ÖZET

KİMLİK DOĞRULAMA İÇİN YÖNTEM VE CİHAZ

Kimlik doğrulama için bir yöntem ve bir cihaz açıklanmaktadır. Yöntem şunları içerir: AKA kimlik doğrulama prosedürü başarısız olduğunda, yerel bilgi veya ağ politikasına göre bir bağlantının serbest bırakılmasına veya varsayılan hizmetin devam etmesine karar verilmesi. EPS AKA kimlik doğrulama prosedürü başarısız olduğunda, bağlantı derhal serbest bırakılmamaktadır, fakat bağlantı serbest bırakılmakta ya da varsayılan hizmet yerel bilgilere ve ağ politikasına göre devam etmektedir, böylece gereksiz bağlantıların serbest bırakılması önlenmekte ve kaynak tasarrufu sağlanmaktadır.

İSTEMLER

1. Bir kimlik doğrulama yöntemi olup, özelliği aşağıdakileri içermesidir:

bir Mobilite Yönetim Varlığı tarafından, MME, bir Erişilemeyen Tabaka, NAS, bir mesajın alınması;

MME'ye göre bir NAS sayım değerinin 1 arttırılması;

NAS sayımı değeri maksimum bir değere yaklaşırsa, MME tarafından bir NAS sinyalleme bağlantısıyla yapılan varsayılan bir hizmet için bir Kimlik doğrulama ve Anahtar Sözleşmesi prosedürünün başlatılması (801);

MME tarafından, varsayılan hizmet için Kimlik doğrulama ve Anahtar Anlaşması prosedürünün başarısız olması durumunda, varsayılan hizmete bir ağ politikasına uygun olarak kimliği doğrulanmamış bir hizmet olarak izin verilip verilmediğinin tespit edilmesi (802);

MME tarafından, varsayılan hizmetin varsayılan bir hizmet türüne veya Hizmet Kalitesine göre kimlik doğrulaması gerektirip gerektirmediğinin tespit edilmesi (802);

MME tarafından, ağ politikasına uygun olarak kimliği doğrulanmamış bir hizmet olarak varsayılan hizmete izin veriliyorsa ve varsayılan hizmetin kimlik doğrulaması gerektirmemesi durumunda, varsayılan hizmetin NAS sinyalleme bağlantısının muhafaza edilmesi (802).

2. İstem 1'e göre yöntem olup, özelliği ayrıca aşağıdakileri içermesidir:
MME tarafından, varsayılan hizmetin ağ politikasına uygun olarak kimliği doğrulanmamış bir hizmet olarak kabul edilmemesi durumunda varsayılan hizmetin NAS sinyalleme bağlantısının serbest bırakılması.

3. İstem 1 veya istem 2'ye göre bir yöntem olup, özelliği ayrıca aşağıdakileri içermesidir:

Ağ politikasına uygun olarak kimliği doğrulanmamış bir hizmet olarak varsayılan hizmete izin veriliyorsa ve varsayılan hizmetin kimlik doğrulaması gerekiyorsa, MME tarafından varsayılan hizmetin NAS sinyalleme bağlantısının serbest bırakılması.

4. İstemler 1 ila 3'ten herhangi birine göre bir yöntem olup, özelliği ayrıca aşağıdakileri içermesidir:
MME tarafından, Kullanıcı Ekipmanının Kullanıcı Ekipmanı kimlik doğrulama yetkinlik bilgisine veya bir Abone Kimlik Modülü tipine uygun olarak Kimlik doğrulama ve Anahtar Anlaşması prosedürünü gerçekleştirip gerçekleştiremediğinin tespit edilmesi.

5. İstemler 2 ila 4'ten herhangi birine göre bir yöntem olup, özelliği varsayılan hizmetin NAS sinyalleme bağlantısının serbest bırakılmasının aşağıdakilerden herhangi birini içermesidir:

bir Erişilemeyen Tabaka sinyalleme bağlantısı tek hizmet taşıyorsa, Erişilemeyen Tabaka sinyalleme bağlantısının serbest bırakılması;

bir Erişilemeyen Tabaka sinyalleme bağlantısı çoklu hizmet taşıyorsa ve çoklu hizmetin bir kısmı kimlik doğrulama gerektiriyorsa ve diğerleri kimlik doğrulama gerektirmiyorsa, kimlik doğrulama gerektiren hizmete karşılık gelen bir Gelişmiş Paket Sistem taşıyıcısını serbest bırakır ve kimlik doğrulaması gerektirmeyen hizmete karşılık gelen Gelişmiş Paket Sistem taşıyıcısını muhafaza eder.

6. İstemler 1 ila 5'ten herhangi birine göre bir yöntem olup, özelliği:
varsayılan hizmetin, Acil Çağrı hizmetinden en az bir tanesini ve bir genel alarm hizmetini içermesidir.

7. Bir Mobilite Yönetim Varlığı, MME, cihaz olup, özelliği aşağıdakileri içermesidir:

bir Erişilemeyen Tabaka, NAS, mesaj almak ve bir NAS sayım değerini 1 artırmak için yapılandırılmış bir araç;

eğer bir NAS sayım değeri maksimum bir değere yaklaşırsa, bir Erişilemeyen Tabaka, NAS tarafından yapılan varsayılan bir hizmet için bir Kimlik doğrulama ve Anahtar Sözleşmesi prosedürünü tetiklemek üzere yapılandırılmış bir tetikleyici modül (63);

varsayılan hizmet için Kimlik doğrulama ve Anahtar Anlaşması prosedürünü yürütmek üzere yapılandırılmış bir yürütme modülü (61); ve

aşağıdakileri içeren bir işlemci (62):

varsayılan hizmet için Kimlik doğrulama ve Anahtar Anlaşması prosedürü başarısız olursa, varsayılan hizmetin bir ağ politikasına uygun olarak kimliği doğrulanmamış bir hizmet olarak izin verilip verilmediğini tespit etmek üzere yapılandırılmış bir birinci değerlendirme birimi (64);

birinci değerlendirme birimi (64) varsayılan hizmetin ağ politikasına uygun olarak kimliği doğrulanmamış bir hizmet olarak izin verildiğini tespit ederse, varsayılan hizmetin varsayılan bir hizmet türüne ya da Hizmet Kalitesi'ne göre kimlik doğrulaması gerektirip gerektirmediğini tespit etmek için yapılandırılmış bir ikinci değerlendirme birimi (66);

ikinci değerlendirme biriminin (67) varsayılan hizmetin kimlik doğrulama gerektirmediğini tespit etmesi durumunda NAS hizmetinin varsayılan hizmetle bağlantıyı sağlayacak şekilde yapılandırılmış bir yürütme birimi (68).

8. İstem 7'ye göre MME cihazı olup, özelliği ayrıca aşağıdakileri içermesidir:
birinci değerlendirme biriminin (64) varsayılan hizmete, ağ politikasına uygun olarak kimliği doğrulanmamış bir hizmet olarak izin verilmediğini tespit etmesi durumunda varsayılan hizmetin NAS sinyalleme bağlantısını serbest bırakmak üzere yapılandırılmış bir birinci serbest bırakma birimi (65).

9. İstem 7 veya istem 8'e göre MME cihazı olup, özelliği ayrıca aşağıdakileri içermesidir:

ikinci değerlendirme birimi (66) varsayılan hizmetin doğrulanması gerektiğini tespit ederse, varsayılan hizmetin NAS sinyalleme bağlantısını serbest bırakmak üzere düzenlenen bir ikinci serbest bırakma birimi (67),

10. İstemler 7 ila 9'dan herhangi birine göre MME cihazı olup, özelliği ikinci değerlendirme biriminin (67), birinci değerlendirme biriminin (64) ağ politikasına göre varsayılan hizmete doğrulanmamış bir hizmet olarak izin verildiğini tespit etmesi durumunda, varsayılan hizmetin kimlik doğrulaması gerektirip gerektirmediğini tespit etmek üzere yapılandırılmasıdır.

11. İstemler 8 ila 10'dan herhangi birine göre MME cihazı olup, özelliği birinci serbest bırakma biriminin (65), aşağıdakilerden herhangi birini serbest bırakmak üzere yapılandırılmış olmasıdır:

Erişilemeyen Tabaka sinyalleme bağlantısı tek bir hizmete sahipse, bir Erişilemeyen Tabaka (Erişilemeyen Tabaka) sinyalleme bağlantısının serbest bırakılması;

Erişilemeyen Tabaka sinyalleme bağlantısı çoklu hizmet taşıyorsa ve tüm çoklu hizmetlerin kimlik doğrulaması gerekiyorsa, Erişilemeyen Tabaka sinyalleme bağlantısının serbest bırakılması;

bir Erişilemeyen Tabaka sinyalleme bağlantısı çoklu hizmet taşıyorsa ve çoklu hizmet sağlayıcıların bir kısmı kimlik doğrulama gerektiriyorsa ve diğerleri kimlik doğrulama gerektirmiyorsa, kimlik doğrulama gerektiren hizmete karşılık gelen bir Gelişmiş Paket Sistemi (Gelişmiş Paket Sistemi) taşıyıcısının serbest bırakılması ve kimlik doğrulama gerektirmeyen hizmete karşılık gelen Gelişmiş Paket Sistemi taşıyıcısının muhafaza edilmesi.

12. İstem 7'ye göre MME cihazı olup, özelliği:
varsayılan hizmetin, Acil Çağrı hizmetinden en az bir tanesini ve bir genel alarm hizmetini içermesidir.

TARİFNAME
KİMLİK DOĞRULAMA İÇİN YÖNTEM VE CİHAZ

Buluşun Sahası

Mevcut buluş, iletişim teknolojileri ve özellikle de kimlik doğrulama için bir yöntem ve cihaz ile ilgilidir.

Buluşun Altyapısı

Erişilemeyen Tabaka (Erişilemeyen Tabaka, kısaltma: NAS) sayımı, Uzun Süreli Evrim (Uzun Süreli Evrim, kısaltma: LTE) sistemindeki bir güvenlik bağlamının bir parçasıdır. LTE sisteminde, NAS sayısı, anahtarı yenilemek için bir anahtarın ömrü boyunca işlev görebilir; ve NAS sayımı, bir anahtarın bir Kullanıcı Ekipmanı (Kullanıcı Ekipmanı, kısaltma: UE) ile bir ağ arasında senkronize edilmesini sağlar ve yeniden oynatma saldırılarına karşı koyar. Her bir Gelişmiş Paket Sistemi (Gelişmiş Paket Sistemi, kısaltma: EPS) güvenlik bağlamında iki bağımsız NAS sayım değeri bulunur: bir çıkış yolu NAS sayım değeri ve bir indirme yolu NAS sayım değeri. İki NAS sayım değerinin sayaçları, sırasıyla UE ve bir Hareketlilik Yönetimi Varlığı (MME) tarafından bağımsız olarak muhafaza edilir.

NAS sayımının uzunluğu, 32 hanedir ve iki bölümden oluşur: NAS dizi numarası (SQN) ve NAS taşma değeri (OVERFLOW). NAS sıra numarası 8 basamaktan oluşur ve NAS taşma değeri 16 basamaktan oluşur. NAS sıra numarası her NAS mesajında taşınır. Güvenlik koruması altında yeni veya yeniden iletilmiş bir NAS mesajı gönderildiğinde, gönderen NAS sıra numarasına 1 ekler; NAS sıra numarası maksimum değere geldiğinde ve bir döngü tamamlandığında NAS taşma değeri 1 artar.

Önceki teknikte, MME, yaklaşık olarak NAS sayım değeri maksimum 2^{24} değerine yaklaştığında, indirme yolu NAS sayım değerinin kaymak üzere olduğunu tespit ettiğinde, diğer bir deyişle MME, yeni bir güvenlik bağlamı oluşturmak için yeni bir EPS Kimlik doğrulama ve Anahtar Anlaşması (Kimlik doğrulama ve Anahtar Anlaşma, kısaltma: AKA) kimlik doğrulama prosedürünü tetikler. Güvenlik bağlamı etkinleştirildiğinde, NAS sayım değeri 0 olarak başlatılır. MME, UE'nin çıkış yolu NAS

sayım değerinin de maksimum değere yakınlaştığını tespit ettiğinde, diğer bir deyişle, kaydırmak üzere olduğunda, MME, bir EPS AKA kimlik doğrulama prosedürünü tetikler.

3GPP Sistem Mimarisi Evrimi (SAE): Güvenlik Mimarisi; (Sürüm 9), Draft-33401-910, LSM'deki kimliği doğrulanmamış UE'ler için bir algoritma anlaşması açıklar. Sınırlı hizmet modunda olan (LSM) ve MME tarafından doğrulanamayan UE'lere (hangi nedenle olursa olsun), acil durum ek talebi mesajı göndererek acil durum çağrıları yapmaya izin verilebilir. MME'nin LSM'deki kimliği doğrulanmamış UE'lerin acil aramalar için taşıyıcılar kurmasına izin verip vermeyeceğini yapılandırmak mümkün olacaktır. Bir MME LSM'de kimliği doğrulanmamış UE'lerin bir acil durum çağrısı için taşıyıcılar kurmasına izin verirse, MME NAS protokolü için sırasıyla bütünlük ve şifreleme algoritması olarak EIA0 ve EEA0'ı kullanmalıdır.

