KOMUNIKACIONI KANAL SA ŠIFROVANJEM INFORMACIJA

Markagić S. *Milorad,* Vojna akademija, Katedra vojnih elektronskih sistema, Beograd

UDC: 621.391

Sažetak:

U radu se opisuje jedan model telekomunikacionog kanala, na kojem su primenjene mere kriptozaštite informacija, sa sastavnim elementima kanala.

Da bi šifrovanje informacija bilo uspešno na celom spojnom putu neophodno je razmotriti neke osnovne odredbe telekomunikacione i kriptološke sinhronizacije i delimično naglasiti način šifrovanja informacije, kao i proces generisanja i distribucije kriptoloških ključeva.

Ključne reči: *telekomunikacioni kanal, šifrovanje, kriptološki ključevi.*

Uvod

Komunikacioni kanal, koji se koristi u komercijalne svrhe, nezavisno od modela i primenjenih uređaja i spojnih puteva, podložan je uticajima koji mogu biti prirodni ili veštački.

Osnovne vrste napada na komunikacioni kanal su: presretanje, obmanjivanje, ometanje i prisluškivanje.

Imajući u vidu da informacije koje koristi veliki broj javnih i državnih službi predstavljaju neki vid tajne, potrebno je da se na tim informacijama primene mere kriptozaštite – šifrovanje informacija.

Sam proces zaštite informacija vezan je za nekoliko parametara koji odlučujuće utiču na kvalitet, vrstu i zaštitu prenosa. To su, pre svega, parametri telekomunikacione i kriptološke sinhronizacije, kao i vrsta primenjenog kriptološkog ključa (ključa za šifrovanje i dešifrovanje).

U radu je prikazan jedan telekomunikacioni kanal sa sastavnim elementima, kako u smislu klasičnog prenosa informacija, tako i u načinu prenosa zaštićenih (kriptovanih) informacija. Analiziran je pojam kriptološke sinhronizacije i osnovni pojmovi telekomunikacione sinhronizacije koja prethodi kriptološkoj sinhronizaciji. Takođe, opisuju se i tri tipa kriptološke sinhronizacije: sinhronizacija na početku, tekuća sinhronizacija i sinhronizacija sa restartom. Analizirane su prednosti i nedostaci svih tipova kriptološke sinhronizacije sa kriptološkog i telekomunikacionog aspekta.

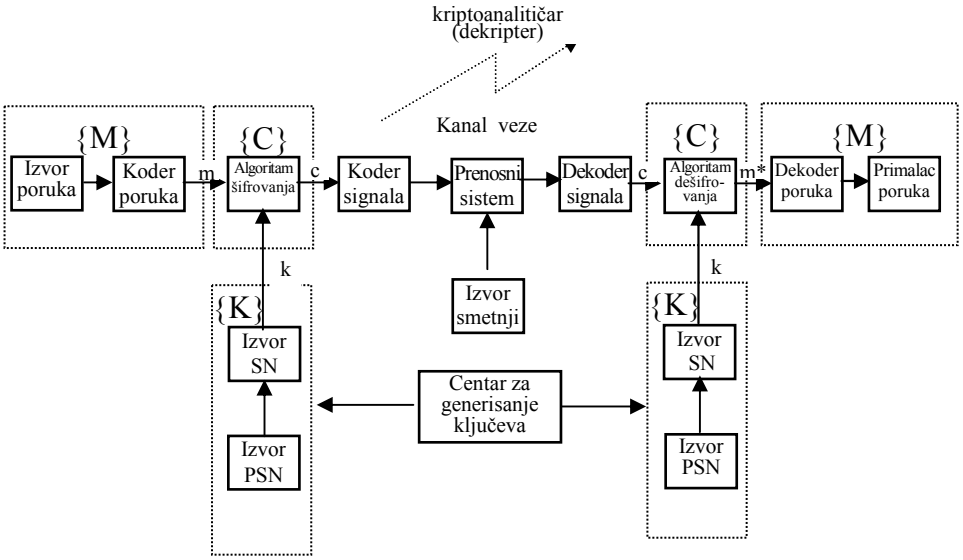
milmarkag@yahoo.com

Izvršena je i analiza parametara kriptološke sinhronizacije (dužina spoljašnjeg ključa, verovatnoća uspešne sinhronizacije i vreme sinhronizacije), na osnovu modernih saznanja iz oblasti kriptologije sa težištem na opštim i uzajamnim ograničenjima pri izboru ovih parametara.

Model komunikaconog kanala sa šifrovanjem informacija

U odnosu na opšti model komunikacionog kanala, komunikacioni kanal sa šifrovanjem informacija u svom sastavu ima još i elemenat – algoritam šifrovanja-dešifrovanja, a koji je realizovan u sklopu kriptouređaja. To može biti samostalni uređaj ili sklop u okviru telekomunikacionog uređaja.

Izgled ovog modela prikazan je na slici 1.



Slika 1 – Šema komunikacionog kanala sa šifrovanjem informacije

Uočava se da je za realizaciju algoritma potrebno obezbediti određene uslove, pa će biti prikazani kao izvori SN (slučajnog niza) i PSN (pseudoslučajnog niza). Ovi izvori najčešće se generišu na jednom mestu – centru za generisanje ključeva.

Shvatanje ovih elemenata, uz prihvatanje činjenica iznetih u poglavlju o elementima komunikacionog kanala bez šifrovanja informacija, pomaže da se sagleda problem kriptološke sinhronizacije i generisanja i distribucije ključeva.

