Best Practices für die SGSN-Authentifizierung und PTMSI-Neuzuweisung der Serie ASR 5x00

Inhalt

Einführung

Dieses Dokument bietet eine grundlegende Erläuterung der Vorteile der Frequenzkonfiguration des Authentifizierungsverfahrens, der Packet Temporary Mobile Subscriber Identity (PTMSI) und der Neuzuordnung der PTMSI-Signaturen. Dieses Dokument ist speziell für ein optionales Projekt-Mobilitätsmanagement der dritten Generation für 2G und 3G für den GPRS Support Node (SGSN) bestimmt, das auf Aggregated Service Router (ASR) der Serie 5000 ausgeführt wird.

In diesem Dokument werden folgende Best Practices erläutert:

- Einstellung der Authentifizierungshäufigkeit
- PTMSI-Neuzuordnung
- Neuzuordnung von PTMSI-Signaturen
- Die Auswirkung, wenn Sie die Einstellung für die Authentifizierungshäufigkeit und die PTMSI-Neuzuweisung und die Signaturneuzuordnung nicht konfigurieren (basierend auf Erfahrungen aus Kundenfällen)
- Konfigurationsrichtlinien und Auswirkungen auf externe Schnittstellen
- Optionen zur Fehlerbehebung

Übersicht

Das Authentifizierungs-, PTMSI- und PTMSI-Signaturzuordnungsframework im Anrufsteuerungsprofil ermöglicht es dem Betreiber, die Authentifizierung oder Zuweisung der PTMSI- und PTMSI-Signatur pro Teilnehmer im 2G- und 3G-SGSN sowie im Mobile Management

Entity (MME) zu konfigurieren. Im SGSN kann derzeit die Authentifizierung für diese Verfahren konfiguriert werden - für das Anhängen, die Service-Anfrage, das Routing-Area-Update (RAU), den Short Messaging-Service und das Trennen.

Die MME verwendet auch dasselbe Framework, um die Authentifizierung für Service-Anfragen und Tracking-Area-Updates (TAUs) zu konfigurieren. Die PTMSI-Neuzuordnung kann für das Anschließen, die Serviceanfrage und die RAUs konfiguriert werden. Die Neuzuordnung der PTMSI-Signatur kann für das Anfügen, den PTMSI-Befehl zur Neuzuordnung und RAUs konfiguriert werden. Authentifizierung und Neuzuordnung können für jede Instanz dieser Prozeduren oder für jede zweite Instanz der Prozedur aktiviert werden, die als selektive Authentifizierung/Neuzuordnung bezeichnet wird. Bestimmte Verfahren unterstützen auch die Aktivierung der Authentifizierung oder Neuzuordnung basierend auf der Zeit, die seit der letzten Authentifizierung bzw. Neuzuweisung verstrichen ist (Periodizität oder Intervall).

Darüber hinaus können diese speziell für UMTS (Universal Mobile Telecommunications System) (3G) oder General Packet Radio Service (GPRS) (2G) oder beide konfiguriert werden. Diese Konfiguration wird nur geprüft, wenn es für den SGSN optional ist, die PTMSI/PTMSI-Signatur eines Teilnehmers zu authentifizieren oder neu zuzuweisen. In Szenarien, in denen diese Prozeduren obligatorisch sind, wird diese Konfiguration nicht überprüft.

Für die Frequenzkonfiguration jeder Prozedur gibt es drei CLI-Typen - eine SET-CLI, eine NO-CLI und eine REMOVE-CLI. Wenn Sie eine SET-CLI aufrufen, möchte der Operator die Authentifizierung oder Neuzuordnung für die spezifische Prozedur aktivieren. Die NO-CLI besteht darin, die Authentifizierung oder die PTMSI-Neuzuordnung für eine Prozedur explizit zu deaktivieren, und die REMOVE-CLI besteht darin, die Konfiguration auf einen Zustand wiederherzustellen, in dem die CLI (SET oder NO) überhaupt nicht konfiguriert ist. Es wird davon ausgegangen, dass alle Konfigurationen ENTFERNT werden, wenn die Struktur in der cc-Profilzuordnung initialisiert wird. Daher ist REMOVE die Standardkonfiguration.