Önceki teknikte, EPS AKA kimlik doğrulama prosedürü başarısız olursa bağlantı kopacaktır. Bu tür güvenlik işlemleri, kaynak israfına yol açmaktadır.

Buluşun Kısa Açıklaması

Mevcut buluşun uygulamaları, kaynakları muhafaza etmek için kimlik doğrulaması için ekli bağımsız istemler 1 ve 7'de tanımlandığı gibi bir yöntem ve bir cihaz sağlar.

Mevcut buluşun bir uygulamasında bir kimlik doğrulama yöntemi şunları içermektedir:

bir Mobilite Yönetim Varlığı tarafından, MME, bir Erişilemeyen Tabaka, NAS, bir mesajın alınması;

MME'ye göre bir NAS sayım değerinin 1 arttırılması;

NAS sayımı değeri maksimum bir değere yaklaşırsa, MME tarafından bir NAS sinyalleme bağlantısıyla yapılan varsayılan bir hizmet için bir Kimlik doğrulama ve Anahtar Sözleşmesi prosedürünün başlatılması;

MME tarafından, varsayılan hizmet için Kimlik doğrulama ve Anahtar Anlaşması prosedürünün başarısız olması durumunda, varsayılan hizmete bir ağ

politikasına uygun olarak kimliği doğrulanmamış bir hizmet olarak izin verilip verilmediğinin tespit edilmesi;

varsayılan hizmetin varsayılan bir hizmet türüne veya Hizmet Kalitesine göre kimlik doğrulaması gerektirip gerektirmediğinin tespit edilmesi;

ağ politikasına uygun olarak kimliği doğrulanmamış bir hizmet olarak varsayılan hizmete izin veriliyorsa ve varsayılan hizmetin kimlik doğrulaması gerektirmemesi durumunda, varsayılan hizmetin NAS sinyalleme bağlantısının muhafaza edilmesi.

Mevcut buluşun bir uygulamasındaki bir cihaz aşağıdakileri içerir:

bir Erişilemeyen Tabaka, NAS, mesaj almak ve bir NAS sayım değerini 1 artırmak için yapılandırılmış bir araç;

eğer bir NAS sayım değeri maksimum bir değere yaklaşırsa, bir Erişilemeyen Tabaka, NAS tarafından yapılan varsayılan bir hizmet için bir Kimlik doğrulama ve Anahtar Sözleşmesi prosedürünü tetiklemek üzere yapılandırılmış bir tetikleyici modül;

varsayılan hizmet için Kimlik doğrulama ve Anahtar Anlaşması prosedürünü yürütmek üzere yapılandırılmış bir yürütme modülü; ve

aşağıdakileri içeren bir Mobilite Yönetimi Varlığına yerleştirilmiş bir işlemci:

varsayılan hizmet için Kimlik doğrulama ve Anahtar Anlaşması prosedürü başarısız olursa, varsayılan hizmetin bir ağ politikasına uygun olarak kimliği doğrulanmamış bir hizmet olarak izin verilip verilmediğini tespit etmek üzere yapılandırılmış bir birinci değerlendirme birimi;

birinci değerlendirme birimi varsayılan hizmetin ağ politikasına uygun olarak kimliği doğrulanmamış bir hizmet olarak izin verildiğini tespit ederse, varsayılan hizmetin varsayılan bir hizmet türüne ya da Hizmet Kalitesi'ne göre kimlik

doğrulaması gerektirip gerektirmediğini tespit etmek için yapılandırılmış bir ikinci değerlendirme birimi;

ikinci değerlendirme biriminin varsayılan hizmetin kimlik doğrulama gerektirmediğini tespit etmesi durumunda NAS hizmetinin varsayılan hizmetle bağlantıyı sağlayacak şekilde yapılandırılmış bir yürütme birimi.

Mevcut buluş kapsamındaki teknik çözümde, EPS AKA kimlik doğrulama prosedürü başarısız olduğunda, bağlantı derhal serbest bırakılmamaktadır, fakat bağlantı serbest bırakılmakta ya da varsayılan hizmet yerel bilgilere ve ağ politikasına göre devam etmektedir, böylece gereksiz bağlantıların serbest bırakılması önlenmekte ve kaynak tasarrufu sağlanmaktadır.

Şekillerin Kısa Açıklaması

ŞEKİL 1, mevcut buluş kapsamında olmayan bir birinci örnekte bir kimlik doğrulama yönteminin bir akış şemasıdır;

ŞEKİL 2, mevcut buluş kapsamında olmayan bir ikinci örnekte bir kimlik doğrulama yönteminin bir akış şemasıdır;

ŞEKİL 3, mevcut buluş kapsamında olmayan bir üçüncü örnekte bir kimlik doğrulama yönteminin bir akış şemasıdır;

ŞEKİL 4, mevcut buluş kapsamında olmayan bir dördüncü örnekte bir kimlik doğrulama yönteminin bir akış şemasıdır;

ŞEKİL 5, mevcut buluş kapsamında olmayan bir beşinci örnekte bir kimlik doğrulama yönteminin bir akış şemasıdır;

ŞEKİL 6, mevcut buluş kapsamında olmayan bir altıncı örnekte bir kimlik doğrulama yönteminin bir akış şemasıdır;

ŞEKİL 7, mevcut buluşun bir birinci uygulamasındaki bir kimlik doğrulama yönteminin bir akış şemasıdır;

ŞEKİL 8, mevcut buluş kapsamında olmayan bir yedinci örnekte bir kimlik doğrulama cihazının yapısını göstermektedir;

ŞEKİL 9, mevcut buluş kapsamında olmayan bir sekizinci örnekte bir kimlik doğrulama cihazının yapısını göstermektedir;

ŞEKİL 10, mevcut buluş kapsamında olmayan bir dokuzuncu örnekte bir kimlik doğrulama cihazının yapısını göstermektedir;

ŞEKİL 11, mevcut buluş tarafından kapsanmayan bir onuncu örnekte bir kimlik doğrulama cihazının yapısını göstermektedir;

ŞEKİL (12), mevcut buluş tarafından kapsanmayan bir on birinci örnekte bir kimlik doğrulama cihazının yapısını göstermektedir;

ŞEKİL 13, mevcut buluşun ikinci bir uygulamasında bir kimlik doğrulama cihazının yapısını göstermektedir.

Uygulamaların Detaylı Açıklaması

Mevcut buluşun altındaki teknik çözüm, ekteki çizimlere ve tercih edilen uygulamalara referansla aşağıda tarif edilmiştir.

ŞEKİL 1, birinci örnekte bir kimlik doğrulama yönteminin bir akış şemasıdır. ŞEKİL 1'de gösterildiği gibi, bu örnekteki yöntem aşağıdaki adımları içerir:

Adım 101: Bir NAS sayım değeri maksimum değere yaklaştığında yerel bilgilerin tespit edilmesi;

Adım 102: Yerel bilgilere göre UE ile Kimlik doğrulama ve Anahtar Anlaşması prosedürünün gerçekleştirilmesi için bir prosedürün başlatılıp başlatılmayacağına karar verilmesi.

NAS sayım değeri maksimum değere yaklaştığında, NAS sayım değeri kaymak üzeredir. Kimlik doğrulama ve Anahtar Anlaşması prosedürü kimlik doğrulama prosedürü bir EPS AKA kimlik doğrulama prosedürü olabilir.

Yukarıdaki iki adımı gerçekleştiren varlık bir MME olabilir. indirme yolu ya da çıkış yolu NAS sayım değeri kaymak üzereyken, MME yerel bilgiyi algılar ve tespit sonucuna göre EPS AKA kimlik doğrulama prosedürünün tetiklenip tetiklenmeyeceğine karar verir.

Çıkış yolu NAS sayım değerinin tespitinin bir örnek olarak alınması durumunda, MME bir NAS mesajı alır ve NAS sayım değeri 1 artar. MME, NAS sayım değerinin bu şekilde maksimum değere yakın olup olmadığını tespit eder: MME, NAS sayım değerinin, maksimum değere yakın olan önceden ayarlanmış bir eşik değere eşit olup

olmadığını kontrol eder; eşitse, MME yerel bilgiyi algılar ve tespit sonucuna göre bir Kimlik doğrulama ve Anahtar Anlaşması prosedürünü tetikleyip tetiklememeye karar verir; eşit değilse, MME NAS mesajını almaya devam eder.

Bu uygulamada, MME, NAS sayım değerinin yaklaşık olarak kaydığını tespit edildiğinde EPS AKA kimlik doğrulama prosedürünü tetiklemez, böylece EPS AKA kimlik doğrulama prosedürlerini tetiklemek için süreleri azaltarak gereksiz EPS AKA kimlik doğrulama prosedürleri kaynaklı atıkları önler ve kaynak tasarrufu sağlar.

Aşağıda, ikinci örnekten önce ilgili teknolojiler açıklanmaktadır.

LTE sisteminde, EPS güvenlik bağlamları iki modda kategorize edilir. Kullanım durumu açısından, EPS güvenlik bağlamları, varsayılan EPS güvenlik bağlamına ve mevcut olmayan EPS güvenlik bağlamına kategorize edilir. Varsayılan EPS güvenlik içeriği, şu anda kullanımda olan güvenlik içeriği olan en son etkinleştirilen güvenlik bağlamını ifade eder. Varsayılan EPS güvenlik içeriği ve varsayılan olmayan bir yerel EPS güvenlik içeriği bir arada bulunabilir. Oluşturma moduna göre, EPS güvenlik bağlamları haritalanmış EPS güvenlik bağlamına ve yerel EPS güvenlik bağlamına kategorize edilebilir. Eşlenen EPS güvenlik içeriği, örneğin bir Evrensel Mobil Telekomünikasyon Sisteminden (UMTS) bir LTE sistemine eşlenen başka bir sistemden eşlenen bir güvenlik içeriğini ifade eder. Yerel EPS güvenlik içeriği, bir LTE sisteminde EPS AKA aracılığıyla oluşturulan bir güvenlik bağlamını ifade eder. Yerel EPS güvenlik bağlamları, kısmi yerel EPS güvenlik bağlamı ve tam yerel EPS güvenlik bağlamında kategorize edilir. Aralarındaki temel fark şudur: Kısmi bir yerel EPS güvenlik içeriği, başarılı bir NAS güvenlik modu prosedüründen geçmez. Bu nedenle, bir kısmi yerel EPS güvenlik bağlamında, bir LTE ağına erişen UE'nin kimlik doğrulaması için bir K_{ASME} anahtarı, bir Anahtar Kümesi Tanımlayıcısı (KSI), UE'nin güvenlik özellikleri ve sadece 0'a ayarlanmış bir NAS sayım değeri bulunur. Tam bir yerel EPS güvenlik içeriği, bir EPS AKA kimlik doğrulama prosedüründen geçer ve başarılı bir NAS Güvenlik Modu Komutu (SMC) prosedürüyle etkinleştirilir ve bir dizi tam EPS NAS güvenlik bağlamı içerir. Bu nedenle, tam yerel EPS güvenlik içeriği NAS'ın Bütünlük Anahtarı (IK) (K_{NASint}) ve NAS'ın Şifreleme Anahtarı (CK) (K_{NASenc}), seçilen bir NAS şifreleme algoritması ve ayrıca bir bütünlük algoritması tanımlayıcısı içerir.

ŞEKİL 2, ikinci örnekteki bir kimlik doğrulama yönteminin bir akış şemasıdır. Bu örnekteki yerel bilgiler, lokal olarak depolanan güvenlik bağlamıdır. Aşağıda belirtilen güvenlik bağlamı, yerel EPS güvenlik bağlamlarına referans verir.

ŞEKİL 2'de gösterildiği gibi. 2, bu örnekte yöntem aşağıdaki adımları içerir:

Adım 201: MME bir NAS mesajı alır ve NAS sayım değeri 1 artar.

Adım 202: MME, NAS sayım değerinin maksimum değere yakın olup olmadığını kontrol eder. Öyleyse, 203 adımı meydana gelir; değilse, 201 adımı meydana gelir.

Spesifik olarak, maksimum değere yakın bir değer, bir eşik değer olarak önceden ayarlanmış olabilir. MME, NAS sayım değerinin maksimum değere eşit olup olmadığını kontrol eder. Öyleyse, 203 adımı meydana gelir; değilse, 201 adımı meydana gelir.

Adım 203: MME, yerel güvenlik bağlamlarının, varsayılan güvenlik bağlamlarına ek olarak varsayılan olmayan herhangi bir güvenlik bağlamını da içerip içermediğini kontrol eder. Öyleyse, 204 adımı meydana gelir; değilse, MME bir EPS AKA kimlik doğrulama prosedürünü tetikler.

Adım 204: MME varsayılan olmayan güvenlik bağlamını etkinleştirir.

MME, bir NAS SMC prosedürünü başarılı bir şekilde çalıştırarak varsayılan olmayan güvenlik bağlamını aktif hale getirebilir. Başarılı bir NAS SMC prosedürü şunları içerir: MME, NAS SMC mesajı için bütünlük koruması sağlamak için güvenlik içeriğini kullanır. UE, NAS SMC mesajının bütünlüğünü başarıyla doğruladığında, UE, MME'ye bir NAS Güvenlik Modu Tamamlandı mesajı gönderir. MME, NAS Güvenlik Modu Tamamlandı mesajının şifresini çözer ve bütünlük kimlik doğrulaması gerçekleştirir. Bu nedenle, MME bu güvenlik bağlamının UE ile paylaşıldığını ve etkinleştirildiğini bilir. Bu adımda, MME NAS SMC prosedürünü başarılı bir şekilde yürüterek varsayılan olmayan güvenlik bağlamını etkinleştirir.