Pojam sinhronizacije

Dva niza su sinhrona ukoliko se odgovarajući događaji u oba niza javljaju jednovremeno.

Sinhronizacija je proces kojim se ostvaruje i održava sinhrona situacija.

U telekomunikacionom sistemu pod sinhronizacijom se podrazumeva niz radnji i postupaka koji omogućuju uređaju na prijemnoj strani da izvrši inverzne transformacije onih transformacija koje vrši uređaj na predajnoj strani nad porukom kako bi je prilagodio kanalu.

U opštem slučaju kriptološka sinhronizacija je postupak koji obezbeđuje da GPSN (generator pseudoslučajnog niza) u prijemnom uređaju vrši inverziju transformacije poruke koju vrši GPSN u predajnom uređaju.

Kao što se zna, transformacija šifrovanja određenim algoritmom zavisi od elemenata: unutrašnjeg ključa (UK) i spoljašnjeg ključa (SK). Uz normalnu pretpostavku da predajni i prijemni GPSN imaju identičan UK, potrebno je obezbediti da imaju i identičan SK. Pošto se za svaku poruku generiše novi SK u predajnom uređaju, neophodno ga je preneti prijemnom uređaju. Prema tome, pod kriptološkom sinhronizacijom podrazumevamo proces prenošenja SK, sa kojim radi predajni GPSN, prijemnom GPSN.

Telekomunikaciona sinhronizacija

Neophodno je naglasiti da je GPSN po svojoj prirodi digitalni sklop koji funkcioniše na osnovu digitalnih ulaznih podataka (UK i SK) i signala takta. Prema tome, čak i u sistemima za zaštitu informacija na analognom nivou (npr. kod zaštite govornog signala na analognom principu) proces kriptološke sinhronizacije je u telekomunikacionom smislu proces digitalnog prenosa SK od predajnog GPSN prijemnom GPSN.

Da bi proces kriptološke sinhronizacije mogao otpočeti neophodno je da se prethodno završi proces tzv. telekomunikacione sinhronizacije. Kao što je rečeno, svi blokovi u modelu prijemnika telekomunikacionog sistema koji se nalaze između izlaza iz kanala i prijemnog GPSN, moraju obaviti inverzije transformacija koje se vrše u predajniku. Zavisno od složenosti telekomunikacionog sistema, postoji čitava hijerarhija sinhronizacionih problema koji se rešavaju u okviru telekomunikacione sinhronizacije. Ako se za prilagođenje kanalu koristi modulacija, onda je prvi nivo sinhronizacije sinhronizacija nosioca (po frekvenciji i fazi), što je potrebno za proces demodulacije. Nakon toga se iz analognog demodulisanog signala vrši ekstrakcija digitskog takta (bitska sinhronizacija) koja omogućuje konverziju analognog demodulisanog signala u digitalni (binarni niz). Nakon toga dolazi sinhronizacija kodnih reči (ukoliko se vrši zaštitno kodovanje poruke), zatim sinhronizacija rama koja omogućuje demultipleksiranje i, konačno, paketska sinhronizacija.

Kada se sve ove faze telekomunikacione sinhronizacije završe, uspostavljen je digitalni kanal i može otpočeti proces kriptološke sinhronizacije.

Tipovi kriptološke sinhronizacije

Kriptološka sinhronizacija predstavlja nalaženje optimuma između, uglavnom oprečnih, kriptoloških i telekomunikacionih zahteva. Iako su kriptološki zahtevi od prvenstvenog značaja, pogodno je izvršiti podelu kriptološke sinhronizacije i sa telekomunikacionog aspekta.

Pošto kriptološka sinhronizacija predstavlja proces digitalnog prenosa SK prijemnom uređaju, za njega, pre svega, treba obezbediti kanal.

Kako je tehnički neprihvatljivo, a materijalno nerentabilno da se sinhronizacija (telekomunikaciona i kriptološka) obavlja odvojenim kanalom, neophodno je izvršiti multipleksiranje sinhronizacionog sadržaja sa informacijom koju treba preneti, te se za prenos može koristiti isti telekomunikacioni kanal. Najčešće se koristi vremenski multipleks. Drugim rečima, kriptološka sinhronizacija prethodi šifratu.

Razlikuju se tri osnovna tipa kriptološke sinhronizacije:

– kriptološka sinhronizacija na početku poruke (sinhronizacija na početku),

– periodična kriptološka sinhronizacija (tekuća sinhronizacija), i

– sinhronizacija sa restartom.

Sinhronizacija na početku

Prednosti sinhronizacije na početku su:

– izuzev početnog kašnjenja ne narušava ukupan kapacitet kanala raspoloživ za prenos šifrata;

– obezbeđuje šifrovanje/dešifrovanje „bit-za-bit“ (jedna greška u šifratu proizvodi jednu grešku u otvorenom tekstu), i

– otežano je otkrivanje i ometanje.

Nedostaci sinhronizacije na početku su:

– ukoliko se iz nekih razloga ne ostvari uspešna sinhronizacija, propada čitava poruka;

– ukoliko dođe do „proklizavanja“ digitskog takta (što je retka, ali realna pojava), što se manifestuje ubacivanjem novog bita ili gubljenjem emitovanog, ostatak poruke je neupotrebljiv, i

– u radio-mreži ne omogućuje naknadno uključivanje učesnika.

