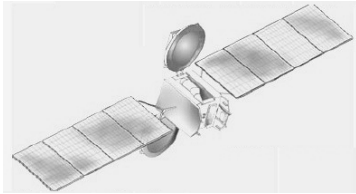


## TRASMISSIONE DATI VIA SATELLITE



Corso di Sicurezza su Reti  
Anno acc.: 2003/2004  
Prof.: Alfredo De Santis

Realizzata da: D'Amato Vito

Trasmissione dati via satellite

1

### Sommario

- **Introduzione**
- Il Sistema DVB
- Tipologie di servizi forniti
- Funzionamento di un sistema DVB IP unidirezionale
- Sistemi di sicurezza
- La Piattaforma AstraNet

Trasmissione dati via satellite

2

### Introduzione (1/2)



- Le tecnologie usate per le trasmissioni di dati via satellite offrono delle velocità di trasmissione pari o anche superiori a quelle dell'ADSL terrestre.
- Le velocità di download possono variare tra i 300 Kbps ai 2 Mbps, a seconda del tipo di servizio.
- Grazie alle tecnologie satellitari è possibile usufruire di una connessione a banda larga anche in località fuori dai centri urbani, non raggiunte dall'ADSL terrestre.
- Si propongono come alternativa economica alle linee dedicate e si rivelano utili per postazioni mobili.

Trasmissione dati via satellite

3

### Introduzione (2/2)



- Grazie all'Internet a banda larga via satellite, è possibile usufruire di servizi gratuiti accessibili offline (senza alcuna connessione terrestre), quali ad esempio:
  - I servizi di Web Casting, come Casablanca;
  - I servizi di News.

Trasmissione dati via satellite

4

### Brevi cenni storici sulle telecomunicazioni via satellite (1/2)

- Già nel 1929, Hermann Noordung pubblica a Vienna un documento tecnico in cui descrive la prima ipotesi di utilizzo dei satelliti geostazionari per le telecomunicazioni.
- Il 4 Ottobre 1957, in piena guerra fredda, il satellite Sputnik 1 di proprietà Russa viene lanciato in orbita per misurare la densità dell'atmosfera e ritrasmetterla a terra sotto codice morse, ma smette di funzionare già il 4 Gennaio 1958. Pesava 85 Kg ed aveva le dimensioni di una palla da basket.
- Il 18 Dicembre del 1958 avviene il lancio del primo satellite per le telecomunicazioni denominato *SCORE (Signal Communication by Orbital Relay)*, il quale invia la prima trasmissione satellitare costituita da un messaggio audio di auguri natalizi del presidente Eisenhower.

Trasmissione dati via satellite

5

### Brevi cenni storici sulle telecomunicazioni via satellite (2/2)

- Nel 1962 grazie al satellite *Telstar*, vengono ricevute le prime immagini televisive provenienti dallo spazio.
- Nel 1965 si realizza la copertura completa della superficie terrestre, ad eccezione delle regioni polari, con la creazione del consorzio *Intelsat* di cui fanno parte oltre 130 paesi.

Trasmissione dati via satellite

6

## Sommario

- Introduzione
- **Il Sistema DVB**
- Tipologie di servizi forniti
- Funzionamento di un sistema DVB IP unidirezionale
- Sistemi di sicurezza
- La Piattaforma AstraNet

Trasmissione dati via satellite

7

## Il sistema DVB (1/2)



Il DVB, acronimo di Digital Video Broadcasting, è lo standard de facto a livello europeo per i servizi di broadcasting dei dati radio e televisivi attraverso il satellite.

- Il progetto DVB è nato nel 1993 da un consorzio di oltre 200 operatori di broadcasting, costruttori e operatori di rete in più di 30 Paesi del mondo.
- Esso definisce un set globale di specifiche per la distribuzione della TV digitale e dei servizi di broadcast digitali in generate.

Trasmissione dati via satellite

8

## Il sistema DVB (2/2)



- E' basato su standard aperti:
  - utilizza MPEG-2 a livello di trasmissione e trasporto;
  - IP per i protocolli di rete riguardanti la comunicazione.
- Grazie allo standard DVB, la tecnologia satellitare viene sfruttata in maniera analoga per le differenti tipologie di trasmissioni (audio, video, dati).
- Sono stati definiti diversi standard DVB applicabili ai differenti mezzi di trasmissione.