Bununla birlikte, eğer NAS SMC prosedürü başarısız olursa, MME bir EPS AKA kimlik doğrulama prosedürünü tetikler.

Varsayılan olmayan yerel güvenlik bağlamı, varsayılan olmayan bir kısmi yerel güvenlik bağlamı veya varsayılan olmayan bir tam yerel güvenlik bağlamı olabilir ve adım 204 şöyle olabilir: MME, varsayılan olmayan kısmi yerel güvenlik bağlamını veya varsayılan olmayan tam yerel güvenlik bağlamını etkinleştirir.

Bu örnekte, MME tarafından tetiklenen başarılı bir NAS SMC prosedürü yoluyla, MME ve UE tarafından paylaşılan varsayılan olmayan yerel güvenlik bağlamı etkinleştirilir. MME UE'den NAS Güvenlik Modu Tamamlandı mesajı almazsa, MME bir EPS AKA kimlik doğrulama prosedürünü tetikler.

Bu örneğin uygulama senaryosu aşağıda iki örnekle açıklanmıştır.

(1) MME, NAS sayım değerinin maksimum değere yaklaştığını tespit ettiğinde, MME, MME ve UMTS Abone Kimlik Modülü Entegre Devre Kartı'nda (UICC) varsayılan olmayan bir kısmi güvenlik bağlamının saklandığını bilmek için güvenlik bağlamını tespit eder. MME, varsayılan olmayan kısmi güvenlik bağlamını etkinleştirir. Bu durumda, NAS sayım değeri 0 olarak başlatılır ve EPS AKA kimlik doğrulama prosedüründen kaçınılır.

Bu senaryoda, MME, EPS AKA kimlik doğrulama prosedürünü derhal tetiklemez, böylece varsayılan olmayan kısmi güvenlik bağlamı kaynaklarının israfını önler ve gereksiz EPS AKA kimlik doğrulama prosedürlerinin uygulanmasının neden olduğu kaynak israfını önler.

(2) UE, EPS'ye erişim sürecinde varsayılan güvenlik bağlamını oluşturur. Daha sonra, UE, Geliştirilmiş Evrensel Karasal Radyo Erişim Ağı'ndan (E-UTRAN) Evrensel Karasal Radyo Erişim Ağı'na (UTRAN) veya GSM/EDGE Radyo Erişim Ağı'na (GERAN) teslim olduğunda, UE, E-UTRAN'da oluşturulan lokal güvenlik bağlamını saklar. Daha sonra, UE E-UTRAN'a geri döndüğünde, eşlenen güvenlik içeriği uygulanır. Eşlenen güvenlik içeriği varsayılan güvenlik içeriği haline gelir. Daha önce UE ve MME tarafından saklanan ve E-UTRAN'da oluşturulan güvenlik içeriği varsayılan olmayan bir tam güvenlik bağlamına dönüşür. Bu senaryoda, MME, NAS sayımı değerinin maksimum değere yakın olduğunu tespit ettiğinde, MME bu varsayılan olmayan tam güvenlik içeriğinin

lokal olarak depolandığını bilmek için güvenlik içeriğini algılar. Bu nedenle, MME varsayılan olmayan tam güvenlik bağlamını etkinleştirir, böylece EPS AKA kimlik doğrulama prosedüründen kaçınır.

Bu senaryoda, MME, EPS AKA kimlik doğrulama prosedürünü derhal tetiklemez, böylece önceden depolanmış olan varsayılan olmayan tam güvenlik bağlamı kaynaklarının israfını önler ve gereksiz EPS AKA kimlik doğrulama prosedürlerinin uygulanmasının neden olduğu kaynak israfını önler.

Bu örnekte, MME, NAS sayım değerinin kaymak üzere olduğunu tespit ettiği anda EPS AKA kimlik doğrulama prosedürünü tetiklemez, böylece EPS AKA kimlik doğrulama prosedürlerini tetiklemek için süreleri azaltıp, gereksiz EPS AKA kimlik doğrulama prosedürlerinin neden olduğu kaynak israfından kaçınır ve kaynak tasarrufu sağlar.

ŞEKİL 3, bir üçüncü örnekteki kimlik doğrulama yönteminin bir akış şemasıdır. Bu örnekte, yerel bilgi zamanlayıcı durumundadır. Bu uygulamada, MME'de bir zamanlayıcı önceden ayarlanmıştır. Zamanlayıcının durumu "çalışıyor" veya "duruyor" haldedir. NAS sayım değeri eşik değere ulaştığında ve EPS AKA kimlik doğrulama prosedürü başarıyla tamamlandığında, zamanlayıcının durumu "çalışıyor" olarak değişir; zamanlayıcının zamanlama süresi ayarlanan zaman eşiği değerini karşıladığında, zamanlayıcının durumu "duruyor" olarak değişir.

ŞEKİL 3'te gösterildiği gibi, bu örnekteki yöntem aşağıdaki adımları içerir:

Adım 301: MME bir NAS mesajı alır ve NAS sayım değeri 1 artar.

Adım 302: MME, NAS sayım değerinin maksimum değere yakın olup olmadığını kontrol eder. Öyleyse, 303 adımı meydana gelir; değilse, adım 301 adımı meydana gelir.

Spesifik olarak, maksimum değere yakın bir değer eşik değer olarak önceden ayarlanmıştır (2^{24}-100 gibi). MME, NAS sayım değerinin 2^{24}-100 değerine eşit olup olmadığını kontrol eder. Öyleyse, adım 303 meydana gelir; değilse, adım 301 meydana gelir.

Adım 303: MME, zamanlayıcının çalışıp çalışmadığını kontrol eder. Öyleyse, adım 304 meydana gelir; değilse, MME bir EPS AKA kimlik doğrulama prosedürünü tetikler.

Adım 304: MME varsayılan olmayan güvenlik bağlamını etkinleştirir.

Varsayılan olmayan güvenlik bağlamı, başarılı bir NAS SMC prosedürü ile etkinleştirilir. Başarılı bir NAS SMC prosedürü şunları içerir: MME, NAS SMC mesajı için bütünlük koruması sağlamak için güvenlik içeriğini kullanır. UE, NAS SMC mesajının bütünlüğünü başarıyla doğruladığında, UE, MME'ye bir NAS Güvenlik Modu Tamamlandı mesajı gönderir. MME, NAS Güvenlik Modu Tamamlandı mesajının şifresini çözer ve bütünlük kimlik doğrulaması gerçekleştirir. Bu nedenle, MME bu güvenlik bağlamının UE ile paylaşıldığını ve etkinleştirildiğini bilir. 304 adımında, MME, NAS SMC prosedürünü başarılı bir şekilde yürüterek varsayılan olmayan yerel güvenlik bağlamını etkinleştirir.

Bununla birlikte, eğer NAS SMC prosedürü başarısız olursa, MME bir EPS AKA kimlik doğrulama prosedürünü tetikler.

Uygulamada, indirme yolu NAS sayım değeri genellikle çıkış yolu NAS sayım değerine yakındır. MME, indirme yolu NAS sayım değerinin kaymak üzere olduğunu tespit ettiğinde, çıkış yolu NAS sayım değerinin kayması yakında tespit edilecektir. Ayrıca, MME, EPS AKA kimlik doğrulama prosedürünü tetikledikten bir süre sonra NAS SMC prosedürünü tetikler. NAS sayım değeri, NAS SMC prosedürünün yürütülmesiyle 0 olarak başlatılır. MME, indirme yolu NAS sayım değerinin kaymak üzere olduğunu tespit ederken, EPS AKA kimlik doğrulama prosedürünü zor bir şekilde tetikliyorsa, ancak çıkış yolu NAS sayım değerinin kaymak üzere olduğunu tespit etmeden önce yeni oluşturulan güvenlik bağlamını etkinleştirmek için NAS SMC prosedürünü tetiklemiyorsa, NAS sayım değeri başlatılmaz ve önceki teknik, çıkış yolu NAS sayım değerinin kaymak üzere olduğunu tespit ettikten sonra tekrar EPS AKA kimlik doğrulama prosedürünü tetikler. Bu örnekte, önceki başarılı EPS AKA kimlik doğrulama prosedürünün tamamlanmasından başlayarak sürenin ayarlanan zaman eşiği değerini karşılayıp karşılamadığını kontrol etmek için zamanlayıcı durumu tespit edilir. Bu zaman eşik değeri, başarılı EPS AKA kimlik doğrulama prosedürünün tamamlanmasından NAS SMC prosedürünün tetiklenmesine kadar geçen süreye göre

tespit edilir. Bu NAS sayım değeri maksimum değere yaklaşırsa ve önceki başarılı EPS AKA kimlik doğrulama prosedürünün tamamlanmasından başlayarak geçen süre ayarlanan zaman eşik değerinden düşükse, MME, NAS SMC prosedürünü tetikler. Bu NAS sayım değeri maksimum değere yaklaşırsa ve önceki başarılı EPS AKA kimlik doğrulama prosedürünün tamamlanmasından başlayarak geçen süre ayarlanan zaman eşik değerinden büyük veya ona eşitse, MME, EPS AKA kimlik doğrulama prosedürünü tetikler. Bu nedenle, yukarıdaki gerçek uygulama senaryosuna gelince, bu uygulama EPS AKA kimlik doğrulama prosedürünün ikinci tetiklemesinden kaçınır, çünkü çıkış yolu NAS sayım değerinin kaymak üzere olduğunu tespit etmeden önce NAS SMC prosedürü tetiklenmez, böylece uygulanan EPS AKA kimlik doğrulama prosedürlerini azaltır, gereksiz EPS AKA kimlik doğrulama prosedürlerinin tetiklenmesinden kaynaklanan kaynak israfını önler ve kaynak tasarrufu sağlar.

ŞEKİL 4, dördüncü örnekteki bir kimlik doğrulama yönteminin bir akış şemasıdır. Bu örnekte, yerel bilgiler bir durum makinesinin durumudur. Bu örnekte, MME'de bir durum makinesi önceden ayarlanmıştır. Durum makinesinin durumu "çalışıyor" veya "boşta"dır. Spesifik olarak, "0" "çalışıyor" ve "1" "boşta"yı temsil eder. "Çalışıyor", önceki başarılı EPS AKA kimlik doğrulama prosedürünün tamamlanmasından başlayarak sürenin ayarlanan zaman eşik değerinden düşük olduğunu göstermektedir; ve "boşta" önceki başarılı EPS AKA kimlik doğrulama prosedürünün tamamlanmasından başlayarak geçen sürenin ayarlanan zaman eşik değerinden büyük veya ona eşit olduğunu göstermektedir. Durum makinesi zamanlayıcı tarafından tetiklenebilir.

ŞEKİL 4'te gösterildiği gibi, bu örnekte yöntem aşağıdaki adımları içerir:

Adım 401: MME bir NAS mesajı alır ve NAS sayım değeri 1 artar.

Adım 402: MME, NAS sayım değerinin maksimum değere yakın olup olmadığını kontrol eder. Öyleyse, adım 403 meydana gelir; değilse, adım 401 meydana gelir.

Spesifik olarak, maksimum değere yakın bir değer eşik değer olarak önceden ayarlanmıştır (2^{24}-100 gibi). MME, NAS sayım değerinin 2^{24}-100 değerine eşit olup olmadığını kontrol eder. Öyleyse, adım 403 meydana gelir; değilse, MME, EPS AKA kimlik doğrulama prosedürünü tetikler.

Adım 403: MME, durum makinesinin durumunun "0" olup olmadığını kontrol eder. Öyleyse, adım 404 meydana gelir; değilse, MME bir EPS AKA kimlik doğrulama prosedürünü tetikler.

Adım 404: MME varsayılan olmayan güvenlik bağlamını etkinleştirir.

Varsayılan olmayan güvenlik bağlamı, başarılı bir NAS SMC prosedürü ile etkinleştirilir. Başarılı bir NAS SMC prosedürü şunları içerir: MME, NAS SMC mesajı için bütünlük koruması sağlamak için güvenlik içeriğini kullanır. UE, NAS SMC mesajının bütünlüğünü başarıyla doğruladığında, UE, MME'ye bir NAS Güvenlik Modu Tamamlandı mesajı gönderir. MME, NAS Güvenlik Modu Tamamlandı mesajının şifresini çözer ve bütünlük kimlik doğrulaması gerçekleştirir. Bu nedenle, MME bu güvenlik bağlamının UE ile paylaşıldığını ve etkinleştirildiğini bilir. 404 adımında MME, NAS SMC prosedürünü başarılı bir şekilde yürüterek varsayılan olmayan yerel güvenlik bağlamını etkinleştirir.

Ancak, NAS SMC prosedürü başarısız olursa, MME bir EPS AKA kimlik doğrulama prosedürünü tetikler.