Die SET-CLI betrifft nur eine bestimmte Prozedur in der Struktur, während die CLI NO CLI und REMOVE die aktuelle Prozedur beeinflusst und auch die unteren Knoten ENTFERNT. Falls KEINE CLI oder REMOVE CLI die Common Tree beeinflusst, wird der Effekt auch auf die entsprechenden Knoten in den zugriffsspezifischen Trees übertragen.

Für die Periodizitätskonfiguration jeder Prozedur gibt es zwei Arten von CLIs: die SET-CLI und die REMOVE-CLI. Die gemäß Periodizität abgeschlossenen SET- und ENTFERNUNGEN wirken sich nur auf die Periodizitätskonfiguration aus und lassen die Frequenzkonfiguration unberührt. Die für die Frequenz ausgeführte NO CLI (genauer gesagt, die NO CLI ist üblich, da sie keine Frequenz- oder Periodizitätsargumente verwendet, aber mit der Frequenzkonfiguration intern während der Speicherung identifiziert wird) löscht auch die Periodizitätskonfiguration.

In den folgenden Szenarien wird die Authentifizierung bedingungslos abgeschlossen:

- International Mobile Subscriber Identity (IMSI) Attach - alle IMSI-Anhänge werden authentifiziert
- wenn der Abonnent noch nicht authentifiziert wurde und Sie keinen Vektor haben
- wenn eine PTMSI-Signatur-Diskrepanz vorliegt
- wenn eine CKSN-Diskrepanz (Ciphering Key Sequence Number) vorliegt.

Derzeit kann die Authentifizierung für diese unter dem Anrufsteuerungsprofil aktiviert werden:

- Attach, Service Request, RAU, Distach, Short Messaging-Service, All-Events und TAU
- TAU wird von MME verwendet

- Das Hinzufügen und die Serviceanfrage werden von SGSN und MME verwendet.
- der Rest wird ausschließlich von SGSN verwendet.

SGSN-Authentifizierung und PTMSI-Signaturprozedurblöcke

Diese Baumstruktur erläutert die Verfahrensblöcke, die SGSN für die Frequenzeinstellungen berücksichtigt.

