FARKLI ŞEBEKELER ÜZERİNDEN UÇTAN UCA EMNİYETLİ HABERLEŞMENİN SAĞLANMASI*

Orkun DİLLİ[1], Sedat NAZLIBİLEK[2], Oğuz BOZOKLU, Murat KOYUNCU[3], Nursel AKÇAM[4]

[1,4]*Elekt.Elek. Müh.Böl.,Müh.Mim.Fak., Gazi Üniversitesi,Maltepe/ANKARA*
[2,3]*Müh.Fak., Atılım Üniversitesi,İncek/ANKARA*
odilli@gazi.edu.tr, snazlibilek@tsk.mil.tr, obozoklu@gmail.com, mkoyuncu@atilim.edu.tr, ynursel@gazi.edu.tr

ABSTRACT

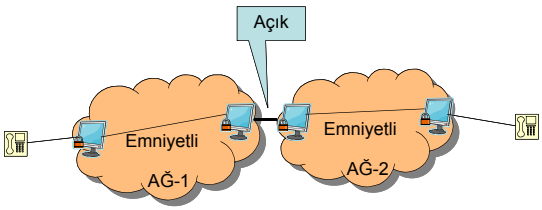
Although new network technologies provide numerous capabilities today, the diversity of the communication networks and their standards has brought out tremendous problems about harmony and interoperability of the communication devices. Providing end-to-end secure communication on different network infrastructures 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, the interoperability among different communication networks and accomplishment of end-to-end secure communication were taken into consideration. The required products for such a secure communication with SCIP (Secure Communication Interoperability Protocol) are analyzed and different military scenarios about their usage are given.

Keywords: Secure Interoperability, Network Enabled Capability and SCIP.

1. GİRİŞ

Bilim ve teknolojideki büyük gelişmeler her alanda olduğu gibi haberleşme alanında da önemli değişimlere yol açmıştır. Bu değişimlerin en önemli sonuçlarından biri de farklı standart ve arayüzleri kullanan haberleşme sistemlerinin geliştirilmesidir [1]. Bu durum beraberinde müşterek çalışabilirlik problemini getirmiştir.

Farklı teknolojik altyapılara sahip haberleşme cihazlarının karşılıklı görüştürülebilmesi günümüzde önemli bir ihtiyaçtır. Dahası, bazı durumlarda bu cihazların emniyetli olarak görüştürülebilmesi büyük önem arz etmektedir. Örneğin askeri şebekelerde haberleşmenin uçtan uca emniyetli olarak yapılması ve bunun da dikişsiz/saydam (seamless) olarak gerçekleştirilmesi hayati öneme haiz bir konudur. Emniyetli haberleşme ihtiyacı sadece askeri ihtiyaçlar için değil birçok kamu kuruluşu için ve günümüzde artık özel sektör içinde önemlidir. Bu çerçevede, farklı haberleşme şebekeleri arasında karşılıklı çalışabilirliğin ve uçtan uca emniyetli haberleşmenin sağlanması, üzerinde çalışmaya değer önemli araştırma alanlarından birisi olarak değerlendirilmektedir [2].



***Şekil-1**: Farklı ağlar üzerinden emniyetli görüşme*

Günümüzde ISDN, PSTN, GSM gibi farklı telekom haberleşme şebekeleri mevcuttur. Askeri şebekelere baktığımızda ise, genelde dar bantlı telsiz ve uydu temelli haberleşme sistemleri karşımıza çıkmaktadır. Bu şebekeler arasında genelde bir şekilde karşılıklı çalışabilirlik sağlanmış durumdadır. Ancak, birkaç farklı şebekeyi kullanan bir haberleşme senaryosunda, uçtan uca dikişsiz emniyetli bir haberleşmenin sağlanması mümkün değildir. Günümüzde kripto cihazları altta kullanılan teknolojiye bağımlıdır ve tüm bu haberleşme ağlarında ortak kullanılacak bir kripto teknolojisi mevcut değildir. Örneğin, ISDN şebeke üzerinde farklı kripto cihazı, PSTN şebeke üzerinde farklı kripto cihazı kullanılmaktadır. Bir abone, farklı teknolojiye sahip başka bir ağın üzerindeki abone ile kriptolu görüşmek isterse, bu görüşme **Şekil-1**'de görüldüğü gibi iki ağ arasında açılmakta ve tekrar kriptolanmaktadır. Bu uygulama, haberleşmenin emniyeti açısından büyük sakınca yaratmaktadır. Farklı teknolojilere sahip çok sayıda ağın ortaya çıkmasının getirdiği bir diğer sorun ise ağlara özgü çok sayıda terminal cihazının kullanılmak zorunda kalınmasıdır. Bu yüzden, günümüzde birçok