Trasmissione dati via satellite

9

## Il sistema DVB: gli standard



- **DVB-S**, adottato nelle trasmissioni via satellite;
- **DVB-SI** (Service Information), amplia il DVB-S fornendo informazioni sul contenuto della trasmissione;
- **DVB-S2**, migliora ed espande la gamma di applicazioni possibili con il DVB-S;
- **DVB-IP**, utilizzato nella distribuzione di dati via satellite;
- **DVB-T**, utilizzato per la trasmissione digitale attraverso ripetitori terrestri;
- **DVB-C** e **DVB-SMATV**, adottati per le trasmissioni via cavo;
- **DVB-MS** e **DVB-MC**, utilizzati per la diffusione del segnale su microonde;
- **DVB-MHP**, adottato per la televisione digitale interattiva;
- **DVB-RCS**, utilizzato per le comunicazioni satellitari interattive;
- **DVB-H** (Handheld), basato su DVB-T e utilizzato per l'IP broadcasting verso dispositivi palmari;
- **DVB-RCT**, per la realizzazione di comunicazioni terrestri interattive.

Trasmissione dati via satellite

10

## Standard DVB-S

- Lo standard DVB-S, specificato nella norma ETS 300 421 degli standard ETSI, è lo standard DVB adottato per i diversi tipi di trasmissioni via satellite.
- Utilizza MPEG-2 Transport Stream (TS) per la codifica, la compressione del segnale sorgente e per la moltiplicazione dei programmi.
- Consente di suddividere la capacità trasmissiva di un transponder, pari a 38.015 Mbits al secondo, tra più programmi moltiplicati contemporaneamente.

Trasmissione dati via satellite

11

## Standard DVB-S

Fornisce la protezione dagli errori attraverso:

- L'**interleaving**, che permette di scomporre errori di tipo burst, ovvero più bit errati consecutivi, in tanti errori che coinvolgono uno o pochi bit per ogni blocco, attraverso l'intreccio dei flussi;
- L'utilizzo dello schema di codifica **Reed Solomon** per il **FEC**, che aggiunge dei bit di parità ai dati per consentire la correzione degli errori nei blocchi di bytes;
- La **codifica convoluzionale parametrizzabile**, che introduce ridondanza per rendere i segnali di informazione resistenti alla corruzione dovuta a segnali di disturbo.



Trasmissione dati via satellite

12

### Lo standard MPEG-2 (1/2)

- E' stato definito nel 1994 dal gruppo di lavoro dell'ISO/IEC Motion Picture Experts Group (MPEG), che sviluppa standard per la codifica ed il trasporto di audio e video digitali.
- Lavora tipicamente a risoluzioni intorno a 720x576 pixel, con bit rate compresi tra 4 e 8 Mbps.
- E' basato sull'eliminazione degli elementi di ridondanza e su alcuni potenti algoritmi in grado di ridurre sensibilmente la dimensione del dato finale.
- E' lo standard MPEG per la codifica, la compressione ed il trasporto di audio e video digitali utilizzato nelle trasmissioni satellitari e nei DVD.

### Lo standard MPEG-2 (2/2)

- Definisce due tipi di multiplexing per le informazioni:
  - il **Program Stream (PS)**;
  - il **Transport Stream (TS)**.

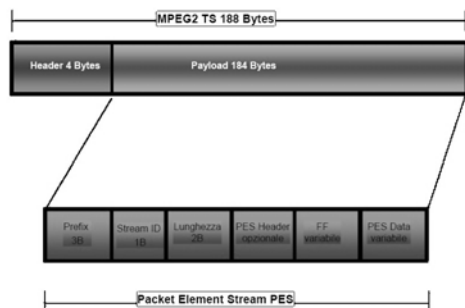
### MPEG-2 Program Stream (PS)

- Contiene l'equivalente di un solo programma TV.
- Può multiplexare uno o più Elementary Streams con una base di tempo comune.
- Permette di utilizzare pacchetti di lunghezza variabile nel processo di multiplexing, i *PS packs*.
- La lunghezza dei pacchetti va normalmente da 1 a 2 Kbytes per poter essere contenuta nei settori dei dischi (tipicamente 2Kbytes).
- I pacchetti possono avere una lunghezza massima di 64 Kbytes.
- È stato pensato per applicazioni con basso livello d'errore, come ad esempio le applicazioni multimediali su CD-ROM.