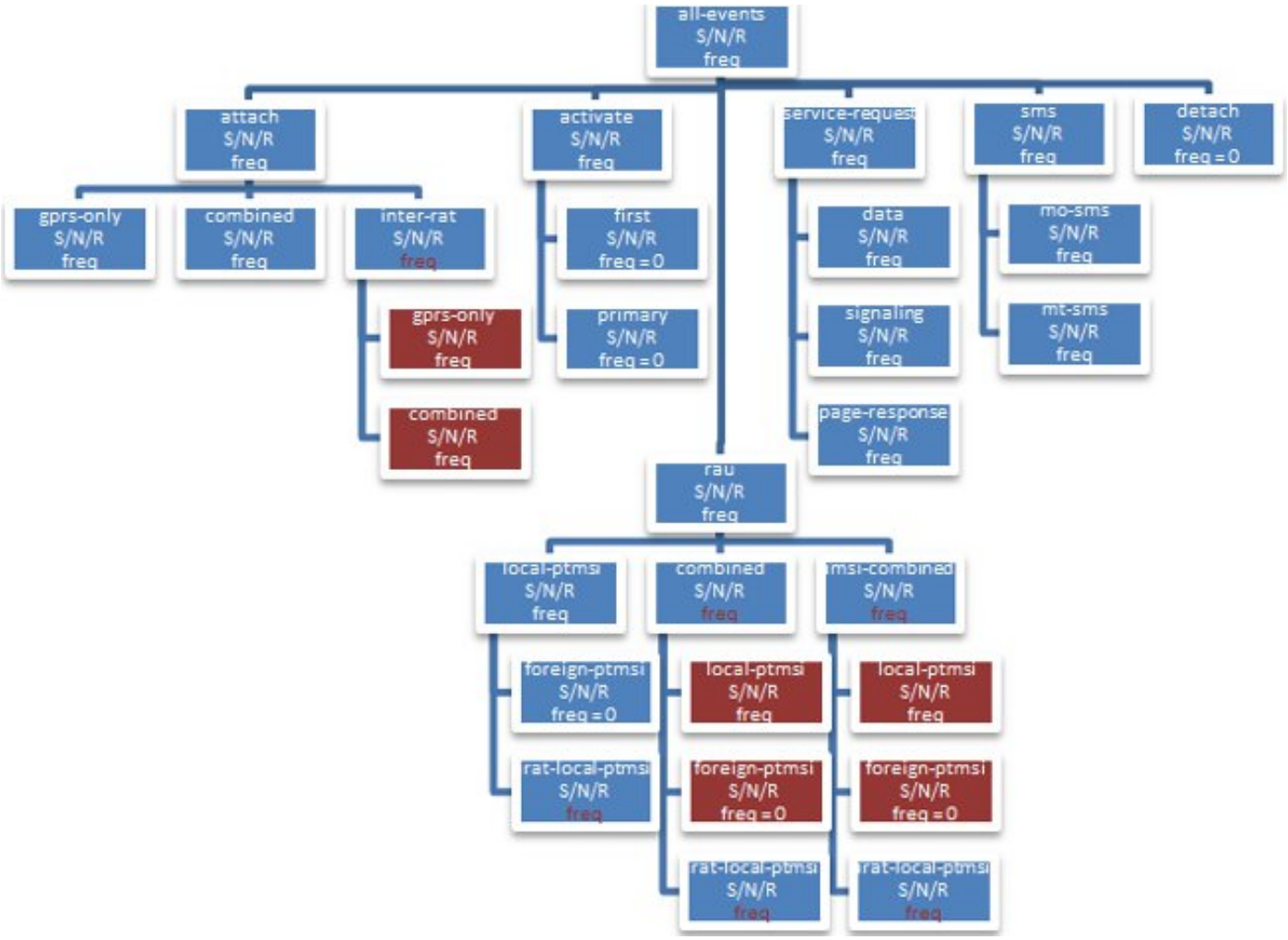

Abbildung 1: Prozedurblöcke SGSN berücksichtigt Frequenzeinstellungen

Die Strukturen für das PTMSI-Neuzuordnungsverfahren sind hier dargestellt.