* Bu bildiri, yazarların çalışmalarını içermekte olup Türk Silahlı Kuvvetleri'nin görüşünü yansıtmamaktadır.

yöneticinin masasında birden fazla terminal cihazı mevcuttur. Karmaşaya neden olan bu durumun sadeleştirilmesi de önemli bir ihtiyaç olarak karşımıza çıkmaktadır.

Problemin idrakinde olan gerek gelişmiş ülkeler, gerekse uluslararası organizasyonlar özellikle son on yıldır ulusal ya da uluslararası ortaklıklar şeklinde karşılıklı çalışabilirlik konusuyla ilgili ciddi araştırma geliştirme faaliyetlerinde bulunmaktadırlar. Konuyla ilgili yapılan çalışmalardan bir tanesi de halen NATO bünyesinde yürütülen SCIP (Secure Communication Interoperability Protocol / Güvenli Karşılıklı Çalışabilir Haberleşme Protokolü) projesidir [2, 5]. Çalışma kapsamında, temel olarak farklı askeri ağlar üzerinde IP tabanlı, uçtan uca emniyetli bir haberleşmenin sağlanması hedeflenmektedir. Yapılan çalışmaları temel olarak iki grupta toplamak mümkündür: IP tabanlı sinyalleşme protokolünün geliştirilmesi ve haberleşmenin kriptolanması. Türkiye, konuyla ilgili yapılan çalışma grubu toplantılarına katılmakta, gelişmeleri izlemekte ve mümkün olan noktalarda destek vermeye çalışmaktadır.

Bu bildiri, farklı haberleşme ağları arasındaki karşılıklı çalışabilirlik ve uçtan uca emniyetli haberleşmenin yapılması konusuna dikkat çekmek, konuyla ilgili NATO ve tarafımızca yürütülen çalışmalar konusunda bilgi vermek ve yapılan çalışmalara katkıda bulunabilecek görüş ve önerilerin toplanması amacıyla hazırlanmıştır.

Bu bildiri beş bölümden oluşmaktadır. Bu tür çalışmalara baz teşkil eden NATO Ağ Destekli Yetenek konsepti ikinci bölümde, SCIP'le ilgili temel bilgiler üçüncü bölümde açıklanmıştır. Dördüncü bölümde SCIP ile ilgili ayrıntılar verilmiş ve Türkiye'de kullanımı ile ilgili senaryolar değerlendirilmiştir. Beşinci bölümde verilen sonuçlarla bildiri sonlandırılmıştır.

2. AĞ DESTEKLİ YETENEK

Ağ Destekli Yetenek (ADY), harekât alanındaki durumun müştereken farkında olunması, komuta hızının artırılması, harekât temposunun yükseltilmesi, vurucu gücün daha da etkinleştirilmesi, bekanın güçlendirilmesi ve kendi kendine senkronizasyonun tesis edilmesi maksadıyla; algılayıcıların, karar vericilerin ve silah sistemi kullanıcılarının ağ altyapıları ile birbirlerine irtibatlanarak muharebe gücünün artırılmasını sağlayan bilgi üstünlüğüne dayalı harekât konseptidir [3].

Ağ Destekli Yetenek Konsepti konusunda NATO'nun üç temel prensibi bulunmaktadır:

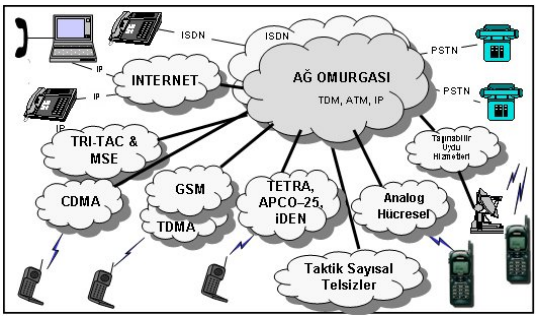
- Sağlam iletişim ağları ile bilgi paylaşımını arttırmak,
- Bilginin mümkün olduğu kadar çok ve yerinde paylaşılmasıyla bilgi kalitesini ve harekât alanındaki mevcut durumla ilgili olarak farkındalığı arttırmak,
- Paylaşılan harekât alanı resmi ile, işbirliği ve harekata katılımı etkin kılarak, komuta kontrolün sürekliliğini ve hızını arttırma suretiyle bunu bir kuvvet çarpanı haline getirmek.

