiny servera PPS signálmi privedenými na sériový port. Takáto implementácia však dosahuje oveľa vyšších neistôt ako predošlá. Je to spôsobené rôznymi časmi odozvy operačného systému na zmenu stavu sériového portu. Isté zlepšenie ponúka výber vhodného operačného systému. [42, 43]

- *záložný zdroj* - Zaisťuje ochranu proti krátkodobému výpadku elektrickej energie a umožňuje korektné vypnutie systému pri dlhodobých výpadkoch.

- *internetové pripojenie* - Umožňuje prepojenie systému s IT systémom TSA. Internetové pripojenie nemusí oplývať veľkou prenosovou rýchlosťou. Výmena dát medzi TSA a kontrolným orgánom je minimálna (jedna časová pečiatka má asi 1 Kb a žiadosť o ňu ešte menej). Dôraz treba klásť na kvalitu a symetrickosť spojenia. Pre navrhovaný systém predpokladmáme 128 kB ISDN pripojenie.

- *modem* - Zabezpečuje spojenie do siete poskytovateľa pripojenia.

- *firewall* - Chráni server pred útokmi z počítačovej siete. Úlohou firewallu je blokovať spojenia na a zo servera a obmedziť tok dát len na tie, ktoré sú nevyhnutne nutné pre činnosť systému.

Pomocou internetového pripojenia, modemu a firewallu modul pre komunikáciu posiela žiadosti a prijíma časové pečiatky. Uloženie dát v databáze, ich zbieranie a štatistické spracovanie je zabezpečované serverom, ktorý sa stará i o logovanie a notifikáciu.

4.8 Odhad zdrojov

Zdroje na zavedenie systému

1. *server* - Na server podľa kritérií stanovených v architektúre predpokladáme cenu 50-100 tis. Sk.

2. *rozširujúca karta s hodinami pre server* - Predpokladaná cena pre kartu s TCXO kryštálovým oscilátorom je 40 tis. Sk.

3. *záložný zdroj* - Predpokladaná cena záložného zdroja pre server je 10 tis. Sk.

4. *operačný systém* - Operačný systém musí podporovať všetky komponenty serveru a musí byť podporovaný výrobcom serveru. Predpokladaná cena je 30 tis. Sk.

5. softvérová aplikácia - Na vývoj aplikácie predpokladáme 40 človekohodín na zber požiadaviek, 40 človekohodín na analýzu a dizajn, 80 človekohodín na implementáciu, 80 človekohodín na testovanie a 10 človekohodín na nasadenie. Predpokladaná cena práce je 2 tis. Sk/hod a konečná cena aplikácie 500 tis. Sk.

6. *zriadenie internetovej prípojky* - Na zriadenie ISDN pripojenia s rýchlosťou 128 kB/s predpokladáme 2 tis. Sk.

7. *modem* - Predpokladaná ISDN modemu je 5 tis. Sk.

8. *firewall* - Predpokladaná cena hardvérového firewallu je 80 tis. Sk.

Zdroje na prevádzku systému

1. *pripojenie do Internetu* - Cenu za 20 hodín spojenia mesačne odhadujeme na 2 tis./mesiac.

2. *výdavky na hardvér* - Predpokladaná cena za výmenu poškodeného hardvéru a zálohovacích médií 1 tis./mesiac.

3. *správa systému* - Cena za administráciu systému je odhadovaná na 3 tis./mesiac.

4. *prevádzka systému* - Cenu pracovníka vykonávajúceho dozor nad výsledkami merania, informovanie o výsledkoch TSA predpokladáme na 5 tis./mesiac.

Výsledná cena 750 tis. Sk na implementáciu a 11 tis. Sk mesačne na prevádzku systému je len hrubým odhadom. Na jej presnejšie stanovenie je nutné vypracovať podrobnejšiu analýzu. Konečná cena bude závisieť od konkrétne nasadených komponentov, technológií a riešení.

Záver

Problematika kontroly autorít časových pečiatok je neľahká. Nikto nemá prílišný záujem byť kontrolovaný. Kontrolný systém preto musí byť navrhovaný tak, aby spĺňal kritéria kontrolného orgánu a zároveň čo najmenej obmedzoval autoritu časových pečiatok. Podarilo sa nám priblížiť základné poznatky z metrológie času a frekvencie, ktoré nám pomohli pri návrhu riešení. Navrhli sme štyri riešenia, každé s trochu inými vlastnosťami a experimentálne overili ich schopnosť dosiahnuť požadovanú neistotu merania. Rozpätie zahrňuje riešenia jednoduché na implementáciu, minimálne obmedzujúce autority časových pečiatok, až po systém dosahujúci veľmi nízku neistotu merania, založený na rovnakej technológii ako medzinárodné porovnávanie národných etalónov.

