Farklı Şebekeler Üzerinden Uçtan Uca Emniyetli Haberleşmede Sinyalleşme
Signaling for End-to-end Secure Communications on Different Networks

Orkun DİLLİ[1], Sedat NAZLIBİLEK[2], Murat KOYUNCU[2], Nursel AKÇAM[1], Oğuz BOZOKLU

[1]Elekt.Elek. Müh.Böl.,Müh.Mim.Fak., Gazi Üniversitesi, Maltepe/ANKARA odilli@gazi.edu.tr, ynursel@gazi.edu.tr

[2]Müh.Fak., Atılım Üniversitesi, İncek/ANKARA snazlibilek@tsk.mil.tr, mkoyuncu@atilim.edu.tr

Özet

Haberleşme ve elektronik teknolojilerindeki çok hızlı gelişmeler, hem askeri hem de sivil alanda kullanılan cihazların çok kısa sürede değişerek yerini yeni teknolojilerle üretilen cihazların almasına neden olmaktadır. Haberleşmenin güvenliğini tam olarak sağlayabilmek ve farklı yapıları uçtan uca görüştürebilmek çok çaba gerektirir hale gelmiştir. Uluslararası kuruluşlar ve gelişmiş ülkeler, farklı haberleşme ağlarının karşılıklı çalışabilirliği konusundaki problemin farkına vardıkları için problemin çözümüne yönelik olarak temelleri 1980'li yıllara dayanan ancak 2000 yılından sonra hız kazanan bir takım çalışmalar içerisine girmişlerdir. Ancak, bugüne kadar sorunu ortadan kaldıracak yeterli çözümü ürettiklerini söylemek mümkün değildir. Farklı teknolojik altyapılara sahip haberleşme cihazlarının karşılıklı, emniyetli görüştürülebilmesi konusundaki çalışmalar devam etmektedir. Bu bildiride, farklı haberleşme ağları arasındaki karşılıklı çalışabilirlik ve uçtan uca emniyetli haberleşmenin yapılması için gerekli sinyalleşme konusuna dikkat çekilmiştir.

Abstract

The new advances on telecommunications and electronical technology cause that equipment produced with new technology frequently substitutes for older equipment used in both military and civil environments. Providing end-to-end secure communication on different network infrastructures has needed much effort than usual. Since International foundations and developed countries were aware of the problem about interoperability of different communication networks, they started some studies whose basis dated to 1980's but gained speed after 2000. It is not possible to say that they have been able to produce enough solutions to eradicate the problem. The studies about interoperability of networks having different technological infrastructure and seamless end-to-end secure communications on them have been continuing. In this study, signaling which requires the interoperability among different communication networks and accomplishment of end-to-end secure communication was taken into consideration.

1. Giriş

Haberleşme ve elektronik teknolojilerindeki çok hızlı gelişmeler, hem askeri hem de sivil alanda kullanılan cihazların çok kısa sürede değişerek yerini yeni teknolojilerle üretilen cihazların almasına neden olmaktadır. Haberleşme ağlarında oluşan ve her geçen gün de giderek artan farklı yapılar, ağların birbirleriyle karşılıklı uyum içerisinde, kesintisiz ve güvenli bir şekilde çalışmaları konusunda birçok problemi beraberinde getirmektedir [1].

Problemin idrakinde olan gerek gelişmiş ülkeler gerekse uluslararası organizasyonlar tarafından özellikle son on yıldır ulusal ya da uluslararası ortaklıklar şeklinde karşılıklı çalışabilirlik konusuyla ilgili ciddi araştırma geliştirme faaliyetlerinde bulunulmaktadır.

Bu faaliyetlerin önemlilerinden bir tanesi, ABD tarafından geçtiğimiz yüzyılın sonlarında geliştirilmesine başlanılan FNBDT (Future Narrow Band Digital Terminal) projesidir. Sonraki dönemlerde bu proje NATO tarafından da kabul görmüş ve kendi bünyesine uygun hale getirilmesi için çalışmalar başlatılmıştır. Bu çalışmalarda sinyalleşme protokolü için FNBDT yapısı esas alınmıştır. NATO/SCIP (Secure Communication Interoperability Protocol) ismi verilen bu çalışma, haberleşme ortamından (fiziksel ve mantıksal düzeyde) bağımsız olmak üzere haberleşen cihazların karşılıklı güvenli çalışabilirliğini sağlamayı esas almaktadır.