### MPEG-2 Transport Stream (TS) (1/3)

- Può contenere uno o più programmi TV e ognuno con la propria base di tempo indipendente.
- Nasce dall'esigenza di creare uno strato di trasporto dati per un ambiente tollerante agli errori.
- Utilizzato nelle trasmissioni via satellite.
- Particolarmente idoneo per la trasmissione di dati via satellite all'interno del flusso di datagrams IP.
- Utilizza pacchetti di 188 bytes, dove:
  - i primi 4 bytes servono per l'intestazione (header);
  - i restanti 184 bytes vengono lasciati al carico utile dei dati (payload).

### MPEG-2 Transport Stream (TS) (2/3)



### MPEG-2 Transport Stream (TS) (3/3)

- L'header contiene 4 bytes di sincronizzazione ed identificazione (PID) del pacchetto.
- Il PID (Packet Identifier) serve ad identificare il tipo del flusso di informazioni.

Esempio:

PID	Trasmissione
234	Video 1
324	Audio 3
512	Dati 1

### Standard DVB IP (1/4)

- Lo standard DVB IP, definito dagli standard ETSI EN 301 192 per Data Broadcasting, basato sugli standard ETSI/DVB per DVB-S e DVB-SI, viene utilizzato per la diffusione di dati via satellite .
- Consente il trasporto di traffico TCP/IP (Internet) all'interno dei pacchetti DVB.

Esso identifica quattro modalità di diffusione dei dati:

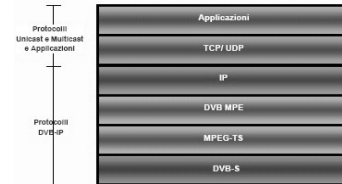
- il **data piping**;
- il **data streaming**;
- il **Multi Protocol Encapsulation (MPE)**;
- il **data carousel**.

Trasmissione dati via satellite

19

### Standard DVB IP (2/4)

- Il **Multi Protocol Encapsulation** è la modalità di diffusione adottata dallo standard DVB IP per la trasmissione di dati via satellite.
- Esso fornisce un meccanismo per incapsulare protocolli di comunicazione su rete (es.: IP) in pacchetti MPEG-2 TS.

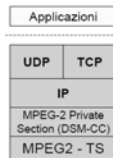


Trasmissione dati via satellite

20

### Standard DVB IP (3/4)

- La trasmissione dei datagrams IP contenenti i dati, avviene incapsulando i datagrams stessi all'interno della sezione privata DSM-CC dei pacchetti MPEG-2 TS.
- Ogni datagram IP deve avere una dimensione non superiore a 4080 bytes .

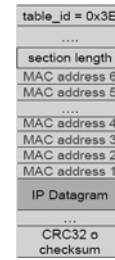


Trasmissione dati via satellite

21

### Standard DVB IP (4/4)

I pacchetti per essere indirizzati verso l'utente (gli utenti) giusto (giusti), vengono marchiati con l'indirizzo MAC (Media Access Control) dell'utente (degli utenti) a cui sono destinati.



Trasmissione dati via satellite

22

### I sistemi DVB IP (1/3)

I sistemi DVB IP esistenti possono essere classificati in due categorie:

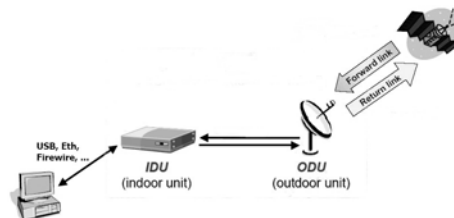
- sistemi bidirezionali**, chiamati DVB-RCS (Return Channel System);
- sistemi unidirezionali**, chiamati DVB IP one way.

Trasmissione dati via satellite

23

### I sistemi DVB IP (2/3)

I sistemi DVB-RCS consentono la trasmissione delle richieste di dati e la ricezione dei dati relativi, attraverso l'utilizzo di apparati che permettono sia l'uplink che il downlink satellitare.

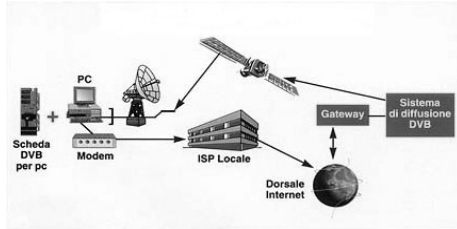


Trasmissione dati via satellite

24

### I sistemi DVB IP (3/3)

I sistemi unidirezionali utilizzano la rete terrestre per effettuare le richieste, mentre la ricezione dei dati avviene attraverso il downlink satellitare (la parabola).