Po analýze sme vybrali systém, ktorý nevyžaduje žiadny zásah do informačného systému autorít časových pečiatok a i zabezpečenie dôvery je implementačne jednoduché. Podarilo sa nám overiť jeho schopnosť dosiahnuť požadovanú neistotu a stanoviť základné požiadavky a bezpečnostné ciele. Ale pre nasadenie do praxe je nutné ešte vypracovať

- hlbšiu analýzu riešenia v praxi
- podrobnú špecifikáciu systému
- analýzu riešenia pri zaťažení prenosového kanálu a zariadenia vydávajúceho časové pečiatky
- analýzu nasadenia v prostredí, v ktorom má autorita časových pečiatok viacero zariadení vydávajúcich časové pečiatky.

Nezávisle od implementácie kontrolného systému by sme navrhovali aj úpravu súčasnej legislatívy. Predovšetkým vyhláška NBÚ 537/2002 Z.z. stanovuje, aby zdroj času autority časových pečiatok bol „synchronizovaný s referenčným zdrojom času“, avšak bližšie nešpecifikuje, kto je poskytovateľom referenčného času alebo správcom referenčného zdroja. Druhá navrhovaná úprava sa týka základnej kontroly zdroja času. Časová pečiatka môže byť používaná na právne a úradne významných dokumentoch. Preto navrhujeme, aby zdroj času akreditovanej certifikačnej autority podliehal metrologickej kontrole v zmysle §9 zákona 142/2000 Z.z o metrológii.

Dodatok A

Zoznam skratiek a názvov inštitúcií udržiavajúcich miestnu aproximáciu UTC, UTC(k).

AOS	Astrogeodynamical Observatory, Space Research Centre P.A.A Borowiec, Poland
APL	Applied Physics Laboratory, Laurel, Maryland, USA
AUS	Consortium of laboratories in Australia
BEV	Bundesamt für Eich- und Vermessungswessen, Vienna, Austria
BIRM	Beijing Institute of Radio Metrology and Measurement, Beijing, P.R. China
CAO	Stazione Astronomica di Cagliari, Cagliari, Italy
CH	METrology and Accreditation Switzerland (METAS)
CNM	Centro Nacional de Metrologia, Querétaro, Mexico (CENAM)
CNMP	Centro Nacional de Metrologia, de Panamá, Panamá
CSIR	Council for Scientific and Industrial Research, Pretoria, South Africa
DLR	Deutsche Zentrum für Luft- und Raumfahrt, Oberpfaffenhofen, Germany
DTAG	Deutsche Telekom AG, Darmstadt, Germany
F	Commission Nationale de l'Heure, Paris, France
GUM	Glowny Urząd Miar, Warsaw, Poland
IEN	Instituto Elettrotecnicco Nazionale Galileo Ferraris, Turin, Italy
IFAG	Bundesamt für Kartographie und Geodäsie, Wettzell, Kötzling, Germany
IGMA	Instituto Geográfico Militar, Buenos Aires, Argentina
INPL	National Physical Laboratory, Jerusalem, Israel
JATC	Joint Atomic Time Commision, Lintong, P.R. China
JV	Justervesenet, Norwegian Metrology and Accreditation Service, Kjeller, Norway
KRIS	Korea Research Institute of Standards and Science, Daejeon, Rep. of Korea
LDS	University of Leeds, Leeds, United Kingdom

Zoznam skratiek a názvov inštitúcií udržiavajúcich miestnu aproximáciu UTC, UTC(k), pokračovanie.

LT	Lithuanian National Metrology Institute, Vilnius, Lithuania
MSL	Measurement Standards Laboratory, Lower Hutt, New Zealand
NAO	National Astronomical Observatoty, Misuzawa, Japan
NICT	National Institute of Information and Communications Technology, Tokyo, Japan
NIM	National Institute of Metrology, Beijing, P.R. China
NIMB	National Institute of Metrology, Bucharest, Romania
NIMT	National Institute of Metrology, Bangkok, Thailand
NIST	National Institute of Standards and Technology, Boulder, Colorado, USA
NMC	National Centre of Metrology, Sofiya, Bulgaria
NMIJ	National Metrology Institute of Japan, Tsukuba, Japan
NML	National Measurement Laboratory, Sydney, Australia
NMLS	National Metrology Laboratory of SIRIM Berhad, Shah Alam, Malaysia
NPL	National Physical Laboratory, Teddington, United Kingdom
NPLI	National Physical Laboratory, New Delhi, India
NRC	National Research Council of Canada, Ottawa, Canada
NTSC	National Time Service Center of China, Lintong, P.R. China
OMH	Országos Mérésügyi Hivatal, Budapest, Hungary
ONBA	Observatorio Naval, Buenos Aires, Argentina
ONRJ	Observatório Nacional, Rio de Janeiro, Brazil
OP	Observatoire de Paris, Paris, France
ORB	Observatoire Royal de Belgique, Brussels, Belgium
PL	Consortium of laboratories in Poland
PTB	Physikalisch-Technische Bundesanstalt, Braunschweig, Germany
ROA	Real Instituto y Observatorio de la Armada, San Fernando, Spain
SCL	Standards and Calibration Laboratory, Hong Kong
SG	Standards, Productivity and Innovation Board, Singapore
SMU	Slovenský metrologický ústav, Bratislava, Slovakia
SP	Sveriges Provnings- och Forskningsinstitut, Borås, Sweden
SU	Institute of Metrology for Time and Space, Mendeleevo, Moscow Region, Russia
TCC	TIGO Concepción Chile, Chile
TL	Telecommunication Laboratories, Chung-Li, Taiwan
TP	Institute of Radio Engineering and Electronics, Academy of Sciences of the Czech Republic, Prague, Czech Republic