NATO/SCIP sinyalleşmesi esas olarak bütün SCIP uygulamalarını kapsayacak şekilde yaygın ihtiyaçları ele almakla birlikte, benzer veya çok farklı ağlar arasında IP tabanlı uçtan uca emniyetli bir haberleşmenin işlerliğini sağlamak konusuna yoğunlaşmaktadır. Haberleşme ağları arasındaki farklılaşmalar daha çok alt seviye protokol katmanlarında olduğundan, SCIP sinyalleşmesi bu farklılaşmayı ortadan kaldırmak hedefiyle, uygulama katmanı gibi daha üst katmanlarda uçtan uca sinyalleşme standartları getirerek problemlere çözüm bulmaya çalışmaktadır.

Bu bildiride, farklı haberleşme ağları arasındaki karşılıklı çalışabilirlik ve uçtan uca emniyetli haberleşmenin yapılmasında kullanılacak sinyalleşme konusu incelenmiştir.

Bu bildiri altı bölümden oluşmaktadır. Sinyalleşmenin kapsamı ikinci bölümde, Sinyalleşmenin amacı üçüncü bölümde, Uygulamada kullanılan ağın tanıtımı dördüncü bölümde açıklanmıştır. Beşinci bölümde Sinyalleşme ile ilgili uygulama verilmiş ve altıncı bölümde verilen sonuçlarla bildiri tamamlanmıştır.

2. Sinyalleşmenin Kapsamı

Sayısal dar band ağlar üzerinde uçtan uca güvenli haberleşme yapan terminaller arasındaki sinyalleşmeyle ilgili bilgiler NATO/SCIP–210 sinyalleşme planında yer almıştır. Sinyalleşme Planında genel olarak aşağıdaki konular açıklanmaktadır:

- Güvenli ses ve veri alışverişinden önce; sertifika, anahtarlar ve diğer bilgi değişimlerinin nasıl olduğu,
- 2,4 kbps'de ses kodlayıcı olan MELP standardını kullanarak uçtan uca haberleşen kullanıcı terminallerinde güvenli ses iletiminin nasıl olduğu,
- Uçtan uca veri terminalleri arasında güvenli veri trafiğinin nasıl sağlandığı,
- Güvenli modlarda haberleşmenin kurulması, sürdürülmesi ve sonlandırılması için gerekli güvenlik kontrol sinyalleşmelerinin neler olduğu,
- Anahtarların elektronik veya havadan (over-the-air) dağıtım veya değişimini nasıl desteklendiği,
- Konuyla ilgilenenler için başlangıç noktası teşkil edebilecek diğer hususlar.

Sinyalleşme Planının bir diğer ana maksadı ise mevcut ticari sayısal telsiz ve PSTN/ISDN ağları kullanarak yapılan haberleşmeleri destekleyerek, ilave standartlar geliştirme çabalarını en aza indirmektir.

Sinyalleşme planında, güvenli veri ve ses öğelerince kullanılacak uçtan uca sinyalleşmenin tanımlanması hedeflenmekte, bunun haricinde terminaller arasında sinyalin taşınması için kullanılacak olan haberleşme linkleri ile ilgili olarak ilave sinyalleşme konularının bulunması beklenmemektedir [2].