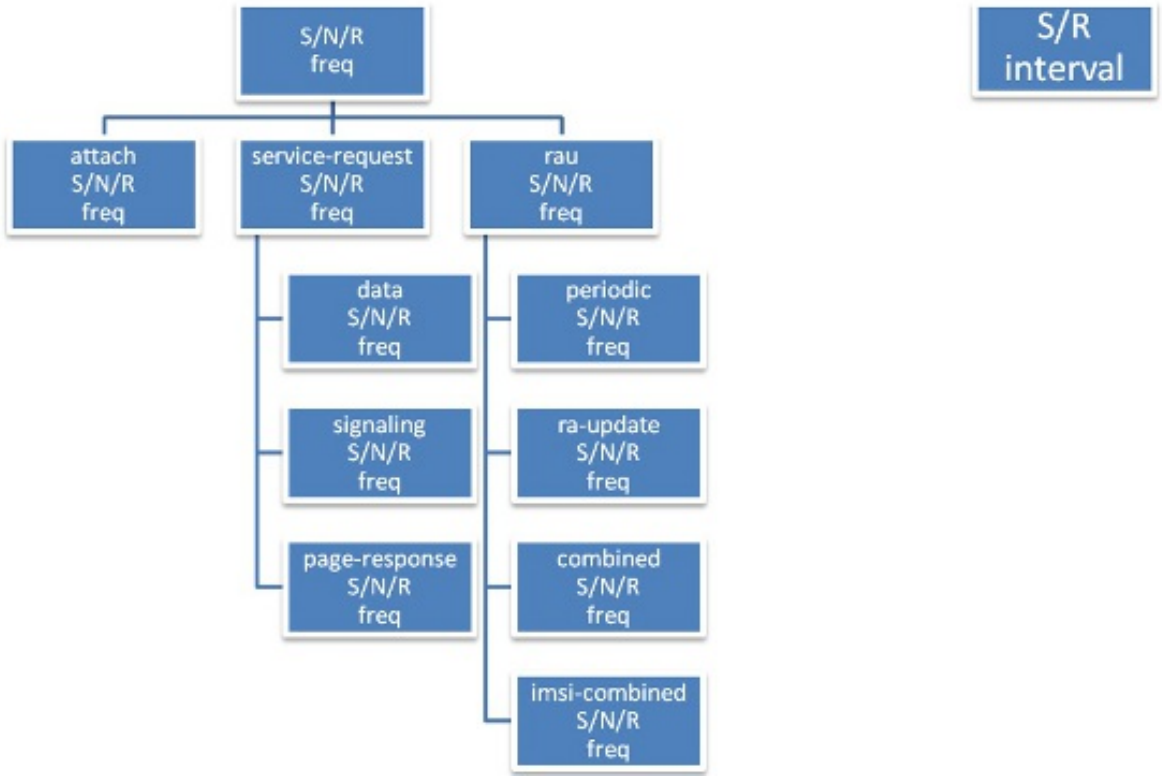

Abbildung 2: Konfigurationsstruktur für die Authentifizierung

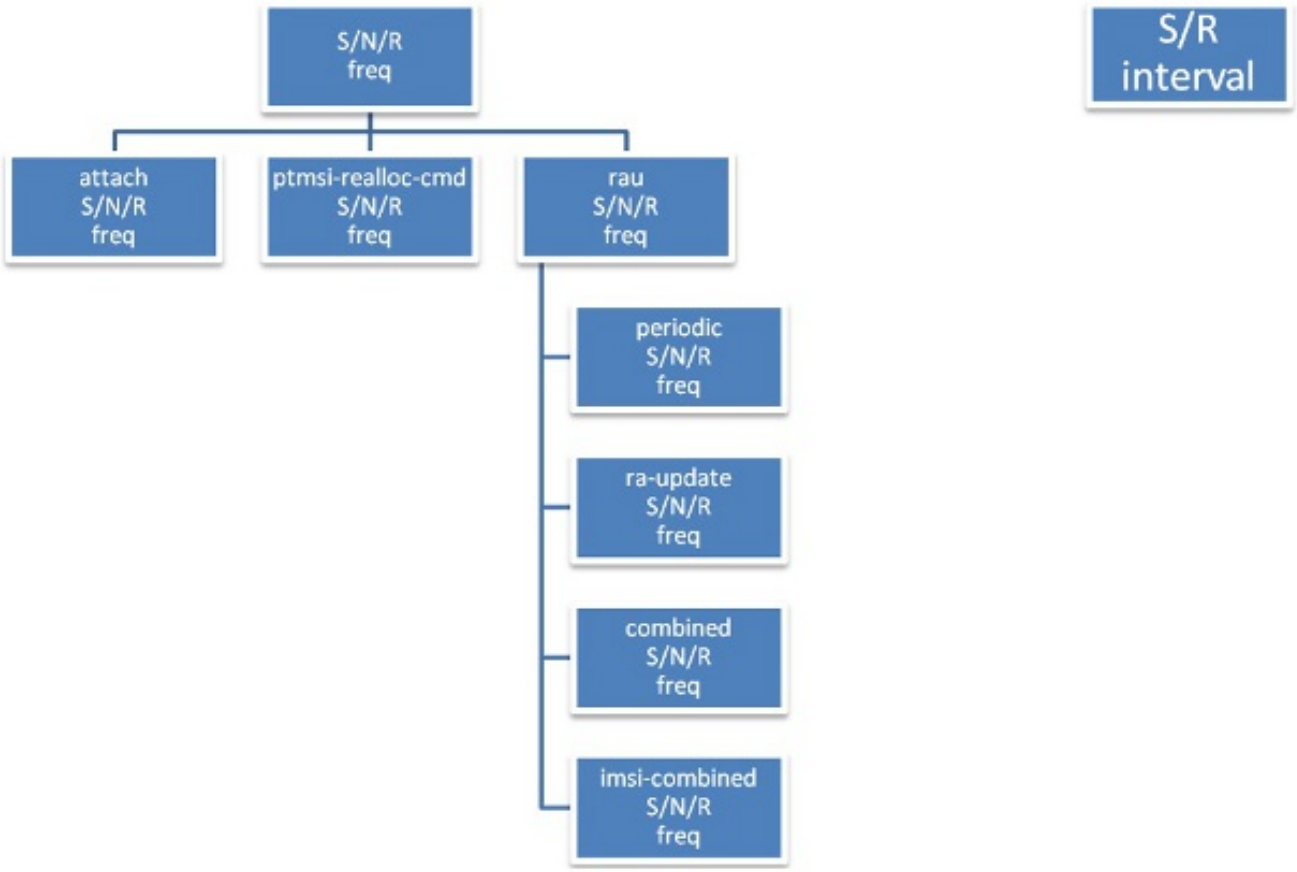

Abbildung 3: Konfigurationsstruktur für die PTMSI-Neuzuweisung

Warum eine Neuzuweisung von Authentifizierung und PTMSI-

Signaturen erforderlich ist

Gemäß 3GPP Technical Specifications (TS) 23.060, Abschnitt 6.5.2, Schritt 4, sind die Authentifizierungsfunktionen in der Klausel "Security Function" definiert. Wenn im Netzwerk kein Mobility Management (MM)-Kontext für die Mobile Station (MS) vorhanden ist, ist eine Authentifizierung erforderlich. Die Verschlüsselungsverfahren werden in Abschnitt "Sicherheitsfunktion" beschrieben. Wenn die PTMSI-Zuweisung abgeschlossen wird und das Netzwerk das Abfangen unterstützt, muss das Netzwerk den Ableitungsmodus festlegen.

Wie bereits erwähnt, führt SGSN eine Authentifizierung nur für neue Registrierungsanfragen wie IMSI-Anhänge und SGSN-übergreifende RAUs in einigen Anrufabläufen durch, bei denen die Validierung der PTMSI-Signatur oder des CKSN nicht mit der gespeicherten Signatur übereinstimmt. Beispielsweise müssen Verfahren wie periodische RAUs und interne RAUs nicht authentifiziert werden, da sie bereits über eine bestehende Datenbank mit einem registrierten SGSN verfügen. Die Authentifizierung ist hier optional. Wenn die Authentifizierung nicht abgeschlossen wird, kann die Benutzerausrüstung (UE) tagelang im Netzwerk verbleiben, ohne dass eine neue Registrierungsanfrage durchgeführt wird. Es besteht die Gefahr, dass die Sicherheitskontextualisierung zwischen dem SGSN und der EU beeinträchtigt wird. Daher ist es immer gut, die Gültigkeit des im SGSN registrierten Teilnehmers regelmäßig anhand einer bestimmten Häufigkeit zu authentifizieren und zu überprüfen. Dies wird ausführlich in Abschnitt 6.8 von 3GPP 23.060 erläutert.

