



MARMARA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ



TELSİZ SİSTEMLERİNDE GÜVENLİ SES HABERLEŞMESİ

SELAHATTİN AKTAŞ

YÜKSEK LİSANS TEZİ

Bilgi Güvenliği Mühendisliği Anabilim Dalı

DANIŞMAN

Prof. Dr. Ensar GÜL

İSTANBUL, 2020



MARMARA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ



TELSİZ SİSTEMLERİNDE GÜVENLİ SES HABERLEŞMESİ

SELAHATTİN AKTAŞ

(527319004)

YÜKSEK LİSANS TEZİ

Bilgi Güvenliği Mühendisliği Anabilim Dalı

DANIŞMAN

Prof. Dr. Ensar GÜL

İSTANBUL, 2020

Telsiz Sistemlerinde Güvenli Ses Haberleşmesi

Bu tez Bilgi Güvenliği Mühendisliği'nde
Tezli Yüksek Lisans Programının bir koşulu olarak

Selahattin AKTAŞ
tarafından

Fen Bilimleri Enstitüsü'ne
sunulmuştur.



MARMARA
ÜNİVERSİTESİ

MARMARA ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

Marmara Üniversitesi Fen Bilimleri Enstitüsü Yüksek Lisans Öğrencisi Selahattin AKTAŞ'ın “**Telsiz Sistemlerinde Güvenli Ses Haberleşmesi**” başlıklı tez çalışması, 26 Haziran 2020 tarihinde savunulmuş ve jüri üyeleri tarafından başarılı bulunmuştur.

Jüri Üyeleri

Prof.Dr. Ensar GÜL (Danışman)
İstanbul Şehir Üniversitesi (İMZA).....

Doç.Dr. Tansal GÜÇLÜOĞLU (Üye)
Yıldız Teknik Üniversitesi (İMZA).....

Dr. Öğr. Üyesi İhsan ÇİÇEK (Üye)
İstanbul Şehir Üniversitesi (İMZA).....

ONAY

Marmara Üniversitesi Fen Bilimleri Enstitüsü Yönetim Kurulu'nun tarih ve sayılı kararı ile Selahattin AKTAŞ'ın Bilgi Güvenliği Mühendisliği Anabilim Dalı Bilgi Güvenliği Mühendisliği Programında Yüksek Lisans derecesi alması onanmıştır.

Fen Bilimleri Enstitüsü Müdürü
Prof. Dr. Bülent EKİCİ

Yazarlık Beyanı

Ben, Selahattin AKTAŞ, başlığı, 'Telsiz Sistemlerinde Güvenli Ses Haberleşmesi' olan tezin ve içinde sunulan bilgilerin şahsıma ait olduğunu beyan ederim. Ayrıca:

- Bu çalışmanın bütünü veya esası bu üniversitede Yüksek Lisans derecesi elde etmek üzere çalıştığım süre içinde gerçekleştirilmiştir.
- Daha önce bu tezin herhangi bir kısmı başka bir derece veya yeterlik almak üzere bu üniversiteye veya başka bir kuruma sunulduysa bu açık biçimde ifade edilmiştir.
- Başkalarının yayımlanmış çalışmalarına başvurduğum durumlarda bu çalışmalara açık biçimde atıfta bulundum.
- Başkalarının çalışmalarından alıntıladığımda kaynağı her zaman belirttim. Tezin bu alıntılar dışında kalan kısmı tümüyle benim kendi çalışmamdır.
- Esaslı yardım aldığım bütün kaynaklara teşekkür ettim.
- Tezde başkalarıyla birlikte gerçekleştirilen çalışmalar varsa onların katkısını ve kendi yaptıklarımı tam olarak açıkladım.

İmza:

Tarih:

Telsiz Sistemlerinde Güvenli Ses Haberleşmesi

Selahattin AKTAŞ

ÖZ

Bu tez çalışmasında, telsiz sistemlerinde güvenli haberleşme için NATO tarafından geliştirilen SCIP-214.6 protokolünün ses kalitesini iyileştirmek amacıyla alternatif çözümler önerilmektedir. Protokolün 2.4 Kbps veri hızını destekleyen dar bant modunda kriptosenkronizasyon sürekliliğini sağlamak amacıyla periyodik olarak ses çerçevelerinin yerine senkronizasyon çerçeveleri yerleştirilir. Bu tez kapsamında yapılan ilk çalışma ile geliştirdiğimiz yöntemde, ses çerçevelerinin frekans cevapları arasındaki çapraz ilişki alıcıya bildirilerek düşürülen çerçevelerin yerine en uygun çerçevenin yerleştirilmesi sağlanır. SCIP protokolünün 16 Kbps veri hızını destekleyen geniş bant modunda, 54 bit uzunluğundaki MELPe çekirdek bitlerine ses kalitesini artırmak amacıyla 120 bit uzunluğundaki ekstra bilgiler eklenir. Bu tez çalışmasında protokolün geniş bant modu için iki yeni faydalı yük çerçevesi oluşturma yöntemi önerilmektedir. Birinci yöntemde, 54 bitlik MELPe çekirdek bitleri hata düzeltme kodlaması ile kodlanarak ve kodlanmış çerçeve üç kez tekrarlanarak faydalı yük çerçevesi oluşturulur. İkinci yöntemde ise MELPe'ye alternatif olarak paket kayıplarına karşı düzeltici mekanizmaları içeren ILBC ses kodlayıcı-kodçözücüsü kullanılmaktadır. Önerilen yöntemler SCIP protokolü ile birlikte benzetim ortamında gerçekleştirilerek farklı SNR seviyelerindeki başarımların analizleri PESQ skorları kullanılarak raporlanmıştır. Dar bant modu için önerilen yöntem, düşük SNR seviyelerinde standarda yakın sonuç verirken yüksek SNR seviyelerinde daha iyi performans sergilemektedir. Geniş bant modunda ise, düşük SNR seviyelerinde Üçlü MELPe yöntemi, yüksek SNR seviyelerinde ILBC yöntemi en iyi ses kalitesi sunmaktadır.

Anahtar Sözcükler: Güvenli Ses Haberleşmesi, SCIP, MELPe, ILBC

Secure Voice Communication over Radio Systems

Selahattin AKTAŞ

Abstract

In this thesis, alternative solutions to the NATO SCIP-214.6 protocol, which has been design for secure voice communication over radio systems, are proposed to enhance voice quality. The late net entry (LNE) mechanism periodically transmits crypto synchronization information by replacing audio frames with the LNE frames in the SCIP narrowband mode supporting 2.4 Kbps data rate. To minimize the voice quality degradation, the receiver replaces the dropped frames with the generated new frames. In the first study conducted in the scope of this thesis, the cross correlation information of the frequency responses of the voice frames is transmitted to the receiver to decide whether the previous or next frame will be used instead of the dropped frame. In the wideband mode of the SCIP protocol supporting 16 Kbps data rate, Extended MELPe frames are used to improve the voice quality, where extra 120 bits are transmitted in addition to the 54 bits MELPe core. In the second study conducted in the scope of this thesis, two methods are proposed to generate the payload frames for the wideband mode of the protocol. In the first method, we add forward error correction (FEC) bits to the 54 bits MELPe core and the encoded bits are repeated three times for majority voting. In the second method, the ILBC vocoder containing corrective mechanisms against packet losses is used. All the methods proposed in this thesis together with the SCIP protocol are implemented in the simulation environment and the performance analysis under different channel conditions is reported using the PESQ scores. The method proposed for the narrowband mode provides higher PESQ scores at high SNR levels while yielding similar performance results at low SNR levels compared to the standard mechanism. In the wideband mode, the best voice quality is provided by the Triple MELPe and ILBC at low and high SNR levels, respectively.

Keywords: Secure Voice Communication, SCIP, MELPe, ILBC

Teşekkür

Bu tez çalışmasında yardım ve katkılarıyla beni yönlendiren tez danışmanım Sayın Prof. Dr. Ensar Gül'e ve çalışmamın her aşamasında varlığını hissettiren Sayın Dr. İbrahim Hökelek'e teşekkürlerimi sunarım.

Değerli fikir ve katkıları ile çalışmamın kalitesini yükseltmemde yardımcı olan değerli iş arkadaşım Ömer Faruk Gemici'ye teşekkür ederim.

Son olarak sevgili eşim Meryem Aktaş'a tez çalışmam boyunca verdiği desteklerden dolayı teşekkür ederim.



İçindekiler

Yazarlık Beyanı	ii
Öz	iii
Abstract	iv
Teşekkür	v
Şekil Listesi	viii
Tablo Listesi	ix
Kısaltmalar	x
1 Giriş	1
1.1 Bilimsel Katkı	5
1.2 Organizasyon	5
2 Tek Yönlü Güvenli Ses Haberleşme Sistemi	7
2.1 Kriptografik Bileşenler	9
2.1.1 Kripto Algoritması	9
2.1.2 Kripto Senkronizasyonu	10
2.1.3 Ağa Sonradan Dahil Olma (ASDO)	10
2.1.4 CRC Yöntemi	11
2.2 Ses Kodlayıcı-Kodçözücüleri	11
2.2.1 MELPe Ses Kodlayıcısı-Kodçözücüsü	12
2.2.2 Uzatılmış MELPe Ses Kodlayıcısı-Kodçözücüsü	14
2.2.3 ILBC Ses Kodlayıcısı-Kodçözücüsü	16
2.3 Hata Düzeltme Kodlamaları	16
2.3.1 BCH Hata Düzeltme Kodlaması	16
2.3.2 Hamming Hata Düzeltme Kodlaması	17
2.4 Ses Kalitesi Analiz Aracı	17
2.5 SCIP-214.6 Güvenli Haberleşme Protokolü	18
2.5.1 Dar Bant Güvenli Ses Haberleşmesi	20
2.5.2 Geniş Bant Güvenli Ses Haberleşmesi	23
3 SCIP-214.6 Protokolü için Önerilen Alternatif Yöntemler	27
3.1 Dar Bant Güvenli Ses Haberleşmesi için Önerilen Rahatlatıcı Ses Yöntemi	28

3.2	Geniş Bant Güvenli Ses Haberleşmesi için Önerilen Alternatif Faydalı Yük Çerçevesi Oluşturma Yöntemleri	30
3.2.1	Üçlü MELPe Yöntemi	30
3.2.2	ILBC Yöntemi	33
3.3	DeneySEL Sonuçlar	36
3.3.1	Benzetim Mimarisi	36
3.3.2	Dar Bant Deney Sonuçları	38
3.3.3	Geniş Bant Deney Sonuçları	40
4	Sonuç ve Tartışma	42
	Kaynakça	44



Şekil Listesi

1.1	SCIP-214.6 için standart ve önerilen yöntemler	4
2.1	Tek yönlü güvenli ses haberleşme sistemi	7
2.2	Benzetim mimarisi bileşenleri	9
2.3	NATO STANAG 4591 ses kodlayıcı performans tablosu	13
2.4	Uzatılmış MELPe kodlayıcısı akış diyagramı	15
2.5	Uzatılmış MELPe kodlayıcısında kullanılan ekstra spektral bileşenler . . .	15
2.6	PESQ'nun algısal değerlendirme modeli	18
2.7	Tek yönlü güvenli ses haberleşme mimarisi	19
2.8	SCIP-214.6 çağrı kurma sinyalleşmesi çerçeve yapısı	19
2.9	Dar bant faydalı yük çerçeve yapısı	21
2.10	Dar bant gönderici protokolü blok şeması	21
2.11	Dar bant alıcı protokolü blok şeması	22
2.12	Geniş bant faydalı yük çerçeve yapısı	23
2.13	Geniş bant gönderici protokolü blok şeması	24
2.14	Geniş bant alıcı protokolü blok şeması	25
3.1	Dar bant ses çerçevesi karşılaştırma yöntemi akış diyagramı	29
3.2	Geniş bant Üçlü MELPe faydalı yük çerçeve yapısı	31
3.3	Geniş bant Üçlü MELPe gönderici protokolü blok şeması	31
3.4	Geniş bant Üçlü MELPe alıcı protokolü blok şeması	32
3.5	Geniş bant ILBC faydalı yük çerçeve yapısı	33
3.6	Geniş bant ILBC gönderici protokolü blok şeması	34
3.7	Geniş bant ILBC alıcı protokolü blok şeması	35
3.8	Benzetim mimarisi akış diyagramı	37
3.9	Dar bant P.862.1 MOS-LQO PESQ sonuçları	38
3.10	Dar bant şifre çözme bilgisi elde etme oranları	39
3.11	Geniş bant P.862.1 MOS-LQO PESQ sonuçları	40
3.12	Geniş bant BER sonuçları	41

Tablo Listesi

2.1	Ses kodlayıcı özellikleri.	11
2.2	MELPe çerçeve özellikleri.	14
2.3	MOS-LQO skorlarına göre ses kalitesi [1].	18
2.4	SCIP-214.6 standart çerçeve özellikleri.	20
3.1	Önerilen yöntem çerçeve özellikleri.	30

Kısaltmalar

AES	A dvanced E ncryption S tandard
ASDO	A ğa S onradan D ahil O lma
AWGN	A dditive W hite G aussian N oise
BCH	B ose C haudhuri H ocquenghem
BER	B it E rror R ate
BPSK	B inary P hase S hift K eying
CBC	C ipher B lock C haining
CFB	C ipher F eed B ack
CRC	C yclic R edundancy C heck
CTR	C ounter
ECB	E lectronic C ode B ook
FEC	F orward E rror C orrection
FFT	F ast F ourier T ransform
HF	H igh F requency
ILBC	I nternet L ow B itrate C odec
KSK	K ripto S enkronizasyonunda K alma
MELPe	M ixed E xcitation L inear P redictive e nhanced
MOS-LQO	M ean O pinion S core - L istening Q uality O bjective
OFB	O utput F eed B ack
PCM	P ulse C ode M odulation
PESQ	P erceptual E valuation of S peech Q uality
SNK	S enkronizasyon
SNR	S ignal to N oise R atio
SCIP	S ecure C ommunications I nteroperability P rotocol
TSVCIS	T actical S ecure V oice C ryptographic I nteroperability S pecification

Bölüm 1

Giriş

Askeri uygulamalarda, kriz ve afet durumlarında, polis, itfaiye ve ambulans hizmetlerinde kablosuz haberleşme sistemleri yaygın olarak kullanılmaktadır. Kablosuz sinyallerin yayılımı nedeniyle kapsama alanı içerisinde yer alan bütün alıcılar sinyali alabilir. Gönderilen verilerin üçüncü şahısların eline geçmesini engellemek için gönderici tarafta şifrelendiği ve sadece alıcıların şifreli verileri çözebildiği güvenli haberleşme mekanizmaları kullanılır. Bant genişliğinin sınırlı olduğu kablosuz haberleşme sistemlerinde kanal kapasitesini verimli kullanmak amacıyla ses kodlayıcı yazılımlar ile ses verisi sıkıştırılarak bir noktadan çok noktaya iletilir.

SCIP-214.6 protokolü NATO tarafından telsiz sistemlerinde güvenli ses haberleşmesi için geliştirilmiştir [2]. Uygulama katmanında çalışacak şekilde tasarlanan protokolün fiziksel katmanla olan bağı minimum tutulmuştur. Protokolde HF telsizlerde çalışmak üzere 2.4 Kbps dar bant ve VHF/UHF telsizlerde çalışmak üzere 16 Kbps geniş bant modları yer almaktadır.

Mevcut HF ve VHF/UHF telsizlerde haberleşme tek yönlüdür ve bir telsiz aynı anda hem gönderme hem alma işlemini gerçekleştiremez. Bunun nedeni telsizin verici ve alıcı birimlerinin aynı frekans kanalını kullanmasıdır. Telsizler belirli frekans aralıklarına göre sınıflandırılmaktadır. HF, VHF ve UHF telsizlerin çalışma frekans aralıkları sırasıyla 3-30 MHz, 30-300 MHz ve 300-512 MHz'dir. Çalışma frekansı HF telsizlerde 3 KHz artımlarla belirlenirken VHF ve UHF telsizlerde 25 KHz artımlarla belirlenmektedir. Artırım miktarları haberleşme kanallarının bant genişlikleri ile aynıdır. VHF ve UHF telsizlerin bant genişliği HF telsizlerin bant genişliğine göre daha büyük olduğu için geniş

bant olarak adlandırılırken HF telsizler dar bant olarak isimlendirilmektedir. Veri iletim hızı HF telsizlerde 2.4 Kbps iken VHF ve UHF telsizlerde 16 Kbps'dir.

Amerika Birleşik Devletleri'nde yeni nesil taktik saha güvenli ses haberleşme cihazları ile sahada kullanılan eski cihazların kriptografik olarak modernize edilmiş modlarının birlikte çalışabilmesi adına Tactical Secure Voice Cryptographic Interoperability Specification (TSVCIS) çalışması NSA tarafından yapılmıştır [3]. Eski cihazlar için modernize edilmiş modlar belirlenirken temel amaç, kript mekanizmasını güncellerken mümkün olduğunca operasyonel performansı iyileştirmek ve iyileştirmelerin mümkün olmadığı yerlerde en azından eski performansı karşılamaktır. Hem dar bant hem de geniş bant haberleşme modları aynı anda modernize edilirken cihazlar arasında birlikte çalışabilirliğin sağlanması temel hedef olarak belirlenmiştir. Ayrıca modernizasyon çalışması ile eski haberleşme sistemlerinde şimdiye kadar tespit edilen hataları düzeltme imkanı da elde edildi. TSVCIS, taktik saha güvenli ses haberleşmesi için ses kodlama, şifreleme, çerçeveleme, senkronizasyon, anahtar yönetimi ve diğer işlevleri tanımlar. Dar bant ve geniş bant ses modları arasında birlikte çalışabilirlik sağlamak amacıyla MELPe 2400 dar bant ses kodlayıcısı geniş bant modunda da kullanılmaktadır. Ek olarak, geniş bant ve dar bant modlarında ortak senkronizasyon yöntemleri, ortak mod kontrol kelimeleri ve ortak şifreleme teknikleri kullanılmaktadır.