Uygulamada, indirme yolu NAS sayım değeri genellikle çıkış yolu NAS sayım değerine yakındır. MME, indirme yolu NAS sayım değerinin kaymak üzere olduğunu tespit ettiğinde, çıkış yolu NAS sayım değerindeki kayma tespit edilecektir. Ayrıca, MME, EPS AKA kimlik doğrulama prosedürünü tetikledikten bir süre sonra NAS SMC prosedürünü tetikler. NAS sayım değeri, NAS SMC prosedürünün yürütülmesiyle 0 olarak başlatılır. MME, indirme yolu NAS sayım değerinin kaymak üzere olduğunu tespit ederken EPS AKA kimlik doğrulama prosedürünü zor bir şekilde tetiklerse, ancak çıkış yolu NAS sayım değerinin kaymak üzere olduğunu tespit etmeden önce NAS SMC prosedürünü tetiklemiyorsa, NAS sayım değeri başlatılmamıştır ve önceki teknik, çıkış yolu NAS sayım değerinin kaymak üzere olduğunu tespit ettikten sonra tekrar EPS AKA kimlik doğrulama prosedürünü tetiklemektedir. Bu örnekte, önceki başarılı EPS AKA kimlik doğrulama prosedürünün tamamlanmasından başlayarak sürenin ayarlanan zaman eşiği değerini karşılayıp karşılamadığını kontrol etmek için durum makinesinin durumu tespit edilir. Bu zaman eşik değeri, başarılı EPS AKA kimlik doğrulama prosedürünün tamamlanmasından NAS SMC prosedürünün tetiklenmesine kadar geçen süreye göre tespit edilir. Bu NAS sayım değeri maksimum değere

yaklaşırsa ve önceki başarılı EPS AKA kimlik doğrulama prosedürünün tamamlanmasından başlayarak geçen süre ayarlanan zaman eşik değerinden düşükse, MME NAS SMC prosedürünü tetikler. Bu NAS sayım değeri maksimum değere yaklaşırsa ve önceki başarılı EPS AKA kimlik doğrulama prosedürünün tamamlanmasından başlayarak geçen süre ayarlanan zaman eşik değerinden büyük veya ona eşitse, MME NAS AKA kimlik doğrulama prosedürünü tetikler. Bu nedenle, yukarıdaki gerçek uygulama senaryosuna gelince, bu uygulama EPS AKA kimlik doğrulama prosedürünün ikinci tetiklemesinden kaçınır, çünkü çıkış yolu NAS sayım değerinin kaymak üzere olduğunu tespit etmeden önce NAS SMC prosedürü tetiklenmez, böylece uygulanan EPS AKA kimlik doğrulama prosedürlerini azaltır, gereksiz EPS AKA kimlik doğrulama prosedürlerinin tetiklenmesinden kaynaklanan kaynak israfını önler ve kaynak tasarrufu sağlar.

ŞEKİL 5, bir beşinci örnekteki kimlik doğrulama yönteminin bir akış şemasıdır. Bu uygulamada, yerel bilgi varsayılan hizmet tipi, Hizmet Kalitesi (QoS) veya UE kimlik doğrulaması yapabilme özelliğidir.

ŞEKİL 5'te gösterildiği gibi, bu örnekteki yöntem aşağıdaki adımları içerir:

Adım 501: MME bir NAS mesajı alır ve NAS sayım değeri 1 artar.

Adım 502: MME, NAS sayım değerinin maksimum değere yakın olup olmadığını kontrol eder. Öyleyse, adım 503 meydana gelir; değilse, adım 501 meydana gelir.

Spesifik olarak, maksimum değere yakın bir değer, bir eşik değer olarak önceden ayarlanmış olabilir. MME, NAS sayım değerinin maksimum değere eşit olup olmadığını kontrol eder. Öyleyse, adım 503 meydana gelir; değilse, adım 501 meydana gelir.

Adım 503: MME, UE tarafından talep edilen ve varsayılan hizmet tipine karşılık gelen varsayılan hizmetin kimlik doğrulama gerektirip gerektirmediğini bilmek için varsayılan hizmet tipini tespit eder; veya MME, UE tarafından talep edilen ve QoS'ye karşılık gelen varsayılan hizmetin kimlik doğrulama gerektirip gerektirmediğini bilmek için QoS'yi tespit eder; veya MME, UE'nin, UE, EPS

AKA kimlik doğrulama prosedürünü uygulayıp uygulayamadığını bilmek için kimlik doğrulama yapma yeteneğini tespit eder.
Öyleyse, MME bir EPS AKA kimlik doğrulama prosedürünü tetikler; değilse, adım 504 meydana gelir.

Adım 504: MME varsayılan güvenlik bağlamını kullanmaya devam eder veya varsayılan hizmet için güvenlik koruması sağlamaz veya varsayılan hizmetin bağlantısını keser.

Örneğin, bu örnekte, MME, UE tarafından talep edilen hizmetin Acil Durum Çağrısı (EMC) hizmeti olduğunu ve UE tarafından istenen EMC hizmetinin kimlik doğrulama gerektirmediğini bilmek için varsayılan hizmet tipini tespit eder ve MME, artık EPS AKA kimlik doğrulama prosedürünü tetiklememektedir. MME, NAS sayım değerinin maksimum değere yaklaştığı ve varsayılan güvenlik bağlamını kullanmaya devam ettiği veya varsayılan hizmet için güvenlik koruması sağlamadığı veya varsayılan hizmetin bağlantısını kestiği tespit sonucunu yoksayar.

Bir Abone Kimlik Modülü (SIM) olan bir UE, bir UMTS ağındaki bir EMC hizmetinden bir LTE ağına teslim edildiğinde, MME, "Kc" güvenlik parametresini, Hizmet Veren GPRS Destek Düğümünden (SGSN) almaktadır (GPRS, Genel Paket Radyo Hizmeti'nin bir kısaltmasıdır) ve CK ve Bütünlük Anahtarına (IK) göre K_{ASME}'yi alır. NAS sayım değeri 0'dan başlar. Bu durumda, LTE ağındaki UE'nin güvenlik koruması K_{ASME}'den türetilen alt anahtar tarafından sağlanır. NAS sayım değeri kaymak üzere olduğunda, MME, UE'nin Kc'ye göre EPS AKA kimlik doğrulama prosedüründe bulunmayan bir SIM kullanıcısı olduğunu tespit edebilir. Bu nedenle, MME artık EPS AKA kimlik doğrulama prosedürünü tetiklemez ve NAS sayım değerinin maksimum değere yaklaştığı tespit sonucunu yoksayar. MME varsayılan güvenlik bağlamını kullanmaya devam eder veya varsayılan hizmet için güvenlik koruması sağlamaz veya varsayılan hizmetin bağlantısını keser.

Bu örnekte, UE tarafından talep edilen hizmet, kimlik doğrulama gerektirmiyorsa veya UE, Kimlik doğrulama ve Anahtar Anlaşması prosedürünü gerçekleştiremiyorsa, MME, EPS AKA kimlik doğrulama prosedürünü başlatmaz, böylece uygulanan EPS AKA kimlik doğrulama prosedürlerini azaltır. Gereksiz EPS AKA kimlik doğrulama

prosedürlerinin tetiklenmesinden kaynaklanan kaynak israfını önler ve kaynak tasarrufu sağlar.

ŞEKİL 6, altıncı örnekteki bir kimlik doğrulama yönteminin bir akış şemasıdır. Şekil 6'da gösterildiği gibi, bu örnekteki yöntem aşağıdaki adımları içerir:

Adım 601: MME bir NAS mesajı alır ve NAS sayım değeri 1 artar.

Adım 602: MME, NAS sayım değerinin maksimum değere yakın olup olmadığını kontrol eder. Öyleyse, 603 adımı meydana gelir; değilse, 601 adımı meydana gelir. Bu NAS sayım değeri, bir çıkış yolu NAS sayım değeri veya bir indirme yolu NAS sayım değeri olabilir.
Spesifik olarak, maksimum değere yakın bir değer, bir eşik değer olarak önceden ayarlanmış olabilir. MME, NAS sayım değerinin eşik değerine eşit olup olmadığını kontrol eder. Öyleyse, 603 adımı meydana gelir; değilse, 601 adımı meydana gelir.

Adım 603: MME, aynı zamanda bir EPS AKA kimlik doğrulama prosedürünü ve bir NAS SMC prosedürünü tetikler ve AKA kimlik doğrulama prosedürü tarafından oluşturulan güvenlik bağlamını etkinleştirir. NAS sayım değeri 0 olarak başlatılır.

Bu örnekte, EPS AKA kimlik doğrulama prosedürü NAS SMC prosedürüne bağlanır, böylece NAS'ın farklı yönlerde kaçınılır (çıkış yolu yönü ve indirme yolu yönü) sayım değerinin kaymak üzere olduğunun tespit edilmesi durumunda EPS AKA kimlik doğrulama prosedürünün tekrar tekrar tetiklenmesinden kaçınılır, EPS AKA kimlik doğrulama prosedürleri azaltılarak, gereksiz EPS AKA kimlik doğrulama prosedürlerinin tetiklenmesinden kaynaklanan kaynak israfı önlenir ve kaynak tasarrufu sağlanır.

ŞEKİL 7, mevcut buluşun birinci uygulamasındaki bir kimlik doğrulama yönteminin bir akış şemasıdır. Şekil 7'de gösterildiği gibi, bu uygulamadaki yöntem aşağıdaki adımları içerir:

Adım 801: MME bir EPS AKA kimlik doğrulama prosedürü başlatır.

Adım 802: Varsayılan hizmet için bir Kimlik doğrulama ve Anahtar Anlaşması (AKA) kimlik doğrulama prosedürü başarısız olursa, MME, yerel bilgiye göre varsayılan hizmetle bağlantıyı serbest bırakmayı veya korumayı tespit eder.

Ayrıca, 801 adımındaki MME, çeşitli koşullar altında EPS AKA kimlik doğrulama prosedürünü başlatabilir. Örneğin, NAS sayım değeri bir sayım eşiğine ulaştığında (maksimum değere yaklaşır), MME EPS AKA kimlik doğrulama işlemini başlatır.

Yerel bilgiler aşağıdakilerden en az birini içerebilir: varsayılan hizmet tipi, QoS, UE kimlik doğrulama yeterliliği gerçekleştirme kabiliyeti, ağ politikası, SIM/Evrensel Abone Kimlik Modülü (USIM) tipi veya SIM/USIM'in UE'ye eklenip eklenmediği hakkında bilgi veya bunların herhangi bir kombinasyonu. Varsayılan hizmet tipi varsayılan hizmetin tipini göstermektedir. MME, varsayılan hizmetin varsayılan hizmet tipine göre kimlik doğrulama gerektirip gerektirmediğini tespit edebilir. QoS, kimlik doğrulama gerektirmeyen hizmeti tanımlar ve MME, varsayılan hizmetin QoS'a göre kimlik doğrulaması gerektirip gerektirmediğini de tespit eder. UE kimlik doğrulama yeteneği, UE'nin EPS AKA kimlik doğrulama prosedürünü gerçekleştirip gerçekleştiremediğini tespit etmesi için MME'nin temelini oluşturur. SIM tipi ayrıca UE'nin EPS AKA kimlik doğrulama prosedürünü gerçekleştirip gerçekleştiremediğini göstermektedir ve MME, UE'nin SIM tipine göre EPS AKA kimlik doğrulama prosedürünü gerçekleştirip gerçekleştiremediğini bilir. Kimlik doğrulama yalnızca UE'ye bir SIM/USIM eklendiğinde uygulanabilir olduğundan, UE'ye bir SIM/USIM eklendikten sonra EPS AKA kimlik doğrulama prosedürü başarısız olursa, NAS sinyalleme bağlantısı serbest bırakılmalıdır; UE'ye SIM/USIM eklenmemişse, MME bağlantının ağ politikasına göre serbest bırakılıp bırakılmayacağına karar verir. Ağ politikası, varsayılan hizmetin doğrulanıp doğrulanmayacağına karar vermek için bir ağ cihazı tarafından kurulur.

Yukarıda belirtilen yerel bilgilere ve ağ politikasına göre, adım 802 şunları içerebilir: MME varsayılan hizmetine, ağ politikasına göre doğrulanmamış bir hizmet olarak izin verilmezse, MME varsayılan hizmetin bağlantısını serbest bırakır.

Ağ politikasına göre varsayılan hizmetin doğrulanmamış bir hizmet olarak kabul edilip edilmediğinin ve aşağıdaki koşullardan herhangi birinin yerine getirilip getirilmediğinin tespiti halinde, MME varsayılan hizmetle bağlantıda bulunur: varsayılan hizmet, varsayılan hizmet türü veya yerel bilgilerdeki QoS.

Ağ politikasının varsayılan hizmete doğrulanmamış bir hizmet olarak izin verdiğini tespit etmek ve aşağıdaki koşullardan herhangi birinin yerine getirildiğini tespit etmek için MME varsayılan hizmetin bağlantısını serbest bırakır: varsayılan hizmet, varsayılan hizmet tipine veya yerel bilgideki QoS'ye göre kimlik doğrulaması gerektirmez.