Trasmissione dati via satellite

25

### Sommario

- Introduzione
- Il Sistema DVB
- **Tipologie di servizi forniti**
- Funzionamento di un sistema DVB IP unidirezionale
- Sistemi di sicurezza
- La Piattaforma AstraNet

Trasmissione dati via satellite

26

### Modalità di diffusione dei dati

- **Broadcast**, se il servizio è fruibile da tutti gli utenti;
- **Multicast**, se il servizio è ristretto ad utilizzatori che fanno parte dello stesso gruppo;
- **Unicast**, se il servizio è riservato ad un solo utente.

Nel caso specifico di applicazioni basate sul protocollo TCP/IP si parla di **IP-unicast** o di **IP-multicast**.

Le trasmissioni satellitari sono di natura broadcast, ma attraverso l'utilizzo di opportune tecniche di cifratura del segnale, si riesce ad offrire un servizio di libero accesso solo agli utenti autorizzati dal gestore del servizio.

Trasmissione dati via satellite

27

### Servizi offerti dagli ISPS (1/4)



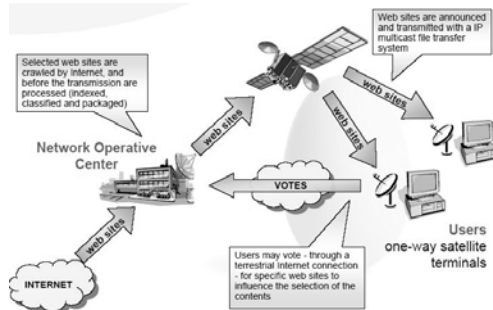
#### Servizi gratuiti

- Sono basati su IP-multicast.
- Alcuni esempi di servizi appartenenti a questa categoria sono:
  - I servizi di **News**;
  - I servizi di **Web Casting** (come il progetto Casablanca).
- Sono accessibili a tutti.
- I dati vengono trasmessi non criptati.

Trasmissione dati via satellite

28

### Servizi offerti dagli ISPS: Casablanca (2/4)



Trasmissione dati via satellite

29

### Servizi offerti dagli ISPS (3/4)



#### Servizi a pagamento

- Sono basati sia su IP-unicast che su IP-multicast.
- Alcuni esempi di servizi appartenenti a questa categoria sono:
  - Il servizio **Fast Download o Fast Internet** (basato su IP-multicast);
  - Il servizio **Web TV** (basato su IP-multicast);
  - Il servizio **Sat ADSL o FastSurf** (basato su IP-unicast).
- Sono accessibili solo dagli utenti autorizzati.
- I dati vengono trasmessi criptati.

Trasmissione dati via satellite

30

## Servizi offerti dagli ISPS (4/4)



Solitamente i provider satellitari che offrono il servizio a pagamento Fast Download possiedono dei server dedicati:

- **Push Server**, sui quali memorizzano i contenuti proposti (audio, video, ecc.), aggiornati periodicamente in base alle richieste più frequenti fatte dagli utenti ed ai contenuti messi a disposizione dalle aziende fornitrici di contenuti;
- **Proxy Server**, i quali provvedono alla ricerca nella Rete dei dati richiesti dall'utente;
- **Streaming Server**, attraverso i quali mettono a disposizione bouquet vasti di dati, audio (MP3), video e canali televisivi (MPEG-4).

Trasmissione dati via satellite

31

## Sommario

- Introduzione
- Il Sistema DVB
- Tipologie di servizi forniti
- **Funzionamento di un sistema DVB IP unidirezionale**
- Sistemi di sicurezza
- La Piattaforma AstraNet

Trasmissione dati via satellite

32

## Gli Annunci (1/2)

Nei servizi basati su IP-multicast, per avvisare gli utenti delle sessioni di download in arrivo dal satellite, vengono inviati in multicast, attraverso il satellite stesso, dei messaggi che in gergo sono detti "Annunci".

```
<FaztAnnouncement version="1.0">
  <entry name="EonZNetworkVideo"
    DioKItaliano10_LUPIN_Microfinger_1_re_dei_falsari.avi" guid="{35E1890A-E5E4-11D6-
    9100-005006BB072B}" type="Z" comment="19:47:20:19 on TP 115 Pushed with EonZFM"
    destination="filefetch:EonZNetworkVideo
    DioKItaliano10_LUPIN_Microfinger_1_re_dei_falsari.avi" size="375429120"
    receive="always">
    <encryption method="Twofish" version="1.0" key="fa2d78077c0f39796793a81da1c0dae37"
    <timing synchronisation="1035397549" start="1035481656" end="1035483568"
    resourceID="115" priority="0">
    <FZInfo method="FFM" version="3.0" digest="00000000000000000000000000000000"
    language="1" type="1" Time="64020000" Date="731148" name="?">
    <EonZInfo version="1.0" comment="Pushed with EonZFM" data="2002/10/24 17:47:00"
    transponder="115" codice="353986">
  </entry>
</FaztAnnouncement>
```