[4] çalışmasında, TSVCIS'te belirtilen MELPe 2400 ile geliştirilmiş 8 ve 12 Kbps'lik çalışma modları SINCGARS [5] askeri telsizlerinde kullanılan mevcut 16 Kbps'lik CVSD ile karşılaştırılmıştır. TSVCIS ile elde edilen ses kalitesi bütün kanal koşullarında CVSD'yi önemli ölçüde geride bırakmıştır. Ayrıca gürültülü kanal koşullarında TSVCIS ile sesin anlaşılabilirliğini korunurken CVSD bunu sağlayamamıştır. Sonuç olarak gürültülü iletişim kanalları üzerinde TSVCIS'in CVSD'den önemli ölçüde daha yüksek kalite ve anlaşılabilirlik sağladığı görülmüştür. TSVCIS protokolünü destekleyen çok sayıda cihazın sahada kullanılması nedeniyle NATO ülkeleri arasında birlikte çalışabilirliği sağlamak amacıyla TSVCIS protokolü uyarlanarak SCIP-214.6 adıyla ortak NATO standardı olarak kabul edilmiştir.

Benzetimini gerçekleştirdiğimiz SCIP-214.6 protokolünün dar bant modunda MELPe 2400 ses kodlayıcısı ile 22.5 ms'lik ses verisi sıkıştırılarak 54 bitlik MELPe çekirdek çerçeveleri elde edilmektedir. Geniş bant modunda ise çekirdek bitlerine ek olarak 120 bit

uzunluğunda ekstra ses kodlayıcı bitlerinin üretildiği Uzatılmış MELPe yöntemi kullanılmaktadır. MELPe 2400'den 2.4 Kbps'lık iletim hızı elde edilirken Uzatılmış MELPe'den 7.73 Kbps hız elde edilmektedir. Geniş bant modu için alternatif olarak seçtiğimiz ILBC ses kodlayıcısının ve MELPe 2400'ün performans analizleri [6] çalışmasında sunulmaktadır. Paket kayıplarına karşı düzeltici mekanizmaları içeren ILBC ses kodlayıcısından 30 ms'de 399 bit sıkıştırılmış ses verisi ile 13.33 Kbps'lık iletim hızı sağlanır [7, 8].

Şifreleme ve şifre çözme algoritmalarının gönderici ve alıcıda aynı durumda olması kriptosenkronizasyon mekanizması olarak ifade edilmektedir. Temelde kriptosenkronizasyonu başlangıç sinyalinde gönderilen bilgilerle sağlanmaktadır. Çok yönlü sönümlenme ve girişim gibi bozucu etkiler bit hata oranını artırarak kriptosenkronizasyonun sürekliliğini zorlaştırmaktadır [9]. Bu nedenle SCIP-214.6 protokolünde başlangıçta kriptosenkronizasyonunu sağlayamayan veya görüşme esnasında kaybeden terminallerin güvenli görüşmeye devam edebilmeleri için Ağa Sonradan Dahil Olma (ASDO) mekanizması tanımlanmaktadır. ASDO mekanizması kriptosenkronizasyon bilgisinin görüşme süresince faydalı yük çerçeveleri üzerinden parçalı şekilde gönderilerek alıcıya iletilmesini gerektirmektedir.

Protokolün dar bant modunda kanal kapasitesi sınırlı olduğu için, göndericide ses çerçeveleri belirli aralıklarla düşürülerek yerine ASDO çerçeveleri yerleştirilmektedir. Alıcıda ise çıkış sesi üretilirken ASDO çerçevesi yerine bir önceki ses çerçevesi kullanılmaktadır. Bu yöntem SCIP-214.6 protokolünde rahatlatıcı ses (comfort noise) yöntemi olarak tanımlanmaktadır.

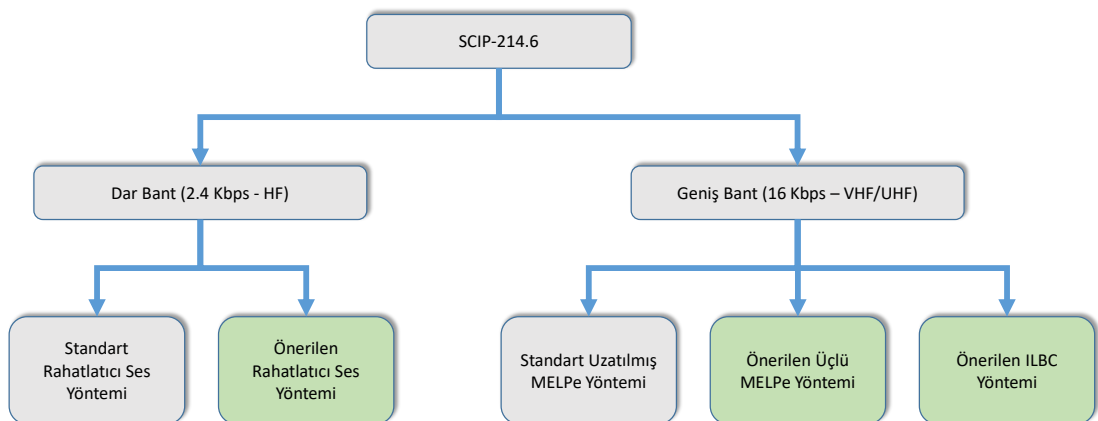
SCIP-214.6 protokolü ile benzer özellikleri içeren SCIP-210 [10] protokolünde de ASDO mekanizması nedeniyle göndericide ses çerçeveleri belirli aralıklarla düşürülerek yerine ASDO çerçeveleri yerleştirilmektedir. SCIP-210 protokolünün HF kanal koşullarındaki başarımların analizi [11] çalışmasında sunulurken, VHF/UHF kanal koşullarındaki performans analizi [12] çalışmasında sunulmuştur. Her iki çalışmada da alıcıda çıkış sesi üretilirken ASDO çerçeveleri yerine boş ses çerçevesi kullanılmaktadır. Ayrıca [13] çalışmasında SCIP-216 protokolünün kablolu haberleşme sistemlerindeki gerçek zamanlı uygulaması yapılmıştır. Bu çalışmaların hepsinde ortak olarak kullanılan MELP [14] ses kodlayıcı-kodçözücü'sünün başarımların analizleri ise [15] çalışmasında sunulmaktadır.

Bu tez kapsamında SCIP-214.6 protokolü incelenerek geliştirilen alternatif çözümlerle

birlikte benzetim ortamında başarımlar analizleri gerçekleştirilmiştir. Şekil 1.1’de gösterilen önerilen çözümlerde protokolde tanımlı olan kript mekanizması kullanılırken faydalı yük çerçevesi oluşturma yöntemlerinde farklılıklar bulunmaktadır. Geniş bant haberleşme modu için farklı ses kodlayıcı-kodçözücüler kullanılarak faydalı yük çerçeveleri oluşturulurken, dar bant modu için alıcıda ASDO’ndan kaynaklı ses kalitesindeki kaybı azaltmak amacıyla çapraz ilişki tabanlı rahatlatıcı ses yöntemi önerilmiştir.

SCIP-214.6 protokolünün geniş bant modunda Uzatılmış MELPe ses kodlayıcısından elde edilen ses bitleri BCH(15,5,3) [16] ve Hamming(16,11) [17] hata düzeltme kodlamaları ile kodlanarak faydalı yük çerçevelerine yerleştirilir. Önerdiğimiz Üçlü MELPe yönteminde, MELPe 2400 ses kodlayıcısından elde edilen ses bitleri BCH(110,54,9) kodlama yöntemi ile kodlandıktan sonra art arda üç kez kopyalanarak faydalı yük çerçevesine yerleştirilir. Önerdiğimiz ikinci yöntemde ise ILBC ile kodlanmış ses bitleri BCH(462,408,6) ile kodlanarak faydalı yük çerçevesine yerleştirilir. SCIP-214.6 protokolünde olduğu gibi önerilen her iki yöntem için ses bitlerine ilave olarak ASDO bilgisini içeren bitler yerleştirilerek faydalı yük çerçeveleri oluşturulur. En düşük hızda çalışan MELPe 2400 ses kodlayıcısı ile tasarlanan Üçlü MELPe yönteminde en yüksek oranda hata düzeltimi uygulanabilirken en yüksek hızda çalışan ILBC ses kodlayıcısı ile geliştirilen yöntemde ise en düşük oranda hata düzeltimi uygulanabilmektedir.

Haberleşme protokolünün farklı sinyal gürültü oranı (Signal to Noise Ratio - SNR) seviyelerinde başarımlar analizini yapmak amacıyla geliştirdiğimiz benzetim modülleri ile birlikte PESQ ses kalitesi analiz aracı kullanılmıştır. Alıcıda elde edilen ses verileri göndericideki referans ses verisi ile birlikte ITU tarafından önerilen PESQ aracına [18] verilerek ses kalitesi sayısal olarak ölçülmüştür.



ŞEKİL 1.1: SCIP-214.6 için standart ve önerilen yöntemler.

1.1 Bilimsel Katkı

Bu tezin katkısı aşağıdaki gibi özetlenmiştir.

- SCIP-214.6 protokolünün dar bant güvenli ses haberleşme modunda alıcıdaki ses kalitesini artırmak amacıyla çapraz ilişki tabanlı rahatlatıcı ses yöntemi sunulmuştur. Bu yöntemde, ASDO çerçevesindeki bir bit kullanılarak düşürülen ses çerçevesinin yerine bir önceki veya bir sonraki ses çerçevelerinden hangisinin yerleştirilmesi gerektiği bu çerçevelerin frekans cevapları arasındaki çapraz ilişki karşılaştırılarak alıcıya bildirilir. Deney sonuçları önerilen çapraz ilişki tabanlı rahatlatıcı ses yönteminin ses kalitesini %7.7'ye kadar iyileştirdiğini göstermektedir.
- SCIP-214.6 protokolünün geniş bant güvenli ses haberleşme modunda alıcıdaki ses kalitesini artırmak amacıyla iki yeni faydalı yük çerçevesi oluşturma yöntemi sunulmuştur. Protokolde tanımlı olan Uzatılmış MELPe ve geliştirdiğimiz Üçlü MELPe ve ILBC yöntemleri benzetim ortamında gerçekleştirilerek ses kalitesi performansları farklı SNR seviyelerinde karşılaştırmalı olarak incelenmiştir. Üçlü MELPe yöntemi 5.5 dB'den düşük SNR seviyelerinde standartta önerilen yönteme göre her zaman daha iyi ses kalitesi performansı sağlarken iyileştirme oranı %43'e kadar çıkmaktadır. Bununla birlikte 5.5 dB'den yüksek SNR seviyelerinde standart yöntem daha iyi sonuç verirken ses kalitesindeki kayıp oranı %4 ile sınırlıdır. ILBC yöntemi standartta önerilen yönteme göre 5.5 dB'den yüksek SNR seviyeleri için ses kalitesini %30'a kadar arttırırken, 5.5 dB'den düşük SNR seviyeleri için %40'a kadar düşürmektedir. Sonuçlar kötü kanal koşullarında Üçlü MELPe yönteminin iyi kanal koşullarında ise ILBC yönteminin kullanılmasının daha uygun olacağını göstermektedir.

1.2 Organizasyon

Bu bölümden sonra gelen Bölüm 2'de incelenen tek yönlü güvenli ses haberleşme sistemi, tez kapsamında kullanılan bileşenler ve benzetimi gerçekleştirilen SCIP-214.6 protokolü hakkında ön bilgi verilmiştir. Bölüm 3'de SCIP-214.6 protokolünün dar bant modu için çapraz ilişki tabanlı rahatlatıcı ses yöntemi geniş bant modu için ise iki yeni faydalı

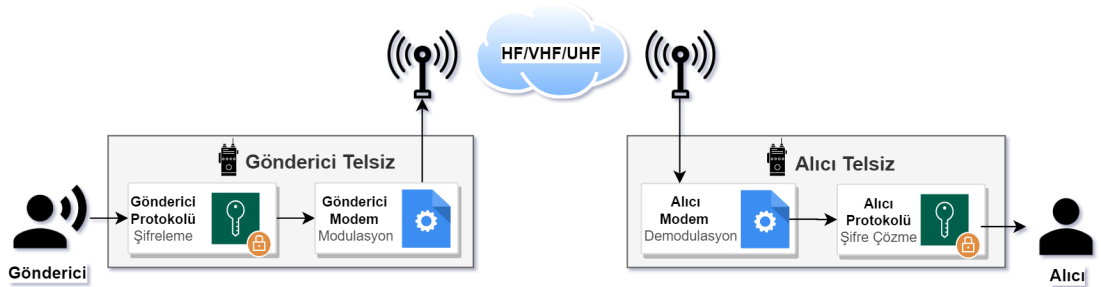
yük çerçevesi oluşturma yöntemi önerilerek standart yöntemler ile karşılaştırılmıştır. Son olarak Bölüm 4’de bu çalışma kapsamında elde edilen sonuçlar tartışılmaktadır.



Bölüm 2

Tek Yönlü Güvenli Ses Haberleşme Sistemi

Bu bölümde Şekil 2.1’de gösterilen HF, VHF ve UHF telsiz sistemleri için oluşturulmuş tek yönlü güvenli ses haberleşme sisteminden bahsedilecektir. HF, VHF ve UHF radyo sistemleri, askeri, diplomatik, havacılık, denizcilik ve amatör radyo hizmetleri tarafından ses ve veri iletişimi için yaygın olarak kullanılmaktadır. HF, VHF ve UHF telsizlerin çalışma frekans aralıkları sırasıyla 3-30 MHz, 30-300 MHz ve 300-512 MHz’dir [19]. Frekans arttıkça iletim mesafesi azaldığı için genellikle HF telsizler uzak mesafeler arası, VHF/UHF telsizler ise yakın mesafeler arası haberleşme amacıyla kullanılmaktadır. HF telsizlerin bant genişliği VHF/UHF telsizlere göre daha düşük olduğu için bilgi taşıma kapasitesi daha azdır. HF radyo dalgaları atmosferdeki iyonosfer tabakasından yansıma özelliğine sahipken VHF/UHF telsizler bu özellikten yoksundur [20]. İyonosfer tabakasından yansıyan HF dalgaları sayesinde birbirleri ile görüş açısında bulunmayan (BLOS) terminaller arasında haberleşme sağlanabilir [21]. VHF/UHF telsizlerde ise iyonosferden



ŞEKİL 2.1: Tek yönlü güvenli ses haberleşme sistemi.

yansıma özelliği olmadığı için sadece görüş açısında (LOS) bulunan terminaller arasında iletişim kurulabilir. Genişletilmiş bir savaş alanında VHF/UHF radyo dalgalarının yayılımı daha az olduğu için sinyale düşmanca müdahale daha zordur.

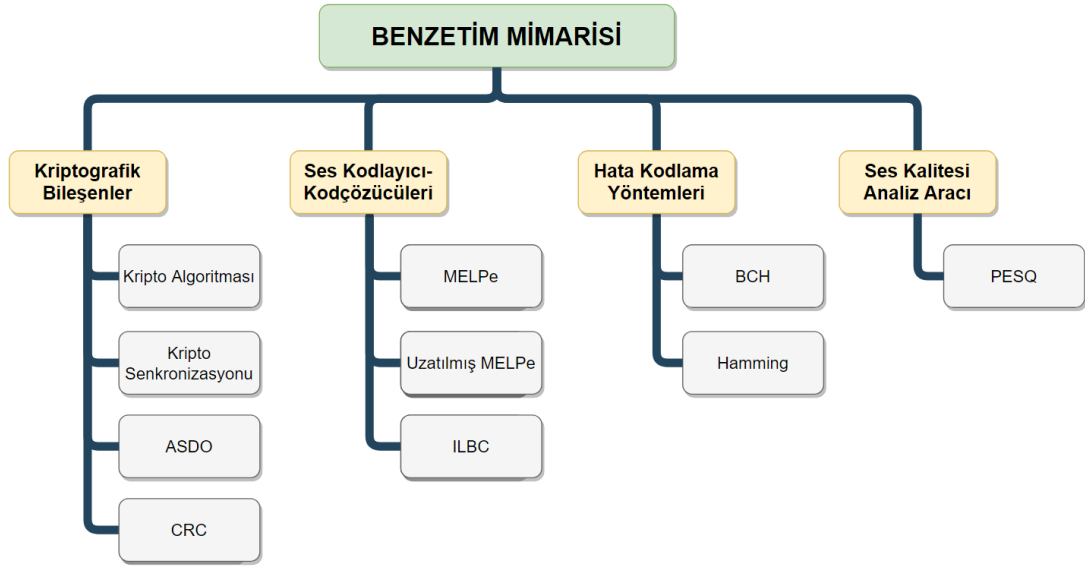
Görüş açısında bulunan terminaller arasında iletişim kurmaya uygun olan VHF/UHF radyo dalgalarının orman, deniz ve engebeli arazi ortamlarında yayılım karakteristikleri [22], [23] ve [24] çalışmalarında ayrıntılı olarak incelenmiştir. Ayrıca el tipi çalışan VHF/UHF telsiz antenlerinden yayılan radyasyonun insan vücuduna etkisini araştıran çalışmalarda mevcuttur [25].

Daha fazla bant genişliğine sahip olan VHF/UHF telsizler ile hata düzeltme kodlaması yöntemleri kullanılarak HF telsizlere göre daha temiz ve hızlı veri akışı sağlanabilir. VHF telsizleri daha çok kara birlikleri tarafından yerel (beş mil veya daha fazla) bir alanda iletişim kurmak için kullanılmaktadır. Antenleri daha küçük olan UHF telsizlerin ise süpersonik avcı uçaklarına monte edilmesi çok daha kolaydır, bu da UHF'yi yerden havaya iletişim için ideal bir seçim haline getirir. Modern askeri güçler artık havadan karaya iletişim için UHF spektrumunu tercih ediyor. Sadece UHF ve sadece VHF frekanslarında çalışan telsizler olmakla birlikte her iki frekans aralığını kapsayan telsizler de vardır.

HF sistemleri ile iyonosfer yoluyla uzun menzilli ve hatta dünya çapında iletişim kurulabilir [19]. Bu nedenle birbirleriyle geniş mesafelerde iletişim kuran baz istasyonları için hayati öneme sahiptirler. HF sistemleri sadece basit vericiler ve antenler gerektirdiğinden, HF bağlantıları uzak konumlardan veya doğal bir felaketten sonra kolayca kurulabilir. Bununla birlikte, iyonosferin değişken ve dağıtıcı doğası, hem donanım hem de iletişim protokolleri için bazı benzersiz gereksinimler getirmektedir.