Tekuća sinhronizacija

Prednosti tekuće sinhronizacije su:

– ukoliko se ne ostvari kriptološka sinhronizacija na samom početku poruke, postoji mogućnost da se ostvari pri sledećem emitovanju u okviru poruke. Drugim rečima, neostvarivanje kriptološke sinhronizacije na početku ne čini čitavu poruku beskorisnom;

– obezbeđuje šifrovanje/dešifrovanje bit-za-bit;

– uz složene tehničke zahvate i narušavanje kapaciteta kanala raspoloživog za prenos šifrata, može se rešiti problem „proklizavanja“ digitskog takta, i

– omogućuje naknadno uključivanje učesnika u radio-mreži.

Nedostaci tekuće sinhronizacije su:

– narušavanje kapaciteta kanala raspoloživog za prenos šifrata (da bi se sinhronizacija mogla periodično ubaciti u šifrat, kapacitet kanala mora biti jednak zbiru kapaciteta sinhronizacionog i informacionog kanala), i

– uočljivost kriptološke sinhronizacije na kanalu.

Izbor jednog od navedena dva tipa kriptološke sinhronizacije zavisi prevashodno od konkretnog telekomunikacionog sistema u kojem se vrši kriptozaštita.

Sinhronizacija sa restartom

Problem narušavanja kapaciteta kanala zbog prenosa kriptološke sinhronizacije, problemi neuspešne sinhronizacije, proklizavanja digitskog takta i naknadnog uključivanja učesnika u radio-mreži rešavaju se na sledeći način: ako se GPSN na predajnoj strani modifikuje tako da stalno prati sadržaj šifrata i da kada se pojavi tačno određena n-torka (određena sadržajem UK) GPSN uvek startuje od istog mesta (takođe određenog sadržajem UK), onda nije potrebno slati kriptološku sinhronizaciju prijemnom GPSN. Dovoljno je da prijemni GPSN prati sadržaj šifrata i čeka navedenu n-torku, zatim startuje od zadatog mesta i sinhronizacija je ostvarena.

Zbog ponavljanja startovanja GPSN od iste pozicije, ovaj način sinhronizacije dobio je ime sinhronizacija sa restartom.

Prednosti ovog metoda kriptološke sinhronizacije su što rešava većinu telekomunikacionih problema:

– nema narušavanja kapaciteta kanala, i

– neostvarivanje ili gubitak sinhronizacije iz bilo kog razloga traju samo do sledećeg restarta.

Glavni nedostatak je kriptološke prirode, pa je ova sinhronizacija teško prihvatljiva.

Prenos SK u skladu sa definicijom kriptološke sinhronizacije se ne vrši zato što je SK već poznat prijemnom GPSN. To je baš n-torka na osnovu koje se vrši restart. Pošto se radi o jednom ili o malom broju različitih SK, delovi jedne poruke se šifruju istim ili malim brojem različitih ključeva, što bitno smanjuje kriptološku vrednost algoritma, uprkos činjenici da se restart dešava na slučajan način. Da bi se iskoristile prednosti ovog metoda kriptološke sinhronizacije, neophodno da se restart relativno često dešava. To direktno utiče na dužinu n-torke i na korišćenje vrlo kratkog dela periode GPSN, koja može biti ekstremno velika, ali bez uticaja na kriptološki kvalitet rešenja.

Pri korišćenju restarta nije moguće šifrovanje/dešifrovanje bit-za-bit. Posledica je da jedna greška u šifratu izaziva više grešaka u otvorenom tekstu. Posebno je nepogodno kada se greška javi u restartnoj n-torki ili ukoliko prevede neku „sličnu“ n-torku u restartnu. U tom slučaju javlja se paket grešaka koji traje do sledećeg uspešnog restarta. To je neprihvatljivo u telekomunikacionim sistemima koji moraju tolerisati relativno veliku verovatnoću greške po bitu, reda 10^{-2} (KT i UVF/VVF radio).

Kod uređaja za zaštitu govora na analognom principu zaštita se može ostvariti, recimo, permutovanjem delova analognog govornog signala u f-t ravni (f-frekvencija, t-vreme). Permutovan signal se u svom analognom obliku šalje prijemniku. Digitalni kanal potreban za kriptološku sinhronizaciju može se ostvariti emitovanjem SK pre analognog šifrata, kada se sinhronizacija granica delova analognog govornog signala nad kojima treba izvršiti inverznu permutaciju ostvaruje zahvaljujući preciznosti oscilatora predajnika i prijemnika koji se sinhronizuju u fazi kriptološke sinhronizacije.

Drugi način, koji se, zahvaljujući jednostavnom tehničkom rešenju koje je inherentno jednom ovakvom uređaju, često koristi, obezbeđuje jedan deo spektra standardnog telefonskog kanala za prenos spoljašnjeg ključa. (Obično se bira deo spektra oko sredine kanala koji je najpogodniji za digitalni prenos). Bitska sinhronizacija ovde ima dvostruku ulogu. S jedne strane, omogućuje uspešnu detekciju spoljašnjeg ključa, a sa druge olakšava precizno određivanje granica delova analognog govornog signala, čime omogućuje preciznije vršenje inverzne permutacije u f-t ravni.

Parametri kriptološke sinhronizacije

Osnovni parametri kriptološke sinhronizacije su:
– dužina spoljašnjeg ključa,
– verovatnoća uspešne sinhronizacije,
– vreme sinhronizacije.

