Università degli Studi di Trento

Facoltà di Ingegneria dell'Informazione e dell'Organizzazione

Relazione sulla sicurezza nei sistemi UMTS

Corso di "Sistemi Operativi e Sicurezza" Docente: Prof. Massacci Fabio
Anno Accademico 2002/2003 Studente: Magagnino Francesco

Introduzione

La parola UMTS (Universal Mobile Telecomunications System), identifica la terza generazione della telefonia cellulare (3G).
I cellulari si sono evoluti secondo tre generazioni.

- **La prima generazione** (anni 80) è stata quella **analogica**: si potevano fare solamente telefonate vocali all'interno dei propri confini nazionali.
- **La seconda generazione** (anni 90) fu quella basata sulla tecnologia digitale: nasce lo standard **GSM** (Global System for Mobile comunication), grazie al quale è possibile comunicare oltre i confini nazionali e trasmettere dati alla velocità di 9.600 bits/s. L'ultimo atto del sistema GSM è rappresentato dalle reti GPRS (General Packet Radio Service) e HSCSD (Hight Speed Circuit Switched Data). La prima si basa sulla commutazione di pacchetto e consente di ottenere alti tassi di trasmissione (115.200 bits/s), mentre la seconda combina più canali GSM per raggiungere velocità di trasmissine fino a 57.600 bits/s.
- **La terza generazione** della telefonia mobile approda all'**UMTS**. L'obiettivo è quello della "mobilità universale", ossia creare un sistema di accesso unificato di tipo wireless che possa essere integrato nelle reti fisse ad alta velocità.
- Intanto **Ericsson** ha già annunciato che sta lavorando su un sistema di telefonia di **quarta generazione**. Secondo le previsioni questa tecnologia in fase di sperimentazione consentirà di realizzare connessioni a velocità 50 volte superiori a quella raggiungibile tramite una rete UMTS e permetterà per la prima volta esperienze di visioni tridimensionali.

L'UMTS è stato progettato per le comunicazioni multimediali comprendenti sia componenti terrestri (1885-2025 MHz e 2110-2200 MHz) sia componenti satellitari (1980-2010 MHz e 2170-2200 MHz). Le comunicazioni personali potranno, così, essere arricchite da immagini video di alta qualità, mentre l'accesso alle informazioni situate su reti pubbliche sarà potenziato da velocità trasmissive più elevate e dalle nuove funzionalità dei sistemi di terza generazione. Queste caratteristiche, unite alla continua evoluzione dei sistemi di seconda generazione abiliteranno nuovi modelli di business non solo per le aziende manifatturiere e gli operatori, ma anche per i fornitori di contenuti e di applicazioni che utilizzano tali reti.

L'UMTS, a differenza del GSM che per la trasmissione dei dati utilizza la tecnologia a commutazione di circuito, integra la trasmissione dati a circuito ed a pacchetto il che consente di ottenere servizi diversificati, come connessioni virtuali continue alla rete, modalità alternative di pagamento (ad esempio pagamenti proporzionali al numero di bit trasferiti o alla larghezza della banda impiegata).

L'UMTS implementa in Europa le specifiche ITU (International Telecommunication Union) per i sistemi di terza generazione denominate **IMT-2000** (International Mobile Telecommunications 2000). L'IMT-2000 è stato definito come standard mondiale aperto per i sistemi di telecomunicazione mobili ad alta capacità ed alta velocità di trasferimento dei dati.
L'European Telecommunications Standards Institute (**ETSI**), in cooperazione con altri organismi di standardizzazione regionali e nazionali di tutto il mondo, è l'organismo che nell'ambito dell'IMT-2000, si occupa della standardizzazione dell'UMTS.