HF radyo iletişiminde alıcılar her yerde radyo gürültüsünden kaçınılmaz olarak etkilenir. Etkilerin nicel olarak değerlendirilmesi gerekir. Yönlendirme ve polarizasyon dikkate alınarak HF radyo gürültüsünün kaynakları ve özellikleri [26] çalışmasında tartışılmaktadır. Ayrıca Avrupa ve Kuzey Amerika'dan Antarktika'ya HF radyo sinyal yayılımının analizi [27] çalışmasında sunulmaktadır.

Bu çalışmada HF, VHF ve UHF telsiz sistemleri arasında güvenli bağlantı kurmak amacıyla uygulama seviyesinde çalışan güvenli haberleşme protokolü üzerinde yoğunlaşmıştır. Bu protokolün performansını analiz etmek amacıyla gerçekleştirilen benzetim mimarisinde kullanılan bileşenler bu bölümde anlatılmaktadır. Benzetim mimarisi Şekil 2.2'de



ŞEKİL 2.2: Benzetim mimarisi bileşenleri.

gösterildiği gibi kriptografik bileşenler, ses kodlayıcı-kodçözücüler, hata düzeltme kodlamaları ve ses kalitesi analiz aracından oluşmaktadır.

2.1 Kriptografik Bileşenler

Kriptografik bileşenler güvenli haberleşme sistemlerinin en temel yapı taşlarıdır. Sağlıklı bir güvenli haberleşme sisteminde bilgi güvenliğinin en temel üç ilkesi olan gizlilik, bütünlük ve erişilebilirlik sağlanmalıdır. Bu çalışmada benzetimini gerçekleştirdiğimiz haberleşme protokolünde yer alan AES şifreleme algoritması ile gizlilik, CRC yöntemi ile bütünlük, krypto senkronizasyon ve ASDO mekanizmaları ile erişilebilirlik ilkeleri yerine getirilmiştir.

2.1.1 Kripto Algoritması

AES kiptolu haberleşmede yaygın olarak kullanılan bir simetrik blok şifreleme algoritmasıdır. Büyük boyuttaki veriler 128 bit uzunluğundaki bloklara bölünerek şifrenmektedir. Şifrelemede ve şifre çözmede kullanılan anahtarlar aynıdır ve uzunlukları 128, 192 veya 256 bit olarak seçilebilir. Anahtar uzunluğu arttıkça AES algoritmasında uygulanan tur sayısı da artmaktadır. 128, 192 ve 256 bit uzunluğundaki anahtarlar için sırasıyla uygulanan tur sayıları 10, 12 ve 14'tür. AES şifrelemesinin günümüz teknolojisi ile kırılması

çok fazla kaynak kullanımı gerektirdiği için uygulanabilir değildir. Anahtar uzunluğunun artması şifreleme algoritmasının kırılmasını zorlaştırırken şifreleme ve şifre çözme sürelerini bir miktar uzatmaktadır.

AES kriptu algoritmasının Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher FeedBack (CFB), Output FeedBack (OFB) ve Counter (CTR) modları bulunmaktadır. Bu modlar [28] çalışmasında ayrıntılı olarak incelenmiştir. Tek yönlü yani geri dönüş mekanizması bulunmayan güvenli haberleşme sistemlerinde kullanılmaya en uygun AES modu CTR modudur [29]. Bu tez kapsamında kriptu algoritması olarak AES-CTR-256 kullanılmıştır.

AES-CTR-256 şifreleme modülü 128 bitlik açık veri bloğunu 256 bit anahtar ve 128 bit başlangıç vektörü (IV) ile şifreli veriye dönüştürmektedir. Bir görüşme sırasında her blok için kullanılan anahtar aynı iken başlangıç vektörü değiştirilerek şifreleme işleminin karmaşıklığı artırılır. Görüşme başında başlangıç vektörü gönderici tarafından rasgele sayılardan oluşturularak alıcı ile paylaşılır. Görüşme sırasında her yeni blok için IV bilgisinin değeri bir artırılarak kullanılır. Bu sayede gönderici ve alıcı aynı IV bilgisini kullanarak kriptolu görüşmeyi sürdürebilirler.

2.1.2 Kripto Senkronizasyonu

Kripto senkronizasyonu şifreleme ve şifre çözme algoritmalarının gönderici ve alıcıda aynı durumda olması ile sağlanır. AES kriptu algoritmasında kripto senkronizasyonu gönderici ve alıcının aynı anahtar ve IV bilgisi üzerinde anlaşmaları ile elde edilir. Simetrik şifreleme sistemlerinde anahtar bilgisi güvenli bir kanal üzerinden gönderici ve alıcıyla önceden paylaşılırken, IV bilgisi her görüşmenin başında gönderici tarafından üretilerek alıcıya iletilir. Gönderici ile aynı anahtar ve IV bilgisine sahip olan alıcı kripto senkronizasyonunu sağlayarak görüşmeye dahil olabilir.

2.1.3 Ağa Sonradan Dahil Olma (ASDO)

Haberleşme kanalında meydana gelen bozucu etkiler kripto senkronizasyonunun başlangıçta elde edilememesine ya da görüşme sırasında kaybedilmesine neden olabilir. İncelediğimiz haberleşme protokolünde kripto senkronizasyonunun görüşme esnasında da elde

edilebilmesine olanak sağlayan ASDO mekanizması tanımlanmaktadır. Görüşme süresince iletilen çerçevelerde ASDO mekanizması için ayrılmış olan bölge senkronizasyon bilgisinin parçalı şekilde gönderilmesi amacıyla kullanılır. Başlangıçta kriptografik senkronizasyonunu sağlayamayan alıcı bu parçaları birleştirilerek ağa sonradan dahil olabilir.

2.1.4 CRC Yöntemi

Dijital ağlarda veya depolama aygıtlarında ham veride yanlışlıkla meydana gelebilecek değişiklikler CRC algoritmaları ile tespit edilir [30]. Haberleşme sistemlerinde genellikle gönderici tarafta mesajın CRC değeri hesaplanarak mesaj sonuna eklenir. Alıcı tarafta ise elde edilen mesajın CRC değeri tekrar hesaplanarak göndericide hesaplanan değerle kıyaslanır. CRC değerleri eşleşmez ise mesaj geçersiz olarak değerlendirilebilir. Gerçek zamanlı haberleşme sistemlerinde yaygın olarak kullanılması nedeniyle CRC hesabı kolaydır. Donanım ve yazılım üzerinde hızlı CRC uygulamaları [31] ve [32] çalışmalarında sunulmaktadır.

2.2 Ses Kodlayıcı-Kodçözücüleri

Kanal kapasitesi sınırlı olan haberleşme sistemlerinde ses kodlayıcı-kodçözücüleri büyük öneme sahiptir. Analog sesin dijitale dönüştürülmesi ile elde edilen ham ses verisi depolanmak veya transfer edilmek için yeterince elverişli değildir. Çok fazla alan kaplayan ham ses verisi ses kodlayıcı yazılımlar ile sıkıştırılarak düşük veri hızına sahip haberleşme sistemlerinde taşınabilir hale getirilir. Bu nedenle düşük hızda veri üreten ve ses kalitesi iyi olan ses kodlayıcı-kodçözücülerine ihtiyaç duyulmaktadır. Bu bölümde tez kapsamında güvenli haberleşme protokolü ile test edilen, farklı hızlara ve ses kalitelerine sahip üç farklı ses kodlayıcısı-kodçözücüsünden bahsedilecektir. Bu ses kodlayıcılarının çalışma hızları ve çerçeve uzunlukları Tablo 2.1’de gösterilmektedir.

TABLO 2.1: Ses kodlayıcı özellikleri.

Ses Kodlayıcısı	Çalışma Hızı	Çerçeve Süresi	Çerçeve Bit Uzunluğu	Sıkıştırma Oranı
MELPe 2400	2.4 Kbps	22.5 ms	54 bit	0.01875
Uzatılmış MELPe	7.73 Kbps	22.5 ms	174 bit	0.06042
ILBC	13.33 Kbps	30 ms	399 bit	0.10390

2.2.1 MELPe Ses Kodlayıcısı-Kodçözücüsü

MIL-STD-3005 [14] askeri ve STANAG 4591 [33] NATO standartları ile bilinen MELPe (Mixed Excitation Linear Predictive Enhanced) ses kodlayıcı-kodçözücüsü genellikle askeri platformlarda güvenli ses haberleşmesi amacıyla kullanılmaktadır. Dar bant ses kodlayıcısı olması nedeniyle kanal kapasitesi sınırlı olan radyo, uydu, VOIP ve cep telefonu gibi haberleşme platformlarında çalışmaya uygundur.

İlk MELP 1995 yılında Alan McCree tarafından icat edildi [34] ve 1997’de MIL-STD-3005 [14] olarak standardize edildi. ABD DoD yarışmasında aşağıda gösterilen diğer aday ses kodlayıcılarından üstün geldi [35].

- Frequency Selective Harmonic Coder (FSHC)
- Advanced Multi-Band Excitation (AMBE)
- Enhanced Multiband Excitation (EMBE)
- Sinusoid Transform Coder (STC)
- Subband LPC Coder (SBC)
- Waveform Interpolative (WI) Coder

İlk beş adaydan daha iyi ses kalitesi elde edilen MELP ses kodlayıcısı WI ses kodlayıcısından daha düşük karmaşıklığı sayesinde yarışmayı kazandı ve MIL-STD-3005 için seçildi.

1998 ile 2001 yılları arasında, SignalCom, AT&T Corporation ve Compendent tarafından yarı hızda çalışan (yani 1200 bps) yeni bir MELP tabanlı ses kodlayıcısı geliştirilerek MIL-STD-3005’e eklendi. Geliştirilmiş MELP eski MELP’in yarı hızında çalışarak aynı ses kalitesini sunarken, 2400 bps hızında eski MELP’ten daha iyi performans sergilemektedir. Enhanced MELP (MELPe) olarak isimlendirilen bu yeni ses kodlayıcısında bulunan ekstra özellikler aşağıda sıralanmıştır [36];

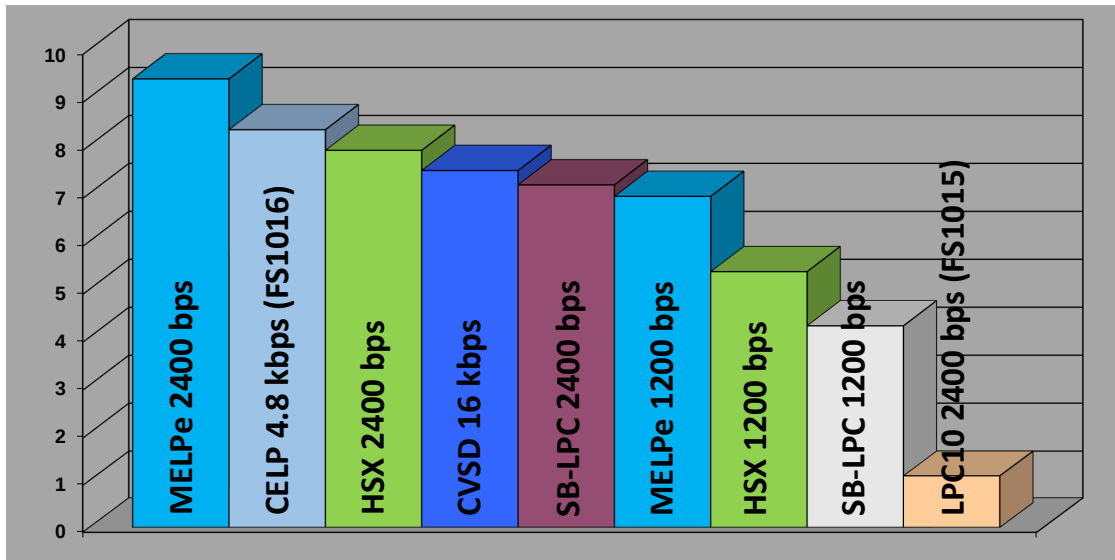
- MELP’in yarı hızında çalışma (1200 bps)
- Önemli ölçüde geliştirilmiş kodlama (analiz)

- Önemli ölçüde geliştirilmiş kod çözme (sentez)
- Arka plan gürültüsünü gidermek için gürültü önileme
- 2400 bps ve 1200 bps modları arasında dönüşüm
- Yeni post filtre

MELPe, eski MIL-STD-3005'e yapılan ekler ve takviyeler ile 2001 yılında yeni MIL-STD-3005 olarak kabul edildi. MELPe 2400'ün en büyük avantajlarından biri, MELP ile aynı bit biçimini paylaşarak eski MELP kullanılan sistemlerle birlikte çalışabiliyor olmasıdır. MELPe, özellikle savaş alanı, araçlar ve uçaklar gibi gürültülü ortamlarda, tüm eski askeri standartlardan çok daha iyi kalite sunmaktadır.

2002 yılında, kapsamlı rekabet ve testlerin ardından, 2400 ve 1200 bps MELPe, STANAG-4591 olarak bilinen NATO standardı olarak da kabul edildi [37]. Yeni NATO standardı testleri sırasında MELPe, Fransa'nın HSX ve Türkiye'nin SB-LPC ses kodlayıcılarının yanı sıra FS1015 LPC-10e (2.4 Kbps), FS1016 CELP (4.8 Kbps) ve CVSD (16 Kbps) gibi eski güvenli ses standartları ile de karşılaştırıldı. Karşılaştırma sonucu Şekil 2.3'de gösterilen performans tablosu elde edildi ve NATO yarışmasını da MELPe kazandı. NATO testi, 200 saatten fazla konuşma verisi kullanılan birlikte çalışabilirlik testlerini de içeriyordu ve dünya çapında 3 test laboratuvarı tarafından gerçekleştirildi.

2400 bps ve 1200 bps hızlarında veri üretebilen MELPe'ye 2005 yılında, Thales Group (Fransa) tarafından 600 bps modu eklendi [36]. Böylece birbirleri arasında kod dönüşümü



ŞEKİL 2.3: NATO STANAG 4591 ses kodlayıcı performans tablosu [36].

TABLO 2.2: MELPe çerçeve özellikleri.

Çalışma Hızı	Çerçeve Örnek Sayısı	Çerçeve Süresi	Çerçeve Bit Uzunluğu	Sıkıştırma Oranı
2400 bps	180	22.5 ms	54 bit	0.01875
1200 bps	540	67.5 ms	81 bit	0.00937
600 bps	720	90.0 ms	54 bit	0.00468

gerçekleştirilebilen ve 3 farklı hızda hizmet alınabilen MELPe ses kodlayıcısı elde edilmiş olundu. Tablo 2.2’de modlara göre MELPe çerçeve özellikleri gösterilmiştir.

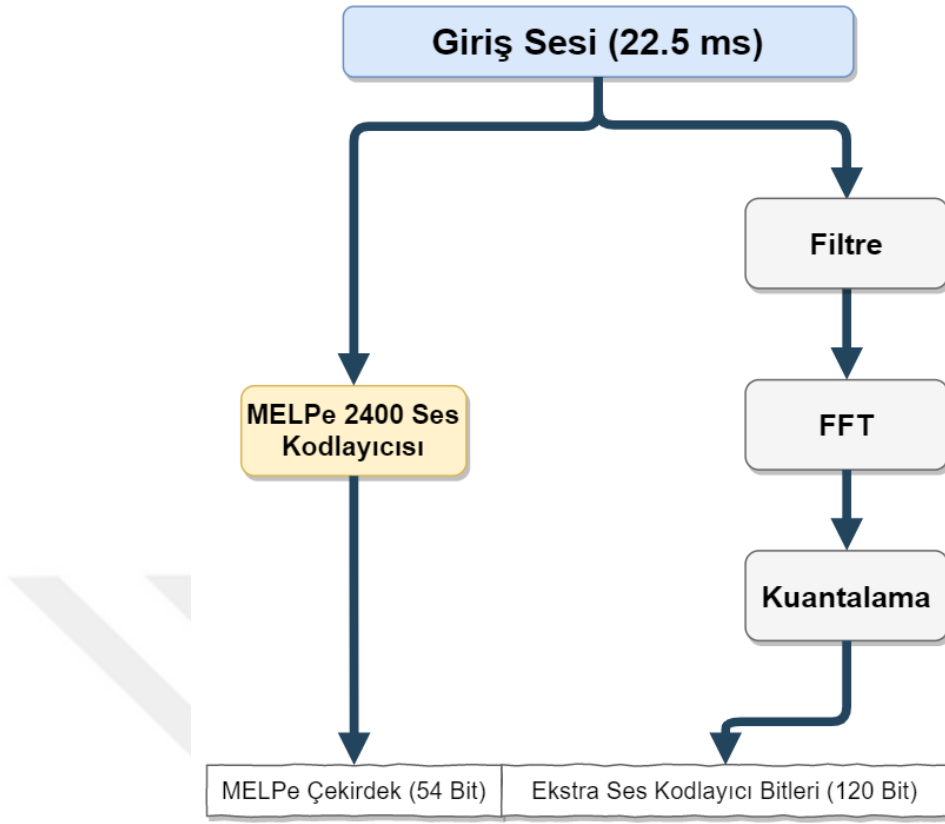
2400, 1200 ve 600 bps olmak üzere üç farklı kodlama hızına sahip olan MELPe ses kodlayıcısı 2400 ve 1200 bps hızlarında senkronizasyon kaybının tespit edilmesinde kullanılan senkronizasyon biti üretme özelliğine de sahiptir.

Bu çalışmada MELPe ses kodlayıcısı-kodçözücüsü 2400 bps hızında kullanılmıştır. MELPe 2400 ses kodlayıcısı 22.5 ms’lik ses verisini (8 KHz’de örneklenmiş 180 örnek) işleyerek 54 bit uzunluğunda kodlanmış ses çerçevesine dönüştürür.