Ova tri parametra su međusobno povezana i na njihovo dimenzionisanje utiču kriptološki i telekomunikacioni zahtevi, kao i ograničenja vezana za konstrukciju uređaja (dimenzije, potrošnja el. energije, masa, itd.).

Telekomunikacioni zahtevi nose i deo taktičkih zahteva. Naime, postojeći telekomunikacioni sistem je već na određeni način korišćen i bez kriptozaštite, pa se obično zahteva da ne narušava njegove performanse.

Telekomunikacioni zahtevi su posebno kritični u dva slučaja:

1. Kada se vrši kriptozaštita signala u realnom vremenu (npr. u slučaju kriptozaštite govornog signala). U tom slučaju se postavljaju vrlo oštri uslovi za početno kašnjenje i nisu dozvoljeni diskontinuiteti u prenosu signala.

2. Kada se digitalni prenos vrši postojećim analognim kanalima (telefonski i radio-kanali). U tom slučaju se u kanalu pri prenosu računa sa verovatnoćom greške čak do $5 \cdot 10^{-2}$

Ova dva slučaja najčešće se javljaju zajedno. Ako se ima u vidu da je kapacitet navedenih kanala relativno mali, potrebno je izvršiti dodatnu kompresiju informacije koja se prenosi, što je čini osetljivijom na greške u prenosu.

S druge strane, ako se kriptozaštita vrši u mrežama za prenos podataka, one su već tako projektovane da korišćenjem niza tehnika obezbeđuju verovatnoću greške u kanalu za nekoliko redova veličine manju nego u navedenim slučajevima. Pored toga, ne postoji problem početnog kašnjenja pri prenosu podataka, tako da se u tom slučaju razmatra samo kriptološki aspekt problema.

Dužina spoljašnjeg ključa

Posmatrano samo sa kriptološkog aspekta, dužina SK trebalo bi da bude što veća, kako bi se dobio što veći broj različitih startnih pozicija GPSN i smanjila opasnost od šifrovanja različitih poruka istim ključem.

Ako se sa n označi dužina SK izražena brojem bita, onda GPSN može imati ukupno 2n različitih startnih pozicija. Ukoliko su one međusobno nezavisne i jednako verovatne (što se obezbeđuje načinom generisanja SK), onda je verovatnoća uzastopnog ponavljanja dva identična SK 2-n. Naravno, sa povećanjem broja poruka raste i verovatnoća da će se ponoviti već generisani SK.

Ako sa N označimo prosečan broj poruka između dve promene UK, onda očigledno mora biti zadovoljen uslov $2^n >> N$ [4].

Da bi se stekao osećaj o ovim vrednostima treba pretpostaviti da se u jednoj radio-telefonskoj mreži koja se intenzivno koristi UK menja svakih mesec dana. Uz pretpostavku da se koristi sinhronizacija samo na početku poruke, da prosečna poruka u ovoj mreži traje 10 s i da je mreža aktivna 24^h dnevno, dobija se da je N = 259200.

Ako se želi ostvariti $2n > 1000\ N$ dobija se $n \approx 28$.

Ukoliko n nije dovoljno veliko, ovaj odnos može se dobiti smanjenjem ukupnog broja poruka između dve promene UK. Češća promena (generisanje i distribucija) UK povezana je sa organizaciono-tehničkim poteškoćama.

U savremenim uređajima za kriptozaštitu GPSN se realizuju pomoću mikro-računara na bazi mikroprocesora. Da bi se olakšala obrada SK, po pravilu se bira da dužina SK bude celobrojni umnožak od 8 bita, odnosno ceo broj bajtova (niz od 8 bita = 1 byte (bajt)).

Verovatnoća uspešne sinhronizacije

Kao što se vidi, argumenti za povećanje dužine SK su vrlo čvrsti. S druge strane, međutim, zahteva se da verovatnoća uspešne sinhronizacije iznosi 0,95 do 0,99, zavisno od namene uređaja. Ova verovatnoća određena je verovatnoćom greške na kanalu kojim se prenosi SK i dužinom SK.

Najjednostavniji način za analizu (koji ne uzima u obzir statistiku grešaka u datom telekomunikacionom sistemu) jeste modeliranje kanala kojim se vrši kriptološka sinhronizacija, preko binarnog simetričnog kanala.

U ovom modelu, nezavisno od toga da li se emituje 0 ili 1, verovatnoća greške iznosi p, a verovatnoća tačnog prijema jednog bita 1-p. Greške su međusobno nezavisne.

U dosadašnjem tekstu nije izričito naglašeno da se SK mora potpuno tačno preneti. U kanalu sa greškama o tome se može suditi samo u okviru teorije verovatnoće.

Zaštitno kodovanje kao činilac verovatnoće uspešne sinhronizacije

Ako se rezultat ne može postići skraćenjem dužine SK na granicu kriptološke prihvatljivosti, jedino rešenje problema jeste korišćenje zaštitnog kodovanja SK.

Zaštitno kodovanje je postupak namernog unošenja redundanse u prenošenu poruku i to na način koji omogućuje detekciju i korekciju grešaka koje se javljaju u primljenoj poruci.

Teorija zaštitnog kodovanja predstavlja naučnu disciplinu u okviru statističke teorije telekomunikacija i nudi veliki broj tipova kodova, optimiziranih sa raznih aspekata (tip kanala, sinhronizacija, itd.).