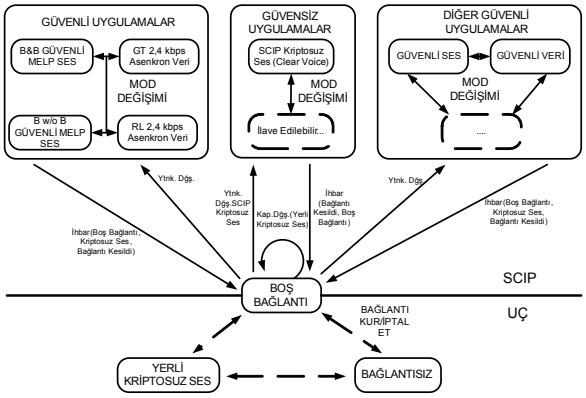
İlave ağlar ve değişik durumlara uyum sağlayabilmesi için sinyalleşme planlarının sonraki sürümlerinde geliştirilebilmesi maksadıyla planın esnek tutulmasına özen gösterilmektedir. Sinyalleşme planında belirli bir uygulama yöntemi tanımlanmadığı gibi dikte de edilmez. Planın kimi yerlerinde bazı uygulama yöntemlerinden bahsedilmekte ise de bu daha çok tarif maksatlı olmaktadır. SCIP uyumlu ilk ürünün ortaya çıkmasından itibaren ürüne yeni özellikler ekleyebilme ve ürünü yeni teknoloji iletişim ağları üzerinde de çalıştırabilme potansiyelinin her zaman mümkün kılınabilmesi sinyalleşme planı hazırlanırken öncelikle göz önünde tutulan hususlardandır.

Sinyalleşme Planı, standart veri taşıyıcı (Data Bearer) hizmetleri kullanan kriptosuz sayısal ses (Clear Digital Voice) ve güvenli ses/veri haberleşme uygulamaları için taslak SCIP sinyalleşmesini tanımlamaya çalışmaktadır. SCIP kriptosuz ses haberleşme sinyalleşmesi; kriptosuz durumdan güvenli haberleşmeye geçişlerin mümkün olamayacağı durumlarda, sesin veri tarafından takip edilmesi ihtimaline dayalı bir sinyalleşme türüdür [2].

3. Sinyalleşmenin Amacı

NATO/SCIP sinyalleşmesinin değişik ağlar üzerinde dahi olsa kullanılan donanım SCIP yetenekli olduğu takdirde aynı özellikli diğer donanımlarla güvenli veya kriptosuz olarak görüşebilme imkân ve kabiliyeti sağlanmaktadır. Uzak uçtaki terminal, ticari standart bir telefon ise haberleşme mevcut ağ altyapısına uygun teknik ve yordamlarla; NATO/SCIP uyumlu bir cihaz ise de sinyalleşme planında detaylandırılan güvenlik yetenekleri kullanılarak gerçeklenmektedir. Güvenli mod olarak da adlandırılabilecek bu durum ses ve veri için ayrı ayrı olmak üzere **güvenli ses** ve **güvenli veri** olarak planda geçmektedir. Bu ayrıma ilave olarak sinyalleşme planı ayrıca, kriptosuz ve güvenli trafik modlarının kurulumunun ve koordinesinin sağlandığı çağrı kurma sinyalleşmesi ve çağrı kurulduktan sonra icra edilen anahtar değişimi faaliyetlerini de kapsayan **kontrol sinyalleşmesi**ni içermektedir [2].

Sinyalleşme dokümanında çok çeşitli harekât modları tanımlanmakta ise de her bir harekât modu için SCIP yetenekli terminaller tarafından kullanılacak asgari sinyalleşme durumları burada tanımlanmaktadır. Bu, sinyalleşme planının ana gövdesinde belirtilen güvenli çağrı kurma gibi "çekirdek SCIP işlevleri" için sinyalleşmeleri kapsar. Sinyalleşme planı "ağdan bağımsız" olma gayretindedir ki bu da ister dar band, ister geniş band ve isterse korumalı sayısal ağlarda olsun sinyalleşmenin işleyebilmesi anlamına gelmektedir.