In generale i requisiti base più significativi dei sistemi di terza generazione possono essere qui elencati :

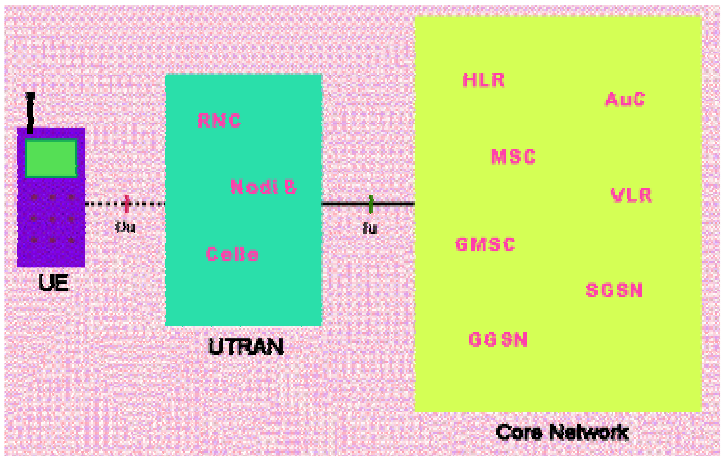
- *bit rate* fino a 2 Mbit/s;
- *bit rate* variabile per offrire ampiezza di banda su richiesta;
- *multiplexing*, su un'unica connessione, di servizi con diversi requisiti di qualità come, ad esempio, voce, video e trasmissione dati;
- requisiti sul ritardo dei pachetti: da traffico *real-time* sensibile a ritardo a traffico *best-effort* su pacchetto;
- coesistenza di sistemi di seconda e terza generazione ed *handover* intersistema per ottimizzare l'utilizzo della copertura radio e bilanciare il traffico sugli elementi di rete;
- Supporto di traffico asimmetrico sulle tratte *uplink* e *downlink* (ad esempio servizi *web browsing* comportano un maggior traffico nella tratta di *downlink* che in *uplink*);

Cenni sull'architettura UMTS

Nell'architettura di rete dei sistemi UMTS si identificano 3 principali componenti

- User Equipment (UE)
- UMTS Terrestrial Radio Access Network (UTRAN)
- Core Network (CN)

Di questi 3 principali componenti, è importante constatare che, mentre i protocolli implementati nel UE e nel UTRAN sono completamente innovativi rispetto al sistema GSM, i protocolli del Core sono rimasti pressoché identici; in questo modo viene assicurata l'integrazione con i vecchi apparati di telefonia mobile.

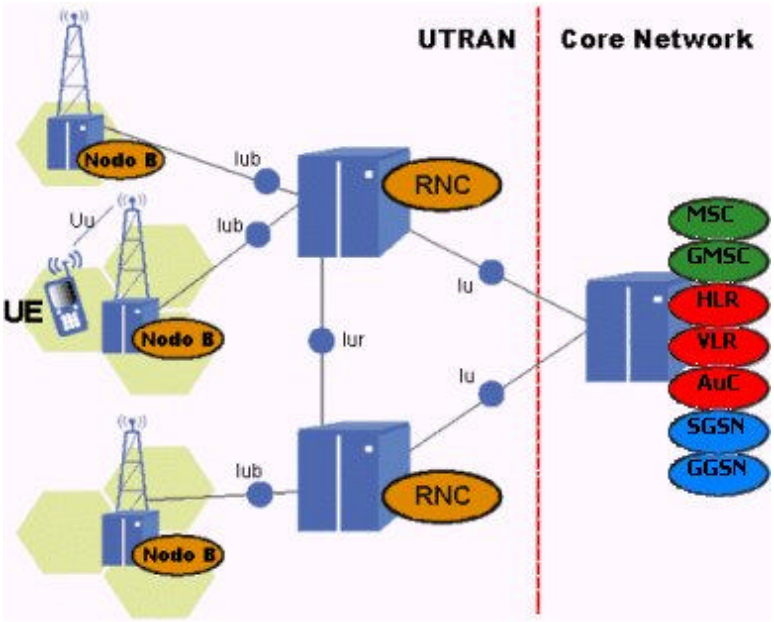


User Equipment (UE)

E' l'equipaggiamento usato dall'utente per accedere ai servizi UMTS. L'equipaggiamento utente (UE) è costituito da un equipaggiamento mobile (Mobile Equipment, ME) e da una o più USIM (User Services Identity Module).
Una USIM è la smartcard che immagazzina e gestisce i dati dell'utente; implementata insieme ad altre applicazioni in un circuito integrato posto su una carta removibile detta UICC (UMTS Integrated Circuit Card).
L'USIM contiene l'IMSI (International Mobile Subscriber Identity) che serve ad identificare in maniera univoca l'utente, sebbene l'utente può non conoscerne il valore.