Trasmissione dati via satellite

33

## Gli Annunci (2/2)

- Questi messaggi contengono informazioni circa il download, come il nome del file, l'ora di trasmissione, la dimensione del file, ecc.
- L'utente per poter ricevere i dati inviati in multicast deve essere in possesso di questi messaggi.
- La gestione degli "Annunci", dei relativi download e dell'eventuale decrypt avviene mediante l'utilizzo di software specifici forniti dal fornitore del servizio (non sempre).
- Se si fa il download di dati criptati non basta il solo possesso di questi messaggi, infatti solo l'utente autorizzato (quindi in possesso di una chiave personale) sarà in grado di decifrarli.

Trasmissione dati via satellite

34

## Funzionamento di un sistema DVB IP unidirezionale a pagamento (1/7)

Il servizio a cui fa riferimento tale sistema DVB IP è il Fast Download (o Fast Internet).

Un utente abbonato ad un provider satellitare è provvisto di un **account** e di una **chiave personale**, stipulati nella fase di registrazione al servizio.

- L'**account**, rappresentato dalla coppia (user name, password), serve all'utente per effettuare il login sul sito web dell'ISPS dal quale può effettuare le richieste di download.
- La **chiave personale** è necessaria per la ricezione dei download ed in taluni casi anche per l'attivazione dei software necessari per la ricezione dei download.

Trasmissione dati via satellite

35

## Funzionamento di un sistema DVB IP unidirezionale a pagamento (2/7)

Nella fase di registrazione, il provider utilizzerà l'indirizzo IP dell'utente per calcolare l'indirizzo MAC a cui mandare i dati.

Alcuni provider richiedono l'attivazione di una connessione VPN (Virtual Private Network), con login e password, in seguito alla quale viene ricavato l'indirizzo MAC (univoco) dell'utente al quale mandare i dati.

Trasmissione dati via satellite

36

### Funzionamento di un sistema DVB IP unidirezionale a pagamento (3/7)

La richiesta di download, la ricezione dei dati e la loro decriptazione solitamente vengono svolte attraverso i seguenti passi:

- l'utente, dopo essersi loggato sul sito web del provider, effettua la richiesta selezionando i files tra i contenuti messi a disposizione dal provider, oppure indicando l'URL della pagina Web dove i dati sono contenuti (oppure l'indirizzo FTP);
- la richiesta passa dall'ISP terrestre locale e arriva attraverso Internet ad una stazione base di terra dotata di un uplink DVB;
- se i dati richiesti non sono contenuti nei server del provider, la stazione di terra li ricava da Internet, mediante l'utilizzo di un Proxy Server, per poi passarli a server dedicati che si occuperanno del loro trattamento;

Trasmissione dati via satellite

37

### Funzionamento di un sistema DVB IP unidirezionale a pagamento (4/7)

- l'IP-Gateway (IP Encapsulator):
  - riceve i datagrams IP provenienti dai Proxy, Streaming e Push servers;
  - seleziona i pacchetti;
  - effettua dei trattamenti sui pacchetti e poi li cifra;
  - incapsula i pacchetti all'interno del flusso di trasporto MPEG-2 TS DVB;
- la stazione di terra invia in multicast, attraverso il satellite, l'Annuncio relativo al download dei dati richiesti, il quale sarà ricevuto dall'utente e utilizzato successivamente per ricevere in modo corretto i dati richiesti;

Trasmissione dati via satellite

38

### Funzionamento di un sistema DVB IP unidirezionale a pagamento (5/7)

- la stazione di terra effettua le operazioni di multiplexing, codifica convoluzionale, modulazione QPSK e conversione del segnale da frequenze intermedie a frequenze alte, necessarie (nel DVB-S) per trasmettere i dati verso il satellite;
- dal trasponder del satellite il flusso dati, sottoforma di segnale, ridiscende a terra attraverso un downlink verso la parabola collegata al PC dell'utente, dotata di un Low Noise Block converter (LNB);
- il Low Noise Block converter amplifica il segnale riflesso dalla parabola e lo converte ad una gamma di frequenze inferiori;