Şekil 1: Uçtan-Uca Uygulama Durum Diyagramı [2]

Şekil 1'de NATO/SCIP uyumlu bir terminalin uçtan-uca sinyalleşmesi kavramsal olarak gösterilmeye çalışılmaktadır. Terminal başlangıçta uzak uca hiç bir haberleşme bağlantısının olmadığı bağlantısız (Connection Terminated) bir durumdadır. Sinyalleşme Planında tanımlanan sinyalleşme durumu tatbik edilmeden önce iki uç arasında SCIP mesajlarının karşılıklı taşınmasını temin etmek maksadıyla kriptosuz bir veri yolu (Clear Data Path) açılması şarttır. İşte uçlar arasında kriptosuz veri yolunun açıldığı ve fakat üzerinde SCIP uygulamalarının henüz başlatılmadığı bu duruma "Boş Bağlantı" (Connection Idle) adı verilmekte, SCIP uygulamaları bahsedilen bu boş bağlantıdan gerçekleştirilebilmektedir. Yetenekler Değişimi (Capabilities

Exchange) tabir edilen ilk SCIP çağrı kurulum değişimi standart SCIP kriptosuz ses uygulamaları [1] kullanılarak yapılır. Yetenekler Değişimine ek olarak, standart güvenli SCIP uygulama parametrelerinden karşılıklı haberdar olabilmek için mesaj alışverişlerine ihtiyaç olmaktadır [2].

Aynı trafik anahtarını kullanan güvenli uygulamalar veya SCIP uyumlu kriptosuz uygulamaların karşılıklı görüşebilmeleri bir Mod Değişimi (Mod Exchange) işlevi ile sağlanabilmektedir. Uygulamalar arası geçişler zaman zaman Boş Bağlantı durumuna dönmekle olabilmektedir. Her hangi bir SCIP durumundan diğer bir duruma geçmek gerekli olduğu durumlarda bu İhbar Mesajlarında (Notification Message) gösterilmektedir. Tekrar SCIP moduna geçileceğinde bir dizi Yetenekler Mesajlaşması karşılıklı olarak yerine getirilir.

Standart bir SCIP durumunda çağrıyı sonlandırarak Boş Bağlantı durumuna, bilahare de kullanılan kriptosuz veri yolunu kapatarak Bağlantı Sonlandırıldı (Connection Terminated) durumuna geçmek için yine İhbar Mesajları kullanılmaktadır.

4. Sinyalleşme İle İlgili Kavramlar

Konuların daha net anlaşılabilmesi için sinyalleşme hususunda temel konu ve kavramlara daha yakından bakmak gerekliliği görülmektedir.

Yukarıda da değinildiği üzere **SCIP sinyalleşmesi** esas olarak **bağlantı kurma** ve **kontrol** sinyalleşmelerinden oluşmaktadır. Bağlantı Kurma Sinyalleşmesi, Yetenekler, Parametre/Sertifika, F(R) ve Kripto Senkronizasyon (CryptoSync); Bağlantı Kontrol Sinyalleşmesi ise İhbar İşlemleri (Notification), Mod Değiştirme ve Senkronizasyonu Tekrar Kurma konularını içermektedir.

Ancak tüm bu konulara daha ayrıntılı bakmadan önce, SCIP iletim katmanında neler meydana geldiğini incelemek ve daha öncesinde buradaki kavramlara aşina olmanın faydalı olacağı değerlendirilmektedir. Öncelikle sinyal alışverişi, Mesaj Başlangıcı (Start of Message - SOM) ile başlayıp Mesaj Bitimi (End of Message - EOM) ile sonlanmaktadır. SOM ve EOM arasında gönderilen çerçeveler "çerçeve grubu (superframe)" olarak tanımlanmaktadır. Her çerçeve grubu gönderme yönünde hata düzeltimi (FEC) ve çevrimsel artıklık denetimi (CRC) ile korunan çerçevelerden meydana gelmekte; FEC ile düzeltilemeyen hataların ortadan kaldırılması içinse olumlu veya olumsuz onay verme mekanizmaları (ACK ve NACK) kullanılmaktadır.

Her bir çerçeve, 1 çerçeve numarası, 13 mesaj, 4 FEC ve 2 CRC olmak üzere 20 bayttan oluşmaktadır. Bu çerçevelerden oluşan ve Mesaj Başlangıcı (SOM) ile başlayıp Mesaj Sonu (EOM) ile sonlanan her çerçeve grubu en az bir en çok 127 adet çerçeveden oluşmaktadır.

