Autenticazione SGSN su ASR serie 5x00 e best practice per la riallocazione PTMSI

Sommario

Introduzione

Questo documento offre una spiegazione di base dei vantaggi della configurazione della frequenza della procedura di autenticazione, della funzionalità Packet Temporary Mobile Subscriber Identity (PTMSI) e della riallocazione della firma PTMSI. In particolare, questo documento è destinato a una procedura opzionale di gestione della mobilità nell'ambito di un progetto di partnership di terza generazione per 2G e 3G su SGSN (GPRS Support Node) in esecuzione su Aggregated Service Router (ASR) serie 5000.

In questo documento vengono illustrate le seguenti procedure ottimali:

- Impostazione della frequenza di autenticazione
- Riallocazione PTMSI
- riallocazione delle firme PTMSI
- L'impatto della mancata configurazione dell'impostazione della frequenza di autenticazione e della riallocazione PTMSI e della riallocazione della firma (in base all'esperienza maturata nelle richieste dei clienti)
- Linee guida per la configurazione e impatto sulle interfacce esterne
- Opzioni per la risoluzione dei problemi

Panoramica

Il framework di riallocazione delle firme PTMSI, PTMSI e PTMSI nel profilo di controllo delle chiamate consente all'operatore di configurare l'autenticazione o l'allocazione della firma PTMSI e

PTMSI per ogni sottoscrittore nei protocolli SGSN 2G e 3G e nella Mobile Management Entity (MME). Nel SGSN, l'autenticazione può essere attualmente configurata per queste procedure: attach, service-request, routing-area-update (RAU), short-messaging-service e detach.

MME utilizza lo stesso framework anche per configurare l'autenticazione per le richieste di servizio e gli aggiornamenti dell'area di tracciamento (Tracking Area Update - TAU). La riallocazione PTMSI può essere configurata per i collegamenti, le richieste di assistenza e le unità di revisione dei dati (RAU). La riallocazione delle firme PTMSI può essere configurata per i comandi attach, PTMSI reallocation e RAU. L'autenticazione e la riallocazione possono essere attivate per ogni istanza di queste procedure o per ogni ennesima istanza della procedura, denominata autenticazione selettiva/riallocazione. Alcune procedure supportano inoltre l'abilitazione dell'autenticazione o della riallocazione in base al tempo trascorso (periodicità o intervallo) dall'ultima autenticazione o riallocazione rispettivamente.

Inoltre, questi possono essere configurati specificamente solo per il sistema di telecomunicazione mobile universale (UMTS) (3G) o per il servizio General Packet Radio (GPRS) (2G) o per entrambi. Questa configurazione viene verificata solo quando è facoltativa per l'autenticazione o la riallocazione della firma PTMSI/PTMSI di un sottoscrittore da parte del servizio SGSN. Negli scenari in cui è obbligatorio eseguire queste procedure, la configurazione non viene verificata.

Esistono tre tipi di CLI per ogni configurazione di frequenza della procedura: SET CLI, NO CLI e REMOVE CLI. Quando si richiama un SET CLI, l'operatore desidera abilitare l'autenticazione o la riallocazione per la procedura specifica. NO CLI consente di disabilitare esplicitamente l'autenticazione o la riallocazione PTMSI per una procedura, mentre REMOVE CLI consente di ripristinare la configurazione su uno stato in cui CLI (SET o NO) non è configurato. Si presume che tutte le configurazioni vengano RIMOSSE quando la struttura viene inizializzata nell'allocazione del profilo cc. Pertanto, REMOVE è la configurazione predefinita.

SET CLI influisce solo su una procedura specifica nella struttura, mentre NO CLI e REMOVE CLI influiscono sulla procedura corrente e anche su REMOVE the lower nodes. Inoltre, se NO CLI o REMOVE CLI ha effetto sull'albero comune, l'effetto deve essere propagato anche sui nodi corrispondenti negli alberi specifici dell'accesso.

Esistono due tipi di CLI per ogni configurazione della periodicità delle procedure: SET CLI e REMOVE CLI. Le istruzioni SET e REMOVE completate rispetto alla periodicità influiscono solo sulla configurazione della periodicità e non modificano la configurazione della frequenza. La configurazione NO CLI eseguita per la frequenza (per essere precisi, la configurazione NO CLI è comune in quanto non richiede argomenti di frequenza o periodicità, ma viene identificata internamente con la configurazione della frequenza durante l'archiviazione) e RIMUOVE anche la configurazione della periodicità.