Zoznam skratiek a názvov inštitúcií udržiavajúcich miestnu aproximáciu UTC, UTC(k), pokračovanie.

UME	Ulusai Metroloji Enstiüsü, Marmara Research Center, Gebze Kocaeli, Turkey
USNO	U.S. Naval Observatory, Washington D.C., USA
VSL	NMi Van Swinden Laboratorium, Delft, the Nederlands

Dodatok B

Zoznam použitých skratiek.

AES	Advaced Encryption Standard
BIH	Bureau international de l'heure
BIPM	Bureau international des poids et mesures
CA	Certifikačná autorita (Certification Authority)
CDMA	Code Division Multiple Access
DCF77	Nemecký rádiový vysielač časových signálov
DES	Data Encryption Standard
EAL	Echelle Atomique Libre
GLONASS	Global Navigation Satellite System
GMT	Greenwich Mean Time
GPS	Global Positioning System
IERS	International Earth Rotation Service
ITU	International Telekommunication Union
JD	Julian Date
MASER	Microwave Amplification by Stimulated Emission of Radiation
MJD	Modified Julian Date
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
NMI	Národná metrologická inštitúcia
NRSR	Národná rada Slovenskej republiky
NTP	Network Time Protocol
OCXO	Oven controlled crystal oscillator
PKI	Public Key Infrastructure
PPS	Pulse Per Second
PTB	Physikalish-Techinische Bundesanstalt
RDS	Radio Data System
SHA	Secure Hash Algorithm
SI	*Système international* d'unités
SMÚ	Slovenský metrologický ústav
STN	Slovenská technická norma

Zoznam použitých skratiek, pokračovanie.

TAI	Temps atomique international
TCXO	Temperature-compensated crystal oscillator
TSA	Autorita časových pečiatok (Time Stamping Authority)
TWSTFT	Two-Way Satellite Time and Frequency Transfer
UTC	Universal Coordinated Time
VLBI	Very Long Baseline Interferometry
ZoEP	Zákon NRSR 215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov
ZoM	Zákon NRSR 142/2000 Z.z. o metrológii a o zmene a doplnení niektorých zákonov

Literatúra

[1] Federal Information Processing Standards (FIPS) Publication FIPS46-3. *Data Encryption Standard (DES).* National Institute of Standards and Technology, October 1999.

[2] Carl H. Meyer and Stephen M. Matyas. *Cryptography: A New Dimension in Computer Data Security.* John Wiley & Sons, 1982.

[3] Federal Information Processing Standards (FIPS) Publication FIPS197. *Advanced Encryption Standard (AES).* National Institute of Standards and Technology, November 2001.

[4] W. Diffie and M.E. Hellman. *New Directions in Cryptography*, volume IT-22. IEEE Transactions on Information Theory., 1976.

[5] NIST Special Publication 800-2. *Public-Key Cryptography.* National Institute of Standards and Technology, April 1991.

[6] Alfred J. Menezes, Pall C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography.* CRC Press, 1997.

[7] Douglas R. Stinson. *CRYPTOGRAPHY Theory And Practice.* CRC Press, 1995.

[8] NIST. *NIST Brief Comments on Recent Cryptoanalytic Attacks on Secure Hashing Functions and Continued Security Provided by SHA-1.* National Institute of Standards and Technology, August 2004.

[9] Federal Information Processing Standards (FIPS) Publication FIPS180-2. *Secure Hash Standard.* National Institute of Standards and Technology, August 2002.

[10] NRSR. *Zákon 215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov*, Máj 2002.

[11] NBÚ. *Vyhláška Národného bezpečnostného úradu 537/2002 Z.z.*, September 2002.

[12] Juraj Vaško. *-Zaznamenávanie času vo virtuálnom prostredí.* Diplomová práca, FMFI UK v Bratislave, 2004.