U uslovima telekomunikacionog kanala ograničenog kapaciteta, koji ne dozvoljava zaštitno kodovanje cele poruke, korišćenje složenijeg zaštitnog kodovanja samo pri prenosu SK nije tehnički opravdano, a ponekad je i neostvarljivo (kada se radi o tekućoj kriptološkoj sinhronizaciji).

Najjednostavnije je zaštitno kodovanje ponavljanjem poruke neparan broj puta i majoritetnim (većinskim) odlučivanjem na prijemu. (Recimo, ako se poruka ponovi 3 puta, onda prijemnik za slučaj da se na istom mestu u sve 3 poruke jave 2 ili 3 jedinice odlučuje da je poslata jedinica. U suprotnom se odlučuje za nulu).

Ako se sa m označi (neparan) broj ponavljanja, onda je verovatnoća greške po bitu [2].

$$p_{1,m} = \sum_{i=\frac{m+1}{2}}^{m} \binom{m}{i} p^i (1-p)^{m-i} \qquad (1)$$

U slučaju trostrukog ponavljanja dobija se

$$p_{1,3} = 3p^2 - 2p^3 \quad (2)$$

a u slučaju petostrukog ponavljanja

$$p_{1,5} = 10p^3 - 15p^4 + 6p^5 \quad (3)$$

Verovatnoća uspešne sinhronizacije data je sa

$$P^{sk} = (1-P_{1,m})^n \quad (4)$$

U tabeli 1 date su vrednosti Psk za parametre iz prethodnog primera, ali za slučaj trostrukog ponavljanja.

Tabela 1

Verovatnoća P_{sk} u slučaju trostrukog ponavljanja

p n	32	64
10^{-2}	0,9905	0,9811
10^{-3}	0,99999	0,99998

U slučaju verovatnoće greške veće od 10^{-2} može se koristiti petostruko ponavljanje. Međutim, pri verovatnoćama greške oko 10^{-1} smetnje su tako velike da naglo raste verovatnoća proklizavanja bitske sinhronizacije, odnosno razlikovanja broja emitovanih i primljenih bita, kada nijedan zaštitni kod ne pomaže.

Pri izradi ovakvih analiza treba neprestano imati na umu da se radi o vrlo visokom stepenu idealizacije prenosnog kanala, tako da se dobijeni rezultati mogu koristiti samo kao gruba procena stvarne situacije. Pravi uvid pružaju samo intenzivna laboratorijska merenja (ukoliko omogućuju simulaciju ključnih fenomena vezanih za prenos u konkretnom telekomunikacionom sistemu), odnosno merenja u realnim uslovima.

Zaštitni kodovi, izuzev specijalno projektovanih, „izlaze na kraj“, uglavnom, sa greškama koje su „raspršene“ u okviru poruke. Međutim, ako se duži niz uzastopnih bita primi sa velikom greškom, zaštitni dekoder postaje nemoćan. Takve greške nazivaju se paketiranim ili usnopljenim greškama.

Paket grešaka definiše se kao niz uzastopnih bita određene dužine, koji se prima sa verovatnoćom greške po bitu koja je znatno veća od prosečne vrednosti verovatnoće greške po bitu u datom telekomunikacionom sistemu. Definicija veličine greške u okviru paketa zavisi od performansi zaštitnog kodera (ukoliko postoji u sistemu) i osetljivosti prenošenih informacija na greške u prenosu. Pri prenosu digitalizovanog govornog signala sa malim vrednostima bitskog protoka to je između 0,1 i 0,5.

Efikasan metod borbe protiv paketa grešaka je tehnika preklapanja (eng. interleaving). Može se koristiti i u kriptološkoj sinhronizaciji, a posebno je popularna pri prenosu pisanog teksta preko radija.

Za primenu ove tehnike potrebno je poznavati statistiku paketiranih grešaka u posmatranom telekomunikacionom sistemu. Potrebno je poznavati raspodelu verovatnoća pojavljivanja paketa određene dužine, kao i raspodelu rastojanja između susednih paketa grešaka.

Ako se to zna, onda se na predajnoj strani vrši „raspršivanje“ susednih bita poruke u vremenu, tako da njihovo međusobno rastojanje bude veće od maksimalne dužine paketirane greške λ. Ako je 1p slučajna promenljiva koja predstavlja dužinu paketa grešaka, onda λ definišemo kao

$$P\{1p \geq \ell\} < \varepsilon$$

gde je ε proizvoljan broj iz intervala (0,1)

Ilustrovaćemo ovu tehniku sledećim primerom:neka je u nekom telekomunikacionom sistemu 1 = 10, a minimalno rastojanje paketa grešaka veće od 100. Ako obeležimo redne brojeve bita neke poruke sa 1, 2, 3,..., onda se u predajniku vrši memorisanje podataka koje treba preneti, a na liniju idu u sledećem redosledu:

1, 11, 21, ... 91,
2, 12, 22, ... 92,
.
.
.
10, 20, 30, ..., 100

U prijemniku se ova poruka ponovo memoriše, a zatim iščita u normalnom redosledu.