Örneğin, eğer MME ağ politikasının varsayılan hizmetin kimlik doğrulamamasına izin verdiğini tespit ederse, MME, UE tarafından talep edilen hizmetin bir EMC hizmeti veya bir genel alarm hizmeti olduğunu bilmek için varsayılan hizmet tipini tespit eder. EMC hizmeti veya genel alarm hizmeti kimlik doğrulaması gerektirmiyorsa ve ağ ilkesi kimliği doğrulanmamış EMC veya genel alarm hizmetine izin veriyorsa, MME ve UE varsayılan hizmete devam eder.

Eğer varsayılan hizmet NAS sinyalleme bağlantısında taşınan tek bir hizmet ise, MME, NAS sinyalleşme bağlantısını serbest bırakarak varsayılan hizmetin bağlantısını serbest bırakabilir. NAS sinyalleme bağlantısı çoklu hizmet taşıyorsa ve varsayılan hizmet tipi varsayılan tüm hizmetlerin kimlik doğrulaması gerektiğine işaret ediyorsa, MME NAS sinyalinin bağlantısını serbest bırakır. Varsayılan hizmetlerin bir kısmının kimlik doğrulaması yapması gerekiyorsa ve diğer varsayılan hizmetler, kimlik doğrulaması gerektirmiyorsa (EMC gibi), MME, kimlik doğrulama gerektiren hizmete karşılık gelen EPS taşıyıcısını serbest bırakır ve kimlik doğrulaması gerektirmeyen hizmete karşılık gelen EPS taşıyıcısını (EMC taşıyıcısı gibi) tutar. Yukarıdaki EPS taşıyıcısı NAS sinyalleme bağlantısına dayanmaktadır.

Bu örnekte, varsayılan hizmet aşağıdaki durumlarda devam edebilir: kimlik doğrulama başarısız olursa; UE tarafından talep edilen hizmet, kimlik doğrulama gerektirmez veya UE, EPS AKA kimlik doğrulama prosedürünü gerçekleştiremez veya UE'ye SIM/USIM eklenemezse; ve ağ politikası, varsayılan hizmetin doğrulanmamasını desteklerse. Bu nedenle, varsayılan hizmetin kesilmesi önlenir ve sistem kaynakları muhafaza edilir.

ŞEKİL 8, bir yedinci örnekte kimlik doğrulama cihazının yapısını göstermektedir. Şekil 8'de gösterildiği gibi, bu örnekteki kimlik doğrulama cihazı bir tespit modülü (11) ve bir işlemci (12) içermektedir. Tespit modülü (11), bir NAS sayım değeri maksimum bir değere yaklaştığında yerel bilgileri tespit etmek üzere yapılandırılmıştır; ve işlemci (12), bir tespit sonucuna göre UE ile Kimlik doğrulama ve Anahtar Anlaşması prosedürünü

gerçekleştirmek için bir prosedürün tetiklenip tetiklenmeyeceğine karar verecek şekilde yapılandırılmıştır.

Bu örnekteki kimlik doğrulama cihazı, yukarıdaki birinci uygulamada sağlanan yönteme göre çalışabilir.

ŞEKİL 9, sekizinci örnekte bir kimlik doğrulama cihazının yapısını göstermektedir. Şekil 9'da gösterildiği gibi, bu uygulama yukarıdaki sekizinci uygulamaya dayanmaktadır, yerel bilgi güvenlik bağlamıdır ve işlemci (12) bir birinci etkinleştirme birimi (21) ve bir birinci tetikleyici birim (22) içerir. Birinci etkinleştirme birimi (21), tespit modülü (11), güvenlik bağlamlarının varsayılan olmayan güvenlik bağlamını içerdiğini tespit ettiği takdirde varsayılan olmayan güvenlik bağlamını etkinleştirmek üzere yapılandırılır. Birinci tetikleyici birim (22), eğer tespit modülü (11), güvenlik bağlamlarının, varsayılan olmayan bir güvenlik bağlamı içermediğini tespit ederse, bir Kimlik doğrulama ve Anahtar Anlaşması prosedürünü tetikleyecek şekilde yapılandırılır.

Bu örnekteki işlemci (12) ayrıca şunları içerebilir: UE'ye bir NAS SMC göndermek, bir NAS Güvenlik Modu Tamamlandı mesajı almak ve işlemcideki (12) birinci etkinleştime birimine (21) bilgi göndermek için yapılandırılmış bir alıcı-verici birim (23), burada bilgi harekete geçmek için birinci etkinleştime birimini (21) tetikler. Birinci etkinleştime birimi (21), varsayılan olmayan güvenlik bağlamını tetikleyici bilgiye göre etkinleştirir. Birinci tetikleyici birim (22), alıcı-verici birim (23), UE'den NAS Güvenlik Modu Tamamlandı mesajı almazsa, bir Kimlik doğrulama ve Anahtar Anlaşması prosedürünü tetikler.

Bu örnekteki kimlik doğrulama cihazı, yukarıdaki ikinci örnekte verilen yönteme göre çalışabilir.

ŞEKİL 10, mevcut buluşun dokuzuncu örneğindeki bir kimlik doğrulama cihazının yapısını göstermektedir. ŞEKİL 10'da gösterildiği gibi, bu örnek yukarıdaki birinci uygulamaya dayanmaktadır, yerel bilgi zamanlayıcı durumudur ve işlemci (12), bir ikinci etkinleştime birimi (31) ve bir ikinci tetikleyici birim (32) içerir. İkinci etkinleştime birimi (31), tespit modülü (11), zamanlayıcı durumunun "çalışıyor" olduğunu tespit ederse, varsayılan olmayan güvenlik bağlamını etkinleştirmek üzere yapılandırılır. İkinci tetikleyici birimi (32), eğer tespit modülü (11), zamanlayıcı durumunun "duruyor"

olduğunu tespit ederse, Kimlik doğrulama ve Anahtar Anlaşması prosedürünü tetikleyecek şekilde yapılandırılır.

Bu örnekteki işlemci (12) ayrıca şunları içerebilir: UE'ye bir NAS SMC göndermek, bir NAS Güvenlik Modu Tamamlandı mesajı almak ve işlemcideki (12) ikinci etkinleştirme birimine (31) bilgi göndermek için yapılandırılmış bir alıcı-verici birim (33), burada bilgi ikinci etkinleştirme biriminin (31) harekete geçmesi için tetikler. İkinci etkinleştirme birimi (31), varsayılan olmayan güvenlik bağlamını tetikleyici bilgisine göre etkinleştirir. İkinci tetikleyici birim (32), alıcı-verici birim (33), UE'den NAS Güvenlik Modu Tamamlandı mesajı almazsa bir Kimlik doğrulama ve Anahtar Anlaşması prosedürünü tetikler.

Bu örnekteki kimlik doğrulama cihazı, yukarıdaki üçüncü örnekte verilen yönteme göre çalışabilir.

ŞEKİL 11, onuncu örnekteki bir kimlik doğrulama cihazının yapısını göstermektedir. ŞEKİL 11'de gösterildiği gibi, bu örnek yukarıdaki sekizinci uygulamaya dayanmaktadır, yerel bilgi bir durum makinesinin durumudur, işlemci (12) bir üçüncü etkinleştirme birimi (41) ve bir üçüncü tetikleyici birim (42) içerir. Üçüncü etkinleştirme birimi (41), tespit modülü (11), durum makinesinin durumunu "çalışıyor" olarak tespit ederse varsayılmayan güvenlik bağlamını etkinleştirmek için yapılandırılır. Üçüncü tetikleyici birim (42), eğer tespit modülü (11) durum makinesinin durumunu "boşta" olarak tespit ederse, bir Kimlik doğrulama ve Anahtar Anlaşması prosedürünü tetikleyecek şekilde yapılandırılır.

Bu örnekteki işlemci (12) ayrıca şunları içerebilir: UE'ye bir NAS SMC göndermek, bir NAS Güvenlik Modu Tamamlandı mesajı almak ve işlemcideki (12) üçüncü etkinleştirme birimine (41) bilgi göndermek için yapılandırılmış bir alıcı-verici birim (43), burada bilginin üçüncü etkinleştime birimini (41) harekete geçmesi için tetikler. Üçüncü etkinleştirme birimi (41), varsayılan olmayan güvenlik bağlamını tetikleyici bilgisine göre etkinleştirir. Üçüncü tetikleyici birim (42), alıcı-verici birim (43), UE'den NAS Güvenlik Modu Tamamlandı mesajı almazsa bir Kimlik doğrulama ve Anahtar Anlaşması prosedürünü tetikler.

Bu örnekteki kimlik doğrulama cihazı, yukarıdaki dördüncü örnekte verilen yönteme göre çalışabilir.

ŞEKİL (12), on birinci örnekteki bir kimlik doğrulama cihazının yapısını göstermektedir. ŞEKİL (12)'de gösterildiği gibi, bu örnek yukarıdaki birinci uygulamaya dayanmaktadır, yerel bilgi varsayılan hizmet tipi veya QoS veya UE kimlik doğrulama gerçekleştirme kabiliyetidir. İşlemci (12), bir dördüncü tetikleyici birim (51) ve bir işlem birimine (52) sahiptir. Dördüncü tetikleyici birim (51), eğer tespit modülü (11) varsayılan hizmet tipine karşılık gelen hizmetin kimlik doğrulaması gerektirdiğini veya QoS'ye karşılık gelen hizmet için kimlik doğrulaması gerektiğini veya UE'nin bir Kimlik doğrulama ve Anahtar Anlaşması prosedürü gerçekleştirme yeteneğine sahip olduğunu tespit ederse, kimlik doğrulama ve Anahtar Anlaşması prosedürünü tetiklemek üzere yapılandırılır. İşlem birimi (52), şu şekilde yapılandırılmıştır: varsayılan güvenlik bağlamını kullanmaya devam etmek veya varsayılan hizmet için hiç bir güvenlik koruması sağlamamak veya tespit modülünün (11), varsayılan hizmet tipine karşılık gelen hizmetin kimlik doğrulaması gerektirmemesini tespit etmesi durumunda varsayılan hizmetin bağlantısını kesmek veya QoS'ye karşılık gelen hizmetin kimlik doğrulaması gerektirmemesi veya UE'nin bir Kimlik doğrulama ve Anahtar Anlaşması prosedürü gerçekleştirememesi durumu.

Bu örnekteki kimlik doğrulama cihazı, yukarıdaki beşinci örnekte verilen yönteme göre çalışabilir.

Bu örnekte verilen cihazda, MME, NAS sayım değerinin kaymak üzere olduğunu tespit ettiği anda EPS AKA kimlik doğrulama prosedürünü tetiklemez, böylece EPS AKA kimlik doğrulama prosedürlerini tetiklemek için süreleri azaltır, gereksiz EPS AKA kimlik doğrulama prosedürlerinin neden olduğu kaynak israfını engeller ve kaynak tasarrufu sağlanır.

ŞEKİL 13, mevcut buluşun ikinci uygulamasındaki bir kimlik doğrulama cihazının yapısını göstermektedir. Şekil 13'de gösterildiği gibi, bu uygulamadaki cihaz şunları içerir: bir AKA kimlik doğrulama prosedürünü yürütmek için yapılandırılmış bir yürütme modülü (61); ve yürütme modülü (61), Kimlik doğrulama ve Anahtar Anlaşması prosedürünü yerine getirmediğinde yerel bağlantıya ve ağ politikasına göre bir

bağlantıyı serbest bırakmaya veya varsayılan bir hizmeti sürdürmeye karar verecek şekilde yapılandırılmış bir işlemci (62).

Bu uygulamadaki cihaz ayrıca şunları içerebilir: maksimum değere yakın NAS sayım değeri gibi tetikleme koşullarına göre bir Kimlik doğrulama ve Anahtar Anlaşması prosedürünü yürütmek üzere yürütme modülünü (61) tetiklemek üzere yapılandırılmış bir tetikleme modülü (63).

İşlemci (62) ayrıca şunları içerebilir: yürütme modülü (61), Kimlik Doğrulama ve Anahtar Anlaşması prosedürünü yerine getirmediği takdirde, ağ politikasının varsayılan hizmetin doğrulanmamasını destekleyip desteklemediğini yargılamak üzere yapılandırılmış bir birinci değerlendirme birimi (64), birinci değerlendirme birimi (64) olumsuz bir değerlendirme yaparsa, varsayılan hizmetin bağlantısını serbest bırakacak şekilde yapılandırılmış bir birinci serbest bırakma birimi (65), bir ikinci değerlendirme birimi aşağıdakiler için yapılandırılmıştır: birinci değerlendirme birimi (64) olumlu bir değerlendirme yaparsa, varsayılan hizmetin varsayılan hizmet türüne veya yerel bilgideki QoS'ye göre kimlik doğrulaması gerektirip gerekmediğini veya UE'nin Kimlik Doğrulama ve Anahtar Anlaşması prosedürünü gerçekleştirip gerçekleştiremediğini değerlendirmek için, eğer ikinci değerlendirme birimi (66) olumlu bir değerlendirme yaparsa, varsayılan hizmetin bağlantısını serbest bırakacak şekilde yapılandırılmış bir ikinci serbest bırakma birimi (67) ve eğer ikinci değerlendirme birimi (66) olumsuz bir değerlendirme yaparsa, varsayılan hizmeti yürütmeye devam etmek üzere yapılandırılmış bir yürütme birimi (68).