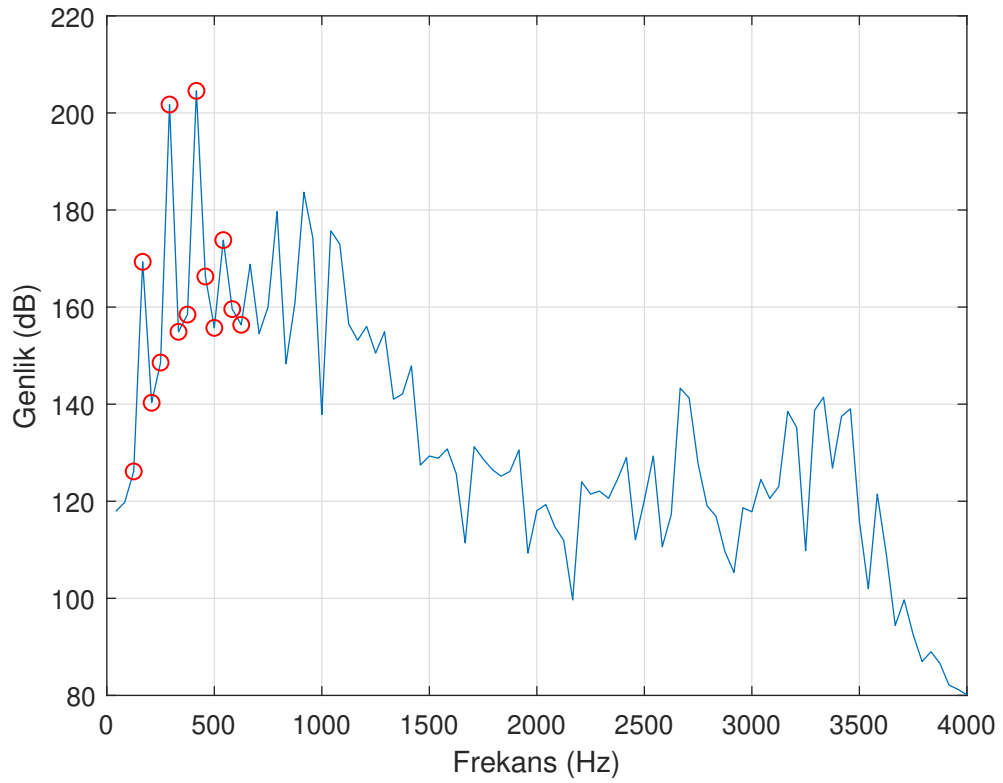
2.2.2 Uzatılmış MELPe Ses Kodlayıcısı-Kodçözücüsü

Uzatılmış MELPe ses kodlayıcısı, MELPe 2400 ses kodlayıcısından 22.5 ms’de elde edilen 54 bitlik ses çerçevelerine 120 bit uzunluğunda ekstra ses kodlayıcı bitlerinin eklenmesiyle elde edilir. Ekstra spektral özellikleri içeren ses kodlayıcı bitleri Şekil 2.4’de gösterildiği gibi giriş sesinin filtreleme, Hızlı Fourier dönüşümü (FFT) ve kuantalama işlemlerinden geçirilmesiyle elde edilir. 4 KHz bant genişliğindeki flitrelenmiş giriş sesinin 96 noktalı kompleks FFT dönüşümü hesaplanır. Böylece her biri 41.67 Hz’lik bölgeleri ifade eden 96 spektrum bilgisi kuantalanarak elde edilir. Şekil 2.5’de kırmızı daireler ile gösterilen 83 Hz ile 667 Hz arasındaki 14 spektral bileşen kullanılarak Uzatılmış MELPe’nin 120 bitlik ekstra bilgileri oluşturulur.

Uzatılmış MELPe ekstra ses kodlayıcı bitleri sayesinde MELPe 2400’e göre daha iyi ses kalitesi sunar. Bunun yanında veri üretim hızı 7.73 Kbps olduğu için haberleşme kanalında MELPe 2400’den daha fazla yer kaplar. Bu nedenle kanal kapasitesi yeterli olan haberleşme sistemlerinde Uzatılmış MELPe tercih edilebilir. Bu çalışmanın geniş bant haberleşme modunda Uzatılmış MELPe ses kodlayıcısı kullanılmıştır.



ŞEKİL 2.4: Uzatılmış MELPe kodlayıcısı akış diyagramı.



ŞEKİL 2.5: Uzatılmış MELPe kodlayıcısında kullanılan ekstra spektral bileşenler.

2.2.3 ILBC Ses Kodlayıcısı-Kodçözücüsü

ILBC, Global IP Sound şirketi tarafından geliştirilmiştir ve değiştirme izni de dahil olmak üzere ücretsiz bir şekilde kullanıma sunulmuş bir ses kodlayıcı-kodçözücüsüdür. IP tabanlı haberleşme sistemlerinde geciken ya da kaybolan paketlerden kaynaklanan ses bozulmalarını düzeltici mekanizmalara sahip olan ILBC'nin 13.33 Kbps ve 15.2 Kbps olmak üzere iki farklı çalışma hızı bulunmaktadır. Her iki çalışma hızında da ses kodlayıcısının örnekleme frekansı 8 KHz iken çerçeve uzunlukları farklıdır. ILBC ses kodlayıcısı 13.33 Kbps hızında iken 30 ms'de 399 bit sıkıştırılmış ses çerçevesi üretirken 15.2 Kbps hızında iken 20 ms'de 303 bit sıkıştırılmış ses çerçevesi üretmektedir [7] [8]. Bu çalışmada ILBC ses kodlayıcısı-kodçözücüsü 13.33 Kbps hızında kullanılmıştır.

2.3 Hata Düzeltme Kodlamaları

Haberleşme sistemlerinde gönderilen verilerin alıcıda doğru elde edilebilmesi güvenilirlik ve kullanılabilirlik açısından büyük öneme sahiptir. Gönderilen veri haberleşme kanalı üzerinden iletilirken çeşitli nedenlerle bit bozulmalarına maruz kalabilir. Bozulan bitler, alıcının gönderilen veriyi doğru şekilde elde edememesine ya da bozulmanın fark edilmediği durumda sahte veri elde etmesine neden olabilir. Hata düzeltme kodlamaları gürtülü haberleşme sistemlerinde gönderilen verilerin bit bozulmalarına karşı korunması amacıyla yaygın olarak kullanılmaktadır. Bu kodlama yöntemleri ile düzeltilebilecek seviyedeki bozulmuş bitlerin tam sayısı ve bozuk bitlerin yerleri tespit edilerek hatalar düzeltilir. [38],[16] ve [17] çalışmalarında BCH ve Hamming hata düzeltme kodlamaları ayrıntılı olarak incelenmiştir. Yeni nesil kodlama yöntemleri geliştirilmiş olmasına rağmen gerçekleştirme kolaylığından dolayı BCH ve Hamming yöntemleri günümüzde hala kullanılmaktadır.

2.3.1 BCH Hata Düzeltme Kodlaması

1959'da Fransız matematikçi Alexis Hocquenghem [39] ve bağımsız bir şekilde 1960'ta Raj Bose ve D.K. Ray-Chaudhuri [40] tarafından icat edilen Bose Chaudhuri Hocquenghem (BCH) blok kodlama yöntemi ismini bu üç kişinin soyadlarından almıştır. Bu

kodlama yönteminde, mesaj bitleri yedek bitler eklenerek kodlanır. Yedek bitler, hata algılamayı ve düzeltmeyi gerçekleştirebilmek için mesaj bitleri üzerinden hesaplanarak elde edilir. BCH hata düzeltme kodlamasında bulunan blok uzunluğu (n), mesaj uzunluğu (k) ve hata düzeltme sayısı (t) parametreleri değiştirilerek farklı oranlarda hata düzeltimi sağlanabilir.

m 2'den büyük pozitif tam sayı olmak üzere aşağıdaki formüllerden BCH parametreleri hesaplanabilir;

$$n = 2^m - 1 \quad (2.1)$$

$$t < 2^{m-1} \quad (2.2)$$

$$k \geq n - m * t \quad (2.3)$$

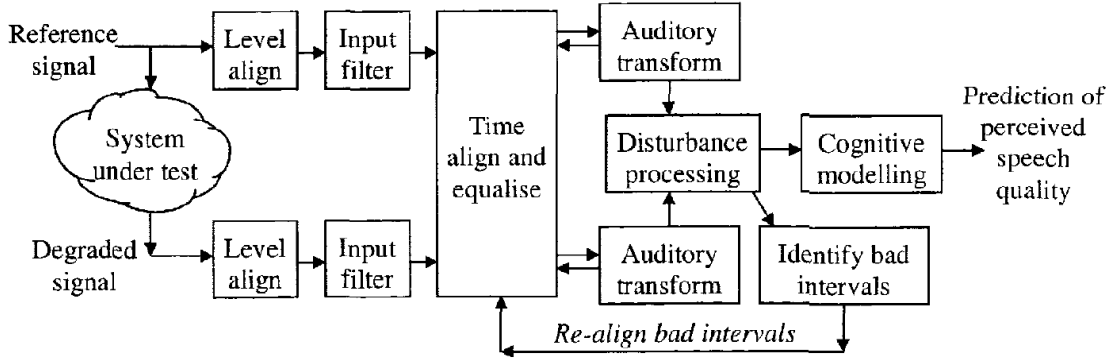
BCH(n,k,t) yöntemi ile k uzunluğundaki mesaj hata kodları eklenerek n uzunluğuna çıkartılır ve rasgele meydana gelebilecek t kadar hataya karşı dayanıklılık elde edilir. Bu çalışmada BCH(462,408,6), BCH(110,54,9) ve BCH(15,5,3) parametrelerine sahip hata düzeltme kodlamaları kullanılmıştır.

2.3.2 Hamming Hata Düzeltme Kodlaması

Hamming kodlaması, aynı anda iki bit hatasının algılanabildiği ve en fazla bir bit hatanın düzeltilebildiği bir blok kodlama yöntemidir. Hata düzeltme için R.W. Hamming tarafından geliştirilmiştir. Hamming, BCH blok kodlama yönteminin bir alt sınıfıdır. Bir bitlik hataları düzeltme yeteneğine sahip BCH, hamming yöntemi olarak isimlendirilir. Bu çalışmada Hamming(15,11,1) [16] geliştirilerek kullanılmıştır.

2.4 Ses Kalitesi Analiz Aracı

Perceptual Evaluation of Speech Quality (PESQ), ses kalitesinin otomatik olarak değerlendirilmesi amacıyla geliştirilmiş ITU tarafından önerilen bir standarttır [41]. Dünya



ŞEKİL 2.6: PESQ'nun algısal değerlendirme modeli [42].

çapında telefon üreticileri, şebeke ekipman satıcıları ve telekom operatörleri tarafından tarafsız bir test aracı olarak kullanılmaktadır.

[42] çalışmasında PESQ'nun algısal değerlendirme modeli Şekil 2.6'da gösterildiği gibi ayrıntılı olarak incelenmiştir.

TABLO 2.3: MOS-LQO skorlarına göre ses kalitesi [1].

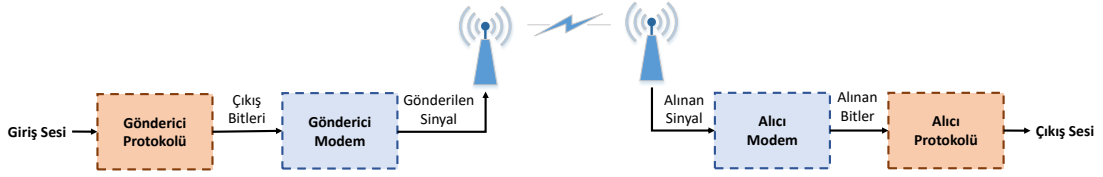
MOS-LQO	Ses Kalitesi
4.55	mükemmel
4.15	iyi
2.82	makul
1.63	düşük
1.02	kötü

P.862.1 [18] ile P.862 [41]'den elde edilen -0.5 ile 4.5 aralığındaki PESQ skoru, 1.02 ile 4.56 aralığında bulunan MOS-LQO değerine dönüştürülmüştür. [1] çalışmasından Tablo 2.3'de gösterilen MOS-LQO skorlarına göre ses kalitesi dereceleri elde edilmiştir.

Bu çalışmada hazır PESQ ses kalitesi analiz aracı kullanılmıştır. Bu araç bozulmuş ses ile bozulmamış ses verisini kıyaslayarak P.862.1'e uygun MOS-LQO değeri üretmektedir. Farklı ses kodlayıcıları ve farklı yöntemlerin kullanıldığı bu çalışmada PESQ aracından elde edilen MOS-LQO değerlerine bakılarak başarımlar analizleri gerçekleştirilmiştir.

2.5 SCIP-214.6 Güvenli Haberleşme Protokolü

Bu bölümde, Şekil 2.7'de gösterilen tek yönlü güvenli ses haberleşme mimarisinde kullanılan SCIP-214.6 protokolü anlatılmaktadır. Haberleşme mimarisi gönderici protokolü,

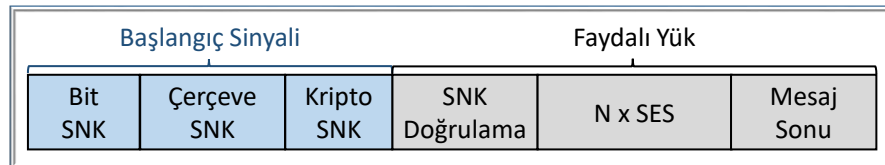


ŞEKİL 2.7: Tek yönlü güvenli ses haberleşme mimarisi.

gönderici modem, alıcı modem ve alıcı protokolü modüllerinden oluşmaktadır. Gönderici ve alıcı protokol modülleri içerisinde gerçekleştirilen SCIP-214.6 protokolü, çağrı kurma sinyalleşmesi, AES kript algoritması, MELPe ses kodlayıcı-kodçözücü ve ASDO fonksiyonlarını içermektedir.

Gönderici ve alıcı arasında haberleşme Şekil 2.8’de gösterilen çağrı kurma sinyalleşmesi mesaj iletim sırasına uygun şekilde gerçekleştirilmektedir. Çağrı kurma sinyalleşmesi görüşmenin başında gönderilen bit senkronizasyonu (bit SNK), çerçeve senkronizasyonu (çerçeve SNK), kript senkronizasyonu (kript SNK), senkronizasyon doğrulama (SNK doğrulama), görüşme süresince gönderilen ses ve görüşme sonunda gönderilen mesaj sonu bölümlerinden oluşmaktadır. Alıcının bit, çerçeve ve kript senkronizasyonunu sağlayabilmesi için gönderilen bölümler başlangıç sinyali olarak ifade edilirken geriye kalan bölümler faydalı yük olarak ifade edilmektedir. Kript senkronizasyonu sağlanana kadar alıcı şifreli verilere erişemeyeceği için başlangıç sinyali tamamen şifresiz gönderilmektedir. Başlangıç sinyali ile sağlanan kript senkronizasyonu SNK doğrulama çerçeveleri ile doğrulanır ve ses çerçevelerinin şifresi çözülerek çıkış sesi elde edilir. Mesaj sonu çerçevelerinin tespit edilmesi ile haberleşme sonlandırılır.

Kript senkronizasyonu şifreleme ve şifre çözme algoritmalarının gönderici ve alıcıda aynı durumda olması ile sağlanır. Haberleşme kanalında meydana gelen bozucu etkiler kript senkronizasyonunun başlangıçta elde edilememesine ya da görüşme esnasında kaybedilmesine neden olabilir. İncelediğimiz haberleşme protokolünde kript senkronizasyonunun görüşme esnasında da elde edilebilmesine olanak sağlayan Ağa Sonradan Dahil Olma (ASDO) mekanizması tanımlanmaktadır. Görüşme süresince iletilen çerçevelerde ASDO



ŞEKİL 2.8: SCIP-214.6 çağrı kurma sinyalleşmesi çerçeve yapısı.

TABLO 2.4: SCIP-214.6 standart çerçeve özellikleri.

	Dar Bant	Geniş Bant
Kanal Kapasitesi	2.4 Kbps	16 Kbps
Ses Kodlayıcısı	MELPe 2400	Uzatılmış MELPe
Çerçeve Süresi	22.5 ms	22.5 ms
Ses Kodlayıcısı Çerçeve Bit Uzunluğu	54 bit	174 bit
Faydalı Yük Çerçeve Bit Uzunluğu	54 bit	360 bit

mekanizması için ayrılmış olan bölge senkronizasyon bilgisinin parçalı şekilde gönderilmesi amacıyla kullanılır. Başlangıç sinyali ile kriptto senkronizasyonunu sağlayamayan alıcı bu parçaları birleştirilerek ağa sonradan dahil olabilir.

Protokolde HF telsizlerde çalışmak üzere 2.4 Kbps dar bant ve VHF/UHF telsizlerde çalışmak üzere 16 Kbps geniş bant modları bulunmaktadır. Geniş bant ve dar bant modlarının çerçeve özellikleri Tablo 2.4’de gösterilmektedir. Protokolün dar bant modunda MELPe 2400 ses kodlayıcısı ile 22.5 ms’lik ses verisi sıkıştırılarak 54 bitlik MELPe çekirdek çerçeveleri elde edilmektedir. Geniş bant modunda ise çekirdek bitlerine ek olarak 120 bit uzunluğunda ekstra ses kodlayıcı bitlerinin üretildiği Uzatılmış MELPe kullanılmaktadır.