Konuyla ilgili ulusal çalışmalara ilk olarak Ocak 2004'de başlanmış, Mart 2004'de NATO ADY Yönlendirme Komitesine üye olunmuştur. Zaman içerisinde yapılan değişik faaliyetlerle, ADY konseptinin uygulanmasına yönelik çalışmalar sürdürülmektedir. Yürütülen tüm çalışmalarda NATO standartları dikkate alınmaktadır.

3. SCIP VE KARŞILIKLI ÇALIŞABİLİRLİK

Günümüz haberleşme altyapıları; içerisinde çok sayıda ses ve görüntü kodlayıcıları, çok çeşitli taşıyıcı (bearer) teknolojileri, değişik kriptoları ve farklı teknolojilerde haberleşme donanımlarını barındıran son derece karmaşık sistemlerdir. Ses haberleşmesinin yanında, veri haberleşmesinin her geçen gün artan bir ihtiyaç olarak görülmesi, ayrıca birden fazla ülkenin müşterek olarak icra ettiği koalisyon tipi harekâtın günümüzde yaygınlaşması, karmaşıklığı daha da artırarak geleneksel ses ağları üzerinden uçtan uca haberleşmeyi günden güne zorlaştırmaktadır [2].

Tipik bir örneği **Şekil-2**'de resmedilen günümüz haberleşme ortamları içerisinde çok sayıda geçityolu (gateway) ile uçtan uca görüşme imkânı sağlanabilse de, bu görüşmenin uluslararası müşterek harekâtlarda anahtarların paylaşıldığı hallerde dahi güvenli olarak yapılabilmesi mümkün olmamaktadır [4].



Şekil-2: *Günümüz Karmaşık Haberleşme Ortamı*

Ağ Destekli Yeteneğin oluşturulmasının önündeki en büyük engel, uçtan uca güvenli ve karşılıklı çalışabilir donanımların olmayışı olarak değerlendirilmektedir. Böylesi teknik açmazlara ek

olarak, **Şekil-2**'deki hemen her telefon (kişisel bilgisayarlar da dâhil olmak üzere) stratejik bir karargâhtaki karar vericinin masasının üzerindeki haberleşme donanımları olarak düşünüldüğünde, mevcut sistemlerde çok ciddi sadeleştirmelere gidilmesi gerektiği açıktır. Nihai hedef bütün bu işlevlerin tek bir terminal tarafından güvenli olarak yerine getirilebildiği bir cihazın ortaya çıkarılmasıdır.

NATO C3 (Consultation, Command and Control) Kurulu tarafından, Ağ Destekli Yeteneğin kazanılması hedefine dönük olarak;

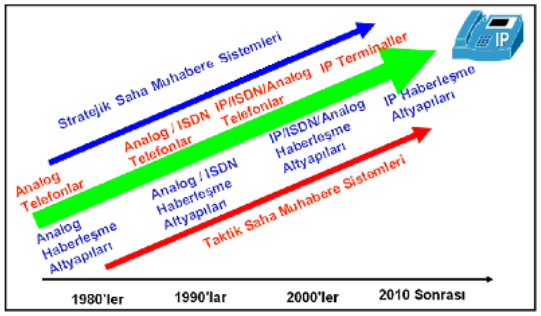
- Bir Terminal üzerinden; tüm emniyetli ses/veri/video haberleşme imkânının kazanılması,
- Taktik ve Stratejik ağlarda tüm haberleşme gereksinimleri için tek bir çoklu-ortam terminal ve tek bir haberleşme altyapısının kullanımının sağlanması,
- Mevcut tüm taktik ve stratejik kriptolu terminaller ile açık/kriptolu terminallerin uyumlu çalışabilmesi, maksatlarıyla SCIP projesi başlatılmıştır [5].