Ako se pri prenosu javio paket grešaka dužine 10 (što je izuzetno redak slučaj), onda će tek svaki deseti bit biti pogrešno primljen. Preciznije, biće primljen sa znatno većom verovatnoćom greške od prosečne. U nekim sistemima je i ovaj princip dovoljan da se poruka primi u granicama prihvatljivosti, a metod je posebno efikasan kada se udruži sa zaštitnim kodovanjem. On ne zahteva prenošenje dodatnih informacija, pa ne smanjuje kapacitet kanala raspoloživ za prenos informacija, a pogodan je i zbog jednostavnosti tehničke realizacije. Njegov nedostatak predstavlja dodatno kašnjenje, koje je jednako trajanju dela poruke na kojem se vrši premeštanje.

Do sada smo u razmatranju implicitno smatrali da prijemnik tačno prepoznaje kada počinje prijem spoljašnjeg ključa. To, međutim, nije ispunjeno u većini slučajeva.

U teoriji zaštitnog kodovanja postoji pojam sinhronizibilnosti, što je osobina koda da bude sinhronizovan na prijemu, odnosno da kao kodna reč ne može biti shvaćen neki pomeraj bilo koje kodne reči za određeni broj bita.

Metod višestrukog ponavljanja zbog potpune slučajnosti SK nema ove osobine. Teorijski, pod nekim uslovima se uz poznatu dužinu SK mogu odrediti granice n-torke SK, tekućim kroskoreliranjem date n-torke sa dve sledeće.

Sličan problem se javlja i pri određivanju granica dela poruke na kojoj se vrši preklapanje. Ovaj problem se rešava tako da se pre emitovanja SK šalje najava ili preambula kojom se obezbeđuje precizan prijem SK (bilo da se koristi zaštitno kodovanje ili ne).

Postoje i kodovi koji omogućuju detekciju i korelaciju greške u sinhronizaciji i to veoma brzo (sa stanovišta broja bita potrebnih za ustanovljenje sinhronizacije).

Jedan od pristupa rešavanju ovog problema jeste da se pošalje niz čija je autokorelaciona funkcija minimalna izvan osnovnog vrha. Postoji čitava klasa nizova sa ovom osobinom, a nazivaju se Barkerovi nizovi.

Pomerački registri sa povratnom spregom

Slične, ali nešto nepovoljnije osobine imaju pseudoslučajni nizovi generisani pomeračkim registrom sa odgovarajućim povratnim spregama. Zbog jednostavnosti generisanja i visoke pouzdanosti jednom ostvarene sinhronizacije oni se često koriste u vidu najave.

Ako je L dužina pomeračkog registra, onda on, kao što je poznato, uz odgovarajuće povratne sprege može generisati pseudoslučajni niz dužine $2^L - 1$, u kojem se nalaze sve L-torke, izuzev one sastavljene od samih nula.

Prema tome, moguće je na predaji postaviti pomerački registar u stanje koje će nakon 2^L-1 koraka dati, recimo, L-torku sastavljenu od svih jedinica. Kada se završi emitovanje ovog pseudoslučajnog niza započinje emitovanje SK.

U prijemniku se nalazi identičan pomerački registar sa povratnom spregom. Njemu je u početku raskinuta povratna sprega i u njega se upisuje sadržaj sa linije. Kada se napuni L bita, povratne sprege se zatvore i registar nastavlja sa autonomnim radom. Istovremeno započinje poređenje lokalno generisanog niza sa onim koji se prima. Ukoliko je pri početnom punjenju prijemnog pomeračkog registra primljeno svih L bita bez greške, poređenje nizova će dati grešku koja odgovara grešci u prenosu. Ukoliko je neki od početnih L bita u pomeračkom registru prijemnika pogrešno primljen, greška će biti jako velika. Odluka o tačnom/pogrešnom prijemu prvih L bita donosi se nakon sekvencijalnog testa, zbog brzine ove vrste testova. Pragovi odlučivanja se određuju prema uslovima greške u kanalu, pri kojima treba izvršiti sinhronizaciju za zadatu vrednost grešaka I i II vrste. Kao što je poznato, greška prve vrste se javlja ako je

primljeno početno stanje registra tačno, a test usled grešaka odbaci ovu hipotezu. Greška druge vrste bi bila kada se pogrešan sadržaj prihvati kao pravi.

Kada se ustanovi da ne postoji sinhronizacija lokalno generisanog i primljenog niza, povratna sprega prijemnog pomeračkog registra se ponovo raskida, novi sadržaj ulazi u registar i procedura se ponavlja.

Kada se ustanovi da je lokalni niz sinhronizovan sa dolazećim, sačeka se da se izgeneriše zadata L-torka (recimo sve jedinice, kao što je rečeno). Kada se ona detektuje to je signal da posle toga nailazi SK.

Verovatnoća korektne sinhronizacije prijemnika, P_N, zavisi od uslova prijema (greške na kanalu), dužine najave (dozvoljenog vremena odlučivanja) i pragova odlučivanja [1].

Prema tome, rezultujuća verovatnoća uspešne sinhronizacije biće data proizvodom

$$P_{us} = P_N \cdot P_S \tag{5}$$

Vreme sinhronizacije

Vreme sinhronizacije predstavlja vreme potrebno da se izvrši kriptološka sinhronizacija.

Ukoliko se radi o sinhronizaciji na početku, to je zbir vremena potrebnog za najavu (T_N) i vremena potrebnog za prijem spoljašnjeg ključa (T_{SK})

$$T_S = T_N + T_S \tag{6}$$

Ukoliko se radi o tekućoj sinhronizaciji može se govoriti o prosečnom vremenu potrebnom za uspešnu sinhronizaciju.