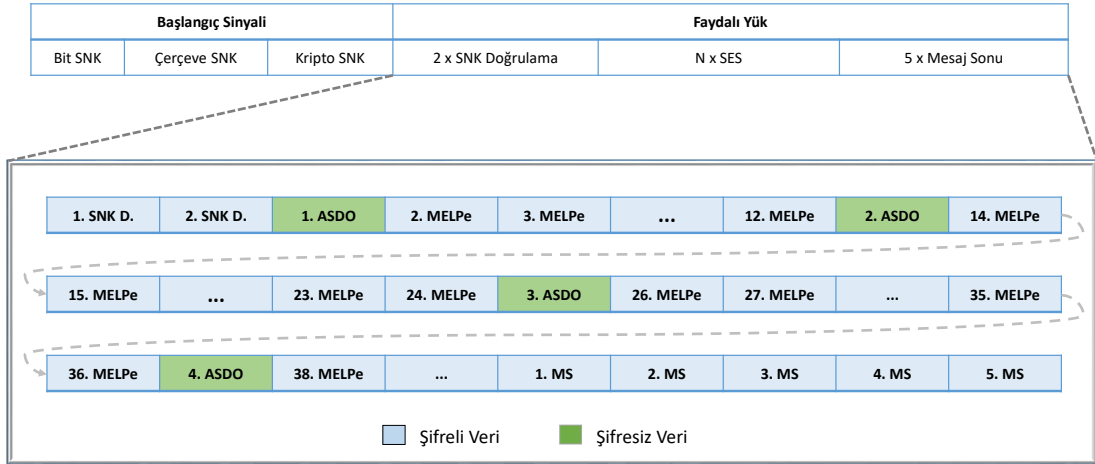
Çerçeve süresi (CS, saniye) ve kanal kapasitesi (KK, bps) bilgileri kullanılarak faydalı yük çerçeve bit uzunluğu (FYCBU, bit) aşağıdaki denklem ile hesaplanabilir:

$$FYCBU = CS * KK \quad (2.4)$$

2.5.1 Dar Bant Güvenli Ses Haberleşmesi

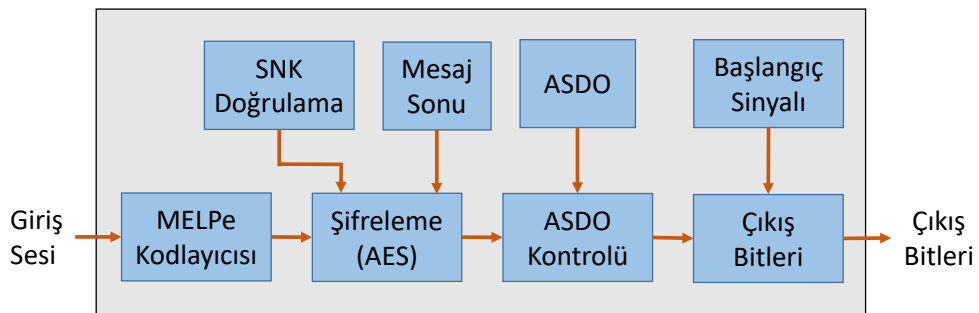
Protokolün dar bant modunda veri iletim hızı ve MELPe 2400 ses kodlayıcısının çalışma hızı aynıdır. Bu nedenle görüşme esnasında ASDO bilgisinin iletilmesi amacıyla belirli aralıklarla MELPe 2400 ses çerçevelerinin yerine ASDO çerçeveleri gönderilmektedir. Bu işlem ses çerçevelerinin tamamının alıcıya iletilmemesine ve ses kalitesinin düşmesine neden olmaktadır. ASDO çerçeveleri Şekil 2.9’da gösterildiği gibi 12 çerçevede bir adet gönderilmektedir. Alıcı beş adet ASDO çerçevesini birleştirerek kriptto senkronizasyon bilgisini elde etmektedir.

Giriş sesini Şekil 2.9’daki çerçeve yapısına uygun işleyerek modeme gönderilecek çıkış bitlerini oluşturan gönderici protokolünün blok şeması Şekil 2.10’da gösterilmektedir. Bu



ŞEKİL 2.9: Dar bant faydalı yük çerçeve yapısı.

protokol dört aşamada gerçekleştirilir. Birinci aşamada alıcının bit, çerçeve ve kripto senkronizasyonunu sağlaması için ihtiyaç duyacağı bilgileri içeren başlangıç sinyali üretilir. Bu aşamada alıcı henüz kripto senkronizasyonunu sağlamadığı için başlangıç sinyali şifrelenmeden iletilir. Kripto senkronizasyon bilgisinin alıcıda elde edilmesi ile alıcı, gönderici ile aynı başlangıç vektörünü oluşturur. İkinci aşamada alıcının da açık haline sahip olduğu senkronizasyon doğrulama bilgisi AES şifreleme algoritması ile şifrelenerek iletilir. Senkronizasyon doğrulama bilgisi alıcının başlangıç sinyalinden doğru başlangıç vektörü oluşturabildiğini kontrol etmesi amacıyla gönderilir. Üçüncü aşamada 8 KHz'de örneklenmiş 16 bit PCM ses verisi 22.5 ms'lik çerçeveler (180 örnek) halinde MELPe 2400 kodlayıcısıyla sıkıştırılır ve 54 bit uzunluğunda kodlanmış ses çerçeveleri elde edilir. Kodlanmış ses çerçeveleri şifrelenip ASDO kontrolü bloğuna iletilir. ASDO kontrolü bloğunda ağa sonradan dahil olma özelliğini sağlamak amacı ile belirli periyotlarda şifrelenmiş MELPe 2400 çerçeveleri düşürülerek boşalan yerlere ASDO çerçeveleri yerleştirilerek çıkış bitleri oluşturulur. Dördüncü aşamada alıcının da açık haline sahip olduğu mesaj

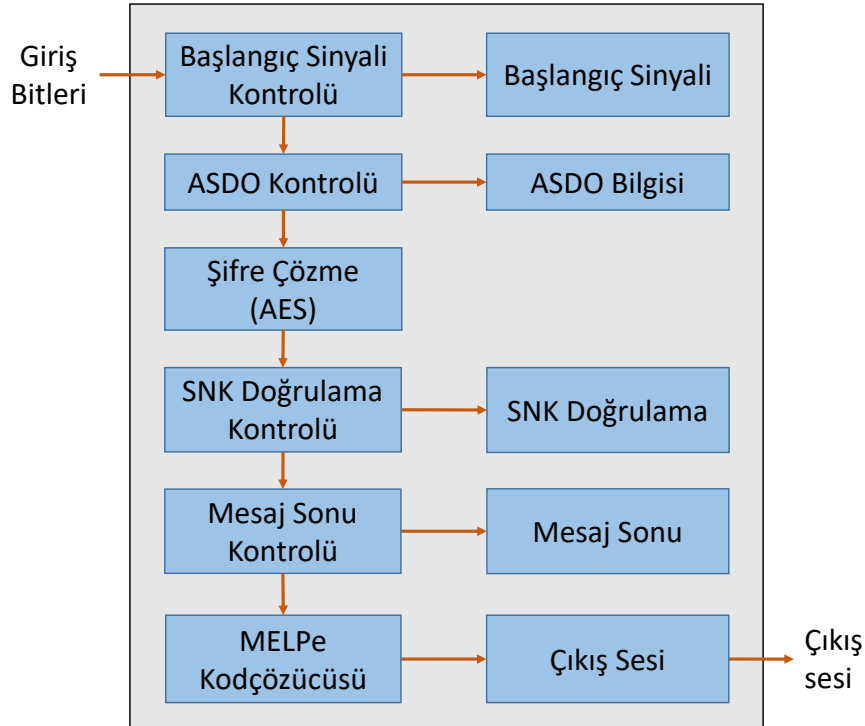


ŞEKİL 2.10: Dar bant gönderici protokolü blok şeması.

sonu bilgisi şifreli olarak iletilerek sinyalleşmenin sonlandığı bildirilir. Üçüncü tarafların sahte mesaj sonu bilgisi göndererek görüşmeyi sonlandırmasını engellemek amacıyla bu bilgi şifrelenmektedir.

Şekil 2.11’de alıcı terminalde modemden elde edilen bitleri işleyerek çıkış sesini oluşturan alıcı protokolü blok şeması gösterilmektedir. Dört aşamada gerçekleştirilen bu protokolün birinci aşamasında başlangıç sinyali tespit edilerek bu sinyal içerisindeki kriptografi bilgisi ile şifre çözmede kullanılacak anahtar üretilir. İkinci aşamada elde edilen anahtar ile SNK doğrulama çerçeveleri için şifre çözme işlemi uygulanarak kriptografi senkronizasyonu kontrolü gerçekleştirilir. Senkronizasyonun sağlanamadığı durumda birinci aşamaya geri dönülürken sağlanabildiği durumda üçüncü aşamaya geçilir. Bu aşamada şifreli olarak elde edilen MELPe 2400 çerçevelerine şifre çözme işlemi uygulanır ve MELPe 2400 kod-çözücüsü ile sıkıştırılmış ses yeniden elde edilir. Bununla birlikte periyodik olarak gelen ASDO çerçeveleri ASDO kontrolü bloğu ile tespit edilerek ASDO bilgisi elde edilir. Son olarak dördüncü aşamada elde edilen mesaj sonu bilgisi tespit edildiğinde mevcut ses haberleşmesi sonlandırılır.

Alıcıda MELPe 2400 ses çerçeveleri yerine gelen ASDO çerçeveleri, ses çerçevelerinin tamamının elde edilememesine ve dolayısı ile ses kalitesinin düşmesine neden olmaktadır.

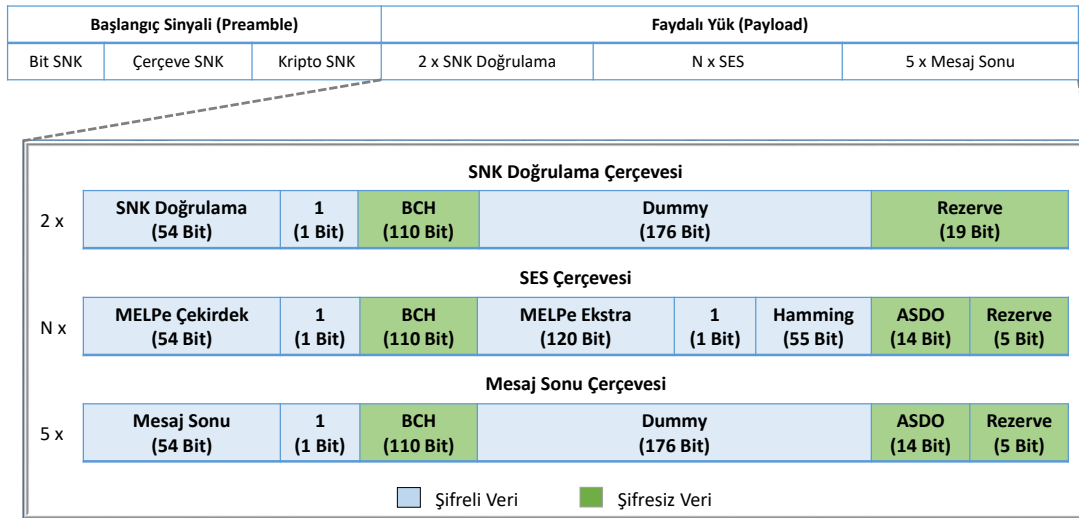


ŞEKİL 2.11: Dar bant alıcı protokolü blok şeması.

Alıcıda ses kalitesini arttırmak amacıyla göndericide düşürülen MELPe 2400 çerçevelerinin yeri rahatlatıcı ses yöntemi uygulanarak doldurulur. Bu yöntem ASDO çerçevesinden önce gelen MELPe 2400 çerçevesinin ASDO çerçevesi yerine yerleştirilmesi ile gerçekleştirilir. Bu çalışmada, alıcıdaki ses kalitesini yükseltmek amacıyla daha verimli bir rahatlatıcı ses yöntemi sunulmaktadır.

2.5.2 Geniş Bant Güvenli Ses Haberleşmesi

Protokolün geniş bant modunda faydalı yük içerisinde yer alan 2 adet SNK doğrulama, değişken sayıda ses ve 5 adet mesaj sonu çerçevesi Şekil 2.12’de gösterildiği gibi şifrelenecek gönderilmektedir. Faydalı yük kısmında gönderilen bütün çerçevelerde aynı bölgeler şifrelendiği için şifre çözme işlemi çerçeve türü bilgisi olmadan gerçekleştirilebilmektedir.

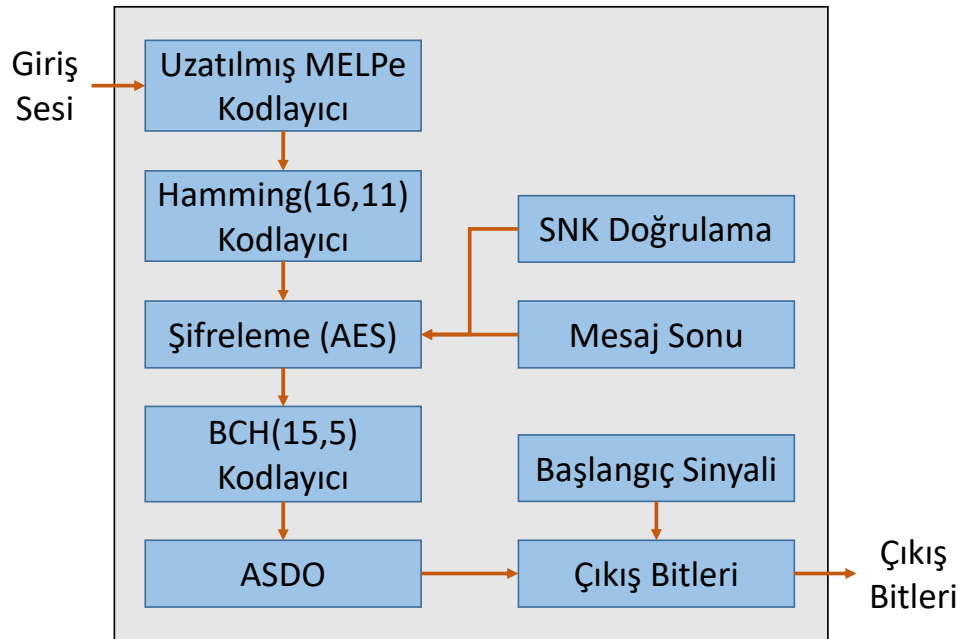


ŞEKİL 2.12: Geniş bant faydalı yük çerçeve yapısı.

Hamming ve BCH kodlama yöntemleri gürültülü haberleşme sistemlerinde gönderilen verilerin bit bozulmalarına karşı korunması amacıyla yaygın olarak kullanılmaktadır. İncelediğimiz haberleşme sisteminde faydalı yük çerçevelerinin ilk 54 bitini oluşturan SNK doğrulama, MELPe çekirdek ve mesaj sonu bölümleri BCH(15,5,3) hata düzeltme kodlaması ile korunmaktadır. Bu kodlama yöntemi 5 bit uzunluğundaki veriye 10 bit BCH kodunun eklenmesi ile oluşan 15 bitlik kodlanmış veri üzerinde 3 bite kadar bozulmaları düzeltebilme yeteneği sağlar. Göndericide faydalı yük çerçevelerinin şifrelenmiş ilk 55 biti 5 bitlik parçalar halinde kodlanır ve elde edilen 110 bit uzunluğundaki BCH kodları Şekil 2.12’de belirtilen bölgeye yazılır. Alıcıda ise BCH kod çözme işlemi uygulanarak

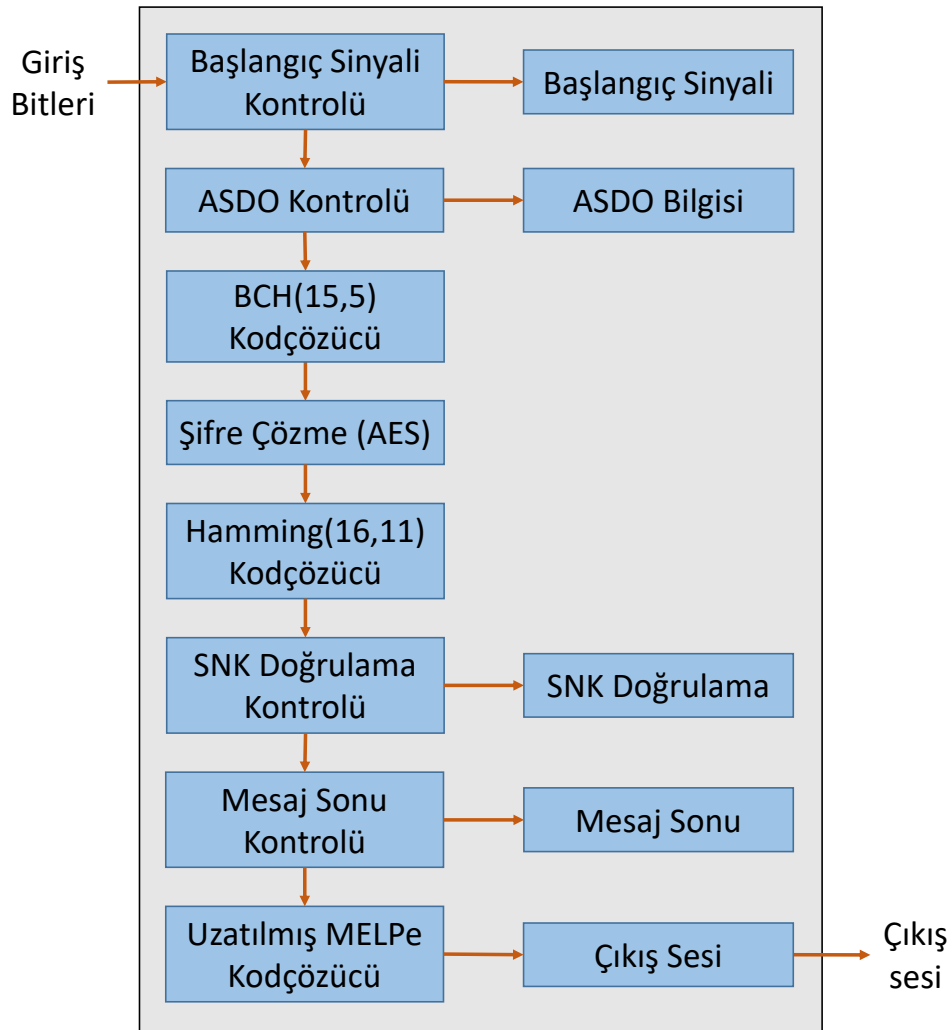
düzeltilerilebilir seviyedeki bit bozulmaları düzeltilir. Ayrıca sadece ses çerçevelerinde bulunan MELPe ekstra ses kodlayıcı bitlerini korumak amacıyla Hamming(16,11,1) kodlama yöntemi kullanılmıştır. Bu kodlama yöntemi 11 bit uzunluğundaki veriye 5 bit Hamming kodunun eklenmesi ile elde edilen 16 bit uzunluğundaki kodlanmış veride meydana gelebilecek 1 bitlik bozulmaların düzeltebilmesini, 2 bitlik bozulmaların ise tespit edilebilmesini sağlar. Göndericide MELPe ekstra bitleri şifrelenmeden önce 11 bit uzunluğundaki parçalara bölünerek Hamming(16,11,1) kodlayıcısı ile kodlanır. Bu işlem 11 kez tekrarlanarak toplamda 55 bit uzunluğunda Hamming kodu elde edilir ve Şekil 2.12’de gösterilen bölgeye yerleştirilir.

Kripto senkronizasyonu şifreleme ve şifre çözme algoritmalarının gönderici ve alıcıda aynı durumda olması ile sağlanır. Haberleşme kanalında meydana gelen bozucu etkiler kripto senkronizasyonunun başlangıçta elde edilememesine ya da görüşme esnasında kaybedilmesine neden olabilir. İncelediğimiz haberleşme protokolünde kripto senkronizasyonunun görüşme esnasında da elde edilebilmesine olanak sağlayan Ağa Sonradan Dahil Olma (ASDO) mekanizması tanımlanmaktadır. Görüşme süresince iletilen çerçevelerde ASDO mekanizması için ayrılmış olan bölge senkronizasyon bilgisinin parçalı şekilde gönderilmesi amacıyla kullanılır. Başlangıç sinyali ile kripto senkronizasyonunu sağlayamayan alıcı bu parçaları birleştirilerek ağa sonradan dahil olabilir.