Sicherheitsfunktionen und zugehörige Referenzen finden Sie in 33.102, Abschnitt 6.8. Wenn beispielsweise die optionale Authentifizierung auf der Grundlage der Abbildungen 18 und 19 in Abschnitt 6.8 von 33.102 aktiviert ist und das SGSN versucht, das UE mit falschen Sicherheitskontext-Parametern zu authentifizieren, kann die EU die Send Response (SRES) oder Expected Response (XRES) niemals mit dem SGSN abgleichen, was zu einer erneuten Verbindung mit dem Netzwerk führt. Dadurch wird verhindert, dass die EU länger mit einer falschen Datenbank im Netzwerk verbleibt.

Um Identitätshinweise bereitzustellen, generiert ein SGSN eine temporäre Identität für eine IMSI, die PTMSI genannt wird. Sobald die MS angeschlossen ist, gibt der SGSN ein neues PTMSI an die MS aus. Anschließend speichert der MS diese PTMSI und identifiziert sich mit dem SGSN in einer neuen zukünftigen Verbindung. Da die PTMSI immer in einer vorgegebenen Verbindung an die MS übergeben wird, ist es niemandem möglich, einen IMSI außerhalb der PTMSI anzuordnen, auch wenn zuweilen eine Klartext-Meldung mit IMSI auftritt. (Zum Beispiel, wenn ein IMSI zum ersten Mal eine IMSI-Einheit anhängt und Identitätsantworten mit einem IMSI-System ausgibt).

Die PTMSI-Neuzuordnung wird in 3GPP 23.060, Abschnitt 6.8 als eigenständiges Verfahren erläutert. Dasselbe kann als Teil eines Uplink-Verfahrens ausgeführt werden, um PTMSI- und PTMSI-Signaturen neu zuzuweisen und so die UE-Identitäten zu schützen. Dadurch wird die Netzwerksignalisierung an keiner Schnittstelle erhöht. Die Neuzuordnung von PTMSI- und PTMSI-Signaturen ist immer gut, da dies die wichtigsten Identitäten sind, die das SGSN der EU im ersten Registrierungsschritt zuweist. Durch die Neuzuweisung dieser Werte basierend auf einer bestimmten Frequenz kann der SGSN die Identität der EU mit unterschiedlichen Werten für einen längeren Zeitraum verbergen, anstatt nur einen PTMSI-Wert zu verwenden. Identitätsverbergen bezieht sich auf das Verbergen von Informationen wie IMSI und IMEI der MS, wenn Nachrichten von/an den MS noch im Klartext gesendet werden und die Verschlüsselung noch nicht begonnen hat.