Di seguito sono riportati alcuni scenari in cui l'autenticazione viene completata senza condizioni:

- Connessione IMSI (International Mobile Subscriber Identity) - tutti gli allegati IMSI sono autenticati
- se il sottoscrittore non è stato autenticato in precedenza e non si dispone di un vettore
- quando la firma PTMSI non corrisponde
- in caso di mancata corrispondenza del numero di sequenza della chiave di crittografia (CKSN)

Al momento, è possibile abilitare l'autenticazione per questi elementi nel profilo di controllo delle chiamate:

- attach, service-request, RAU, detach, short-messaging-service, all-events e TAU

- TAU è utilizzato da MME
- attach e service-request vengono utilizzati sia da SGSN che da MME
- gli altri sono utilizzati esclusivamente da SGSN

Blocchi di procedure di autenticazione SGSN e di firma PTMSI

In questa struttura vengono illustrati i blocchi di routine considerati da SGSN per le impostazioni della frequenza.

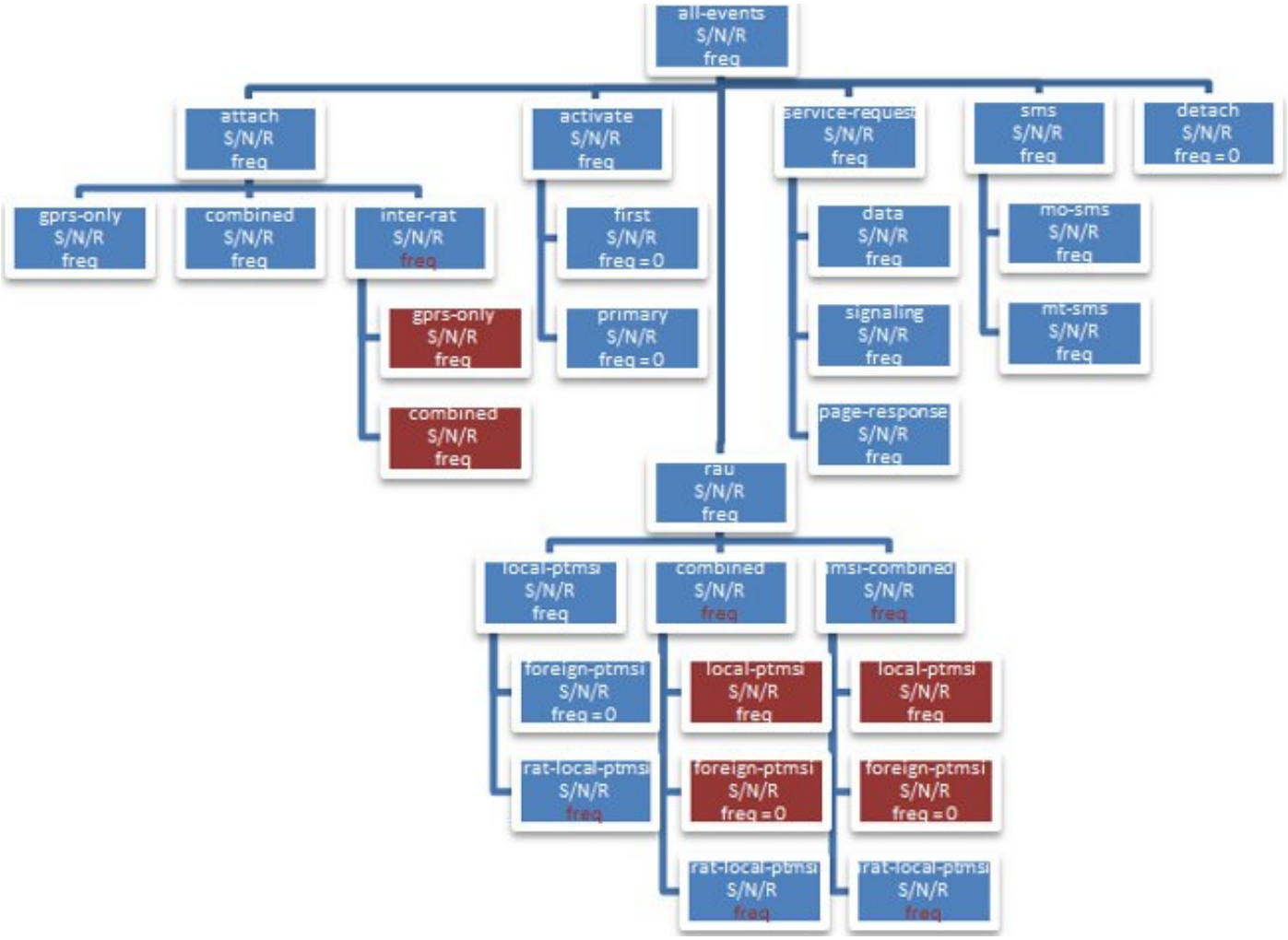

Figura 1: Blocchi di routine presi in considerazione da SGSN per le impostazioni di frequenza

Di seguito sono illustrate le strutture per la procedura di riallocazione PTMSI.