SCIP Projesi, daha önce ABD tarafından başlatılan FNBDT (Future Narrow Band Digital Terminal, Gelecek Darband Sayısal Terminali) projesi üzerine oturtulmuş [6,7] ve protokolün NATO standartları arasında yer alması için çalışmalara başlanmıştır. Gerekli sinyalleşme ve kriptolama protokollerini kapsayan bu çalışmayla, üzerinde iletildiği ağ altyapısından bağımsız, uçtan uca güvenli haberleşme sağlanabilmesi tasarlanmaktadır. SCIP'in ülkelerin kendi sinyalleşme ve kriptografik protokollerini geliştirmelerinde de temel olarak kullanılması amaçlanmaktadır. Bu sayede, hem milli hem de NATO amaçları için uçtan uca güvenli haberleşme imkânı sağlanabileceği düşünülmektedir.

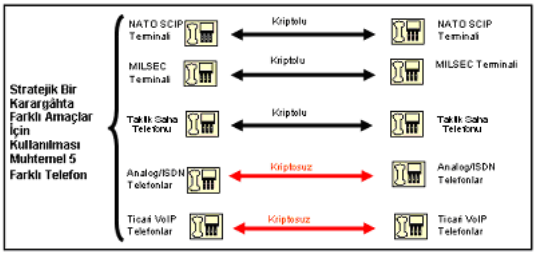
Türkiye, bir kaç ülke ile beraber bu proje kapsamında konu hakkında ciddi çalışmalar içerisinde olan öncü ülke konumunda bulunmakta, birikimlerini artırmak suretiyle hızla çözüm yolunda ilerlemektedir.

4. KAVRAMSAL YAKLAŞIM

Geçmişten bugüne haberleşme altyapıları ve onlara bağlı terminal cihazları gelişimi **Şekil-3**'te verilmiştir. Haberleşme teknolojilerindeki bu değişim ve gelişmeler, doğrudan ya da dolaylı olarak taktik ve stratejik askeri muhabere sistemlerini de etkisine almıştır. Günümüz teknolojileri dikkate alındığında, artık üretilecek ve tesis edilecek haberleşme sistemlerinin beka yeteneği yüksek ve güvenli IP tabanlı olması gerekliliği ortadadır. Ülke içerisinde yürütülen çalışmaların bu doğrultuda olması öngörülmektedir.



Şekil-3: *Haberleşme Altyapıları ve Kullanıcı Terminalleri Değişimi*

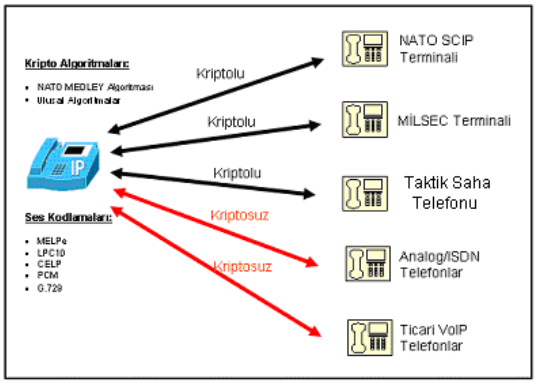


Şekil-4: *Kullanıcı İhtiyacı Olan Telefonlar*

Örnek olarak, **Şekil-4**'te mevcut yapı içerisinde değişik işlevlere ve maksatlara dönük ihtiyaç duyulan kullanıcı bölgesi haberleşme olanakları görülmektedir. Görüldüğü üzere her bir fonksiyon ve görev çeşidi için farklı terminal cihazı kullanımı söz konusudur. Mevcut muhabere donanımlarının bazıları ile değişik kripto algoritmaları ve anahtar yapıları kullanılırken, diğerleriyle de komuta ve kontrolün gereği itibariyle, açık (emniyetsiz/kriptosuz) ses haberleşmesi yerine getirilmektedir. Her bir haberleşme sistemi kendine özgü iletim ve ağ teknolojileri ile kripto altyapısını kullanmaktadır.