Mesaj Başlangıcı (SOM) her çerçeve grubunun iletiminden önce gönderilen sekiz baytlık veri dizisidir. Bu veri dizisi farklı kanallarda tespit edilebilecek şekilde tasarlanmıştır. Mesaj Bitimi de 8 bayt olup farklı kanallarda tespit edilebilmektedir. Bu noktada EOM, ESCAPE ve REPORT kavramlarına değinmek gereği vardır. EOM alındığında öncelikle son alınan çerçevenin ESCAPE veya REPORT olup olmadığına bakılır, eğer değilse o ana kadar alınmış çerçeveler için rapor hazırlanır ve gönderilir. ESCAPE mesajı band genişliği kullanımı, REPORT mesajı ise gelen çerçevelerin hata oran onayları ile ilgili kavramlar olup ayrıntılarına burada girilmeyecektir.

Benzer şekilde SCIP sinyalleşmesinde karşılaşılabilinecek mesaj türlerinden diğer bir tanesi RESET mesajıdır ki bu mesaj gerekli durumlarda iletim katmanını yeniden senkron hale getirmek için kullanılır. RESET mesajı çerçeve numaralarını sıfırlar ve bir SOM ve EOM arasında yalnızca bir RESET mesajı gönderilir.

Mesaj türleri Tablo 1'de topluca verilen SCIP sinyalleşmesinde, bağlantı kurma sinyalleşmesinin ilk adım olarak terminaller birbirlerine Yetenekler Mesajını (Capabilities Message) göndermektedirler. Bu mesaj sayesinde terminaller birbirleriyle uyumlu olarak ne şekilde çalışabileceklerini (açık veya kapalı modlar) belirli bir esasa bağlamakta ve güvenli modda haberleşilecek ise uygun anahtar listesinin seçilmesi de bu sayede mümkün olmaktadır. Yetenekler Mesajı gönderildiği anda ilk mesaj zamanlayıcısı başlamakta, bu zamanlayıcı karşı taraftan SCIP uyumlu mesaj gelmemesi halinde bağlantının zaman aşımına uğramasını temin etmektedir. Zaman aşımı sonunda Boş Bağlantı haline dönülür.

İlk mesajlaşma sonunda eğer güvenli haberleşme kararı verildiyse SCIP bağlantısı kurulabilmesi maksadıyla trafik anahtarını oluşturabilmek için karşılıklı sertifikaların ve F(R)'ların değiş tokuş yapılması gerekmektedir. Bunlardan sertifikanın gönderilmesi Parametre/Sertifika mesajı ile olur.

F(R) mesajı anahtar takımı ile ilgili bir takım bilgiler (anahtarın tip, uzunluğu vb.), F(R) uzunluğu ve F(R)'ın kendisini kapsayan bir mesajdır. F(R) mesajı iletilmeden önce mutlaka parametre/sertifika mesajı iletilmiş olmalıdır.

SCIP bağlantısı kurmada diğer bir adım kripto senkronizasyon mesajlarının değişimidir. Değişimi yapılan sertifika ve F(R) bilgileri ile trafik anahtarı oluşturulmakta, bu anahtar ile test paketi şifrelenip Kripto Senkronizasyon Mesajı haline getirilmektedir. Tablo 1'de çağrı kurma ve kontrol mesajlarının isim ve kimlikleri toplu olarak görülmektedir.

Tablo 1: Mesaj Kimlik Bilgileri [2]

Mesaj	**Kimlik Bilgisi**
Yetenekler (Capabilities)	0x0002
Parametre/Sertifika	0x0010
F(R)Mesajı	0x0004
Kripto Senkronizasyon	0x0008
İhbar (Notification)	0x000E
Mod Değişimi İstek	0x001A
Mod Değişimi Cevap	0x001C
Rapor	0x0020
Sıfırlama (Reset)	0x0080

[1] Sinyalleşme Planında sadece kriptosuz 2,4 Kbps MELP tanımlanmıştır

Bağlantı kurma sinyalleşmesinden sonra kurulan bağlantının değişikliklere tabi tutulmasıyla ilgili bir takım sinyalleşme tanımları mevcuttur. Bağlantı kontrol sinyalleşmesinin maksadı; herhangi bir sebeple bağlantıyı sonlandırmak, mevcut uygulamayı değiştirmek, diğer terminali ikaz etmek ve/veya kripto senkronizasyonunu baştan sağlamak olabilir. Bağlantı kontrol sinyalleşmesinde dört farklı mesaj vardır. Bunlar İhbar (Notification), Mod Değişim İsteği (Mode Change Request), Mod Değişim Yanıtı (Mode Change Response) ve Kripto Senkronizasyon (CryptoSync) olabilir.