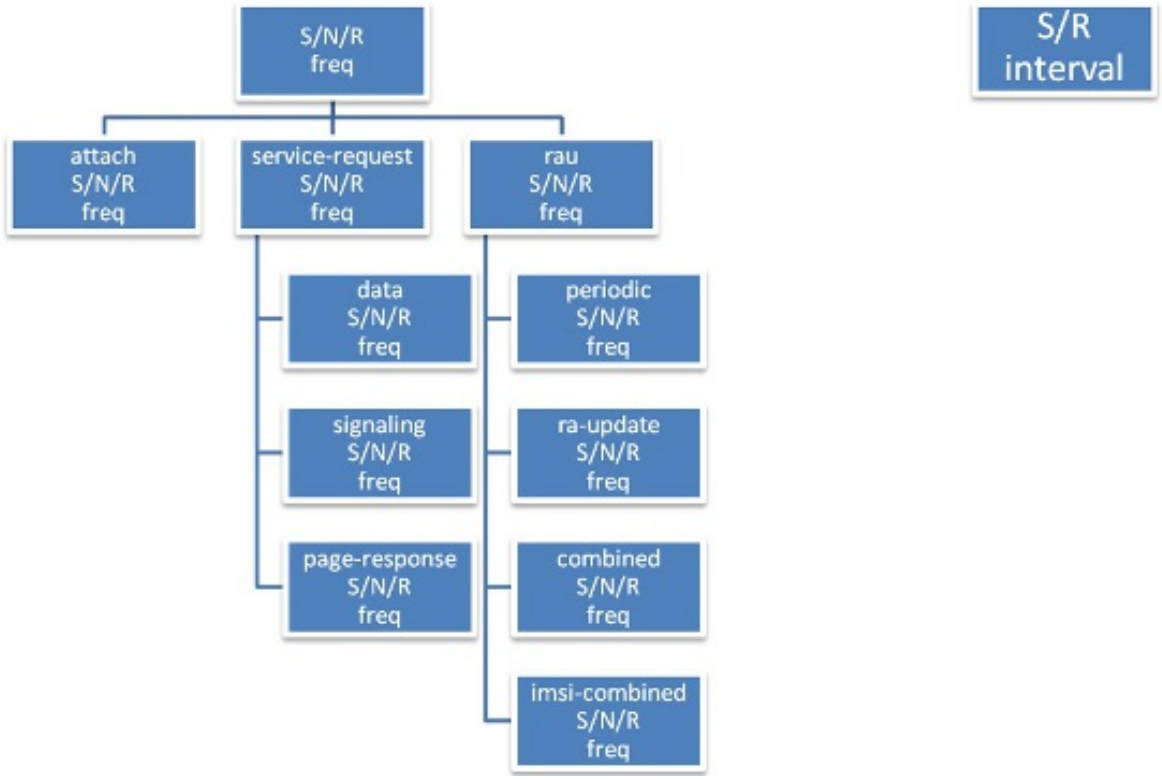

Figura 2: Albero configurazione autenticazione

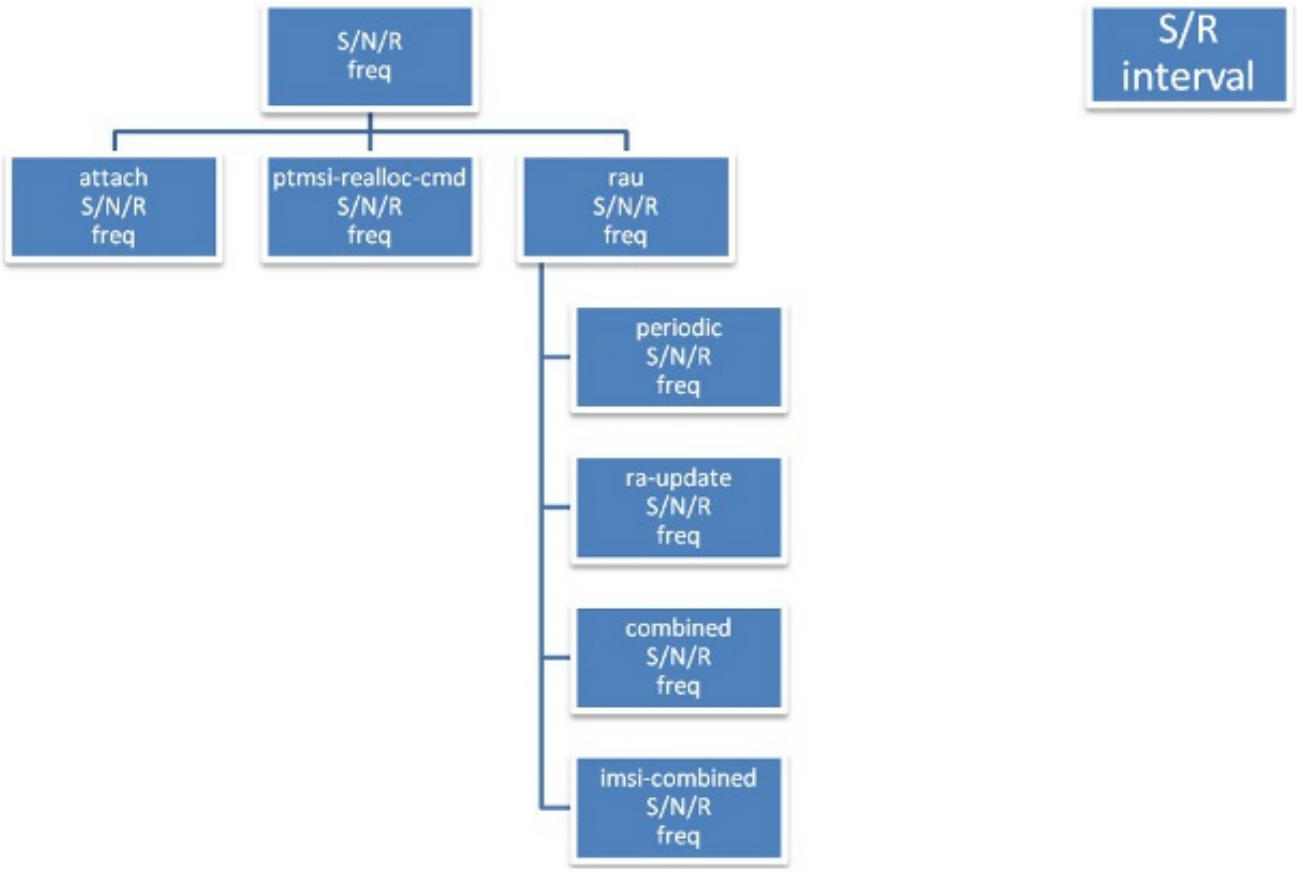

Figura 3: Albero di configurazione riallocazione PTMSI

Perché è necessaria l'autenticazione e la riallocazione della firma

PTMSI

In base alle specifiche tecniche 3GPP (TS) 23.060, sezione 6.5.2, passaggio 4, le funzioni di autenticazione sono definite nella clausola "Security Function". Se nella rete non esiste alcun contesto di Mobility Management (MM) per la stazione mobile (MS), l'autenticazione è obbligatoria. Le procedure di cifratura sono descritte nella clausola "Security Function". Se l'allocazione PTMSI verrà completata e la rete supporta la cifratura, la rete imposterà la modalità di cifratura.

Come accennato in precedenza, SGSN esegue l'autenticazione solo per le nuove richieste di registrazione, ad esempio le connessioni IMSI e le richieste RAU inter-SGSN, in alcuni flussi di chiamate in cui la convalida della firma PTMSI o della firma CKSN non corrisponde a quella archiviata. Ad esempio, non è necessario autenticare routine quali RAU periodica e intra-RAU, in quanto dispongono già di un database con un SGSN registrato. L'autenticazione qui è facoltativa. Non completare l'autenticazione non è sempre una buona cosa in quanto l'Apparecchiatura Utente (UE) può rimanere nella rete per giorni insieme senza eseguire una nuova richiesta di registrazione. È possibile che la configurazione del contesto di sicurezza tra SGSN