ŞEKİL 2.13: Geniş bant gönderici protokolü blok şeması.

Çağrı kurma sinyalleşmesindeki başlangıç sinyali ve faydalı yük bölümlerinin oluşturulmasında kullanılan gönderici protokolü blok şeması Şekil 2.13’de gösterilmektedir. Gönderici protokolü içerisinde yapılan işlemler 4 farklı aşamada gerçekleştirilir. Birinci aşamada şifrelenmeden gönderilecek olan başlangıç sinyali üretilir ve çıkış bitleri oluşturulmaya başlanır. İkinci aşamada alıcının başlangıç sinyali ile sağlayacağı kripto senkronizasyonunu doğrulaması için gönderilecek olan SNK doğrulama çerçeveleri Şekil 2.12’de gösterilen çerçeve yapısına uygun şekilde üretilir. Üçüncü aşamada 8 KHz’de örneklenmiş 16 bit PCM giriş sesi 22.5 ms’lik parçalar halinde Uzatılmış MELPe ses kodlayıcısı ile sıkıştırılarak 174 bit uzunluğunda veri elde edilir. Elde edilen bu bitlerden ilk 54’ü MELPe çekirdek bitlerini oluştururken geriye kalan 120’si MELPe ekstra bitlerini oluşturmaktadır. MELPe ekstra bitleri şifreleme işleminden önce hamming kodlaması ile



ŞEKİL 2.14: Geniş bant alıcı protokolü blok şeması.

korunurken MELPe çekirdek bitleri şifreleme işleminden sonra BCH kodlaması ile korunmaktadır. BCH kodlamasından sonra ASDO mekanizmasından gelen 14 bitlik veri ses çerçevesine Şekil 2.12’de gösterildiği gibi yerleştirilir. Dördüncü aşamada görüşmenin sonlandığının bildirilmesi amacıyla 5 adet mesaj sonu çerçevesi üretilerek çıkış bitlerine eklenir. Üçüncü şahıslar tarafından mesaj sonu bilgisi üretilmesinin engellenmesi amacıyla bu çerçevelerde şifreli olarak gönderilmektedir. Gönderici protokolü modülünden elde edilen çıkış bitleri gönderici modem modülünde BPSK modülasyonu uygulanarak gönderici sinyale dönüştürülür.

Göndericiden gelen sinyale alıcı modem modülünde BPSK demodülasyonu uygulandıktan sonra elde edilen alıcı bitleri Şekil 2.14’de gösterilen alıcı protokolü blok şemasına uygun şekilde işlenir. Bu işlemler 4 farklı aşamada gerçekleştirilmektedir. Birinci aşamada başlangıç sinyalini yakalayarak kriptografik senkronizasyonunu sağlayan alıcı ikinci aşamada bu senkronizasyonun doğruluğunu kontrol etmek amacıyla alacağı iki adet SNK doğrulama çerçevesinin şifresini çözerek olması gereken açık veri ile kıyaslar. İlk iki aşamanın başarılı şekilde tamamlanması ile alıcı ses çerçevelerini işleyeceği üçüncü aşamaya geçer. Bu aşamada alıcı mesaj sonu çerçevesi tespit edene kadar elde edeceği Uzatılmış MELPe bitlerini Uzatılmış MELPe kodçözücüsü’ne ileterek çıkış sesinin üretilmesini sağlar. Dördüncü aşamada ise açık hali gönderici ve alıcıda bilinen mesaj sonu bilgisi tespit edilir ve görüşme sonlandırılır.

Bölüm 3

SCIP-214.6 Protokolü için Önerilen Alternatif Yöntemler

Bu bölümde SCIP-214.6 protokolünün dar bant ve geniş bant haberleşme modları için alıcıda elde edilen ses kalitesini iyileştirmek amacıyla geliştirilen alternatif çözümler önerilmektedir. Şekil 1.1’de gösterilen önerilen çözümlerde protokolde tanımlı olan kripto mekanizması kullanılırken faydalı yük çerçevesi oluşturma yöntemlerinde farklılıklar bulunmaktadır.

Protokolün 2.4 Kbps veri iletim hızını destekleyen dar bant modunda, alıcıda Ağa Sonradan Dahil Olma (ASDO) mekanizmasından kaynaklı ses kalitesindeki kaybı azaltmak amacıyla çapraz ilişki tabanlı rahatlatıcı ses yöntemi önerilmiştir. Bu yöntemde, ASDO çerçevesindeki bir bit kullanılarak düşürülen ses çerçevesinin yerine bir önceki veya bir sonraki ses çerçevelerinden hangisinin yerleştirilmesi gerektiği bu çerçevelerin frekans cevapları arasındaki çapraz ilişki karşılaştırılarak alıcıya bildirilir. Deney sonuçları önerilen çapraz ilişki tabanlı rahatlatıcı ses yönteminin ses kalitesini %7.7’ye kadar iyileştirdiğini göstermektedir.

Protokolünün 16 Kbps veri hızını destekleyen geniş bant modu için ise ortak kripto mekanizmasının kullanıldığı iki yeni faydalı yük çerçevesi oluşturma yöntemi önerilmektedir. Faydalı yük çerçeveleri NATO protokolünde Uzatılmış MELPe yöntemi ile oluşturulurken önerdiğimiz Üçlü MELPe olarak isimlendirilen birinci yöntemde, 54 bitlik MELPe 2400 çekirdek bitleri hata düzeltme kodlaması ile kodlanarak ve kodlanmış çerçeve üç

kez tekrarlanarak oluşturulmaktadır. Önerdiğimiz ikinci yöntemde ise MELPe'ye alternatif olarak paket kayıplarına karşı düzeltici mekanizmaları içeren ILBC ses kodlayıcı-kodçözücüsü kullanılmaktadır. Bahsi geçen üç yöntem benzetim ortamında gerçekleştirilerek farklı SNR seviyelerinde ses kalitesi performansları Perceptual Evaluation of Speech Quality (PESQ) skorları ölçülerek karşılaştırılmıştır. Deney sonuçları düşük SNR seviyelerinde Üçlü MELPe yönteminin, yüksek SNR seviyelerinde ise ILBC yönteminin Uzatılmış MELPe'ye göre daha yüksek PESQ skoru üreterek en iyi ses kalitesi sağladığını göstermektedir.

3.1 Dar Bant Güvenli Ses Haberleşmesi için Önerilen Rahatlatıcı Ses Yöntemi

Bu bölümde, alıcıda elde edilen ses kalitesini artırmak amacıyla önerdiğimiz rahatlatıcı ses yöntemi anlatılmaktadır. NATO protokolündeki rahatlatıcı ses yöntemi ile alıcıda çıkış sesi üretilirken ASDO çerçevesi yerine bir önceki ses çerçevesi kullanılmaktadır. Önerdiğimiz yöntemde ise ASDO çerçevesi yerine her zaman önceki ses çerçevesi değil sonraki ses çerçevesi de kullanılabilir. Bunun için göndericide ses çerçevesi düşürülmeden önce bu çerçeveye daha çok benzeyen çerçevenin belirlenmesi gerekmektedir. Bu işlem düşürülecek ses çerçevesinin frekans cevabının bir önceki ve bir sonraki çerçevelerin frekans cevapları ile olan çapraz ilişkilerinin karşılaştırılmasıyla sağlanmaktadır. Gerçek zamanlı olarak 22.5 ms içerisinde sadece bir ses çerçevesinin FFT'sinin hesaplanması işlemci yükü anlamında sorun teşkil etmemektedir.

Aynı konuşmacı için, konuşma içeriğindeki farklı kelimeler farklı frekans cevaplarına sahip olduğu bilgisi göz önüne alınarak yapılan [43] çalışmasında konuşma tanıma algoritmaları incelenmektedir. [43] çalışmasında, daha önce kaydedilen referans konuşma kayıtları ile tanınacak konuşmanın frekans cevapları arasındaki çapraz ilişkisi karşılaştırılarak konuşma içeriğinin tespiti sağlanmaktadır. Benzer şekilde önerdiğimiz rahatlatıcı ses yönteminde, düşürülen ses çerçevesi yerine yerleştirilecek ses bilgisinin belirlenmesinde ses çerçevelerinin frekans cevapları arasındaki çapraz ilişki kullanılmaktadır.

Önerdiğimiz yöntem alıcıda ASDO çerçeveleri yerine koyulacak olan ses çerçevelerinin belirlenmesi için göndericiden alıcıya bir bit kullanılarak bildirim yapılmasını gerektirmektedir. Şekil 3.1'de alıcıya, düşürülen ses çerçevesi yerine bir önceki veya bir sonraki

3.2 Geniş Bant Güvenli Ses Haberleşmesi için Önerilen Alternatif Faydalı Yük Çerçevesi Oluşturma Yöntemleri

Bu kısımda SCIP-214.6 protokolünün geniş bant modu için farklı SNR seviyelerinde standart yöntemden daha iyi ses kalitesi elde edilebilen alternatif güvenli ses haberleşme yöntemleri sunulmaktadır. Bu alternatif yöntemlerde Şekil 2.8’de gösterilen çağrı kurma sinyalleşmesi mesaj iletim sırasında, başlangıç sinyalinde ve kript algoritmasında değişiklik bulunmaz iken ses kodlayıcı-kodçözücü’lerinde, faydalı yük çerçeve yapılarında, ASDO mekanizmalarında, gönderici ve alıcı protokolü blok şemalarında farklılıklar bulunmaktadır.

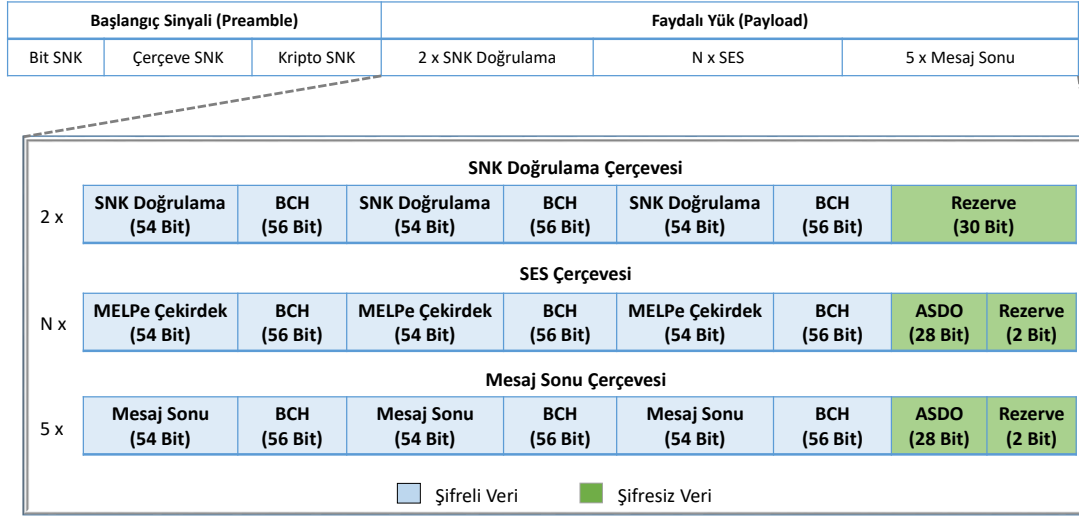
TABLO 3.1: Önerilen yöntem çerçeve özellikleri.

	Üçlü MELPe Yöntemi	ILBC Yöntemi
Kanal Kapasitesi	16 Kbps	16 Kbps
Ses Kodlayıcısı	MELPe 2400	ILBC
Çerçeve Süresi	22.5 ms	30 ms
Ses Kodlayıcısı Çerçeve Bit Uzunluğu	54 bit	399 bit
Faydalı Yük Çerçeve Bit Uzunluğu	360 bit	480 bit

Önerilen yöntemlerin çerçeve özellikleri Tablo 3.1’de gösterilmektedir. Tabloda yer alan faydalı yük çerçeve bit uzunlukları Denklem 2.4 kullanılarak hesaplanabilir.

3.2.1 Üçlü MELPe Yöntemi

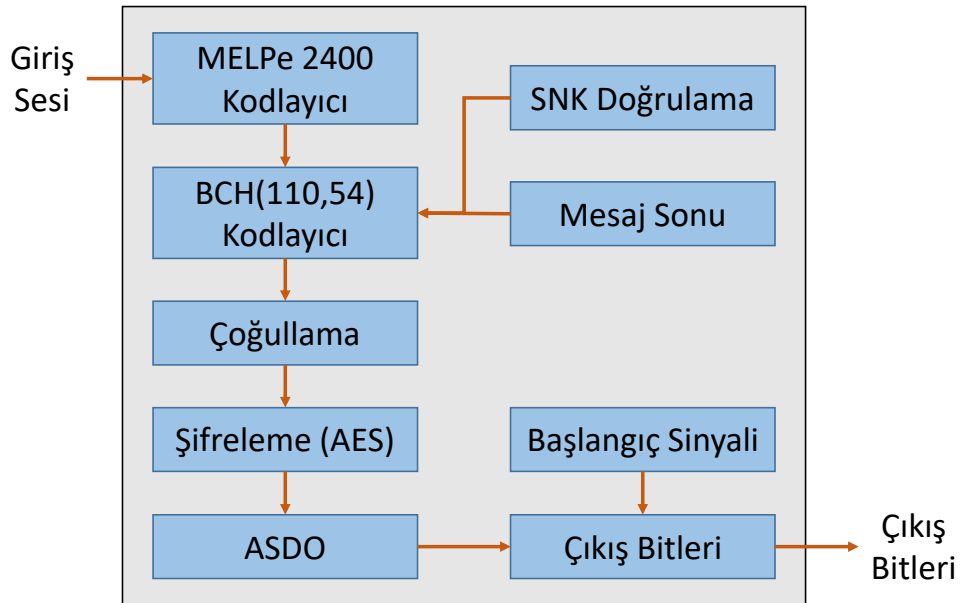
Bu bölümde, standart güvenli haberleşme sisteminde kullanılan Uzatılmış MELPe yöntemine alternatif olarak tasarlanan Üçlü MELPe yöntemi anlatılacaktır. Düşük SNR seviyelerine sahip kanal koşullarında daha iyi ses kalitesi elde etmek amacıyla standart yöntemde küçük değişiklikler yapılarak alternatif haberleşme yöntemi elde edilmiştir. Üçlü MELPe yönteminde başlangıç sinyali ve faydalı yük kısımları standart yöntemde olduğu gibi Şekil 2.8’de gösterilen çağrı kurma sinyalleşmesi mesaj iletim sırasına uygun üretilmektedir. Başlangıç sinyali standart ile aynı iken faydalı yük kısmında değişiklikler bulunmaktadır. MELPe 2400 ses kodlayıcısı 22,5 ms’de 54 bit veri üretirken Uzatılmış MELPe ses kodlayıcısı bu 54 bite ilave olarak 120 bit ekstra ses kodlayıcı biti üretmektedir. MELPe 2400 ile tasarlanan Üçlü MELPe yönteminde ekstra ses kodlayıcı bitleri olmadığı için MELPe çekirdek bitleri daha fazla korunarak gönderilmektedir. Faydalı yük içerisinde yer alan SNK doğrulama, ses ve mesaj sonu çerçeveleri Şekil 3.2’de gösterilen



ŞEKİL 3.2: Geniş bant Üçlü MELPe faydalı yük çerçeve yapısı.

çerçeve yapısına uygun şekilde üretilmektedir. Bu çerçevelerde ASDO mekanizması için ayrılan alan standarttakinin iki katına çıkartılarak ağa sonradan dahil olma süresi yarıya indirilmiştir.

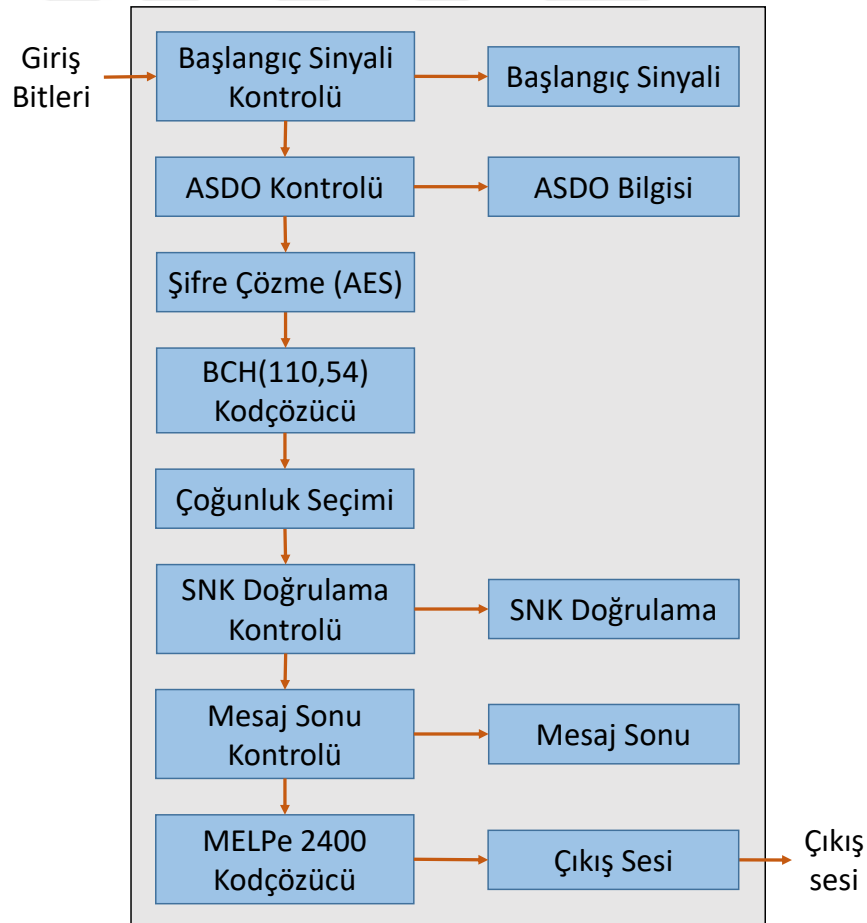
Üçlü MELPe yönteminin gönderici ve alıcı protokol blok şemaları faydalı yük çerçeve-lerinde yapılan değişikliklerden dolayı standart yöntemden biraz farklıdır. Üçlü MELPe gönderici protokolü giriş sesini Şekil 3.3’de gösterilen blok şemasına uygun şekilde işle-yerek çıkış bitlerini oluşturmaktadır. Görüşmenin başında gönderilen başlangıç sinyali



ŞEKİL 3.3: Geniş bant Üçlü MELPe gönderici protokolü blok şeması.