Bu uygulamadaki kimlik doğrulama cihazı yukarıdaki birinci uygulamada sağlanan yönteme göre çalışabilir.

Bu uygulamada, varsayılan hizmet, aşağıdaki durumlarda devam edebilir: kimlik doğrulama, başarısız olursa; UE tarafından talep edilen hizmet, kimlik doğrulama gerektirmez veya UE, EPS AKA kimlik doğrulama prosedürünü gerçekleştiremez veya UE'ye SIM/USIM eklenemezse; ve ağ politikası, varsayılan hizmetin doğrulanmamasını desteklerse. Bu nedenle, varsayılan hizmetin kesilmesi önlenir ve sistem kaynakları muhafaza edilir.

Teknikte sıradan uzmanlığa sahip kişiler, mevcut buluşun uygulamalarına göre yöntem adımlarının tamamının veya bir kısmının, ilgili donanımı öğreten bir program tarafından uygulanabileceğini anlamalıdırlar. Program, bilgisayar tarafından okunabilen bir depolama ortamında saklanabilir. Program çalıştığında, mevcut buluşun uygulamalarına göre yöntemin adımları gerçekleştirilir. Depolama ortamı, Salt Okunur Bellek (ROM), Rasgele Erişim Belleği (RAM), manyetik disk veya Kompakt Bir Salt Okunur Bellek (CD-ROM) gibi program kodlarını depolayabilen herhangi bir ortam olabilir.

Son olarak, yukarıdaki uygulamaların sadece mevcut buluşun teknik çözümlerini tarif etmek için sağlandığı, ancak mevcut buluşu sınırlama amacı taşımadığı belirtilmelidir. Teknikte uzman kişilerin, buluşun kapsamından ayrılmadan buluş üzerinde çeşitli modifikasyonlar ve değişiklikler yapabilecekleri açıktır. Mevcut buluş, aşağıdaki istemlerle veya bunların eşdeğerleriyle tanımlanan koruma kapsamına girmeleri koşuluyla, modifikasyonları ve varyasyonları kapsamayı amaçlamaktadır.

Mevcut buluşun başka uygulamaları aşağıda verilmiştir. Aşağıdaki bölümde kullanılan numaralandırmanın, önceki bölümlerde kullanılan numaralandırmaya uyması gerekmediğine dikkat edilmelidir.

Uygulama 1. Bir kimlik doğrulama yöntemi olup aşağıdakileri içerir:

bir kablosuz iletişim ağı varlığı tarafından, varsayılan hizmet için bir Kimlik doğrulama ve Anahtar Anlaşması prosedürü başarısız olursa, varsayılan bir hizmetin bir ağ politikasına uygun olarak kimliği doğrulanmamış bir hizmet olarak izin verilip verilmediğinin tespit edilmesi;

ağ politikasına uygun olarak kimliği doğrulanmamış bir hizmet olarak varsayılan hizmete izin veriliyorsa ve varsayılan hizmetin doğrulanması gerekmiyorsa, varsayılan hizmetin bir bağlantısının muhafaza edilmesi; veya

ağ politikasına uygun olarak kimliği doğrulanmamış bir hizmet olarak varsayılan hizmete izin veriliyorsa ve bir Kullanıcı Ekipmanı, Kimlik doğrulama ve Anahtar Anlaşması prosedürünü gerçekleştiremezse, varsayılan hizmetin bir bağlantısının muhafaza edilmesi; veya

ağ politikasına uygun olarak kimliği doğrulanmamış bir hizmet olarak varsayılan hizmete izin veriliyorsa ve Kullanıcı Ekipmanına kart eklenmemişse, varsayılan hizmetin bir bağlantısının muhafaza edilmesi.

Uygulama 2. Uygulama 1'e göre yöntem olup, ayrıca aşağıdakileri içerir
ağ politikasına uygun olarak kimliği doğrulanmamış bir hizmet olarak varsayılan hizmete izin verilmiyorsa, varsayılan hizmetin bağlantısının serbest bırakılması.

Uygulama 3. Uygulama 1 veya uygulama 2'ye göre bir yöntem olup, ayrıca aşağıdakileri içerir:

ağ politikasına uygun olarak kimliği doğrulanmamış bir hizmet olarak varsayılan hizmete izin veriliyorsa ve varsayılan hizmetin doğrulanması gerekiyorsa, varsayılan hizmetin bağlantısının serbest bırakılması; veya

ağ politikasına uygun olarak kimliği doğrulanmamış bir hizmet olarak varsayılan hizmete izin veriliyorsa ve Kullanıcı Ekipmanı, Kimlik doğrulama ve Anahtar Anlaşması prosedürünü yerine getirebiliyorsa, varsayılan hizmetin bağlantısının serbest bırakılması; veya

ağ politikasına uygun olarak kimliği doğrulanmamış bir hizmet olarak varsayılan hizmete izin verilirse ve Kullanıcı Ekipmanına bir kart eklenmişse, varsayılan hizmetin bağlantısının serbest bırakılması.

Uygulama 4. Ayrıca, aşağıdakileri içeren 1 ila 3 arasında yer alan uygulamalardan herhangi birine göre yöntem olup, aşağıdakileri içerir:
varsayılan hizmetin varsayılan hizmet tipine veya Hizmet Kalitesine göre kimlik doğrulaması gerektirip gerektirmediğinin tespit edilmesi.

Uygulama 5. 1 ila 3 arasında yer alan uygulamalardan herhangi birine göre bir yöntem olup, ayrıca aşağıdakileri içerir:
Kullanıcı Ekipmanının, Kullanıcı Ekipmanı kimlik doğrulama yeteneği bilgisi veya bir Abone Kimlik Modülü tipine göre Kimlik doğrulama ve Anahtar Anlaşması prosedürünü gerçekleştirip gerçekleştiremediğinin tespit edilmesi.

Uygulama 6. 2 ila 5 arasında yer alan uygulamalardan herhangi birine göre bir yöntem olup, burada varsayılan hizmetin bağlantısının serbest bırakılması aşağıdakileri içerir:

bir Erişilemeyen Tabaka sinyalleme bağlantısı tek hizmet taşıyorsa, Erişilemeyen Tabaka sinyalleme bağlantısının serbest bırakılması veya

Erişilemeyen Tabaka sinyalleme bağlantısı çoklu hizmet taşıyorsa ve tüm çoklu hizmetlerin kimlik doğrulaması yapması gerekiyorsa, Erişilemeyen Tabaka sinyalleşme bağlantısının serbest bırakılması.

Uygulama 7. 2 ila 5 arasında yer alan uygulamalardan herhangi birine göre bir yöntem olup, burada varsayılan hizmetin bağlantısının serbest bırakılması aşağıdakileri içerir:

bir Erişilemeyen Tabaka sinyalleme bağlantısı çoklu hizmet taşıyorsa ve çoklu hizmetin bir kısmı kimlik doğrulama gerektiriyorsa ve diğerleri kimlik doğrulama gerektirmiyorsa, kimlik doğrulama gerektiren hizmete karşılık gelen bir Gelişmiş Paket Sistem taşıyıcısını serbest bırakır ve kimlik doğrulaması gerektirmeyen hizmete karşılık gelen Gelişmiş Paket Sistem taşıyıcısını muhafaza eder.

Uygulama 8. 1 ila 7 arasında yer alan uygulamalardan herhangi birine göre bir yöntem olup, burada:

Kimlik doğrulama ve Anahtar Anlaşması prosedürü aşağıdaki koşullar altında tetiklenir: bir Erişilemeyen Tabaka sayım değeri bir sayma eşiğine veya bir operatör politikasına veya ağlar arasında bir Kullanıcı Ekipmanı devrine ulaşır.

Uygulama 9. 1 ila 7 arasında yer alan uygulamalardan herhangi birine göre bir yöntem olup, burada:

varsayılan hizmet, Acil Çağrı hizmetinden en az bir tanesini ve bir genel alarm hizmetini içerir.

Uygulama 10. Uygulama 9'a göre yöntem olup, burada:

Acil Çağrı hizmeti, kimlik doğrulama gerektirmeyen veya kimlik doğrulama gerektiren EMC hizmetidir;

genel alarm hizmeti, kimlik doğrulama gerektirmeyen veya kimlik doğrulama gerektiren genel alarm hizmetidir.

Uygulama 11. 1 ila 10 arasında yer alan uygulamalardan herhangi birine göre bir yöntem olup, burada kablosuz iletişim ağı varlığı bir Mobilite Yönetimi Varlığı içerir.

Uygulama 12. Bir cihaz olup, aşağıdakileri içerir:

Bir Kimlik doğrulama ve Anahtar Anlaşması prosedürünü yürütmek üzere yapılandırılmış bir yürütme modülü; ve

bir kablosuz iletişim ağı varlığına yerleştirilmiş bir işlemci olup, aşağıdakileri içerir:

varsayılan hizmet için Kimlik doğrulama ve Anahtar Anlaşması prosedürü başarısız olursa, bir varsayılan hizmetin bir ağ politikasına göre bir kimliği doğrulanmamış hizmet olarak izin verilip verilmediğini tespit etmek üzere yapılandırılmış bir birinci değerlendirme birimi;

varsayılan hizmetin kimlik doğrulaması gerektirip gerektirmediğini veya Kullanıcı Ekipmanının Kimlik doğrulama ve Anahtar Anlaşması prosedürünü gerçekleştirip gerçekleştiremediğini veya birinci değerlendirme birimi varsayılan hizmete ağ politikasına göre kimliği doğrulanmamış bir hizmet olarak izin verildiğini tespit ederse, Kullanıcı Ekipmanına bir kart eklenip eklenmediğini tespit etmek üzere yapılandırılmış bir ikinci değerlendirme birimi;

ikinci değerlendirme birimi varsayılan hizmetin kimlik doğrulaması gerektirmemesi durumunda ya da Kullanıcı Ekipmanı Kimlik doğrulama ve Anahtar Anlaşması prosedürünü gerçekleştiremiyorsa ya da Kullanıcı Ekipmanına kart eklenmemişse, varsayılan hizmetin bağlantısını sürdürecek şekilde yapılandırılmış bir yürütme birimi.

Uygulama 13. Uygulama 12'ye göre cihaz olup, ayrıca şunları içerir:

birinci değerlendirme biriminin varsayılan hizmete, ağ politikasına uygun olarak kimliği doğrulanmamış bir hizmet olarak izin verilmediğini tespit etmesi durumunda, varsayılan hizmetin bağlantısını serbest bırakacak şekilde yapılandırılmış bir birinci serbest bırakma birimi.

Uygulama 14. Uygulama 12 veya uygulama 13'e göre cihaz olup, ayrıca şunları içerir:

ikinci değerlendirme birimi varsayılan hizmetin kimlik doğrulaması gerektirdiğini tespit ederse veya Kullanıcı Ekipmanı Kimlik doğrulama ve Anahtar Anlaşması prosedürünü gerçekleştirebiliyorsa veya kart Kullanıcı Ekipmanına eklenmişse, varsayılan hizmetin bağlantısını serbest bırakacak şekilde yapılandırılmış bir ikinci serbest bırakma birimi.

Uygulama 15. 12 ila 14 arasında yer alan uygulamalardan herhangi birine göre cihaz olup, burada ikinci değerlendirme birimi, varsayılan hizmetin mevcut bir hizmet tipine veya Hizmet Kalitesine göre kimlik doğrulama gerektirip gerektirmediğini veya Kullanıcı Ekipmanının Kimlik doğrulama ve Anahtar Anlaşması prosedürünü gerçekleştirip gerçekleştiremediğini veya birinci değerlendirme biriminin varsayılan hizmete ağ politikasına uygun olarak kimliği doğrulanmamış bir hizmet olarak izin verildiğini tespit etmesi durumunda kartın Kullanıcı Ekipmanına eklenip eklenmediğini tespit etmek için yapılandırılır.

Uygulama 16. 12 ila 14 arasında yer alan uygulamalardan herhangi birine göre cihaz olup, burada ikinci değerlendirme birimini, varsayılan hizmetin kimlik doğrulaması gerektirip gerektirmediğini veya Kullanıcı Ekipmanının, Kullanıcı Ekipmanına veya yerel bilgideki bir kart tipine uygun olarak Kimlik doğrulama ve Anahtar Anlaşması prosedürünü gerçekleştirip gerçekleştiremediğini veya birinci değerlendirme biriminin varsayılan hizmete ağ politikasına uygun olarak kimliği doğrulanmamış bir hizmet olarak izin verildiğini tespit etmesi durumunda kartın Kullanıcı Ekipmanına eklenip eklenmediğini tespit etmek için yapılandırılır.

Uygulama 17. 13 ila 16 arasında yer alan uygulamalardan herhangi birine göre cihaz olup, burada birinci serbest bırakma birimi, aşağıdaki şekilde yapılandırılır:

Erişilemeyen Tabaka sinyalleme bağlantısı tek bir hizmete sahipse, bir Erişilemeyen Tabaka (Erişilemeyen Tabaka) sinyalleme bağlantısının serbest bırakılması;
Erişilemeyen Tabaka sinyalleme bağlantısı çoklu hizmet taşıyorsa ve tüm çoklu hizmetlerin kimlik doğrulaması gerekiyorsa, Erişilemeyen Tabaka sinyalleme bağlantısının serbest bırakılması.