e UE venga compromessa. È pertanto consigliabile eseguire periodicamente l'autenticazione e verificare la validità del sottoscrittore registrato in SGSN in base a una determinata frequenza. Questa condizione è spiegata in dettaglio in 3GPP 23.060, sezione 6.8.

Le funzioni di sicurezza e i relativi riferimenti si trovano nella sezione 6.8 della 33.102. Ad esempio, se l'autenticazione facoltativa è abilitata in base alle figure 18 e 19 della sezione 6.8 della 33.102 e SGSN tenta di autenticare l'UE con parametri di contesto di sicurezza non corretti, l'UE non sarà mai in grado di far corrispondere la risposta di invio (SRES) o la risposta prevista (XRES) con SGSN, il che comporta un nuovo collegamento alla rete. Ciò impedisce all'UE di rimanere nella rete con un database falso per un periodo di tempo più lungo.

Per consentire di nascondere l'identità, un SGSN genera un'identità temporanea per un IMSI denominato PTMSI. Una volta che il MS si collega, il SGSN invia un nuovo messaggio PTMSI al MS. Il server MS archivia quindi questo file PTMSI e lo utilizza per identificarsi nel file SGSN in ogni nuova connessione futura avviata. Poiché il protocollo PTMSI viene sempre fornito al sistema MS in una connessione cifrata, nessuno sarà in grado di mappare un IMSI al PTMSI esterno, anche se potrebbe vedere un messaggio di testo normale con IMSI in corso a volte. Ad esempio, la prima volta che un file IMSI viene collegato e riceve risposte di identità con un file IMSI.