Yukarıda çerçevesi çizilmeye çalışılan sorunların çözümü için, altta bulunan şebekelerden bağımsız olarak IP protokolü ile mevcut haberleşme sistemlerini tek bir yapı içinde bütünleştirilmesi ve IP terminalleri ile uçtan uca emniyetli haberleşme yapılması öngörülmüştür. IP terminallerinin güvenli haberleşme için SCIP uyumlu olarak tasarlanması planlanmaktadır. Üretilebilecek böyle bir terminal ile **Şekil-4**'de görülen tüm işlevlerin tek bir Emniyetli IP Terminal üzerinde birleştirilerek, mevcut karmaşıklığa son verilebilmesi de mümkün olabilecektir.

Şekil-5'de açıkça görüldüğü üzere tek bir IP terminali üzerinde değişik ses kodlama ve kripto algoritmalarının koşturulabilmesi teknik olarak mümkün olduğundan, bu çözümle bir çok farklı cihaz ve sistemle uyumlu ve gerektiğinde güvenli olarak karşılıklı çalışabilme olanağı doğmuş olacaktır.

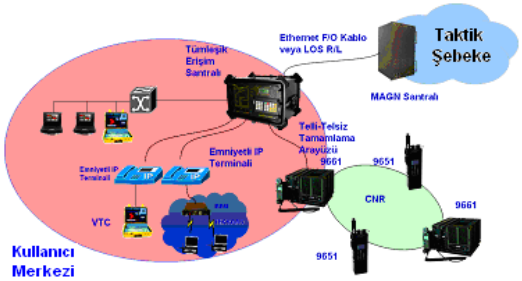


Şekil-5: *Emniyetli IP Terminali (Örnek)*

IP Telefon, çeşitli işlevlere sahip birden fazla donanımın bir arada ses ve veri aktarım hizmetlerini yürüttüğü bir sistemdir. Bu sistemin içerisinde IP Telefon haricinde bir adet IP Telefon Yöneticisi, bir adet Geçityolu ve emniyetli görüşmeler için anahtar dağıtım ve yönetim faaliyetlerini yerine getirilebilmesi için bir adet Emniyet Yönetici Birimi bulunmaktadır. Emniyetli bir IP Telefon görüşmesinin yapılabilmesi, tüm bu sistemin bir arada çalışabilmesine bağlıdır. Dolayısıyla, Emniyetli IP terminale sahip olmak kadar, diğer tüm işlevleri yerine getirebilecek birimlerin üretilebilmesi de önem arz etmektedir. Sistem için gerekli işlevleri yapmak üzere ayrı donanımlar üretmek yerine, ilgili bütün yeteneklere haiz tümleşik tek bir santralin tasarlanmasının mümkün olduğu değerlendirilmektedir.

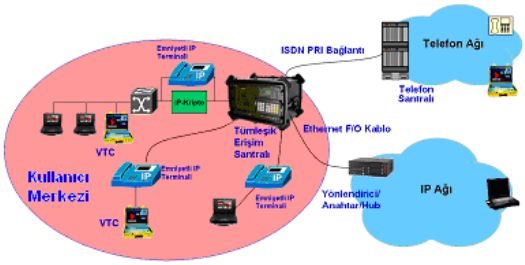
Yukarıda tarifi yapılan Tümleşik Erişim Santralinin, Emniyetli IP Haberleşme Sisteminde son derece önemli işlevleri bulunmaktadır. Bu santral tarafından verilmesi tasarlanan hizmetlere bakıldığında, üzerinde çok sayıda geçityolu (SCIP uyumlu IP Yönetici Birimi, Çoklu Ortam Geçityolu, H.323 için Gatekeeper Birimi vb.), yönlendirme ve anahtarlama işlemleri (ticari yönlendiricilerdeki özellikler de dâhil olmak üzere), çok çeşitli arayüzler (V35, Gbit F/O, Ethernet, ISDN PRI arayüzleri vb.) bulundurması gerekmektedir. Buna ek olarak tümleşik santralin telli ve telsiz tamamlama birimlerine sahip olması ve harekât ortamı etkilerine dayanıklı olarak işlevlerini yerine getirebilmesi önemlidir. SCIP yetenekli olarak tasarımlanması öngörülen gerek Emniyetli IP Terminali gerekse Tümleşik Erişim Santraline SCIP özelliğinin gömülü (embedded) olarak geliştirilmesi dikkate alınmalıdır.