üretimi standart ile aynı şekildedir. Ardından gönderilecek olan faydalı yük çerçevelerinde göndericinin alıcıya şifreli olarak iletmesi gereken SNK doğrulama, ses ve mesaj sonu bilgileri 54 bit uzunluğundadır. Bu veri 9 bit bozulmaya kadar dayanıklı olan BCH(110,54,9) hata düzeltme kodlaması ile kodlanarak 110 bit uzunluğuna çıkartılır. Alıcıda çoğunluk seçimi yöntemi uygulanması amacıyla kodlanmış veri üç kopya halinde faydalı yük çerçevelerine yerleştirilerek AES şifreleme algoritması ile şifrelenir. Ses ve mesaj sonu çerçevelerine ASDO mekanizmasından gelen 28 bit uzunluğundaki veri şifresiz olarak yerleştirilir.

Alıcıda modemden alınan bitler Şekil 3.4'de gösterilen Üçlü MELPe alıcı protokolü blok şemasına uygun şekilde işlenerek çıkış sesi oluşturulur. Başlangıç sinyali standart protokoldeki gibi işlendikten sonra faydalı yük çerçeveleri işlenmeye başlanır. ASDO kontrolü bloğunda standart protokoldeki gibi faydalı yük çerçevelerindeki şifresiz ASDO verileri işlenir ve kayıp edilen ya da başlangıçta sağlanamayan kriptografik senkronizasyonu tekrar

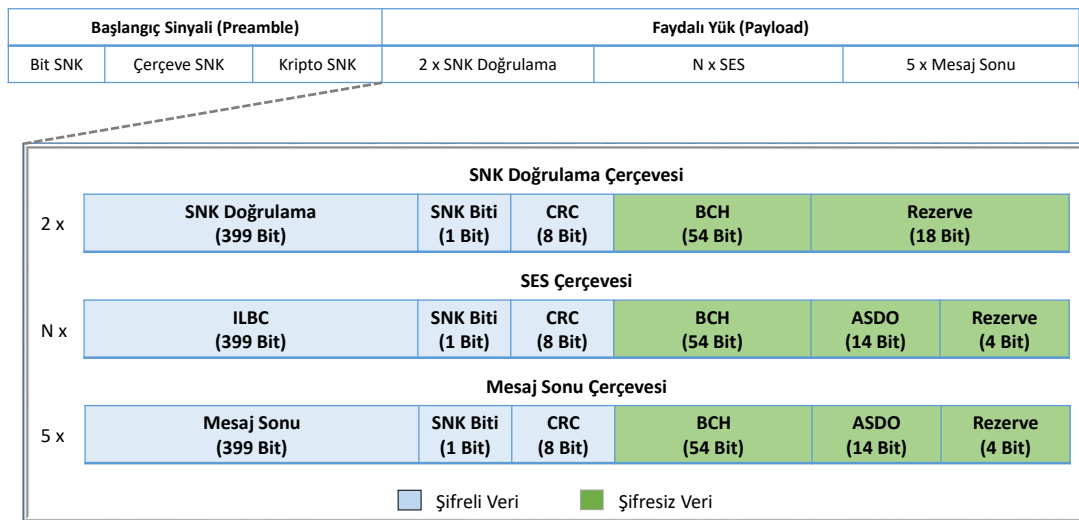


ŞEKİL 3.4: Geniş bant Üçlü MELPe alıcı protokolü blok şeması.

sağlanır. Şifre çözme bloğunda faydalı yük çerçevelerinin ilk 330 bitlik bölgesinin şifresi çözülür ve BCH kodçözücüsü bloğunda kodlanmış bölgelerdeki olası bit bozulmaları düzeltilir. Ardından çoğunluk seçimi bloğunda üç kopya halinde elde edilen 54 bit uzunluğundaki faydalı yük verileri üzerinde çoğunluk seçim yöntemi uygulanarak doğru olan 54 bitlik veriye ulaşılmaya çalışılır. Çoğunluk seçimi üç ayrı kopyanın aynı pozisyonlarındaki bitlerin incelenmesiyle sağlanır. Aynı pozisyonundaki üç bitin toplamı 1 den büyük ise bu bit 1 olarak kabul edilirken diğer durumlarda 0 olarak kabul edilir. Çoğunluk seçimi sonrası elde edilen 54 bit uzunluğundaki veri SNK doğrulama, ses veya mesaj sonu bilgisi olabilir. SNK doğrulama ve mesaj sonu bilgileri alıcı tarafındaki kontrol bloklarında olması gereken değerler ile kıyaslanarak tespit edilirken bu iki bilgi ile eşleşmeyen veriler ses verisi olarak kabul edilir ve MELPe 2400 kodçözücüsü ile işlenerek çıkış sesi oluşturulur.

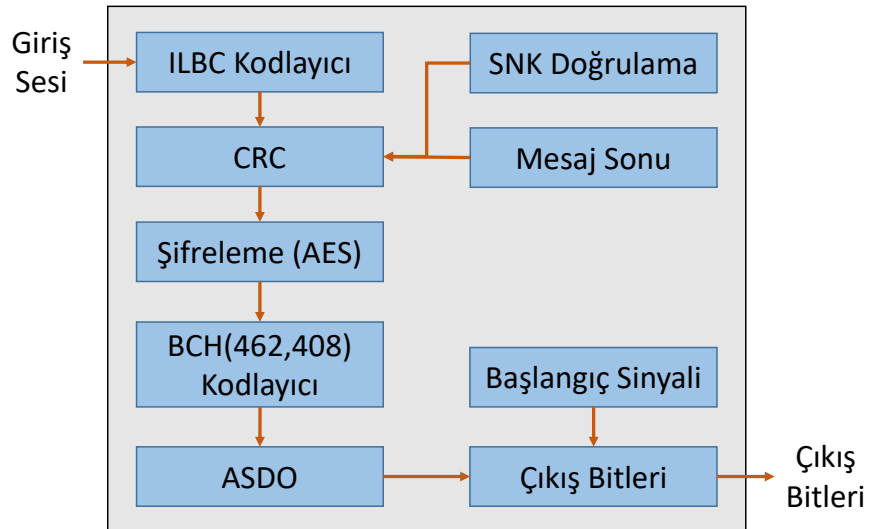
3.2.2 ILBC Yöntemi

Bu bölümde, standart haberleşme sisteminde kullanılan MELPe ses kodlayıcı-kodçözücüsü yerine seçilen ILBC ses kodlayıcı-kodçözücüsü ile geliştirilmiş alternatif güvenli ses haberleşme yönteminden bahsedilecektir. Başlangıç sinyali haberleşme sisteminde kullanılan ses kodlayıcısı-kodçözücüsü'nden bağımsız üretildiği için bu kısım standart ile aynı tutulmuştur. Faydalı yük bölümünde gönderilen çerçevelerin uzunluklarında ses kodlayıcılarının örnekleme sürelerindeki farklılıklardan dolayı değişiklik yapılırken mesaj iletim



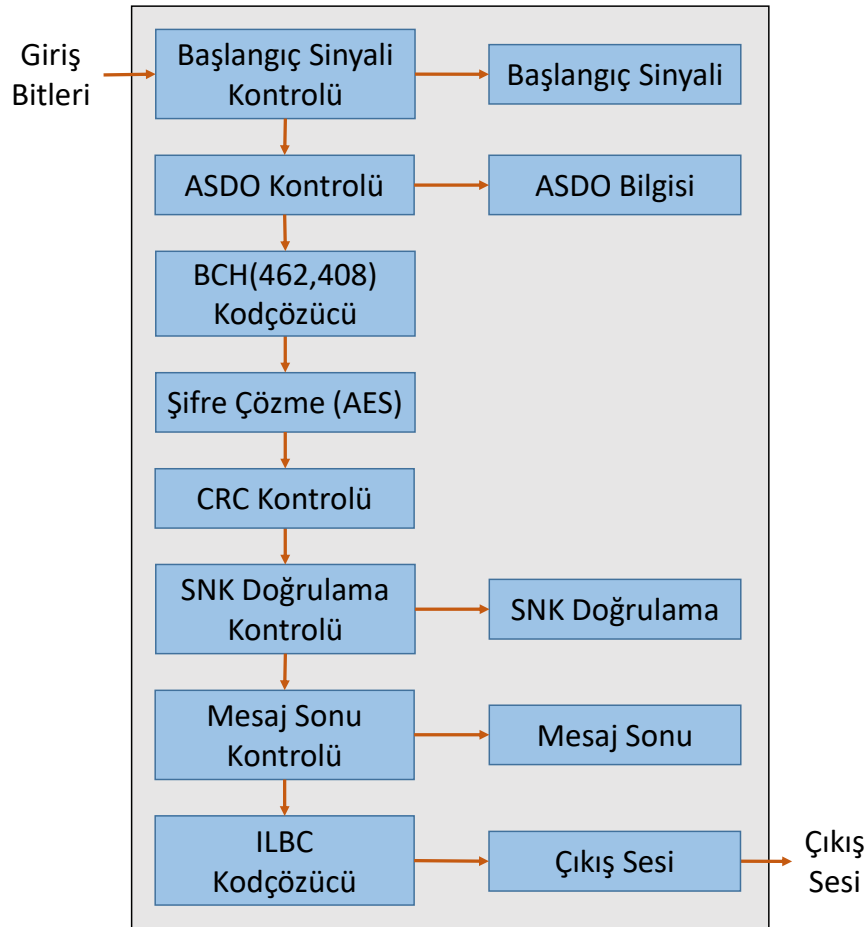
ŞEKİL 3.5: Geniş bant ILBC faydalı yük çerçeve yapısı.

sırası değiştirilmemiştir. Standart yöntemde ses kodlayıcısından 22.5 ms’de 174 bit kodlanmış ses verisi elde edilirken ILBC ses kodlayıcısından 30 ms’de 399 bit kodlanmış ses verisi elde edilmektedir. Kanal kapasitesinin 16 Kbps olduğu haberleşme sisteminde 30 ms’de 480 bit veri gönderilebilmektedir. Bu nedenle ILBC ses kodlayıcısı ile yapılan yeni tasarım Şekil 3.5’de görüldüğü gibi 480 bit çerçeve uzunluğuna sahiptir. Standart haberleşme yönteminde MELPe ses kodlayıcısı senkronizasyon biti üretirken ILBC ses kodlayıcısı böyle bir özelliğe sahip değildir. Bu nedenle her yeni çerçevedeki değeri bir önceki değerinin tersi olan SNK biti faydalı yük çerçevelerine Şekil 3.5’de görüldüğü gibi eklenmiştir. Bu bit sayesinde alıcı görüşme esnasında senkronizasyon sürekliliğini kontrol etmektedir. ILBC ses kodçözücüsü kaybedilen ses çerçevelerinden kaynaklı ses kalitesinde meydana gelecek bozulmaların etkisini azaltacak bir özelliğe sahiptir. Bu özelliğin kullanılabilmesi amacıyla faydalı yük çerçevelerindeki ilk 400 bit üzerinde hesaplanan 8 bit uzunluğunda CRC özelliği eklenmiştir. CRC kontrolü başarısız olan çerçeveler için alıcı ILBC ses kodçözücüsüne sadece kayıp çerçeve bilgisi vermektedir. Faydalı yük çerçevelerinin ilk 408 bitlik bölümü şifrelendikten sonra BCH(462,408,6) hata düzeltme kodlaması ile kodlanır. Bu kodlama işlemi sonrası elde edilen 54 bitlik BCH kodu Şekil 3.5’de görüldüğü gibi çerçeveye yerleştirilir. Bu kodlama sayesinde faydalı yük çerçevesinin ilk 462 bitinde meydana gelebilecek 6 bite bozulma alıcı tarafından düzeltilebilir. Standart haberleşme yöntemindeki ASDO mekanizması değiştirilmediği için ses ve mesaj sonu çerçevelerindeki ASDO bilgisi 14 bit uzunluğunda yer kaplamaktadır.



ŞEKİL 3.6: Geniş bant ILBC gönderici protokolü blok şeması.

ILBC ses kodlayıcı-kodçözücüsü ile geliştirilen bu alternatif haberleşme yönteminin gönderici ve alıcı bloğunda yapılan işlemler faydalı yük çerçevelerindeki farklılıklardan dolayı standart haberleşme yönteminden biraz farklıdır. Şekil 3.6'da gösterilen gönderici protokolü içerisinde yapılan işlemler 4 farklı adımda ifade edilebilir. Birinci adımda başlangıç sinyali üretimi standart gönderici protokolü ile aynı şekilde gerçekleştirilirken ikinci adımda Şekil 3.5'de gösterilen 2 adet SNK doğrulama çerçevesi üretimine başlanır. Bu işlem sırasında SNK doğrulama bilgisi ve SNK biti üzerinde yapılan CRC hesabı ile elde edilen 408 bitlik veri AES şifreleme algoritması ile şifrelenir. Elde edilen şifreli veri BCH(462,408,6) hata düzeltme kodlaması ile kodlanarak çıkış bitlerine eklenir. Üçüncü adımda görüşme süresince gönderilecek olan ILBC ses çerçevelerinin üretimi gerçekleştirilir. Giriş sesi ILBC ses kodlayıcısı ile sıkıştırılarak elde edilen 399 bit kodlanmış ses verisine SNK biti eklenerek CRC, şifreleme ve BCH kodlama işlemleri sırasıyla gerçekleştirilir. Bu adımda ASDO mekanizması devreye gireceği için üretilecek olan çerçeveye 14 bit uzunluğunda ASDO bilgisi eklenir. Dördüncü adımda görüşmeyi sonlandırmak



ŞEKİL 3.7: Geniş bant ILBC alıcı protokolü blok şeması.

amacıyla 5 adet mesaj sonu çerçevesi üretilerek çıkış bitlerine eklenir.

ILBC gönderici protokolü bloğunda üretilen çıkış bitleri modemlerden ve haberleşme kanalından geçtikten sonra Şekil 3.7’de gösterilen ILBC alıcı protokolü bloğunda işlenmektedir. Alıcı bloğunda yapılan işlemler göndericide olduğu gibi 4 adımda gerçekleştirilir. Birinci adımda alıcı başlangıç sinyali yakalayarak kriptografik senkronizasyonu sağlar. İkinci adımda SNK doğrulama çerçeveleri ile ilk adımda sağlanan kriptografik senkronizasyonu doğrulanır. Üçüncü adımda ses çerçeveleri işlenerek çıkış sesi elde edilirken ILBC kodçözücüsü iki farklı modda kullanılabilir. Birinci modda CRC kontrolünden geçemeyen ses çerçeveleri için ILBC kodçözücüsüne kayıp çerçeve bilgisi verilir. ILBC kodçözücüsü kaybedilen ses çerçevelerinden kaynaklı ses kalitesinde meydana gelecek bozulmaların etkisini azaltarak çıkış sesini üretir. İkinci modda ise CRC kontrolü sonucuna bakılmaksızın bütün ses çerçeveleri ILBC kodçözücüsü ile işlenerek çıkış sesi elde edilir. Dördüncü adımda şifresi çözülen çerçevelerde mesaj sonu bilgisi yakalanarak görüşme sonlandırılır.

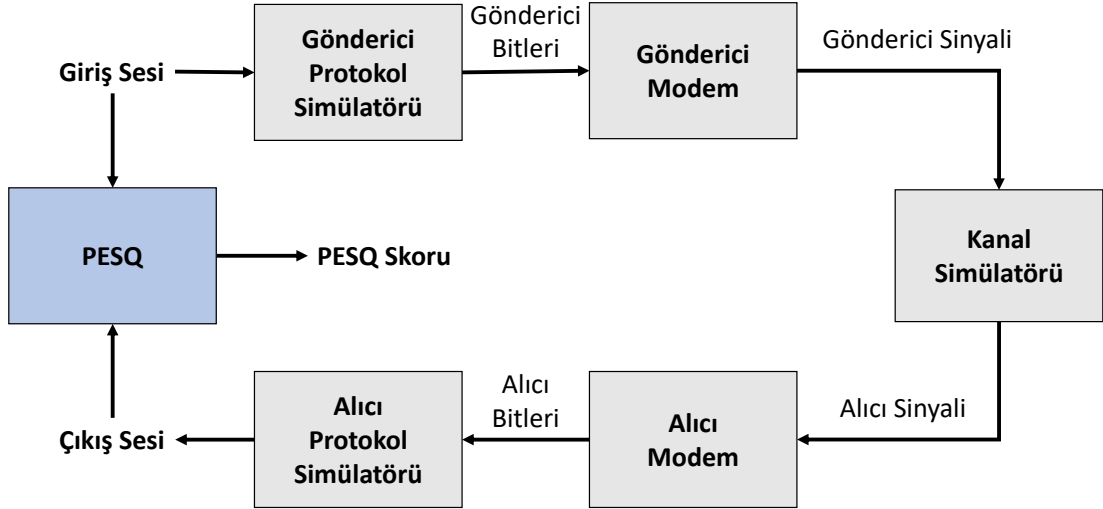
3.3 Deneysel Sonuçlar

Bu bölümde NATO protokolündeki standart yöntemlerin ve önerdiğimiz alternatif yöntemlerin farklı SNR seviyelerindeki ses kalitesi performanslarını analiz etmek amacıyla gerçekleştirilen benzetim mimarisi ve elde edilen deney sonuçları sunulmaktadır.

3.3.1 Benzetim Mimarisi

İncelemekte olduğumuz tek yönlü güvenli ses haberleşme protokolünün gerçekleştirildiği benzetim mimarisi Şekil 3.8’de görüldüğü gibi; gönderici/alıcı protokol modülleri, gönderici/alıcı modem modülleri, kanal simülatörü ve ses kalitesi analiz aracı olarak kullanılan PESQ modülünden oluşmaktadır. Gönderici ve alıcı protokol modülleri içerisinde bulunan ses kodlayıcıları ve PESQ ses kalitesi analiz aracı için hazır yazılımlar kullanılırken mimarideki diğer bileşenler simülasyon ortamında geliştirilmiştir.