Problem

In einigen Kundennetzwerken wurde beobachtet, dass einige Schlüsselidentitäten wie MSIDN/PTMSI zwischen verschiedenen Teilnehmern gemischt und in GTPC-Signalisierungsnachrichten an der Gn-Schnittstelle und in Call Data Records (CDRs) gesendet werden.

Die Cisco Bug-IDs CSCut62632 und CSCuu67401 behandeln einige Ecken der Sitzungswiederherstellung, die die Identität eines Teilnehmers einem anderen zuordnen. Nachfolgend sind drei Fälle aufgeführt. Alle diese Fälle werden vom Qualitätssicherungsteam analysiert und reproduziert.

Szenario Nr. 1 (Doppelter Fehler bei Sessmgr, der zum Verlust der Teilnehmernummer führt)

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

Double kill der sessmgr-Instanz. SGSN hat UE1-Details verloren.

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

PTMSI1 wird für UE2 wiederverwendet.

UE1 - Intra-RAU - PTMSI1- SGSN verarbeitet diesen Uplink, da die Authentifizierung für das Intra-RAU nicht obligatorisch ist.

Dies führt dazu, dass Datensätze von zwei verschiedenen Sitzungen gemischt werden.

Szenario Nr. 2 (Transaction Capabilities Application Part (TCAP): Abbruch einer Sitzung, bei der die Teilnehmeridentitäten vermischt werden)

UE1 - Attach - IMSI1 - UGL-Satz (TCAP - intern abgebrochen aufgrund von Sessmgr-Absturz)

UE2 - Attach - IMSI2 - UGL mit demselben TCAP - OTID gesendet

HLR sendet TCAP - Fortsetzung der vorherigen Anfrage, UD1 MSISDN

SGSN aktualisiert in diesem Fall die falsche MSISDN von UE1 mit UE2. Dies führt dazu, dass Datensätze von zwei verschiedenen Sitzungen gemischt werden.

Szenario 3 (TCAP-Abbruch einer Sitzung, die zur Vermischung von Teilnehmeridentitäten führt)

UE1 - Attach - IMSI1 - SAI gesendet (TCAP - intern abgebrochen aufgrund von Sessmgr-Absturz)

UE2 - Anhang - IMSI2 - SAI mit demselben TCAP - OTID gesendet

HLR sendet TCAP - Fortsetzung der vorherigen Anfrage mit Authentifizierungsvektoren von UE1 (Triplets oder Fünftel)

SGSN aktualisiert die falschen Authentifizierungsvektoren von UE1 mit UE2

Dies führt dazu, dass SGSN UE1-Vektoren für die Authentifizierung von UE2 verwendet.

Stabilisierungsansatz

Wenn die Authentifizierung für die RAU-interne Authentifizierung aktiviert oder die PTMSI-Neuzuordnung aktiviert ist, authentifiziert SGSN den Client mit einem gespeicherten Vektorsatz. Wenn die UE von der gespeicherten UE abweicht, durchläuft UE/SGSN die Authentifizierungsphase nicht, um im Netzwerk weiter fortzufahren. Dadurch sinkt die Wahrscheinlichkeit, dass die EU mit einer falschen Datenbank im Netzwerk verbleibt. Dies sind einige bekannte Bereiche im Code. Der Geschäftsbereich wird weitere Fälle analysieren, um dieses Problem besser zu verstehen.

Plan beheben

Die Behebung der Fehler-IDs von Cisco ist ein Best Effort-Ansatz. Analysieren Sie mehr Codebereiche, und stellen Sie diesen in einem weniger dichten Knoten für die Überwachung bereit, bevor Sie ihn zu einem Knoten mit hoher Dichte bringen.

Konfigurationsrichtlinien

Durch die Aktivierung der Authentifizierung wird die Gr- und Iu-Schnittstellensignalisierung erhöht, da das SGSN den Authentifizierungsvektor-Satz aus dem Home Location Register (HLR) abrufen und zusätzliche Authentifizierungsverfahren für den Zugriff durchführen muss. Betreiber müssen sorgfältig Frequenzwerte auswählen, die sich weniger auf das Netzwerk auswirken.