La riallocazione PTMSI è spiegata in 3GPP 23.060, sezione 6.8 come procedura standalone. La stessa procedura può essere completata come parte di qualsiasi procedura di uplink per riallocare le firme PTMSI e PTMSI per proteggere le identità UE. In questo modo la segnalazione di rete su qualsiasi interfaccia non verrà aumentata. La riallocazione delle firme PTMSI e PTMSI è sempre valida in quanto queste sono le identità chiave assegnate da SGSN all'utente nella fase di registrazione iniziale. La riallocazione di questi valori in base a una certa frequenza aiuta SGSN a nascondere l'identità dell'UE con valori diversi per un tempo prolungato invece di utilizzare un solo valore PTMSI. La funzione di nascondere l'identità si riferisce all'occultamento di informazioni quali IMSI e IMEI degli Stati membri, quando i messaggi da/verso gli Stati membri sono ancora inviati in testo normale e quando la crittografia non è ancora iniziata.

Problema

In alcune reti di clienti è stato osservato che alcune identità chiave, ad esempio MSIDN/PTMSI,

vengono mescolate tra diversi abbonati e inviate in messaggi di segnalazione GTPC sull'interfaccia Gn e in Call Data Records (CDR).

Gli ID dei bug Cisco CSCut62632 e CSCuu67401 riguardano alcuni casi angolo di ripristino della sessione, in cui viene mappata l'identità di un sottoscrittore con un altro. Di seguito sono elencati tre casi. Tutti questi casi sono sottoposti a revisione del codice, analisi e riproduzione da parte del team di controllo qualità.

Scenario 1 (doppio errore in sessmgr che comporta la perdita delle identità del sottoscrittore)

UE1 - Attach - IMSI1 - MSISDN (Mobile Station International Subscriber Directory Number) 1 - PTMSI1 - Smgr#1

Doppio arresto dell'istanza di sessmgr. SGSN ha perso i dettagli UE1.

UE2 - Attach - IMSI2 - MSISDN 2 - PTMSI1 - Smgr#1

PTMSI1 viene riutilizzato per UE2.

UE1 - Intra RAU - PTMSI1- SGSN elabora questo uplink, poiché l'autenticazione per intra-RAU non è obbligatoria.

In questo modo vengono mescolati record di due sessioni diverse.

Scenario n. 2 (interruzione della parte applicativa TCAP (Transaction Capabilities Application Part) di una sessione che determina la combinazione di identità sottoscrittori)

UE1 - Attach - IMSI1 - UGL impostato (TCAP - interrotto internamente a causa di un arresto anomalo di sessmgr)

UE2 - Attach - IMSI2 - UGL inviato con lo stesso TCAP - OTID

RLN invia TCAP - continua dalla richiesta precedente, MSISDN di UE1

In questo caso, SGSN aggiorna il MSISDN errato di UE1 con UE2. In questo modo vengono mescolati record di due sessioni diverse.

Scenario n. 3 (interruzione di una sessione TCAP con conseguente combinazione delle identità dei sottoscrittori)

UE1 - Attach - IMSI1 - SAI inviato (TCAP - interrotto internamente a causa di un arresto di sessmgr)

UE2 - Attach - IMSI2 - SAI inviato con lo stesso TCAP - OTID

RLN invia TCAP - continua da richiesta precedente, vettori di autenticazione UE1 (triplette o quintuplette)

SGSN aggiorna i vettori di autenticazione errati di UE1 con UE2

In questo modo, SGSN utilizza vettori UE1 per l'autenticazione di UE2.

Approccio di stabilizzazione

Se l'autenticazione per intra-RAU è abilitata o la riallocazione PTMSI è abilitata, SGSN autentica il client con un set di vettori archiviato. Se UE è diverso da quello archiviato per, UE/SGSN non supererà la fase di autenticazione per procedere ulteriormente nella rete. In questo modo si riduce la possibilità che l'UE rimanga in rete con un database non corretto. Queste sono alcune aree note del codice. L'unità operativa continuerà ad analizzare un numero maggiore di casi per comprendere meglio questo problema.

Piano di correzione

Il modo migliore per risolvere il problema è tramite gli ID dei bug Cisco. Analizzare più aree di codice e distribuirle in nodi meno densi per il monitoraggio prima di utilizzarle in nodi ad alta densità.

Linee guida per la configurazione

L'abilitazione dell'autenticazione aumenta la segnalazione dell'interfaccia Gr e Iu in quanto SGSN deve recuperare il vettore di autenticazione impostato dal registro di località (RLN) ed eseguire procedure di autenticazione aggiuntive per l'accesso. Gli operatori devono fare attenzione a scegliere valori di frequenza che abbiano un impatto minore sulla rete.

Gli indicatori di prestazioni chiave (KPI) GPRS Mobility Management (GMM)/Mobile Application Protocol (MAP) sono importanti da analizzare prima di derivare i valori di frequenza per ogni procedura. In base agli indicatori KPI, verificare la procedura che viene eseguita in modo elevato. Per questa procedura, impostare valori elevati di frequenza. In questo modo è possibile ottimizzare ogni parametro in base a un modello di chiamata di rete.