Bu mesajlardan belki de en sık başvurulanı ve kullanılanı olan ihbar mesajı ile yerine getirilen Tablo 2'de işlem kodları verilen 6 farklı işlev vardır. Bunlar Bağlantı Sonlandırma (Connection Terminate), Yerel Açık Ses (Native Clear Voice), Boş Bağlantı (Connection İdle) ve Gizliliği İhlal Edilmiş Anahtar Listesi-CKL (Compromised Key List) alışverişi, Güvenli Arama (Secure Dial) ve İkaz (Attention) mesajlarıdır. Bu mesajlardan güvenli arama dışındaki diğer bütün ihbar mesajları açık olarak iletilirler. Yalnızca güvenli arama için üzerinde anlaşılmış ve uzlaşılmış ve de onaylanmış bir anahtara ihtiyaç duyulduğundan; bu mesaj sadece kripto senkronizasyon mesajlarının ardından gönderilebilmektedir.

Tablo 2: İhbar Mesajı Eylem Kodları [2]

Kimlik	**Eylem Kodu**
0x0002	Bağlantıyı Sonlandır
0x0004	Yerel Açık ses
0x0008	Boş Bağlantı Moduna Dön
0x0010	CKL Transferi
0x0020	Güvenli Arama
0x0040	İkaz mesajı

Mod değiştirme işlemi yukarıda belirtildiği üzere talep ve buna verilen yanıt şeklinde iki türlü olabilir ve sadece her iki terminal de güvenli uygulama trafiğinde iken mümkün olabilir.

Tablo 3: Çalışma Modları Listesi [2]

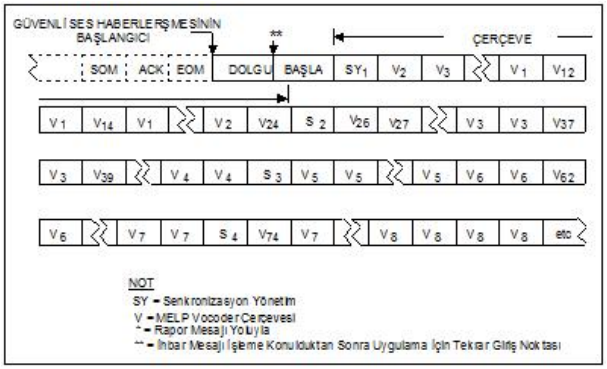
Kodu	**İşlem modu**
0x0001	Kapalı tip 1 ses
0x0002	Kapalı tip 1 veri
0x0004	Açık 2,4 kbps MELP ses
0x0008	Standart açık ses

Tablo 3'de gösterilen çalışma modlarından (Kapalı Tip 1) Güvenli Ses için beş farklı çağrı mevcuttur. Bunlar [2];

- Güvenli 2,4 kbps MELP kodlu Ses – Blank & Burst (DTX),
- Güvenli 2,4 kbps MELP kodlu Ses – Blank & Burst (FCT),
- Güvenli MELP kodlu Ses –Burst w/o Blank (DTX),
- Güvenli MELP kodlu Ses –Burst w/o Blank (FCT),
- Güvenli, Gelişmiş Çoklu-Band Uyarımı (AMBE).

Görüldüğü üzere SCIP' de Blank & Burst uygulamalı MELP ve Burst w/o Blank olmak üzere iki tip güvenli ses çağrısı yapılabilmektedir.