Ako se sa $T_Š$ obeleži vreme za koje se emituje šifrat između dve kriptosinhronizacije, prosečno vreme sinhronizacije će, u slučaju naknadno uključenog učesnika u radio-mreži biti

$$\overline{T_S} = 0,5T_Š + \sum_{i=1}^{\infty}\left[iT_S + (i-1)T_Š\right]\pi(i) \tag{7}$$

gde je $T_S = T_N + T_{SK}$

$\pi(i)$ predstavlja verovatnoću da je sinhronizacija ostvarena u i-tom pokušaju,

$\pi(1) = P_{US}$

$\pi(2) = P_{US}(1-P_{US})$,

.

.

.$\pi(i) = P_{US}\,(1-P_{US})^{i-1}$.

Na osnovu ovih relacija dobija se:

$$\overline{T}_S = \frac{T_S + T_{\check{S}}}{P_{US}} - 0,5 \cdot T_{\check{S}} \tag{8}$$

Kao što je objašnjeno, u sistemima za kriptozaštitu signala u realnom vremenu kašnjenje informacije na putu do prijemnika može biti oštro ograničeno.

Ukupno kašnjenje predstavlja zbir vremena potrebnog za telekomunikacionu sinhronizaciju, kriptološku sinhronizaciju, dešifrovanje i eventualno početno kašnjenje D/A konvertora.

Pri prenosu govornih informacija već je kašnjenje od 0,5 s značajno, a kašnjenje od 1 s već je praktično neprihvatljivo.

Ovde treba ukazati na još jedan problem. Kada se uređaj prebaci na predaju, korisnik mahinalno počinje da govori. Pošto po proceduri u tom trenutku kreće najava, a zatim SK, deo informacije propada, jer je tehnički neopravdano njeno memorisanje i naknadno emitovanje čitave poruke sa kašnjenjem [4]. To se obično prevazilazi tako što se u vreme slanja kriptološke sinhronizacije u slušalici emituje ton, kao znak zauzeća kanala. Ima, međutim, situacija kada je to neprihvatljivo i kod kojih je i vreme sinhronizacije kritično. Jedan primer je radio-veza, gde je veliki deo poruka veoma kratak, čak oko 1 s. Posebno je neprihvatljivo da pilot u fazi borbenih dejstava čeka da se završi upozoravajući ton, pa da počne da govori. Čitava situacija je otežana činjenicom da se za prebacivanje radio-uređaja koristi VOX (elektronski prekidač koji reaguje na pojavu govora).

Značaj vremena sinhronizacije (izraženog brojem bita potrebnog za njegovo postizanje) bitno zavisi od veličine bitskog protoka u posmatranom sistemu veze. Tako 1000 bita za sinhronizaciju nema isti značaj pri prenosu govora komprimovanog nekim od metoda analize i sinteze, gde su brzine prenosa do 2400 bit/s i prenosa govora digitalizovanog pomoću delta-modulacije, gde je brzina prenosa 32 kbit/s.

S druge strane, kao što je rečeno, pri prenosu podataka (u računarskim mrežama ili pri prenosu pisanog teksta) ovaj parametar, praktično, nije bitan.

Zaključak

Izloženi materijal daje osnovne informacije o komunikacionom kanalu sa zaštitom informacija i kriptološkoj sinhronizaciji. Istovremeno, data je više kvalitativna nego kvantitativna analiza problema koji se javljaju pri dimenzionisanju parametara kriptološke sinhronizacije.

Može se zaključiti da je problem rešavanja kriptološke sinhronizacije problem nalaženja optimuma između kriptoloških, telekomunikacionih i taktičkih zahteva i da je za njegovo rešavanje potrebno dobro poznavanje svih ovih elemenata, što znači da se u principu različito rešava zavisno od sistema veze u kome se vrši kriptozaštita.

Ova razmatranja, kao i razmatranja o telekomunikacionoj sinhronizaciji, omogućavaju sagledavanje problema generisanja i distribucije kriptoloških ključeva, odnosno izbor sistema kojim će se vršiti šifrovanje informacije.

Literatura

[1] Grupa autora, Elementi moderne kriptologije, GŠ VJ, Beograd, 1997.

[2] Dukić, M., Principi telekomunikacija, Akademska misao, Beograd, 2008.

[3] Šumonja, P., Zaštitno kodovanje kratkih binarnih sekvenci – magistarski rad, ETF, Beograd, 1992.

[4] Markagić, M., Interni radovi, Vojna Akademija, Beograd.

COMMUNICATION CHANNEL WITH THE ENCRYPTION OF INFORMATION

Introduction

According to predefined concepts as a basic provision of telecommunications, encryption synchronization and communication threats, it is possible to determine terms for a safe commercial communication channel.

The basis of this work is a model of a telecommunication channel with its elements, with encryption and without it. Pursuant to this model, this paper examines the problems of encrypting commercial communication channels.

The concept of encryption synchronization, realized by different types of synchronization, is discussed.

Model of a communication channel with information encryption

Compared with a general model, this one is composed of an algorithm for encryption and decryption. It could be realized as an element of a telecommunication device or as a separate device.

Understanding this element as well as a model without encryption helps comprehending a problem of encryption synchronization, generation and distribution of encryption keys.

Notion of synchronization

Generally, synchronization is a process which implies implementation and maintenance of a synchronous situation.