Uygulama 18. 13 ila 16 arasında yer alan uygulamalardan herhangi birine göre cihaz olup, burada birinci serbest bırakma birimin, aşağıdaki şekilde yapılandırılır:

bir Erişilemeyen Tabaka sinyalleme bağlantısı çoklu hizmet taşıyorsa ve çoklu hizmet sağlayıcıların bir kısmı kimlik doğrulama gerektiriyorsa ve diğerleri kimlik doğrulama gerektirmiyorsa, kimlik doğrulama gerektiren hizmete karşılık gelen bir Gelişmiş Paket Sistemi (Gelişmiş Paket Sistemi) taşıyıcısının serbest bırakılması ve kimlik doğrulama gerektirmeyen hizmete karşılık gelen Gelişmiş Paket Sistemi taşıyıcısının muhafaza edilmesi.

Uygulama 19. 12 ila 18 arasında yer alan uygulamalardan herhangi birine göre cihaz olup, ayrıca aşağıdakileri içerir
bir Erişilemeyen Tabaka sayım değeri bir sayı eşiğine ulaşırsa veya bir Kullanıcı Ekipmanı ağlar arasında devredilirse veya bir operatör politikasına göre tetiklenirse, Kimlik doğrulama ve Anahtar Anlaşması prosedürünü yürütmek üzere yürütme modülünü tetiklemek üzere yapılandırılmış bir tetikleme modülü.

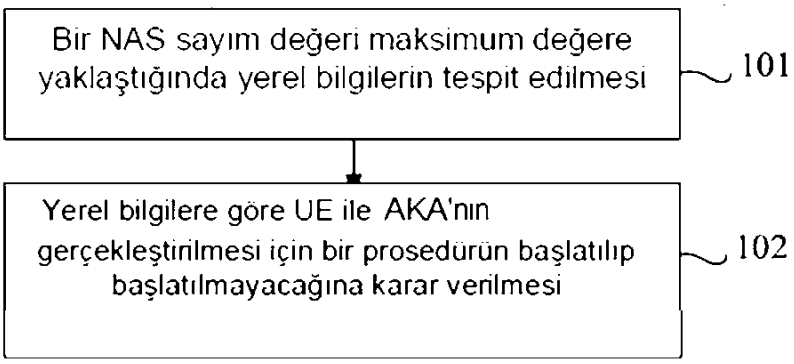
Uygulama 20. 12 ila 18 arasında yer alan uygulamalardan herhangi birine göre cihaz olup, burada:
varsayılan hizmet, Acil Çağrı hizmeti ve bir genel alarm hizmetinden en az bir tanesini içerir.

Uygulama 21. Uygulama 20'ye göre cihaz olup, burada:

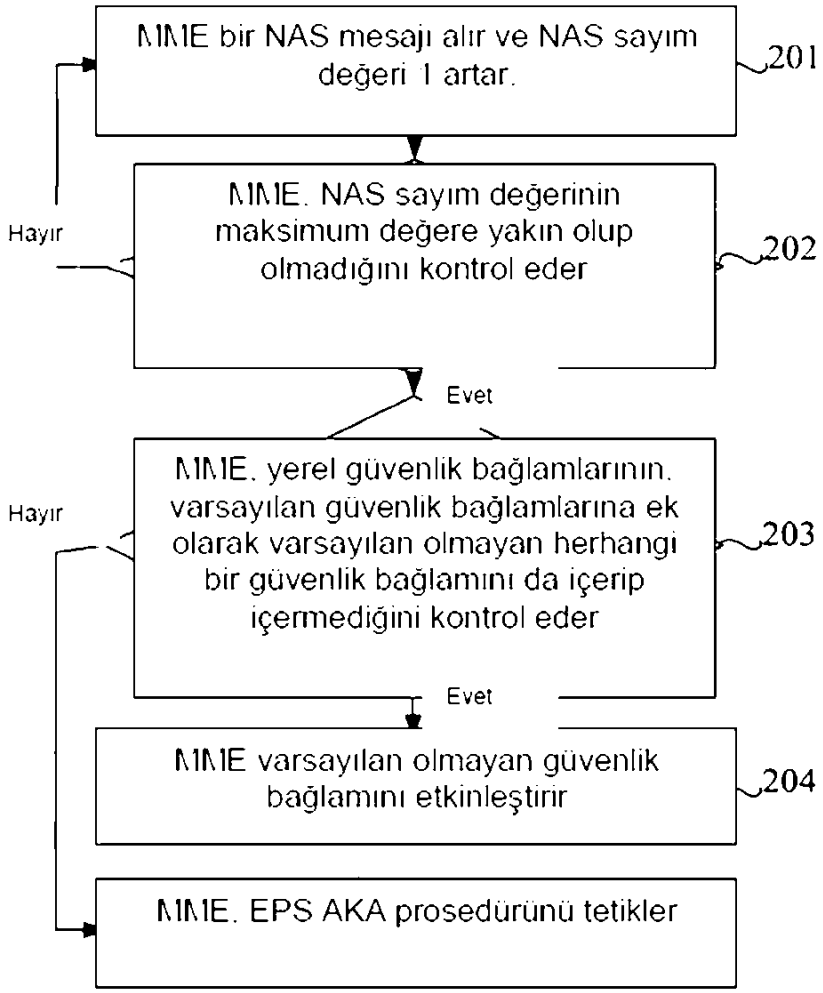
Acil Çağrı hizmeti, kimlik doğrulama gerektirmeyen veya kimlik doğrulama gerektiren EMC hizmetidir;

genel alarm hizmeti, kimlik doğrulama gerektirmeyen veya kimlik doğrulama gerektiren genel alarm hizmetidir.

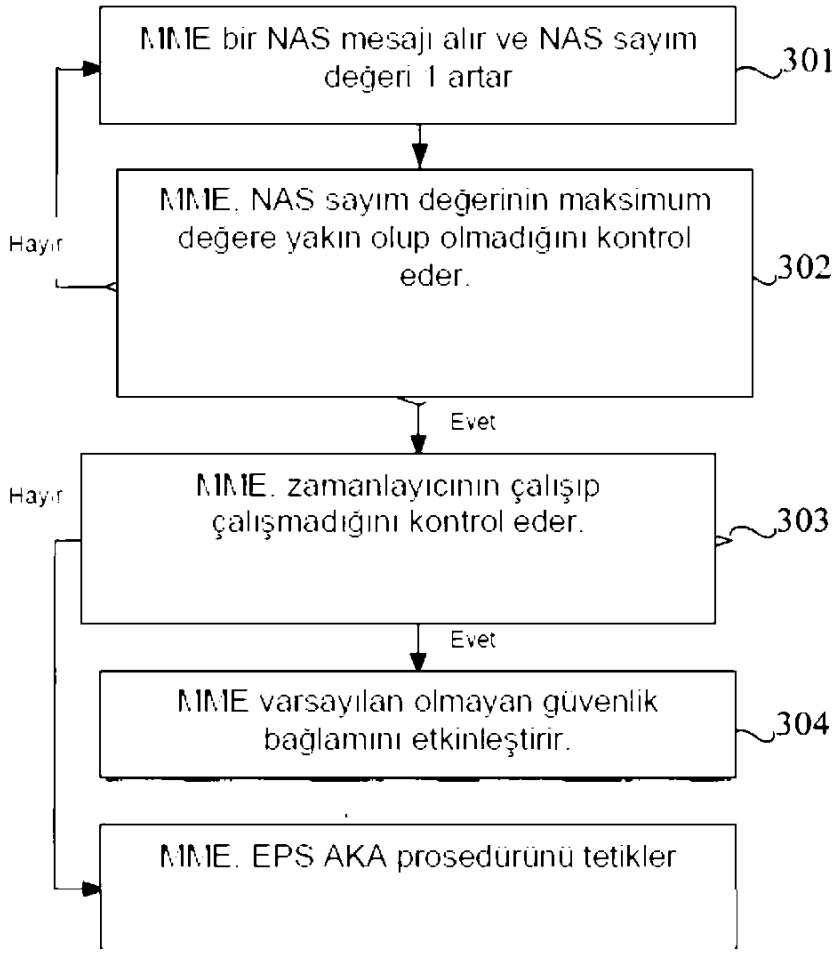
Uygulama (22). 12 ila 21 arasında yer alan uygulamalardan herhangi birine göre cihaz olup, burada kablosuz iletişim ağı varlığı bir Mobilite Yönetimi Varlığı içerir.


Bir NAS sayım değeri maksimum değere yaklaştığında yerel bilgilerin tespit edilmesi
101
Yerel bilgilere göre UE ile AKA'nın gerçekleştirilmesi için bir prosedürün başlatılıp başlatılmayacağına karar verilmesi
102

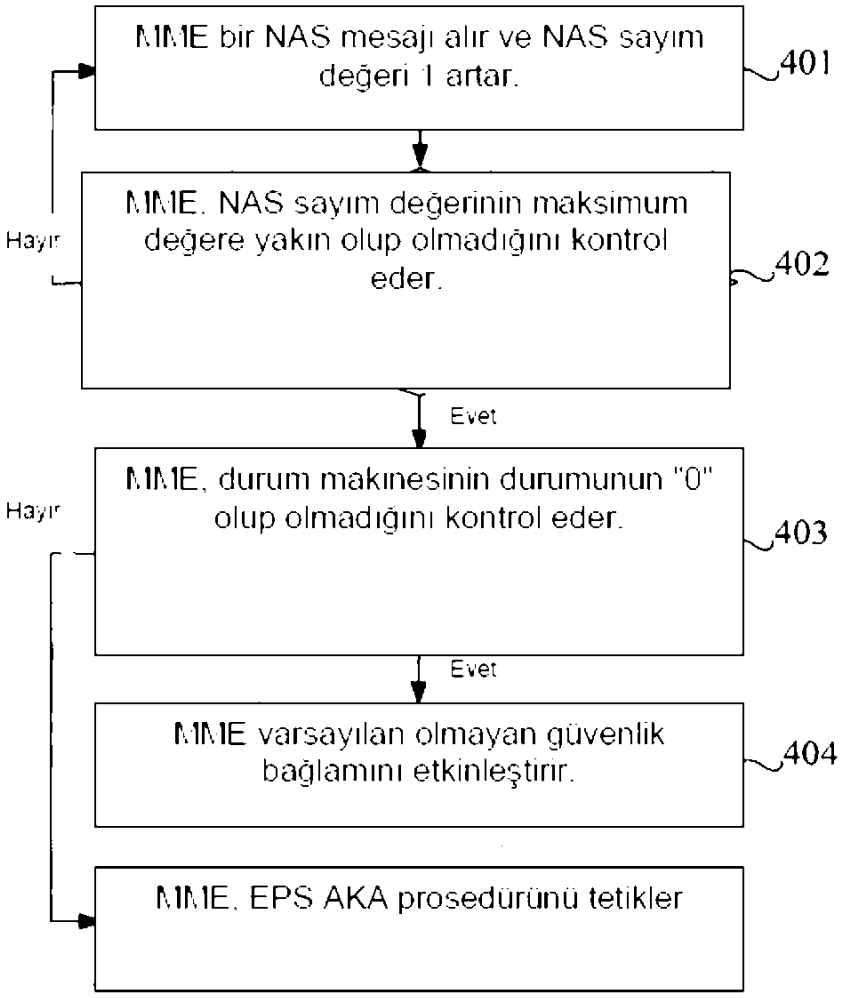
Şekil 1


MME bir NAS mesajı alır ve NAS sayım değeri 1 artar.
201
MME, NAS sayım değerinin maksimum değere yakın olup olmadığını kontrol eder
202
Hayır
Evet
MME, yerel güvenlik bağlamlarının, varsayılan güvenlik bağlamlarına ek olarak varsayılan olmayan herhangi bir güvenlik bağlamını da içerip içermediğini kontrol eder
203
Hayır
Evet
MME varsayılan olmayan güvenlik bağlamını etkinleştirir
204
MME, EPS AKA prosedürünü tetikler