Emniyetli IP Terminali ve Tümleşik Erişim Santralinin (TES) çok farklı görevlerde farklı maksatlara yönelik kullanım alanları bulabileceği öngörülmektedir. Kazanılması planlanan bu yeteneğin taktik ve stratejik sahada değişik kullanım senaryoları mevcuttur. Ortaya konan senaryolar, mevcut yapı içerisinde Emniyetli IP Terminal Haberleşme Sisteminin nasıl ve ne şekillerde kullanılabileceğini belirlemeyi hedeflemektedir. Düşünülen senaryolardan birkaçı aşağıda verilmiştir.



Şekil-6: *Emniyetli IP Terminalin Taktik Sahada Kullanımı*

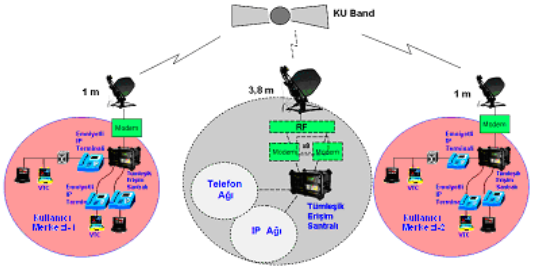
Tasarlanan yapının Taktik Sahada kullanımı **Şekil-6**'da tasvir edilmektedir. Görüldüğü üzere sistemin, fiber optik kablo bağlantısı veya radyo link bağlantılarıyla Taktik Saha Muhabere Sistemine bağlanması tasarlanmaktadır. Muharebe sahasındaki diğer komuta kontrol ve muharebe telsizleriyle bağlantı tümleşik santral üzerinden ve telli-telsiz tamamlama arayüzüyle sağlanmaktadır.



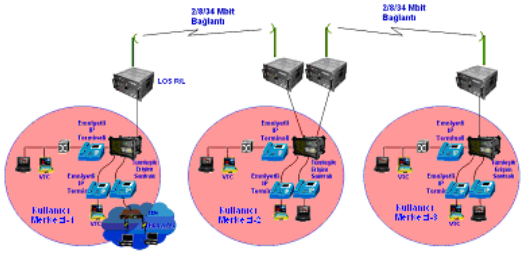
Şekil-7: *Emniyetli IP Terminalin Stratejik Şebekede Kullanımı*

Şekil-7'de Emniyetli IP Terminalinin Stratejik Şebekede kullanımı görülmektedir. Terminal, TES üzerinden Stratejik Şebeke Telefon ve IP Ağlarına bağlanabilmektedir. Emniyetli IP Terminali ile Stratejik Şebeke Telefon Ağı üzerinden açık görüşme yapılabileceği gibi IP Kripto cihazının kullanılmasıyla güvenli görüşme imkânının da sağlanabileceği değerlendirilmektedir. IP Terminallerle stratejik şebekeye bağlantı TES üzerinden ve doğrudan IP ağına dâhil olmak üzere iki şekilde de gerçekleştirilebilecektir.

Şekil-8'de Emniyetli IP Terminal Haberleşme Sisteminin, herhangi bir karasal erişim noktasından ya da Stratejik Şebeke üzerinden haberleşmeleri gösterilmektedir. Sistem karasal erişim yapılmaksızın doğrudan da harekât merkezleri arasında görüşmeyi sağlayabilmektedir. Bağlantının TES çıkışında uygun modem kullanılmak suretiyle **Ku** ve **X** Band Uydu üzerinden yapılması tasarlanmıştır.

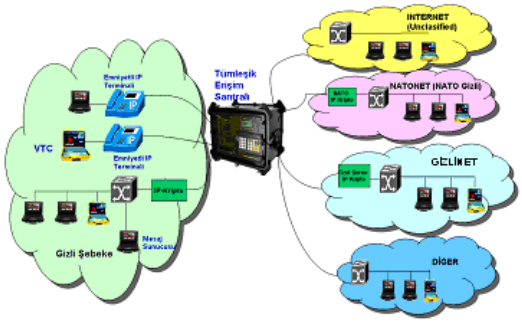


Şekil-8: *Emniyetli IP Terminalin Uydu Sistemleri ile Kullanımı*



Şekil-9: *Hareketli Kullanıcıların R/L ile Bağlantısı*

Şekil-9'da Hareketli Kullanıcıların mevcut Radyo Link Sistemlerini kullanarak değişik band genişliklerinde birbirleriyle doğrudan görüşebilmesinin mümkün olduğu görülmektedir.