UMTS Terrestrial Radio Access Network (UTRAN)

L'UTRAN è l'interfaccia radio dell'UMTS. Consiste di uno o più insieme di Radio Network Sub-system (RNS); un RNS è un sottosistema all'interno dell'UTRAN e consiste di un Radio Network Controller (RNC) e di uno o più Nodi B, ognuno dei quali può servire una o più celle.
Nella figura, sulla sinistra della linea verticale è raffigurato parte dell'UTRAN e sulla destra un'entità del Core Network. Dell'UTRAN sono raffigurati due RNS; il primo costituito da un RNC e due nodi B (il primo dei quali con una cella, il secondo con tre celle), il secondo da un RNC ed un nodo B (con tre celle).



Sicurezza nei sistemi UMTS

RNS
E' il punto di accesso dell'utente alla rete UMTS in quanto è responsabile della concessione e del rilascio di specifiche risorse radio. Ogni RNS è responsabile delle risorse del suo insieme di celle. Svolge due ruoli, quello di stabilire e gestire la connessione tra UE e UTRAN e quello di fornire le risorse radio richieste durante tale connessione.

RNC
E' la centrale di controllo che gestisce il funzionamento dei Nodi B, l'attivazione ed il rilascio dei canali radio, gli handover interni ed altro ancora. In pratica controlla l'uso e l'integrità di tutte le risorse radio.

Nodo B
E' un nodo logico responsabile della ricezione e trasmissione in una o più celle rispettivamente da e verso l'UE. Corrisponde logicamente alle stazioni radio base del GSM. Lo strano nome 'Nodo B' fu inizialmente adottato come termine temporaneo nel corso del processo di standardizzazione e non è stato più cambiato.

Cella
E' la regione geografica in cui si estende la copertura radio di un solo Nodo B. Più celle geograficamente adiacenti sono raggruppate in una Location Area/Routing Area (LA/RA) e posseggono un identificatore LAI/RAI. Ad ogni cella è assegnato un identificativo numerico, detto Cell Identifer (C-Id) usato per identificare in maniera univoca una cella dentro un RNS.

Core Network (CN)

Rappresenta la parte più interna della rete di comunicazione e più lontana dall'utente finale.
Al suo interno la trasmissione dati avviene solo e soltanto via cavo. E' l'unica infrastruttura, delle 3 considerate, che è rimasta pressoché uguale a quella operante per i telefoni mobili di seconda generazione.
Il traffico utente viene gestito in due modi distinti.

- A circuito -**Circuit Switched (CS)**- di cui fanno parte i network elements **MSC** e **GMSC**
  Una connessione di tipo CS è una connessione in cui le risorse richieste vengono concesse nel momento in cui la connessione viene stabilita e vengono rilasciate nel momento in cui la connessione viene rilasciata.
- A pacchetto -**Packet Switched (PS)**- costituita dai nodi **SGSN** e **GGSN**
  Una connessione di tipo PS trasporta l'informazione dell'utente usando autonome concatenazioni di bit chiamate "pacchetti"; ogni pacchetto può seguire un percorso diverso da quello seguito dal pacchetto che lo precede, cioè ogni pacchetto si muove in maniera autonoma.

Altri network element non sono riconducibili ai domini a circuito o a pacchetto, perché svolgono funzioni del tutto generali: **HLR**, i **VLR** e gli **AuC**.

Home Location Register (HLR)
E' il database centrale nel quale vengono memorizzati in modo permanente i dati relativi agli utenti che hanno sottoscritto un abbonamento UMTS. In particolare, l'HLR contiene gli identificatori IMSI mediate i quali vengono identificati gli utenti.

Visitor Location Register (VLR)
E' un database nel quale viene registrata e tenuta aggiornata la posizione sul territorio dell'UE. Il VLR è il registro delle locazioni per i servizi che utilizzano la trasmissione a commutazione di circuito (CS).