Trasmissione dati via satellite

39

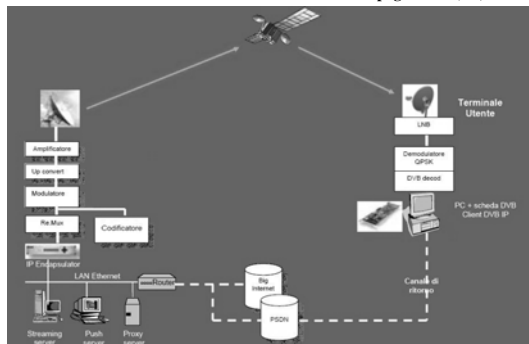
### Funzionamento di un sistema DVB IP unidirezionale a pagamento (6/7)

- la scheda DVB, di cui è dotato il PC dell'utente, esegue sul segnale i processi di:
  - demodulazione QPSK;
  - decodifica convoluzionale;
  - demultiplexing;
  - ricostruzione dei pacchetti di dati IP del flusso MPEG-2.
- I dati ottenuti vengono resi disponibili alle applicazioni utente che si occuperanno della loro decifrazione.

Trasmissione dati via satellite

40

### Funzionamento di un sistema DVB IP unidirezionale a pagamento (7/7)



Trasmissione dati via satellite

41

### Sommario

- Introduzione
- Il Sistema DVB
- Tipologie di servizi forniti
- Funzionamento di un sistema DVB IP unidirezionale
- Sistemi di sicurezza
- La Piattaforma AstraNet

Trasmissione dati via satellite

42

### Limiti delle reti IP basate su satellite (1/2)

Le reti broadband IP basate su satellite presentano delle sfide notevoli per quanto concerne la sicurezza:

- Lo sniffing dei dati e le intrusioni attive sono molto più semplici che nelle reti fisse o mobili terrestri. Ciò è dovuto alla natura broadcast dei satelliti;
- Modificando i settaggi relativi ai filtri satellitari è possibile intercettare i pacchetti destinati ad altri indirizzi MAC;
- I sistemi satellitari sono risorse vincolate, in particolare in aree con limitata potenza di trasmissione e con capacità limitate di elaborazione e di commutazione;
- I canali satellitari sono soggetti ad alti tassi di errore nei bit, il che può portare alla perdita della sincronizzazione nella sicurezza.

Trasmissione dati via satellite

43

### Limiti delle reti IP basate su satellite (2/2)

I satelliti geostazionari risentono anche del ritardo di propagazione delle informazioni.

I sistemi di sicurezza devono tener conto di tutte queste limitazioni e aggiungere solo un minimo ritardo al traffico.

Trasmissione dati via satellite

44

### Sistemi di sicurezza

Il progetto **EU IST GEOCAST**, sviluppato all'interno del programma EU 5th Framework IST, si occupa della sicurezza end-to-end dei dati nelle trasmissioni via satellite.

Un sistema di sicurezza sviluppato nell'ambito di questo progetto è il protocollo per il trasferimento sicuro di file in multicast **SAT-RMTP (Satellite Reliable Multicast Transfer Protocol)**.

Trasmissione dati via satellite

45

### Il progetto GEOCAST (1/2)

In questo progetto la componente sicurezza è stata focalizzata su due aree:

- La sicurezza del Core attraverso:
  - l'autenticazione delle entità (stazioni utente terrestri);
  - l'assegnazione delle risorse satellitari (allocazione di frequenza e capacità di canale);
  - la cifratura del traffico, collegato ai dati sull'uplink e downlink satellitare, per fornire privacy.
- La sicurezza end-to-end: la sicurezza per la privacy, fornita tipicamente allo strato di rete, di trasporto o di applicazione.

Trasmissione dati via satellite

46

### Il progetto GEOCAST (2/2)

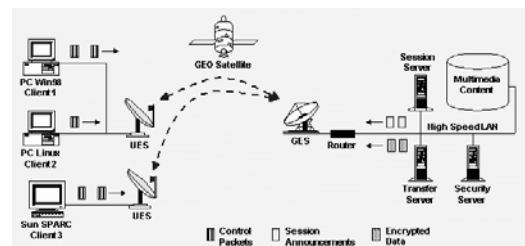
Garantisce i quattro obiettivi principali della sicurezza digitale:

- **Autenticazione**, attraverso l'uso di un certificato digitale X.509;
- **Confidenzialità**, cifrando il traffico di comunicazione usando un algoritmo a chiave privata;
- **Integrità**, attraverso l'uso dell'Hashed Message Authentication Code (HMAC) calcolato sulle informazioni da spedire;
- **Non ripudio**, creando il Message Authentication Code (MAC) del messaggio attraverso l'uso della chiave pubblica dell'utente, contenuta nel suo certificato digitale.