SCIP uyumlu bir terminalde, kripto senkronizasyonunun sürekliliği için belirli periyotlarla terminal tarafından 2,4 kbps'de üretilen MELP kodlu ses bilgisinin üzerine kripto senkronizasyon bilgisi yazılır. Bu işleme "B&B" (Blank and Burst) protokolü denilmekte ve bu uygulamada zaman zaman ses bilgisi silinerek yerine kripto bilgisi yazılmasından dolayı ses kalitesinde ufak çapta düşüşler yaşanmaktadır. NATO/SCIP'de iletişim 54 bit'lik kriptolanmış ve MELP ile kodlanmış 23 tane ses verisi taşıyan paket ve bu paketlerden önce gönderilen ve kripto senkronizasyonu amacıyla kullanılan Synchronization Management (SM) çerçevesi ile birlikte toplam 24 paketten oluşan çerçeve grupları ile gerçekleştirilir. Blank & Burst uygulamalı MELP kodlu ses çağrılarında kripto senkronizasyonu amacıyla kullanılan SM çerçevesi her MELP Çerçeve Grubunun ilk çerçevesi olarak karşı terminale gönderilir. Şekil 2'de B&B uygulaması görülmektedir.



Şekil 2: Blank & Burst Çerçeve Dizilimi [3]

Burst w/o Blank uygulamalı MELP kodlu ses çağrılarında ise SM çerçevesi MELP her çerçeve grubu başlamadan hemen önceki çerçeve olarak karşıya iletilir. Blank & Burst çerçeve grubu 24 çerçeveden oluşmasına karşın, Burst w/o Blank uygulaması 25 çerçeveden oluşmaktadır. Dolayısıyla Burst w/o Blank uygulaması için gerekli kanal kapasitesi 2,4 kbps'den fazla (overhead) olmaktadır. Aynı zamanda, MELP kodlanmış ses bilgilerinin üzerine kripto senkronizasyon bilgisi yazılmadığı için ses kalitesi B&B'ye göre daha iyidir.

Açık MELP ses çağrı hizmeti görüşmesinde de ortaya çıkan yapı tıpkı B&B'de olduğu gibidir. Mesaj yine, biri SM çerçevesi olmak üzere toplam 24 çerçeveden oluşan çerçeve gruplarıyla yapılır. Ancak burada kriptolama yapılmadığından SM çerçevesinin başlık kısmından sonraki tamamı sıfır ile doldurularak mesaj gönderilir.

Ayrıca ister güvenli isterse açık olarak görüşen tüm SCIP uyumlu terminallerin DTX ve FCT durumları desteklemesi beklenmektedir. Bunlardan DTX; bir ses çağrısı sırasında, terminalin kullanıcısı konuştuğu sürece çerçeve gruplarının oluşturularak gönderilmesi, kullanıcı sustuğunda ise gönderme yapmanın kesilmesi prensibini; FCT ise; ses çağrısı sırasında

terminalin kullanıcısının sustuğu sürede de çerçeve gruplarının oluşturularak karşı terminale iletilmesi yani MELP kodlayıcı biriminin sürekli çalışmasını ifade etmektedir.

SCIP, veri haberleşmesinde ise iki veri hizmetini desteklemektedir. Bunlar "Güvenli Aktarım (Reliable Transport-RT) Asenkron Veri Hizmeti" ve "Garanti İş (Guaranteed Throughput-GT) Asenkron Veri Hizmetleridir. RT Asenkron Veri hizmetinde, güvenli ses hizmetinde kullanılan sinyalizasyon mekanizmalarının aynısını kullanarak veri çağrısı başlatılır ve kanal kapasitesi %70 verimlilikle kullanılır. GT Asenkron Veri hizmeti ise kanal kapasitesinin tamamının kullanıldığı bir servistir.