[13] Slovenská technická norma. *STN 01 0115 Terminológia v metrológii.* Slovenský ústav technickej normalizácie, Január 2001.

[14] A. Hajduk and J. Štohl a kol. *Encyklopédia Astronómie.* Obzor, 1987.

[15] R.A. Nelson, D.D. McCarthy, S. Malys, J. Levine, B. Guinot, H.F. Fliegel, R.L. Beard, and T.R. Bartholomew. The leap second: its history and possible future. *Metrologia*, (38), 2001.

[16] Claude Audoin and Bernard Guinot. *The Measurement of Time.* Cambridge University Press, 2001.

[17] S. Michal. *Hodiny (od gnómonu k atomovým hodinám).* SNTL, 1987.

[18] Hewlett Packard. *HP53131A/132A 225 MHz Universal Counter; Operating Guide*, 1998.

[19] František Lamoš. *Pravdepodobnosť a štatistika.* Prednáška na FMFI UK, 2001.

[20] David W. Allan. Statistics of atomic frequency standards. In Věnceslav F. Kroupa, editor, *Frequency Stability: Fundamentals and Measurement.* IEEE Press, February 1966.

[21] Judah Levine (NIST). Precision synchronization of computer network clocks. In Allen Kent, James G. Williams, and Carolyn M. Hall, editors, *Encyclopedia of Computer Science and Technology*, volume 37. Marcel Dekker, 1997.

[22] Hewlett Packard. *Timekeeping and Frequency Calibration.* Application Note 52-2, August 1979.

[23] J. Tolman, V. Ptáček, A. Souček, and R. Stecher. Microsecond Clock Comparison by Means of TV Synchronizing Pulses. *IEEE Transactions on Instrumentation and Measurement*, IM-16(3), September 1967.

[24] IETF. *Network Time Protocol (Version 3) Specification, Implementation and Analysis*, 1992.

[25] Otokar Buzek and Jan Čermák. OMA 50-kHz Transmission System and Its Applications. *TESLA Elektronics*, IM-16(4), 1981.

[26] PTB. Sendemast des Zeitsignal- und Normalfrequenzsenders DCF77 in Mainflingen. *Zur Zeit*, März 1989.

[27] Michael A. Lombardi (NIST). Time Flies! Radio Signals Used for Time and Frequency Measurements. *Cal Lab*, April, May, June 2003.

[28] B. Hoffmann-Wellenhof, H. Lichtenegger, and J. Collins. *GPS Theory and Practice*. Springer-Verlag/Wien, fifth edition, 2001.

[29] Annual report of the BIPM time section. Pavillon de Breteuil, F-92312 SÉVRES Cedex, France, 2003.

[30] NRSR. *Zákon 142/2000 Z.z. o metrológii a o zmene a doplnení niektorých zákonov*, Máj 2000.

[31] Hewlett Packard. *HP 5071A Primary Frequency Standard; Operating and Programming Manual*, October 1997.

[32] BIPM. *Circular T 206*. http://www.bipm.org, March 2005.

[33] ISO. *Guide to the Expression of Uncertainty in measurement*. International Organization for Standardization, 1993.

[34] SNAS. *Vyjadrovanie neistôt merania pri kalibrácii*. Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky, December 1997.

[35] Time Business Forum. *Time Authentication Infrastructure Guideline*, March 2003.

[36] Vladimír Smotlacha. *Measurement of Time Servers*. Technical Report 18, CESNET, December 2001.

[37] D. Mills. *The Autokey Security Architecture, Protocol and Algorithms*. University of Delaware, August 2003.

[38] Judah Levine, Michael A. Lombardi, and Andrew N. Novick. *NIST Computer Time Services: Internet Time Service (ITS), Automated Computer Time Service (ACTS), and time.gov Web Sites*. NIST Special Publication 250-59, May 2002.

[39] NPL. *Time & Frequency Services, NPL TrueTime*. http://www.npl.co.uk/time/ctm002v02.pdf, April 2000.

[40] METAS. *Time Transmission Service via Modem, Time and Date Coding*. http://www.metas.ch/en/labors/official-time/pdf/metas_phoneclock_e_dr.pdf.

[41] Ján Ivan. *Počet pravdepodobnosti a matematická štatistika*. Slovenská vysoká škola technická v Bratislave, 1975.

[42] J. Mogul, D. Mills, J. Brittenson, J.Stone, and U. Windl. *Pulse-Per-Second API for UNIX-like Operating Systems, Version 1.0*. RFC 2783, March 2000.

[43] David L. Mills and Paul-Henning Kamp. *The Nanokernel*. http://www.eecis.udel.edu/ mills/databse/brief/nano/nano.pdf, November 2OOO.