Un modo ideale per configurare questi parametri consiste nell'impostare i valori sulle foglie, ma non alla radice della struttura. Ad esempio, la Figura 2 illustra la struttura di configurazione dell'autenticazione. Gli operatori possono scegliere di impostare il valore su un livello inferiore, come illustrato di seguito, anziché configurare direttamente la connessione di autenticazione.

```
authenticate attach attach-type gprs-only frequency 10
authenticate attach attach-type combined frequency 10
```

Èsempre consigliabile impostare valori di alta frequenza (unità come 10) e quindi monitorare le soglie di segnalazione dell'interfaccia Gr/Iu. Se il segnale rientra nei limiti, definire i valori finché il segnale non raggiunge un luogo sicuro vicino alle soglie che l'operatore desidera impostare per le proprie reti.

Impostare la frequenza sulle varie procedure in 20/30 e portarle a 5-10 con un attento monitoraggio sul traffico dell'interfaccia esterna. È necessario verificare l'impatto sulla CPU della memoria di linkmgr e sessmgr con questo carico in eccesso.

La riallocazione delle firme PTMSI e PTMSI non causerà la punta di segnalazione diretta, ma è sempre importante impostare valori di frequenza elevati in modo che le PTMSI siano disponibili con le istanze di sessmgr (cosa che accade raramente). Si sconsiglia di modificare il protocollo PTMSI per ogni procedura di uplink dall'UE, poiché questa non è la procedura ottimale. Un valore di 10 potrebbe essere decente. Dopo tutte queste modifiche è importante monitorare ed eseguire

controlli di integrità standard sul sistema.

Ad esempio:

```
Authentication:

authenticate attach ( we can still fine tune this based on KPIs of
Inter RAT attach & attach type).

authenticate rau update-type periodic frequency 10

authenticate rau update-type ra-update frequency 5



PTMSI & PTMSI signature allocation:

ptmsi-reallocate attach

ptmsi-reallocate routing-area-update update-type ra-update

ptmsi-signature-reallocate attach frequency 10

ptmsi-signature-reallocate routing-area-update frequency 20

ptmsi-reallocate routing-area-update update-type periodic frequency 10
```

Risoluzione dei problemi

Quando si esegue l'autenticazione o si alloca la firma PTMSI o PTMSI, i registri di debug vengono stampati per comprendere il motivo per cui la procedura è stata completata. In questo modo è possibile risolvere eventuali discrepanze. Questi registri includono la configurazione dal profilo cc e il valore corrente di tutti i contatori, nonché lo spostamento della logica di decisione tramite i vari contatori e configurazioni. Inoltre, i valori del contatore correnti per sottoscrittore possono essere visualizzati con i comandi **show subscribers sgsn-only** o **show subscribers gprs-only**.