Authentication Centre (AuC)
E' il centro di autenticazione dei dati incaricato di generare i parametri necessari per l'autenticazione degli utenti. Tali parametri vengono memorizzati nel database HLR al quale l'AuC è associato. Quando un utente richiede un servizio, l'AuC verifica, consultando l'HLR, se si tratta di un utente regolarmente registrato.

Mobile-services Switching Centre (MSC)
E' un interfaccia tra il sistema radio e la rete fissa. Esegue le funzioni di commutazione necessarie per istaurare, controllare, tassare le chiamate da e verso un mobile presente nell'area geografica da esso servita.

Gateway MSC (GMSC)
Questo elemento è un particolare MSC che si occupa delle chiamate provenienti da MSC di altri gestori o da rete fissa

Serving GPRS Support Node (SGSN)
Costituisce, insieme al GGSN, l'interfaccia tra il sistema radio e la rete fissa per i servizi che utilizzano la trasmissione a commutazione di pacchetto.
Gateway GPRS Support Node (GGSN)
Ha funzioni analoghe al gateway MSC (GMSC). Rappresenta il punto d'ingresso alla rete che supporta la trasmissione a pacchetto.

Sicurezza nell'UMTS

Accesso non autorizzato ai dati

- *Ascolto del traffico utente*: Intrusi potrebbero intercettare il traffico sull'interfaccia radio.
- *Ascolto di segnalazione o dati di controllo*: Intrusi potrebbero intercettare traffico di segnalazione o di controllo.
- *Mascheramento network*: Intrusi potrebbero mascherarsi come network element per intercettare il traffico.
- *Analisi passiva del traffico*: Intrusi potrebbero osservare il tempo, il rate, la lunghezza di messaggi da e verso l'interfaccia radio.
- *Analisi attiva del traffico*: Intrusi potrebbero attivamente iniziare sessioni di comunicazione.

Minacce contro l'integrità

- *Manipolazione del traffico utente:* Intrusi potrebbero modificare, inserire, replicare o cancellare il traffico utente sull'interfaccia radio.
- *Manipolazione di segnalazione e controllo:* Intrusi potrebbero modificare, inserire, replicare o cancellare il traffico di segnalazione o di controllo.

Attacchi di Denial of Services

- *Interventi fisici*: Intrusi potrebbero impedire il traffico dati, segnalazione o controllo trasmessi sull'intertaccia radio, utilizzando tecniche di interferenza (jamming).
- *Interventi di protocollo*: Intrusi potrebbero impedire il traffico dati, segnalazione o controllo trasmessi sull'intertaccia radio, grazie all'introduzione di specifici segnali di failure del protocollo.
- *Denial of Service per mascheramento dei partecipanti*: Intrusi potrebbero impedire il servizio al legittimo utente mascherandosi da network element.

Accesso non autorizzato ai servizi

- *Mascheramento da utente*: Un intruso potrebbe mascherarsi come un altro utente verso la rete. L'intruso prima si maschera come una stazione radio base (Nodo B) verso un utente e quindi dirotta la sua connessione dopo che la sua autenticazione è stata fatta.

Identificazione dell'utente

Identificare l'utente vuol dire determinare il suo identificatore IMSI (International Mobile Subscriber Identity). La rete identifica l'utente o chiedendo l'IMSI direttamente all'utente o determinandolo tramite l'identificatore temporaneo TMSI (Temporary Mobile Subscriber Identity). Per motivi di sicurezza l'IMSI viene chiesto all'utente solo quando quest'ultimo non può essere identificato tramite il suo codice temporaneo TMSI. Questo per evitare che un intruso possa intercettare l'IMSI lungo la tratta radio mentre l'utente è collegato alla rete. Anche perchè l'intruso è agevolato dal fatto che l'IMSI non viene cifrato lungo la tratta radio, per cui durante la sua trasmissione, il codice IMSI è particolarmente esposto ad attacchi di intercettazione e quindi la sua mancata cifratura rappresenta un punto debole nell'ambito della riservatezza dell'identità dell'utente. Motivo per cui di norma per identificare l'utente e quindi per risalire al suo codice IMSI, si usa l'identificatore temporaneo TMSI. Il codice TMSI, contrariamente all'IMSI, viene protetto in due modi; viene cifrato mediante l'algoritmo f8 ed il suo valore viene cambiato almeno ogni volta che l'utente passa da una Location Area (LA) (o Routing Area (RA)) all'altra.