Trasmissione dati via satellite

47

### Il sistema di sicurezza SAT-RMTP (1/2)



Trasmissione dati via satellite

48

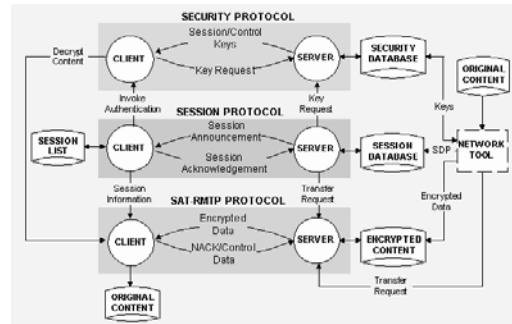
## Il sistema di sicurezza SAT-RMTP (2/2)

Il protocollo SAT-RMTP fornisce la trasmissione sicura di files (clip multimediali, bulk data) in multicast.

A tale scopo è stato sviluppato un tool applicativo composto da tre moduli:

- modulo di sessione;
- modulo SAT-RMTP;
- modulo di sicurezza.

## Architettura tool applicativo SAT-RMTP



## Moduli tool applicativo SAT-RMTP (1/4)

- Il **modulo di sessione** annuncia i servizi (trasferimenti di file) offerti e ne coordina le trasmissioni e lo scheduling.
  - Il Session Server periodicamente trasmette sessioni di annunci (announcements) ai riceventi in ascolto.
  - Gli annunci includono il tempo d'inizio e di fine sessione, il tipo del file e altri parametri relativi alla sessione.
- Il **modulo SAT-RMTP** fornisce trasmissioni attendibili di dati criptati tra la sorgente (il trasmettitore) e quei riceventi che si sono registrati per un particolare trasferimento di file.

## Moduli tool applicativo SAT-RMTP (2/4)

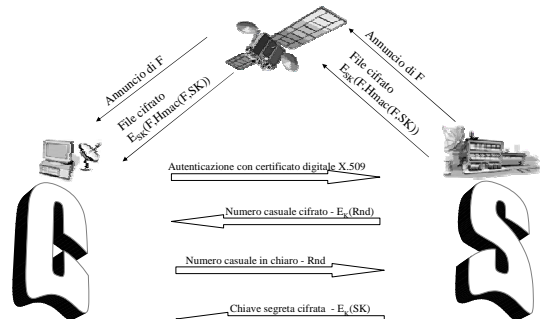
- Il **modulo di sicurezza** implementa le seguenti caratteristiche di sicurezza:
  - Autenticazione degli utenti (client), usando un algoritmo a chiave pubblica e un certificato digitale X.509;
  - Il controllo di accesso utente per ogni file;
  - Lo scambio di chiavi usando un algoritmo a chiave pubblica;
  - Confidentialità, basata sulla cifratura dei file usando un algoritmo a chiave privata;
  - Integrità dell'intero file usando HMAC;
  - Scoperta degli attacchi a replay usando numeri casuali.

## Moduli tool applicativo SAT-RMTP (3/4)

Il **modulo di sicurezza** lavora nel modo seguente:

- genera una chiave segreta (SK) e cripta l'intero file (F) con essa;
- trasmette il file criptato usando il protocollo SAT-RMTP;
- il security server autentica ogni client (interessato alla chiave di cifratura) usando il certificato digitale X.509 inviategli dal client stesso;
- controlla i permessi di accesso del client (controllo di accesso utente);
- il security server scopre attacchi a replay inviando un numero casuale (Rnd) cifrato, con la chiave pubblica (K) del client, al client stesso;
- il client lo decifra, con la propria chiave privata (P), e lo invia al server, il quale lo confronta con il numero che lui generato;
- se il client ha i permessi corretti, il security server cifra la chiave segreta con la chiave pubblica del client (contenuta nel suo certificato digitale) e gliela invia in unicast;
- il client, decifra la chiave di cifratura con la propria chiave privata, può quindi decrittare il file e controllare la sua integrità utilizzando HMAC.