Viene fornito un output di esempio. I contatori correnti e l'ultimo timestamp autenticato vengono aggiunti all'output completo del comando **show subscribers**.

```
[local]# show subscribers sgsn-only full all
.
.
.
DRX Parameter:
Split PG Cycle Code: 7
SPLIT on CCCH: Not supported by MS
Non-DRX timer: max. 8 sec non-DRX mode after Transfer state
CN Specific DRX cycle length coefficient: Not specified by MS
Authentication Counters
Last authenticated timestamp : 1306427164
Auth all-events UMTS : 0 Auth all-events GPRS : 0
Auth attach common UMTS : 0 Auth attach common GPRS : 0
Auth attach gprs-only UMTS : 0 Auth attach gprs-only GPRS : 0
Auth attach combined UMTS : 0 Auth attach combined GPRS : 0
Auth attach irat UMTS : 0 Auth attach irat GPRS : 0
Auth attach irat-gprs-only UMTS : 0 Auth attach irat-gprs-only GPRS : 0
```

```
Auth attach irat-combined UMTS : 0 Auth attach irat-combined GPRS : 0
Auth UMTS : 0 Auth GPRS : 0
Auth serv-req : 0 Auth serv-req data : 0
Auth serv-req signaling : 0 Auth serv-req page-rsp : 0
Auth rau UMTS : 0 Auth rau GPRS : 0
Auth rau periodic UMTS : 0 Auth rau periodic GPRS : 0
Auth rau ra-upd UMTS : 0 Auth rau ra-upd GPRS : 0
Auth rau ra-upd lcl-ptmsi UMTS : 0 Auth rau ra-upd lcl-ptmsi GPRS : 0
Auth rau ra-upd irat-lcl-ptmsi UMTS : 0 Auth rau ra-upd irat-lcl-ptmsi GPRS : 0
Auth rau comb UMTS : 0 Auth rau comb GPRS : 0
Auth rau comb lcl-ptmsi UMTS : 0 Auth rau comb lcl-ptmsi GPRS : 0
Auth rau comb irat-lcl-ptmsi UMTS : 0 Auth rau comb irat-lcl-ptmsi GPRS : 0
Auth rau imsi-comb UMTS : 0 Auth rau imsi-comb GPRS : 0
Auth rau imsi-comb lcl-ptmsi UMTS : 0 Auth rau imsi-comb lcl-ptmsi GPRS : 0
Auth rau imsi-comb irat-lcl-ptmsi UMTS: 0 Auth rau imsi-comb irat-lcl-ptmsi GPRS: 0
Auth sms UMTS : 0 Auth sms GPRS : 0
Auth sms mo-sms UMTS : 0 Auth sms mo-sms GPRS : 0
Auth sms mt-sms UMTS : 0 Auth sms mt-sms UMTS : 0
PTMSI Realloc Counters
Last allocated timestamp : 1306427165
PTMSI Realloc Freq UMTS : 0 PTMSI Realloc Freq GPRS : 0
PTMSI Realloc Attach UMTS : 0 PTMSI Realloc Attach GPRS : 0
PTMSI Realloc Serv-Req : 0 PTMSI Realloc Serv-Req Data : 0
PTMSI Realloc Serv-Req Signaling : 0 PTMSI Realloc Serv-Req Page-rsp : 0
PTMSI Realloc Rau UMTS : 0 PTMSI Realloc Rau GPRS : 0
PTMSI Realloc Rau Periodic UMTS : 0 PTMSI Realloc Rau Periodic GPRS : 0
PTMSI Realloc Rau Ra-Upd UMTS : 0 PTMSI Realloc Rau Ra-Upd GPRS : 0
PTMSI Realloc Rau Comb-Upd UMTS : 0 PTMSI Realloc Rau Comb-Upd GPRS : 0
PTMSI Realloc Rau Imsi-Comb-Upd UMTS : 0 PTMSI Realloc Rau Imsi-Comb-Upd GPRS : 0
PTMSI Sig Realloc Counters
Last allocated timestamp : 0
PTMSI Sig Realloc Freq UMTS : 0 PTMSI Sig Realloc Freq GPRS : 0
PTMSI Sig Realloc Attach UMTS : 0 PTMSI Sig Realloc Attach GPRS : 0
PTMSI Sig Realloc Ptmsi-rel-cmd UMTS : 0 PTMSI Sig Realloc Ptmsi-rel-cmd GPRS : 0
PTMSI Sig Realloc Rau UMTS : 0 PTMSI Sig Realloc Rau GPRS : 0
PTMSI Sig Realloc Rau Periodic UMTS : 0 PTMSI Sig Realloc Rau Periodic GPRS : 0
PTMSI Sig Realloc Rau Ra-Upd UMTS : 0 PTMSI Sig Realloc Rau Ra-Upd GPRS : 0
PTMSI Sig Realloc Rau Comb-Upd UMTS : 0 PTMSI Sig Realloc Rau Comb-Upd GPRS : 0
PTMSI Sig Realloc Rau Imsi-Comb UMTS : 0 PTMSI Sig Realloc Rau Imsi-Comb GPRS : 0
CAE Server Address:
Subscription Data:
.
.
```

Se il problema si verifica nella rete, immettere questi comandi per raccogliere informazioni che la Business Unit deve utilizzare per analizzare ulteriormente il problema:

```
show subscribers gprs-only full msisdn <msisdn>
show subscribers gprs-only full imsi <imsi>
show subscribers sgsn-only msisdn <msisdn>
show subscribers sgsn-only msisdn <imsi>
show subscribers gprs-debug-info callid <callid> (get o/p for both callid)
show subscribers debug-info callid <callid> (get o/p for both callid)
task core facility sessmgr instance < >
task core facility imsimgr instance < >
Mon sub using MSISDN or pcap traces
SSD during issue.
Syslogs during the issue.
```

Rischi

Aumento del segnale verso le interfacce Gr/Iu e leggero impatto sulla CPU del processo interno (linkmgr) se si esegue l'autenticazione troppo frequentemente.