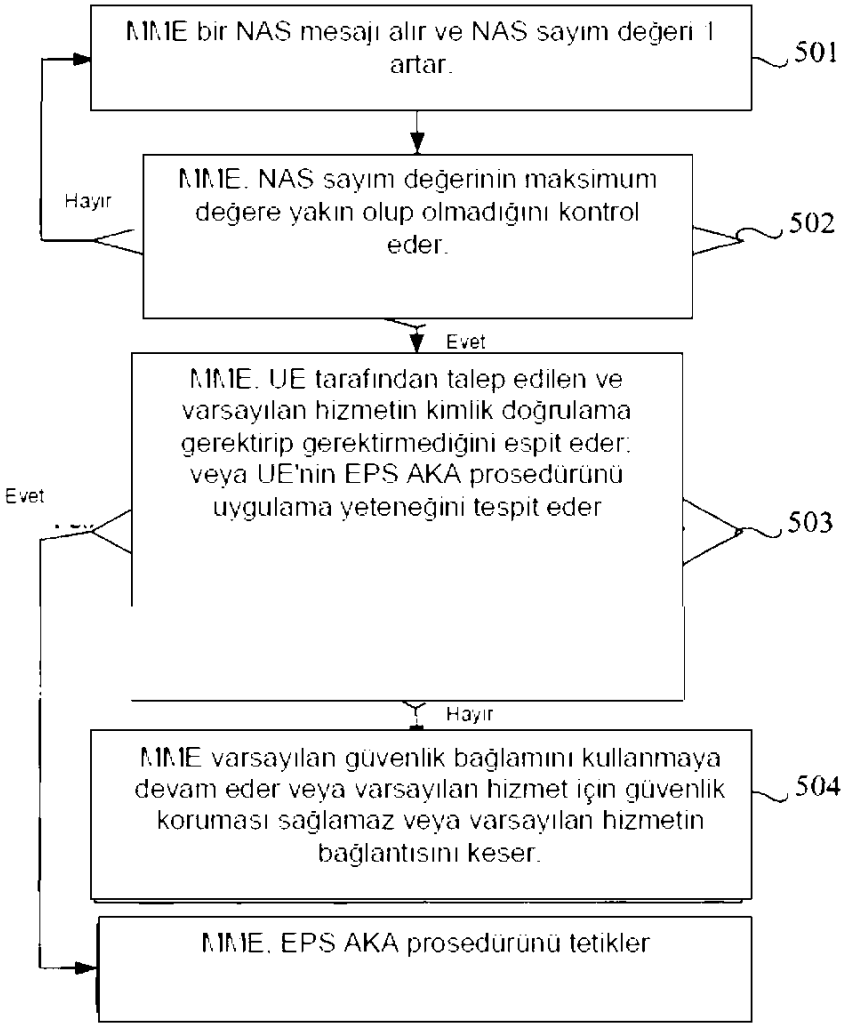
Şekil 2


MME bir NAS mesajı alır ve NAS sayım değeri 1 artar
301
MME, NAS sayım değerinin maksimum değere yakın olup olmadığını kontrol eder.
302
Hayır
Evet
MME, zamanlayıcının çalışıp çalışmadığını kontrol eder.
303
Hayır
Evet
MME varsayılan olmayan güvenlik bağlamını etkinleştirir.
304
MME, EPS AKA prosedürünü tetikler

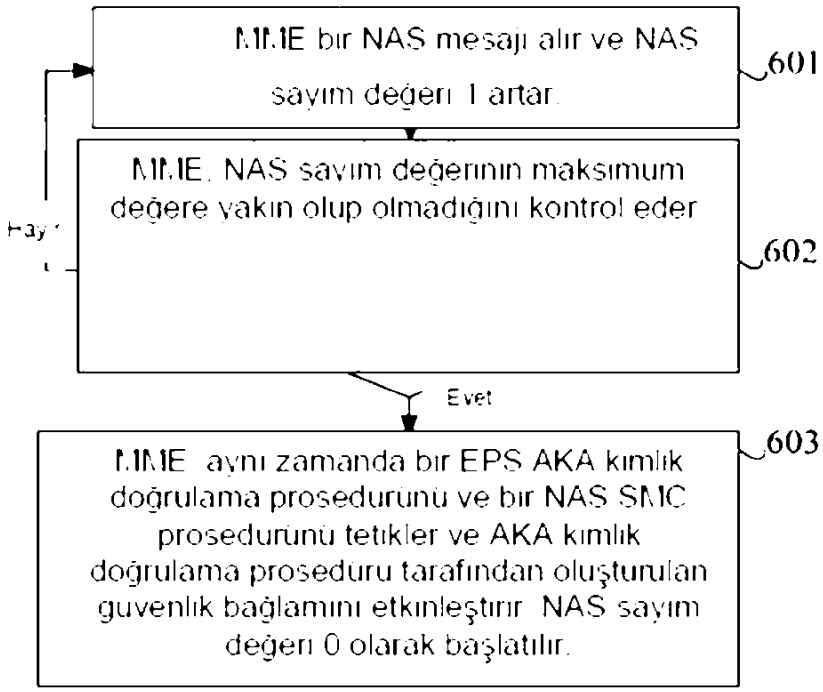
Şekil 3


MME bir NAS mesajı alır ve NAS sayım değeri 1 artar.
401
MME, NAS sayım değerinin maksimum değere yakın olup olmadığını kontrol eder.
402
Hayır
Evet
MME, durum makinesinin durumunun "0" olup olmadığını kontrol eder.
403
Hayır
Evet
MME varsayılan olmayan güvenlik bağlamını etkinleştirir.
404
MME, EPS AKA prosedürünü tetikler

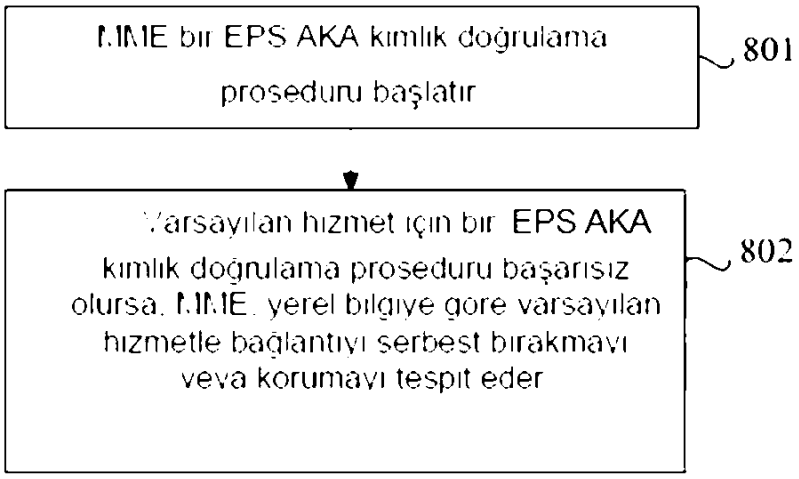
Şekil 4


MME bir NAS mesajı alır ve NAS sayım değeri 1 artar.
501
MME, NAS sayım değerinin maksimum değere yakın olup olmadığını kontrol eder.
502
Hayır
Evet
MME, UE tarafından talep edilen ve varsayılan hizmetin kimlik doğrulama gerektirip gerektirmediğini espit eder; veya UE'nin EPS AKA prosedürünü uygulama yeteneğini tespit eder
503
Evet
Hayır
MME varsayılan güvenlik bağlamını kullanmaya devam eder veya varsayılan hizmet için güvenlik koruması sağlamaz veya varsayılan hizmetin bağlantısını keser.
504
MME, EPS AKA prosedürünü tetikler

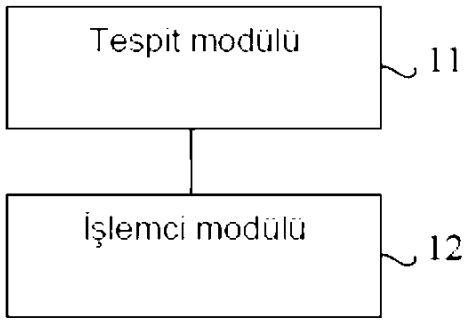
Şekil 5



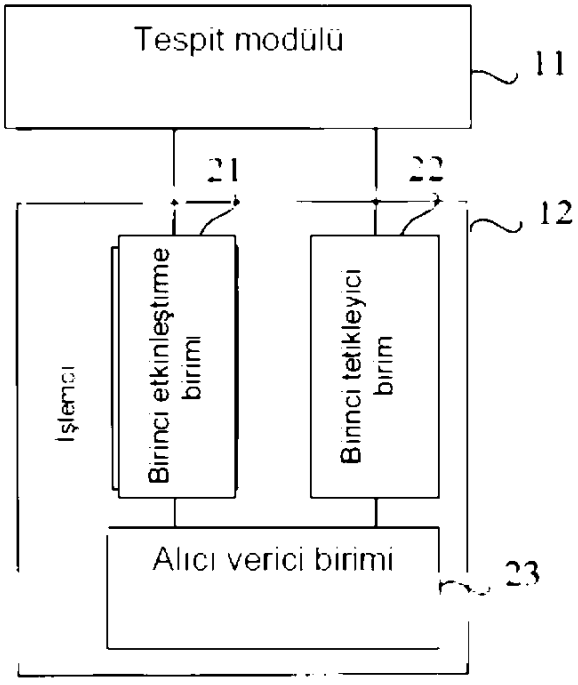
Şekil 6



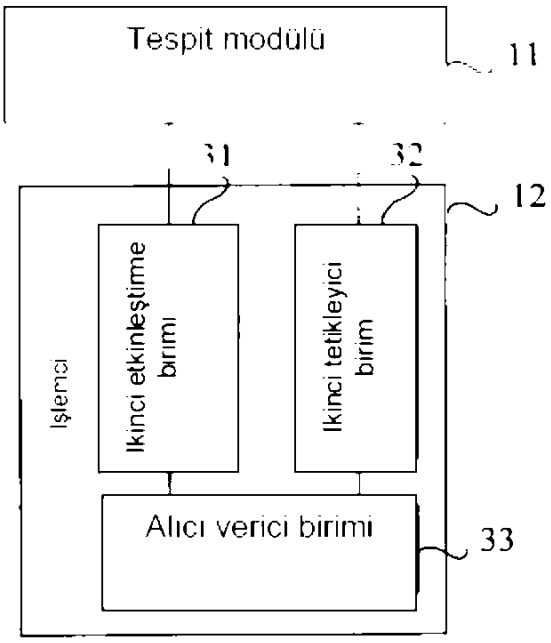
Şekil 7



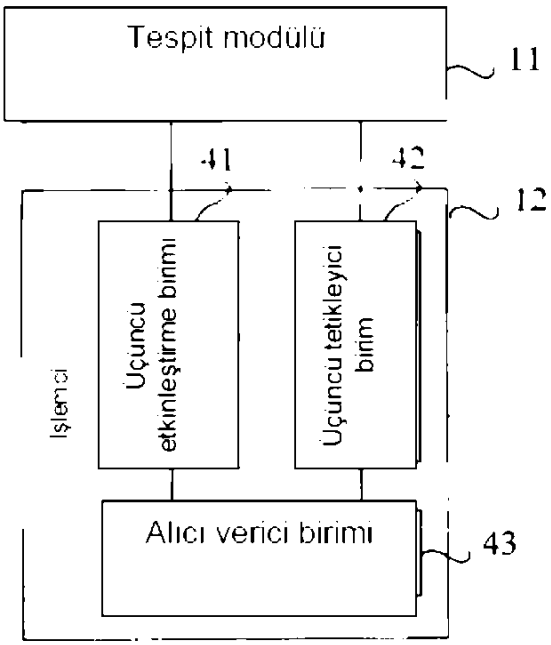
Şekil 8



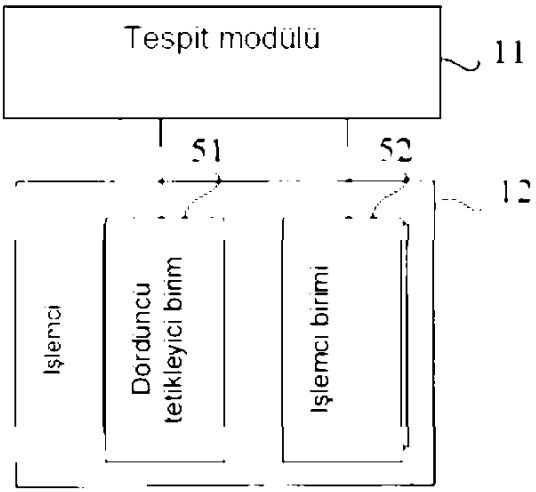
Şekil 9



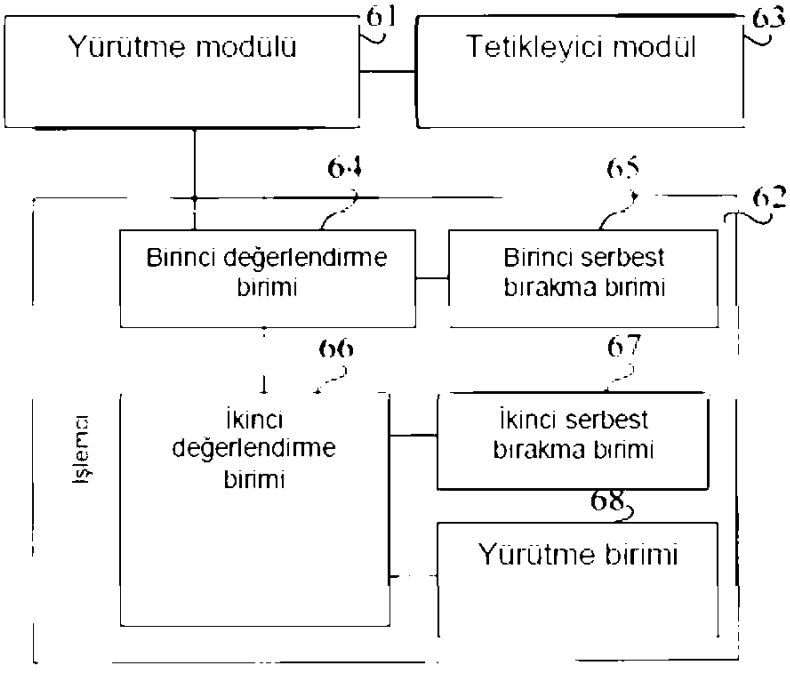
Şekil 10



Şekil 11



Şekil 12



Şekil 13