La rete distingue due identificatori temporanei, il TMSI ed il P-TMSI. L'identificatore TMSI viene generato ed assegnato all'utente dal dominio CS (Circuit Switched), cioè dal registro VLR, invece l'identificatore P-TMSI viene generato ed assegnato all'utente dal dominio PS (Packet Switched), cioè dal registro SGSN.

Il TMSI viene usato dalla rete per identificare l'utente quando quest'ultimo chiede una connessione alla rete, un distacco dalla rete, un aggiornamento della locazione, ecc.

Per evitare equivoci l'identificatore TMSI viene associato al numero LAI che identifica la Location Area (LA) nella quale l'utente è stato registrato, cioè nella quale l'utente stazionava quando il registro VLR ha generato per lui il codice TMSI. L'associazione di TMSI con LAI permette di identificare univocamente l'utente mediante il solo identificatore TMSI quando l'utente si trova nella LA identificata dal numero LAI al quale TMSI è associato; al di fuori di quella LA per identificare l'utente non è più sufficiente il solo TMSI (risp. P-TMSI) ma è necessario anche il numero LAI ossia è necessaria la coppia TMSI/LAI.

Ogni volta che l'utente passa in un'altra LA (risp. RA), il suo codice TMSI (risp. P-TMSI) viene aggiornato insieme all'identificatore LAI (risp. RAI) della locazione. Così mediante la coppia TMSI/LAI (risp. P-TMSI/RAI) è possibile identificare l'utente senza possibilità di equivoci, su tutto il territorio ed è possibile conoscere istante per istante la posizione dell'utente sul territorio.

Funzioni crtittografiche

La 3rd Generation Partnership Project (3GPP), un ente internazionale nato per lo sviluppo degli standard per telefoni mobili di terza generazione, ha fornito al sistema UMTS una serie di parametri di sicurezza mediante l'uso di algoritmi crittografici relativamente facili da computare ma difficili da invertire.
Dati i parametri in input esiste un algoritmo molto veloce che li computa, generando l'output, d'altro canto non esiste un algoritmo efficiente che conoscendo l'output riesce a dedurre l'input.

f0 Funzione per la generazione del numero (pseudo) casuale RAND.

f1 Funzione per l'autenticazione della rete.

f1* Funzione per l'autenticazione del massaggio di ri-sincronizzazione

f2 Funzione per l'autenticazione dell'utente.

f3 Funzione per la generazione della chiave CK (Cipher Key) che viene data in input alla funzione f8.

f4 Funzione per la generazione della chiave IK (Integrity Key) che viene data in input alla funzione f9.

f5 Funzione per la generazione della chiave AK (Anonymity Key) usata nelle normali operazioni.

f5* Funzione per la generazione della chiave AK (Anonymity Key) usata nei messaggi di risincronizzazione.