5. Sinyalleşme ile İlgili Uygulama

Bu bölümde, teoriği önceki bölümlerde anlatılan protokolün uygulamasını göstermek amacıyla A ve B cihazları arasında geçen bir iletişim senaryosu gösterilmektedir [4]. Şekilsel olarak Tablo 4'de verilen sinyalleşme adımları sırasıyla aşağıda açıklanmıştır:

Tablo 4: Hatasız kapabilite mesajı transferi

	Terminal A				Terminal B			
	Mesaj katmanı		İletim katmanı		İletim katmanı		Mesaj katmanı	
	TX	RX	TX	RX	TX	RX	TX	RX
1	Kapabilite							
2			SOM					
3			1					
4			2			SOM		
5			3			1		
6			EOM			2		
7						3		
8						EOM		
9					SOM			Veri 1-3
10					RPT(3/0)			
11				SOM	EOM			
12				RPT(3/0)				
13				EOM				
14		Tamamlandı						

1. Terminal A tarafında mesaj katmanı iletim katmanına Kapabilite mesajı gönderme talebinde bulunur. Bu örnekte bu mesajın 3 çerçeveye sığacak uzunlukta olduğu (27-39 sekizlik uzunluğunda) varsayılmıştır.
2. İletim katmanı gönderilmek istenen mesajı alır ve bunu 3 çerçeve haline getirir, SOM ile mesaj göndermeyi başlatır.
3. Terminal A çerçeve 1'i gönderir.
4. Terminal A çerçeve 2'yi gönderir. Terminal B SOM'u alır ve bir mesajın gelmekte olduğunu anlar.
5. Terminal A çerçeve 3'ü gönderir. Terminal B çerçeve 1'i almaya başlar.
6. Mesaj tamamlandığı için terminal A EOM yollar. Terminal B çerçeve 2'yi alır.
7. Terminal B çerçeve 3'ü alır.
8. Terminal B EOM alır, mesajın tamamlandığını anlar.
9. Terminal B aldığı çerçevelere karşılık rapor mesajı hazırlar ve SOM ile bu raporun gönderimine başlanır. 1-3 arası gelen çerçevelere ait veriler mesaj katmanına iletilir, burada bu verilerin kapabilite mesajı oluşturduğu tesbit edilir.
10. Terminal B 1,2,3 no'lu çerçevelerin doğru alındığını onaylayan çerçeveyi yollar.
11. Terminal A yeni mesaj geldiğini gösteren SOM alır. Terminal B raporun bittiğini gösteren EOM gönderir.
13. Terminal A gönderdiği tüm çerçevelerin karşı terminal tarafından doğru alındığını anlar.
14. Terminal A mesajın bittiğini gösteren EOM alır.
15. Terminal A tarafında iletim katmanı mesaj katmanına kapabilite mesajının karşıya ulaştırıldığını bildirir. Bundan sonra diğer mesajların iletimi ile devam edilir.

6. Sonuçlar

SCIP sinyalleşme esaslarının NATO ihtiyaçlarına uyumlu hale getirmek için başlatılan çalışmalar devam etmektedir. FNBDT Sinyalleşmesi kullanılmaya başlanmış ve belli bir olgunluğa erişmiş olduğundan SCIP Sinyalleşmesine geçiş sürecinin çok uzun ve zor olmayacağı değerlendirilmektedir.

Yukarıda belirtilen gelişmelerden dolayı bu çalışmaya uzak kalınmamalı ve henüz ürünlerin tasarım veya üretim öncesi aşamasında olduğu şu zaman zarfında üzerinde gerekli incelemeler yapılıp NATO kanalıyla gerek görülen yerlere ülke çıkarları doğrultusunda müdahale edilmelidir.

7. Kaynaklar

[1] GÖNEN, Serkan. "**Taktik Saha Muhabere Sistemleri Arasında Müşterek Çalışabilirliğin Sağlanması**" (Yüksek Lisans Tezi), Kara Harp Okulu Savunma Bilimleri Enstitüsü, Ankara, Şubat 2006.

[2] General Dynamics Communication Systems, **FNBDT Signaling Plan** (Revision 1.1), Needham, Eylül 1999.

[3] LUCK, J. **Details of FNBDT Signalling**, SHAPE / NC3A FNBDT Workshop, The Hauge, 26 Şubat 2003.

[4] ÖREN, Özgür. "**Geleceğin Darband Sayısal Terminali**" (Yüksek Lisans Tezi), Sakarya Üniversitesi FEN Bilimleri ENSTİTÜSÜ, Adapazarı, Haziran 2005.