Sintassi dei comandi

Tutti i comandi sono in modalità configurazione/controllo chiamate-profilo e vengono applicati i privilegi dell'operatore. Di seguito è riportata un'istantanea dei comandi del profilo cc:

```
Authentication
1. Attach
authenticate attach {inter-rat} {attach-type [gprs-only | combined ]}
{frequency <1..16>} {access-type [umts | gprs]}
no authenticate attach {inter-rat} {attach-type [gprs-only | combined ]}
{access-type [umts | gprs]}
remove authenticate attach {inter-rat} {attach-type [gprs-only | combined ]}
{access-type [umts | gprs]}

2. Service-request
authenticate service-request {service-type [data | signaling | page-response]}
{frequency <1..16> | periodicity <1..10800>}
no authenticate service-request {service-type [data | signaling | page-response]}
remove authenticate service-request {service-type [data | signaling | page-response]}
{periodicity}
3. Rau
authenticate rau {update-type periodic} {frequency <1..16> | periodicity <1..10800>}
{access-type [umts | gprs]}
authenticate rau {update-type [ra-update | combined-update | imsi-combined-update]}
{with [local-ptmsi | inter-rat-local-ptmsi]} {frequency <1..16> |
periodicity <1..10800>}
{access-type [umts| gprs]}
authenticate rau {update-type [ra-update | combined-update | imsi-combined-update]}
{with foreign-ptmsi} {access-type [umts| gprs]}
no authenticate rau {update-type periodic} {access-type [umts | gprs]}
no authenticate rau {update-type [ra-update | combined-update | imsi-combined-update]}
{with [local-ptmsi | inter-rat-local-ptmsi | foreign-ptmsi]}
{access-type [umts| gprs]}
remove authenticate rau {update-type periodic} {periodicity}
{access-type [umts | gprs]}
remove authenticate rau {update-type [ra-update | combined-update |
imsi-combined-update]}
{with [local-ptmsi | inter-rat-local-ptmsi]} { periodicity} {access-type [umts| gprs]}
remove authenticate rau {update-type [ra-update | combined-update |
imsi-combined-update]}
{with foreign-ptmsi} {access-type [umts| gprs]}
4. Sms
authenticate sms {sms-type [mo-sms | mt-sms]} {frequency <1..16>}
{access-type [umts | gprs]}
no authenticate sms {sms-type [mo-sms | mt-sms]} {access-type [umts | gprs]}
remove authenticate sms {sms-type [mo-sms | mt-sms]} {access-type [umts | gprs]}
5. Detach
authenticate detach {access-type [umts | gprs]}
no authenticate detach {access-type [umts | gprs]}
remove authenticate detach {access-type [umts | gprs]}
6. All-events
authenticate all-events {frequency <1..16>} {access-type [umts | gprs]}
no authenticate all-events {access-type [umts | gprs]}
remove authenticate all-events {access-type [umts | gprs]}

PTMSI Reallocation
```

1. **Attach**

```
ptmsi-reallocate attach {frequency <1..50>} {access-type [umts | gprs]}
no ptmsi-reallocate attach {access-type [umts | gprs]}
remove ptmsi-reallocate attach {access-type [umts | gprs]}
```

2. **Service-request**

```
ptmsi-reallocate service-request {service-type [data | signaling | page-response]}
{frequency <1..50>} no ptmsi-reallocate service-request
{service-type [data | signaling | page-response]}
remove ptmsi-reallocate service-request {service-type [data | signaling |
page-response]}
```

3. **Routing-area-update**

```
ptmsi-reallocate routing-area-update {update-type [periodic | ra-update |
combined-update | imsi-combined-update]} {frequency <1..50>}
{access-type [umts | gprs]}
no ptmsi-reallocate routing-area-update {update-type [periodic | ra-update |
combined-update | imsi-combined-update]} {access-type [umts | gprs]}
remove ptmsi-reallocate routing-area-update {update-type [periodic | ra-update |
combined-update | imsi-combined-update]} {access-type [umts | gprs]}
```

4. **Interval/frequency**

```
ptmsi-reallocate [interval <60..1440> | frequency <1..50>] {access-type [umts | gprs]}
no ptmsi-reallocate [interval | frequency] {access-type [umts | gprs]}
remove ptmsi-reallocate [interval | frequency] {access-type [umts | gprs]}
```

PTMSI-Signature Reallocation

1. Attach

```
ptmsi-signature-reallocate attach {frequency <1..50>} {access-type [umts | gprs]}
no ptmsi-signature-reallocate attach {access-type [umts | gprs]}
remove ptmsi-signature-reallocate attach {access-type [umts | gprs]}
```

2. PTMSI Reallocation command

```
ptmsi-signature-reallocate ptmsi-reallocation-command {frequency <1..50>}
{access-type [umts | gprs]}
no ptmsi-signature-reallocate ptmsi-reallocation-command {access-type [umts | gprs]}
remove ptmsi-signature-reallocate ptmsi-reallocation-command
{access-type [umts | gprs]}
```

3. Routing-area-update

```
ptmsi-signature-reallocate routing-area-update {update-type [periodic | ra-update |
combined-update | imsi-combined-update]} {frequency <1..50>}
{access-type [umts | gprs]}
no ptmsi-signature-reallocate routing-area-update {update-type [periodic | ra-update |
combined-update | imsi-combined-update]} {access-type [umts | gprs]}
remove ptmsi-signature-reallocate routing-area-update {update-type [periodic |
ra-update | combined-update | imsi-combined-update]} {access-type [umts | gprs]}
```

4. Interval/frequency

```
ptmsi-signature-reallocate [interval <60..1440> | frequency <1..50>]
{access-type [umts | gprs]}
no ptmsi-signature-reallocate [interval | frequency] {access-type [umts | gprs]}
remove ptmsi-signature-reallocate [interval | frequency] {access-type [umts | gprs]}
```