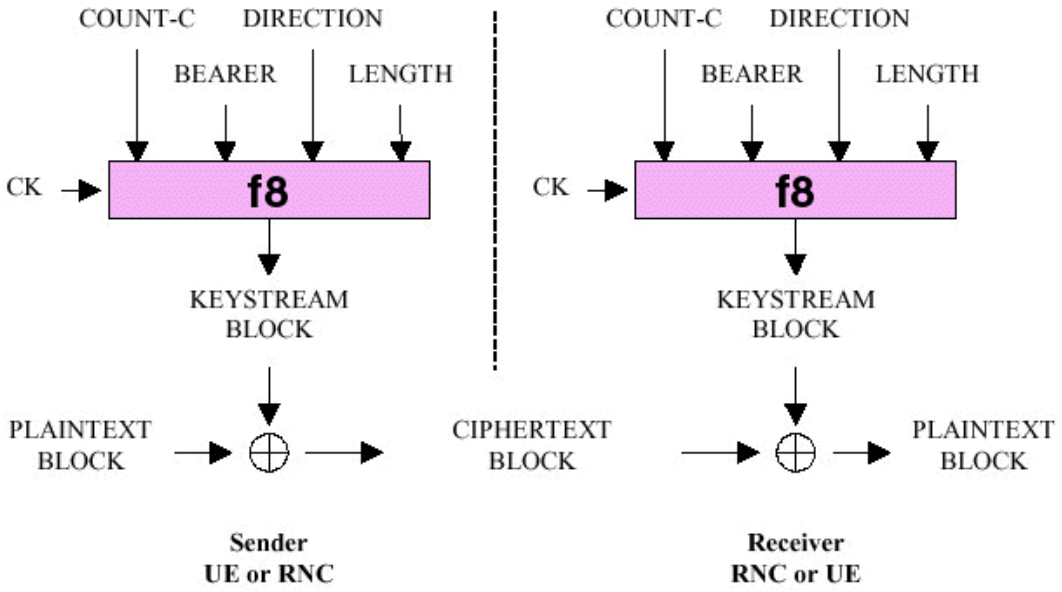
f8 Funzione per la riservatezza dei dati. Genera una keystream. Data confidentiality

f9 Funzione per l'integrità dei dati. Genera un codice MAC-I (Message Authentication Code - Integrity). Data integrity

Il 3GPP ha stabilito la standardizzazione delle sole funzioni f8 ed f9.
Sono state appositamente progettate per l'UMTS, dai partecipanti al 3GPP. Il lavoro per la realizzazione di tali funzioni è iniziato nell'agosto 1999 ed è terminato nel novembre dello stesso anno. Sono state pubblicate dall'ETSI, nella loro prima versione, il 23 dicembre 1999. L'ETSI ha provveduto anche alla loro standardizzazione.

Crifratura del traffico utente e di segnalazione sulla tratta radio (f8)

La riservatezza (confidentiality) è la proprietà dell'informazione di non essere disponibile ad entità non autorizzate.
I dati relativi all'utente (es: traffico telefonico, e-mail) ed alcuni dati di segnalazione (es: i dati che l'UE ed il registro VLR/SGSN si scambiano quando deve essere verificata l'identità dell'utente), vengono considerati sensibili e quindi necessitanti di riservatezza. Per questo viene introdotta la funzione di cifratura f8.
Mediante tale funzione viene generata una keystream che viene poi utilizzata per cifrare i dati in chiaro che vengono trasmessi dall/all utente.



Viene eseguita un'operazione di xor tra la keystream ed il testo in chiaro; il risultato è un testo cifrato. Dal testo cifrato si può riottenere il testo in chiaro generando la stessa keystream mediante l'utilizzo degli stessi parametri di input ed applicando un'operazione di xor tra la keystream ed il testo cifrato.

In realtà l'algoritmo f8 genera piccoli blocchi che concatenati costituiscono la keystream. Ogni blocco della keystream viene usato per cifrare un solo frame. Perciò la sequenza dei dati viene cifrata mediante una concatenazione di piccoli blocchi della keystream.
L'algoritmo f8 è uno stream cipher usato per cifrare/decifrare blocchi di dati lunghi tra 1 e 5114 bit; si basa sull'algoritmo KASUMI per generare una keystream costituita da un numero di bit pari ad un multiplo di 64.

CK (Cipher Key)

La chiave di cifratura CK è lunga 128 bit.
Vi può essere una chiave CK per le connessioni di tipo CS (cioè una chiave CKCS) stabilite tra il dominio del servizio CS e l'utente, e una chiave CK per le connessioni di tipo PS (cioè una chiave CKPS) stabilite tra il dominio del servizio PS e l'utente.