Şekil 10. *Aynı Sistemde Beş Farklı IP Ağı*

Son olarak **Şekil-10**'da TES marifetiyle aynı sistem üzerinde beş farklı IP Ağının gerçeklenmesi gösterilmektedir. Mevcut durumda üzerlerinde farklı güvenlik düzeylerinde işler görülmesi nedeniyle bahsi geçen ağların hiç birisinin bir diğerine doğrudan ya da dolaylı fiziki irtibatı mevcut değildir. Kurulacak olan yapıyla ağ üzerinde mantıksal ayrıştırmalara gidilmek suretiyle bunun mümkün olması hedeflenmektedir.

5. SONUÇLAR

Bilim, enformasyon ve iletişim teknolojilerinde yaşanan gelişmeler öncekilerden farklı yeni haberleşme sistemlerin oluşturulmasına yol açmıştır. Bu nedenle daha öncesinde problem olmayan müşterek çalılaşabilirlik, sistem güvenirliliği ve servis kalitesi için engel haline gelmiştir. Diğer taraftan, bilgi üstünlüğüne duyulan ihtiyaç beraberinde Ağ Destekli Yetenek konseptinin gelişmesine yol açmıştır. Gerek ülkeler bazında gerekse uluslararası kuruluş ve organizasyonlarca bu konsept yaygın olarak kabul görmüş ve ülke ya da organizasyon savunma planlarının esasını teşkil eder hale gelmiştir.

Konuyla ilgili olarak, farklı şebeke teknolojileri üzerinden IP tabanlı uçtan uca emniyetli bir haberleşmenin sağlanması konusunda NATO'da SCIP Projesi başlatılmıştır. Bu bildiri kapsamında, SCIP ile ilgili bilgi verilmiş, söz konusu protokolün kullanımına yönelik olarak geliştirilmesi gereken ürünler ve bunların haberleşmede kullanımı ile ilgili bazı senaryolar verilmiştir.

Bu bildiride açıklanan haberleşme yeteneğinin kazanılması durumunda bu gelişmenin, harekât alanındaki muhabere ortamlarının çehresini değiştireceği değerlendirilmektedir. Bu konuda yapılan çalışmaların, silahlı kuvvetler ve NATO'nun Ağ Destekli Yetenek istikametindeki dönüşüm gayretlerine önemli katkıda bulunacağı düşünülmektedir.

SCIP haberleşme protokolü NATO standartları arasındaki yerini alacaktır. Bu nedenle bu teknolojiye uzak kalınmamalı ve henüz tasarım çalışmalarının devam ettiği şu zaman zarfında üzerinde gerekli incelemeler yapılıp NATO kanalıyla gerek görülen yerlere müdahale edilmelidir [8].

KAYNAKLAR

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

[2] BOZOKLU, Oğuz. "**Uyumlu ve Birlikte Çalışabilir Güvenli Muhabere Kapsamında NATO/SCIP Bünyesindeki Kripto Standartlarına Türkiye'nin Yaklaşımı**" (Yüksek Lisans Tezi), Ankara, Kara Harp Okulu Savunma Bilimleri Enstitüsü, Haziran 2007.

[3] Draft Basic Communications and Information Systems (CIS) Principles of Network Enabled Capabilities, "**AC / 322 (SC/6) N (2005) 0010**", 1 Şubat 2005.

[4] KREBS, Ron. "**FNBDT : An Architecture for NATO and NATO Nations**", ICWG Workshop for FNBDT, Verizon Labs. Boston, 10 – 12 Şubat 2004.

[5] Strategy on the Introduction of the Secure Communications Interoperability Protocol (SCIP) in NATO, "**AC/322(SC/6-AHWG/3)N(2006)0004-REV1**", 13 Haziran 2006.

[6] EDWARD, J. Daniel ve Diğerleri. "**The Future Narrowband Digital Terminal**", IEEE Magazine, 2002, II–589–592.

[7] EDWARD, J. Daniel ve Keith A.Teague. "**Federal Standard 2.4 kbps MELP Over IP**", IEEE Magazine, Aug. 8-11, 2000, 568–571.

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