Encryption synchronization is, consequently, a procedure which means that the PRNG – (Pseudo Random Number Generator) in the

receiver performs the inversion of a transformation message made by the PRNG in the transmitter.

Encryption transformation using a particular algorithm depends on internal and external encryption keys.

Assuming that both the receiver and the transmitter have the same internal encryption key, and according to the fact that the device uses a new external encryption key for every new message, it is necessary to transmit that key to the receiver.

Encryption synchronization is, therefore, a process of transmitting the external encryption key from the PRNG of the transmitter to the PRNG of the receiver.

Communication synchronisation

In order to start the process of encryption synchronization, it is necessary to finish the communication synchronization.

During the communication synchronization, depending on how complex the communication system is, there is a hierarchy of synchronization problem solving.

Types of encryption synchronization

The types of encryption synchronization are:
– Encryption synchronization at the beginning of the message,
– Periodical encryption synchronization (current synchronization),
– Encryption synchronization with a restart.

Encryption synchronization at the beginning

The advantages of this synchronization are:

– except for initial delay, it does not impair the total channel capacity available for transmission of the ciphertext;

– it provides encryption / decryption „bit for a bit“ (an error in the ciphertext produces an error in the plaintext); and

– detection and jamming are difficult.

The disadvantages of synchronization at the beginning:

– if synchronization is not successful for some reason, the whole message is lost,

– if slipping of the digit clock happens, the rest of the message is useless,

– in radio-network, the later inclusion of participants is not allowed.

Periodical encryption synchronization

The advantages are:

– if there is no encryption synchronization at the beginning of the message, it can be realized in the next mailing;

– it provides encryption / decryption „bit for a bit“ (an error in the ciphertext produces an error in the plaintext);

– slipping of the digit clock can be solved;
– inclusion of participants is allowed later, in radio-network.
The disadvantages are:
– it impairs the total channel capacity available for transmission of the ciphertext;
– visibility of encryption synchronization on the channel.

Encryption synchronization with a restart

Due to the repetition of the same starting position, this synchronization is called synchronization with a restart.
The advantages are:
– total channel capacity is available for transmission,
– if there is no synchronization at the beginning of the message, it can be realized after the next restart.
The main disadvantage results from the encryption nature itself, and, as such, this type of synchronization is hardly acceptable.

Parameters of the external encryption key

The basic parameters of the external encryption keys are:
– length of the external encryption key;
– probability of successful synchronization;
– time of synchronization.
These three parameters are interrelated and their determination depends on encryption and communication requirements as well as on device limitations (dimensions, power consumption, mass, etc.)

Length of the external encryption key

From the encryption aspect, the length of the external encryption key should be as great as possible, in order to get as big number of starting positions of PRNGs s possible and to reduce the risk of various posts with the same encryption key.
In modern encryption devices, PRNGs are realized by means of microprocessor-based microcomputers.

Probability of successful synchronization

The arguments that the length of external encryption keys should be as great as possible are very strong. However, probability of successful synchronization is from 0.95 to 0.99, depending on a device.
The previous text does not explicitly emphasize that the external encryption key must be transferred completely correctly. Within an error channel, this can be judged only by the theory of probability.

Protective encoding as a factor of successful synchronization probability

Protective coding is a process of deliberate introduction of redundancy in the transmitted message and in a manner that allows detection and correction of errors that appear in the message.

The protective coding theory is a scientific discipline within the statistical theory of telecommunications and offers many types of codes optimized with various aspects (type of channel, synchronization, etc.). In terms of telecommunication channels of limited capacity which does not allow protective coding of an entire message, the use of protective complex encoding only during the transfer of external encryption key is not technically justified, and is sometimes impossible (when it comes to current encryption synchronization).

This section deals with protective coding by repeating messages an odd number of times and by majority decision-making at the reception.

Feedback shift registers

Similar, but slightly less favorable characteristics are those of pseudo-random sequences generated by feedback shift registers. Due to their generating simplicity and high reliability of once-realized synchronization, they are often used at the beginning.

Time of syncronization

Synchronization time is the time needed to perform encryption synchronization.

The importance of synchronization time (measured by a number of bits needed for its achievement) significantly depends on the size of channel rate in the monitored system. 1000 bits for synchronization does not have the same significance in the transfer of speech compressed by some of the methods of analysis and synthesis, where the transfer speed is up to 2400 bit / s, and in transmitting voice using delta-modulation, where the rate is 32 kbit / s.

On the other hand, as mentioned before, in data transmission (in computer networks and transmission of written text) this parameter is practically of no sifnificance.

Conclusion

The basic information about the communication channel with encryption of information and encryption synchronization is given here together with a more qualitative than quantitative analysis of the problems that occur when dimensioning parameters of encryption synchronization.

It can be concluded that the problem of solving encryption synchronization is a problem of finding the optimum between encryption, telecommunications and tactical requirements and that, in order to solve it, a good knowledge of all these elements is necessary, i. e. each particular problem is addressed separately, depending on a communication system in which cryptography is applied.

This consideration and the consideration of the telecommunications synchronization allow the assessment of the problem of generating and distributing encryption keys as well as selecting a system for information encryption.

Key words: *telecommunication chanel, encoding, encryption key.*

Datum prijema članka: 06. 08. 2009.

Datum dostavljanja ispravki rukopisa: 29. 01. 2010.

Datum konačnog prihvatanja članka za objavljivanje: 01. 02. 2010.