La chiave CK viene generata nell'HLR/AuC e viene memorizzata nell'USIM. Una copia su richiesta dell'ME (Mobile Equipment), viene mandata dall'USIM all'ME dove viene memorizzata. Un meccanismo garantisce l'utilizzo di una particolare chiave CK solo per un periodo di tempo limitato; questo per evitare che il valore della chiave CK possa essere determinato e quindi per evitare possibili attacchi. Tale meccanismo contenuto nell'USIM limita la quantità di dati che una particolare chiave CK può proteggere. Il meccanismo è semplice; all'USIM vengono comunicati, durante una connessione, i valori STARTCS e STARTPS. L'USIM memorizza questi due valori e li incrementa durante le successive connessioni. Quando uno di tali valori raggiunge un valore limite THRESHOLD, una nuova chiave CK viene generata.
L'ME (Mobile Equipment) cancella la chiave CK dalla sua memoria quando viene spento o quando la CK viene rimossa dall'USIM.

Count-c
Il numero della sequenza di cifratura COUNT-C è lungo 32 bit.
E' un contatore di frame composto di due parti; una sequenza "corta" ed una sequenza "lunga". La sequenza "corta" è costituita dai bit meno significativi mentre la sequenza "lunga" è costituita dai bit più significativi di COUNT-C. Le dimensioni della sequenza "corta" e "lunga", il valore e l'aggiornamento di COUNT-C dipendono dal tipo di trasmissione.

Bearer
L'identificatore BEARER è lungo 5 bit.
E' l'identificatore della portante radio (canale logico) usata per la connessione.
La stessa chiave CK può essere usata per le differenti portanti radio che sono simultaneamente associate allo stesso utente. Allora per evitare che la stessa keystream venga usata per cifrare su più di una portante, è stato posto BEARER come parametro di input, in tal modo la keystream viene generata in base all'identità della portante radio.

Direction
L'identificatore DIRECTION è lungo 1 bit.
Viene posto uguale a 0 per i messaggi inviati dall'UE (User Equipment) all'RNC (Radio Network Controller) e viene posto uguale ad 1 per i messaggi inviati dall'RNC all'UE.
La stessa chiave CK può essere usata per i differenti canali simultaneamente associati allo stesso UE (User Equipment); alcuni di tali canali trasmettono i dati in una direzione mentre altri trasmettono nella direzione opposta. Allora per evitare che la stessa keystream venga usata sia per cifrare i messaggi trasmessi dall'UE verso l'RNC che per cifrare i messaggi trasmessi nella direzione opposta, è stato introdotto il parametro DIRECTION. In tal modo la keystream viene generata in base alla direzione della trasmissione.

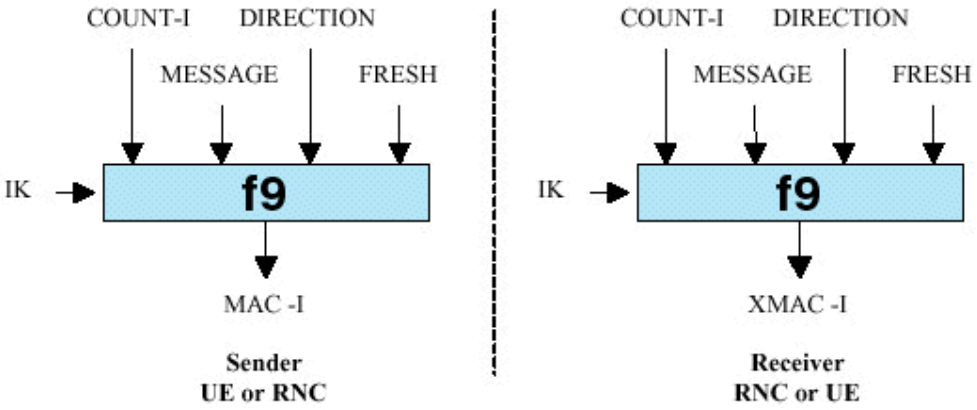
Length
L'indicatore LENGTH è lungo 16 bit.
Per un fissato canale ed una fissata direzione di trasmissione, la lunghezza del blocco del testo in chiaro (da cifrare) che viene trasmesso, può variare. E' necessario perciò generare di volta in volta, una keystream di lunghezza appropriata. Il parametro LENGTH indica proprio quanto lunga deve essere generata la keystream.
E' stato stabilito che LENGTH contenga un valore compreso tra 1 e 5114.