## Moduli tool applicativo SAT-RMTP (4/4)



## Sommario

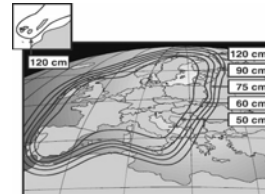
- Introduzione
- Il Sistema DVB
- Tipologie di servizi forniti
- Funzionamento di un sistema DVB IP unidirezionale
- Sistemi di sicurezza
- **La Piattaforma AstraNet**

Trasmissione dati via satellite

55

## La Piattaforma AstraNet

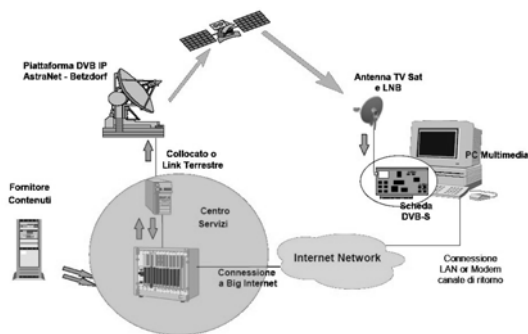
- La Piattaforma AstraNet ha iniziato ad operare in questo campo dal 1997.
- Ha la sua Stazione Hub in Lussemburgo, a Betzdorf, ed opera in Europa sul satellite Astra 19.2°E.
- Offre una copertura territoriale estesa alla maggior parte dei Paesi Europei.



Trasmissione dati via satellite

56

## La Piattaforma AstraNet: Architettura



Trasmissione dati via satellite

57

## La Piattaforma AstraNet: servizi di base

- > **Package Delivery:** distribuzione condizionale e cifrata di package contenenti file di qualsiasi tipo (documenti, video, ecc.) con modalità *store-and-forward* (con storage intermedio);
- > **Streaming Delivery:** distribuzione condizionale e cifrata di flussi continui di informazioni (stream di pacchetti IP) senza storage intermedio;
- > **Accesso Veloce a Internet:** servizio di interconnessione a banda larga su protocollo IP al Backbone Internet, simile al Sat ADSL.

Trasmissione dati via satellite

58

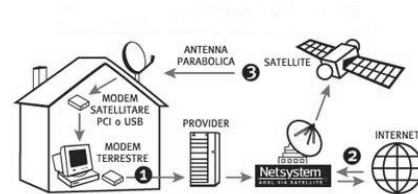
## La Piattaforma AstraNet: Netsystem (1/2)

- Netsystem, il cui Centro Servizi ha sede a Milano, è l'Operatore Italiano che opera con la Piattaforma AstraNet.
- E' connesso alla piattaforma di Betzdorf mediante fibra ottica a 140 Mbps.
- La sua offerta di servizio riguarda la connessione ADSL like, denominata Sat ADSL.
- Offre una velocità massima in download di 300 Kbps (non garantita).

Trasmissione dati via satellite

59

## La Piattaforma AstraNet: Netsystem (2/2)



Trasmissione dati via satellite

60

## Bibliografia

- Maurizio Crespi, "Il futuro è in orbita", DEV n° 83, marzo 2001
- Piero Baudino, "Internet via satellite", DEV n° 83, marzo 2001
- Roberto Borri, "Il satellite come supporto infrastrutturale alle reti terrestri", anno 2001, <http://www.garr.it/ws4/pdf/Borri.pdf>
- Giorgio Fusari, "Internet via satellite: oltre ogni ostacolo", anno 2000, <http://www.idgworld.it/networking/nwi2000/TL060001.htm>
- AERSAT, "Sistemi DVB IP via satellite", <http://www.aersat.it/docs/DVB1.pdf>
- Michael P. Howart, Sunil Iyengar, Haltham Cruikshank, Zhili Sun, "Security systems for multicast data transfer over satellite", TD-02-024-P, [http://www.ee.surrey.ac.uk/Personal/M.Howarth/cost272\\_td-02-024-p.pdf](http://www.ee.surrey.ac.uk/Personal/M.Howarth/cost272_td-02-024-p.pdf)
- ETSI, "Digital Video Broadcasting (DVB): DVB specification for data broadcasting", ETSI EN 301 192 v1.4.1 (08/2004), [http://webapp.etsi.org/action%5CCOP/OP20041022/en\\_301192v010401o.pdf](http://webapp.etsi.org/action%5CCOP/OP20041022/en_301192v010401o.pdf)
- RAI, "DVB-S Digital Video Broadcasting: La TV digitale – Il Sistema DVB-S per la diffusione da satellite", anno 2002, <http://www.raiway.rai.it/dvbs.htm>