GPRS Mobility Management (GMM)/Mobile Application Protocol (MAP) Key Performance Indicators (KPIs) müssen analysiert werden, bevor Frequenzwerte für jede Prozedur abgeleitet werden. Überprüfen Sie anhand der KPIs die Prozedur, die hoch ausgeführt wird. Legen Sie für dieses Verfahren hohe Frequenzwerte fest. (Auf diese Weise können die einzelnen Parameter auf Basis eines Netzwerkanrufmodells angepasst werden.)

Eine ideale Möglichkeit, diese Parameter zu konfigurieren, besteht darin, Werte auf Leafs festzulegen, jedoch nicht auf dem Stammbaum. Abbildung 2 erläutert beispielsweise den Konfigurationsbaum für die Authentifizierung. Operatoren können den Wert auf eine niedrigere Ebene einstellen, wie hier gezeigt, anstatt direkt "Authentifizieren des Anfügens" zu konfigurieren.

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

Es ist immer gut, Hochfrequenzwerte (Einheiten mit 10 s) festzulegen und dann die Signalisierungsschwellen für die Gr/Iu-Schnittstelle zu überwachen. Wenn die Signalisierung weit innerhalb der Grenzwerte liegt, definieren Sie Werte, bis die Signalisierung einen sicheren Ort in der Nähe von Grenzwerten erreicht, die der Operator für sein Netzwerk festlegen möchte.

Legen Sie die Frequenz für die verschiedenen Prozeduren in 20/30 fest, und reduzieren Sie sie auf 5-10, indem Sie den externen Schnittstellenverkehr genau überwachen. Bei dieser Überlastung muss die Auswirkung auf die Arbeitsspeicher-CPU von linkmgr und sessmgr überprüft werden.

PTMSI- und PTMSI-Signatur-Neuzuordnungen führen nicht direkt zu einer Spitze der Signalisierung. Es ist jedoch immer wichtig, Hochfrequenzwerte festzulegen, damit die PTMSIs mit Sessmgr-Instanzen verfügbar sind (was selten vorkommt). Es wird nicht empfohlen, PTMSI für jedes Uplink-Verfahren der EU zu ändern, da dies nicht die empfohlene Vorgehensweise ist. Ein Wert von 10 könnte anständig sein. Nach all diesen Änderungen ist es wichtig, die

Standardstatusprüfung im System zu überwachen und durchzuführen.

Als Beispiel:

```
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
```

Fehlerbehebung

Wenn eine Authentifizierung durchgeführt oder eine PTMSI- oder PTMSI-Signatur zugewiesen werden soll, werden Debug-Protokolle ausgegeben, um festzustellen, warum das Verfahren abgeschlossen wurde. Dies erleichtert die Fehlerbehebung im Falle von Unstimmigkeiten. Diese Protokolle beinhalten die Konfiguration aus dem cc-Profil und den aktuellen Wert aller Zähler sowie die Bewegung der Entscheidungslogik über die verschiedenen Konfigurations- und Zählerarten. Außerdem können die aktuellen Zählerwerte pro Abonnent mit den Befehlen **show subscribers sgsn-only** oder **show subscribers gprs-only** angezeigt werden.

Eine Beispielausgabe hierfür wird bereitgestellt. Die aktuellen Zähler und der aktuelle authentifizierte Zeitstempel werden dem Befehl **show subscribers** (Abonnenten anzeigen) mit voller Ausgabe hinzugefügt.

```
[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:
.
.
```

Wenn das Problem im Netzwerk auftritt, geben Sie die folgenden Befehle ein, um Informationen für den Geschäftsbereich zu sammeln, mit denen das Problem weiter analysiert werden kann:

```
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.
```

Risiken

Verbesserte Signalisierung für Gr/Iu-Schnittstellen sowie geringe CPU-Auswirkungen (linkmgr) durch interne Prozesse bei zu häufiger Authentifizierung

Befehlssyntax

Alle Befehle befinden sich im Konfigurations-/Anrufsteuerungsprofilmodus, und es gelten die entsprechenden Operatorberechtigungen. Ein Snapshot der Befehle unter dem cc-Profil ist wie folgt:

```
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]}
```