Protezione dell'integrità della segnalazione dentro UTRAN (f9)
L'integrità dei dati è la proprietà dei dati di non poter essere alterati in maniera non autorizzata.

La maggior parte dei dati di segnalazione che viaggiano tra l'UE (User Equipment) e l'RNC (Radio Network Controller) sono sensibili ed è necessario perciò proteggere la loro integrità.

L'algoritmo f9 viene usato per autenticare l'integrità di un messaggio di segnalazione. Il suo impiego è perciò, in tutti quei protocolli nei quali è necessario proteggere l'integrità dei dati di segnalazione che si scambiano l'UE e l'RNC.

Non viene invece protetta, sulle portanti radio (cioè lungo la tratta radio), l'integrità dei dati dell'utente.



Il codice MAC-I viene aggiunto al messaggio (o dato) di segnalazione MESSAGE quando quest'ultimo viene inviato sui collegamenti radio. Il ricevente calcola il codice XMAC-I utilizzando gli stessi parametri che sono stati utilizzati per calcolare MAC-I da chi ha mandato il messaggio MESSAGE; in particolare il ricevente utilizza come parametro di input anche il messaggio MESSAGE che ha ricevuto. Una volta calcolato XMAC-I, il ricevente lo confronta con il codice MAC-I che ha ricevuto insieme al messaggio; se i due codici coincidono vuol dire che il messaggio MESSAGE non ha subito alterazioni.
La funzione f9 è memorizzata nell'UE (User Equipment) e nell'RNC (Radio Network Controller).
L'algoritmo f9, come l'algoritmo f8, è basato sull'algoritmo KASUMI.
f9 genera un codice di autenticazione del messaggio detto MAC-I (Message Authentication Code - Integrity) lungo 32 bit, per un messaggio che ha una lunghezza compresa tra 1 e 5114 bit.

IK (Integrity Key)
La chiave IK per l'integrità dei dati è lunga 128 bit.
Vi può essere una chiave IK per le connessioni di tipo CS (cioè una chiave IKCS) stabilite tra il dominio del servizio CS e l'utente, e una chiave IK per le connessioni di tipo PS (cioè una chiave IKPS) stabilite tra il dominio del servizio PS e l'utente.
Il funzionamento della chiave IK è pressoché identico a quello della chiave CK nell'algoritmo f8.

Count-I
La lunghezza di COUNT-I è di 32 bit.
E' un contatore di frame introdotto come protezione contro i tentativi di replicare i messaggi di segnalazione durante una connessione. E' composto da due parti; una sequenza "corta" ed una sequenza "lunga". La sequenza "corta" è costituita dai 4 bit meno significativi mentre la sequenza "lunga" è costituita dai 28 bit più significativi. COUNT-I contiene un valore che viene incrementato ogni volta che un messaggio viene protetto.

Fresh
E' un parametro lungo 32 bit.
Per ogni utente vi è un parametro FRESH.
La stessa chiave IK può essere usata per diverse connessioni consecutive. Questo parametro protegge la rete contro i tentativi da parte dell'utente di replicare i messaggi di segnalazione. Quando la connessione è attivata, l'RNC (Radio Network Controller) genera un valore casuale FRESH e lo manda all'utente. Il parametro FRESH viene poi usato sia dalla rete che dall'utente per tutta la durata di una singola connessione. Questo meccanismo assicura la rete che l'utente non ha replicato qualche vecchio codice MAC-I.

Direction
L'identificatore DIRECTION è lungo 1 bit.
Il funzionamento è pressoché identico a quello dell'algoritmo f8.

Message
E' il messaggio di segnalazione la cui integrità l'algoritmo f9 deve proteggere.

Bibliografia

http://www.etsi.org/ Sito della European Telecommunications Standards Institute

http://www.gsmworld.it/ Sito italiano di telefonia mobile

http://www.3gpp.org Sito della 3rd Generation Partnership Project

http://www.abczone.it Specifiche sull'UMTS

http://www.dia.unisa.it/ads.dir/corso-security/www/CORSO-9900/umts/umts.htm

http://www.dia.unisa.it/~ads/corso-security/www/CORSO-9900/a5/testo.htm

http://www.umts-forum.org/