Benzetim mimarisinde giriş sesi olarak 128 Kbyte büyüklüğünde, 8 KHz’de örneklenmiş 16 bit PCM ses dosyası kullanılmıştır [44]. Gönderici protokol modülü giriş sesini işleyerek gönderici bitlerini modem girişine iletir. Gönderici modem modülünde BPSK



ŞEKİL 3.8: Benzetim mimarisi akış diyagramı.

modülasyonu sonucu elde edilen sinyal kanal simülatörü ile bozucu etkilere maruz bırakıldıktan sonra alıcı sinyali elde edilir. Sinyaldeki bozulma seviyesi kanal koşullarına bağlıdır. Kanal simülatörü modülü AWGN kanal için farklı SNR seviyelerinde gönderilen sinyale bozucu etkiler oluşturur. Bozulmuş sinyal alıcı modem modülünde BPSK demodülasyonundan geçirilerek alıcı bitleri elde edilir. Alıcı protokol modülü bu bitleri protokole uygun şekilde işleyerek çıkış sesini oluşturur. Alıcıda elde edilen çıkış sesi ile giriş sesi PESQ ses kalitesi analiz aracı ile analiz edilerek PESQ skoru elde edilir.

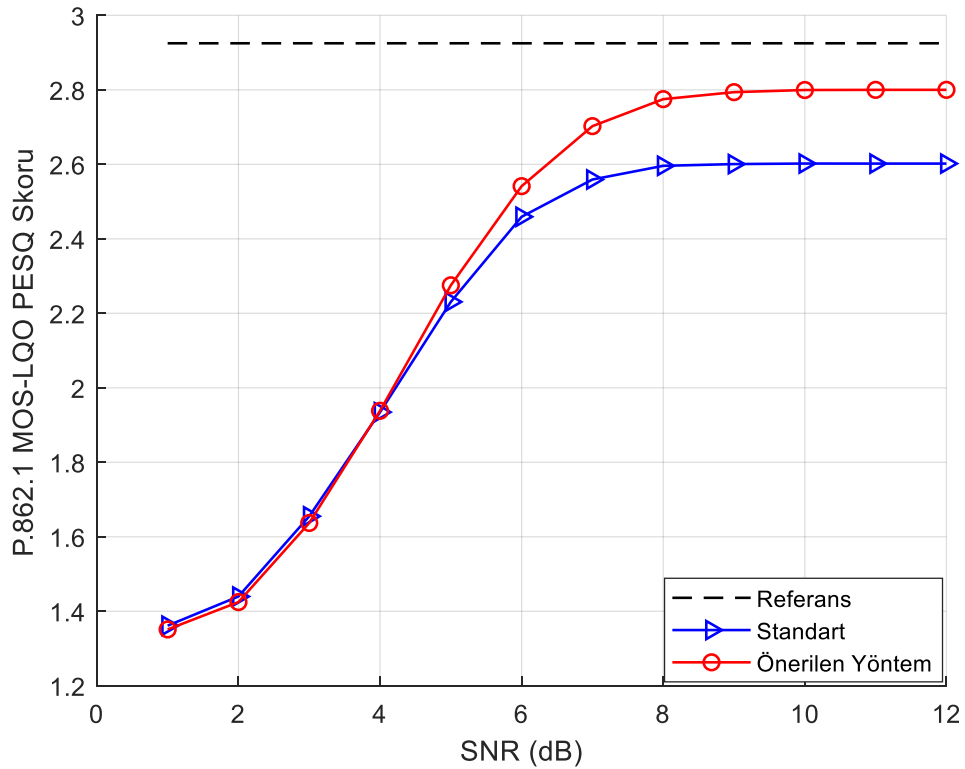
Protokolün dar bant modu için ayrıca alıcı protokol modülü içerisinde sesin doğru çözülmesi için ihtiyaç duyulan şifreleme bilgilerinin elde edilme oranları da raporlanmıştır. Bu parametreler kript o senkronizasyonunu doğru elde etme, ASDO bilgisini doğru elde etme ve kript o senkronizasyonunda kalma oranı olarak ifade edilmiştir. Alıcıda elde edilen kript o senkronizasyonu çerçeve sayısının göndericinin ilettiği çerçeve sayısına oranlanması ile kript o SNK elde etme oranı hesaplanır. Benzer şekilde ASDO bilgisi elde etme ve kript o senkronizasyonunda kalma (KSK) oranları da hesaplanır. Kript o senkronizasyonu veya ASDO bilgisini elde edebilen alıcı kript o senkronizasyonunu sağlayacağından, bu iki veri alıcının KSK oranını da belirler.

Protokolün geniş bant modu için ses kalitesi dışında raporlanan bir diğer sonuç ta farklı SNR seviyelerinde ses bitlerinde meydana gelen bit hata oranlarıdır. Gönderici protokol simülatörü içerisindeki ses kodlayıcısından elde edilen ses bitleri ile alıcı protokol simülatörü içerisindeki ses kodçözücüsüne verilen ses bitleri kıyaslanarak bit hata oranları hesaplanmıştır.

Gerçekleştirilen deneyler her farklı SNR seviyesi için 1000 kez tekrarlanarak elde edilen sonuçların ortalama değerleri sunulmuştur. Deneylerde kullandığımız AWGN kanalı belirli bir olasılık dağılımına göre bit hatalarının yerlerini belirlemektedir. Bu rastgelelik nedeniyle aynı SNR seviyesinde her zaman aynı PESQ skoru elde edilemediği gözlemlenmiştir. 128 Kbyte büyüklüğündeki ses dosyası ile 1000'den fazla deney yapılması sonuçlarda değişiklik göstermediği için her SNR seviyesi için 1000 deney yapmak yeterli görülmüştür.

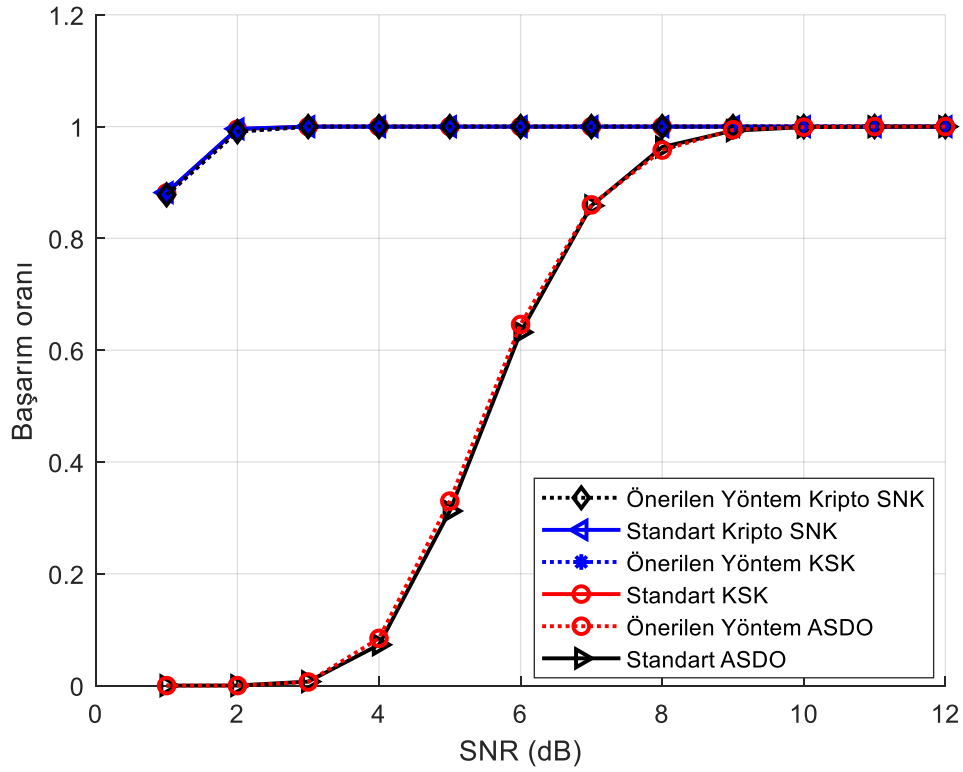
3.3.2 Dar Bant Deney Sonuçları

Şekil 3.9'da AWGN kanal modeli için farklı SNR seviyelerinde güvenli haberleşme sisteminin PESQ aracı ile elde edilen ses kalitesi ölçüm sonuçları gösterilmektedir. Analiz sonuçları önerilen yöntem ve referans yöntem için ses kalitesinin SNR seviyesinin yükselmesi ile iyileştğini gösterirken, önerilen yöntemden yüksek SNR seviyelerinde daha iyi performans sonuçları elde edilmiştir. Giriş sesinin MELPe 2400 kodlayıcısı ile sıkıştırılıp herhangi bir kayba uğratılmadan MELPe 2400 kodçözücüsü ile yeniden sentezlenmesi



ŞEKİL 3.9: Dar bant P.862.1 MOS-LQO PESQ sonuçları.

ile elde edilen ses analiz edilerek şekilde belirtilen referans PESQ skoru elde edilmiştir. Alıcıda elde edilen ses kalitesinin referans değere ulaşamamasının sebebi düşürülen ses çerçevesinin alıcıdaki rahatlatıcı ses çerçevesi ile aynı olmamasıdır. Tablo 2.3'e göre 1.63'ün altındaki PESQ skorlarında ses kalitesi kötü olduğu için 3 dB'den düşük SNR seviyesine sahip kanal koşullarında sağlıklı güvenli ses haberleşmesi gerçekleştirilemez. SNR seviyesinin 10 dB'nin üzerine çıkması ile her iki yöntem ulaşabilecekleri en yüksek ses kalitesini sağlarken önerilen yöntemin PESQ skorunu standarda göre %7.7'ye kadar iyileştirdiği görülmektedir.



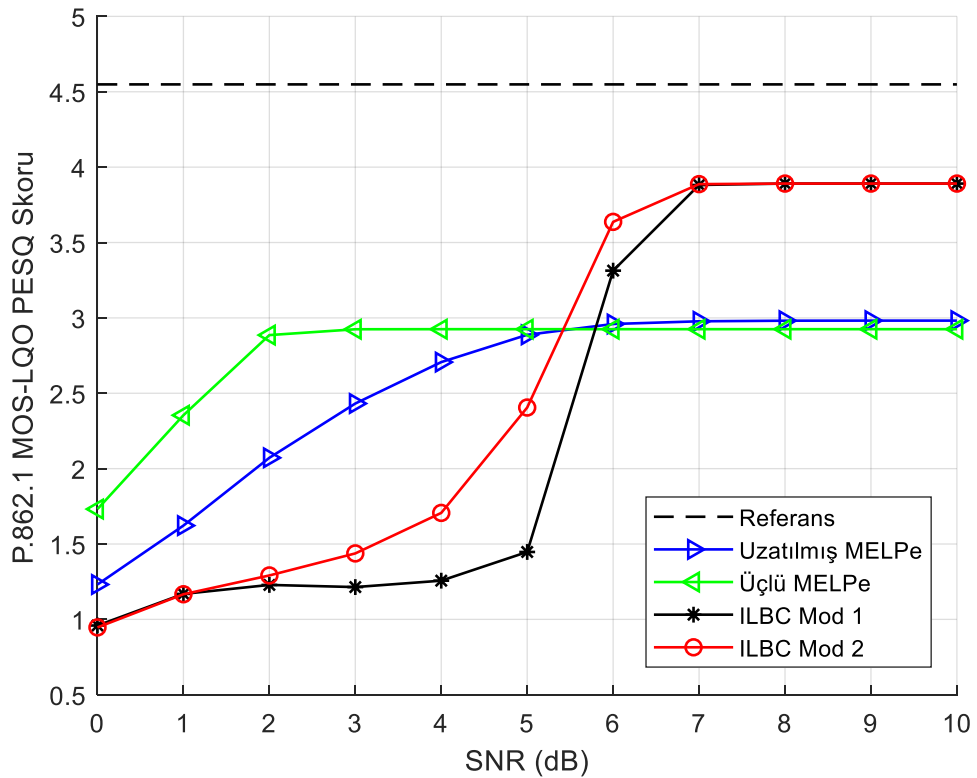
ŞEKİL 3.10: Dar bant şifre çözme bilgisi elde etme oranları.

Şekil 3.10'da farklı SNR seviyelerinde alıcı protokol modülünde elde edilen kripto senkronizasyonunda kalma (KSK) oranı, kripto SNK ve ASDO bilgisi elde etme başarımları gösterilmektedir. Kripto senkronizasyonunda kalabilmek için kripto SNK veya ASDO bilgilerinden herhangi birisinin elde edilmesi yeterli olduğundan KSK oranı bu iki orandan yüksek olan kripto SNK ile benzer çıkmaktadır. SNR seviyesi 3 dB üzerinde iken kripto SNK kayıpsız elde edilirken ASDO bilgisi 10 dB üzerindeki SNR seviyelerinde kayıpsız elde edilebilmektedir. Bunun nedeni, kripto SNK bilgisine göndericide hata düzeltimi (FEC) işlemi uygulanırken ASDO bilgisi için böyle bir işlemin gerçekleştirilmemesidir.

Önerilen yöntemin şifre çözme bilgisi elde etme performansı standart yöntem ile benzerlik göstermektedir.

3.3.3 Geniş Bant Deney Sonuçları

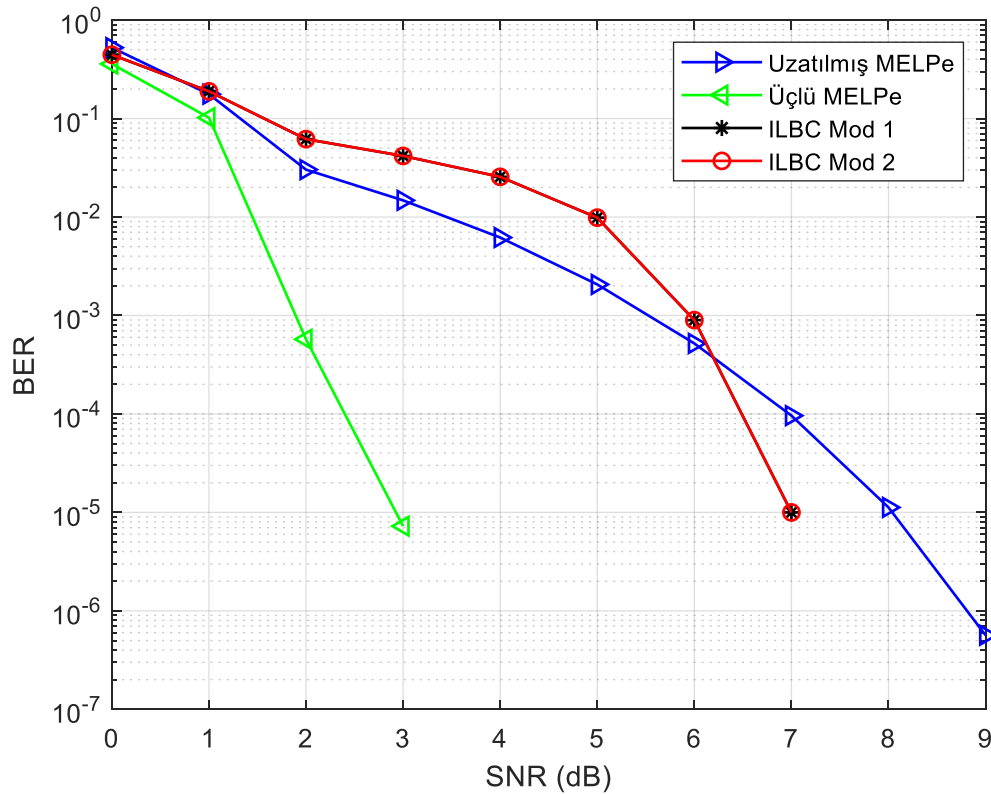
Uzatılmış MELPe, Üçlü MELPe ve ILBC yöntemleri ile farklı SNR seviyelerinde AWGN kanal modeli üzerinde yapılan deneyler sonucu elde edilen PESQ skorları Şekil 3.11’de gösterilmektedir. Referans PESQ skoru çıkış sesinin giriş sesine eşit olması durumunda elde edilecek skordur. Deneysel sonuçlar en yüksek performansın SNR seviyesi 5.5 dB üzerinde iken ILBC yönteminden 5.5 dB altında iken Üçlü MELPe yönteminden elde edildiğini göstermektedir. Düşük SNR seviyelerinde Üçlü MELPe yönteminin performansının daha iyi olmasının sebebi 16 Kbps’lık kanal kapasitesinin büyük kısmının ses kodlayıcısından elde edilen ses bitlerini korumak amacıyla kullanılmasıdır. Bu nedenle Üçlü MELPe yöntemine kanalda meydana gelebilecek bit bozulmalarına karşı ses bitlerini en fazla koruyan haberleşme yöntemi diyebiliriz. Her üç yöntem için SNR seviyesi yükseldikçe ulaşılabilecek maksimum performansa ulaşılır. Bit bozulmaları olmaksızın ILBC ses



ŞEKİL 3.11: Geniş bant P.862.1 MOS-LQO PESQ sonuçları.

kodlayıcısı MELPe ses kodlayıcısından daha iyi ses kalitesine sahip olduğu için yüksek SNR seviyelerinde en yüksek performans ILBC yönteminden elde edilmiştir.

Güvenli haberleşme yöntemlerinin temel amacı ses bitlerinin göndericiden alıcıya en az bit hata oranı ile iletilmesidir. Uzatılmış MELPe, Üçlü MELPe ve ILBC yöntemlerinde ses bitleri üzerindeki bit hata oranları Şekil 3.12’de gösterilmektedir. Ses bitlerinde meydana gelen bit hata oranları bu bitlerin haberleşme protokolünde ne kadar iyi korunduğu ile ilişkilidir. Bir ses çerçevesindeki ses bitlerinin uzunluğu ile bu bitleri korumak amacıyla eklenmiş hata düzeltme kodlarının uzunlukları kıyaslanarak ses bitleri üzerindeki koruma seviyesi anlaşılabilir. Haberleşme yöntemlerinin Şekil 2.12, Şekil 3.2 ve Şekil 3.5’de gösterilen faydalı yük çerçeve yapılarından ses bitlerini en fazla koruyan yöntemin Üçlü MELPe olduğu, en az koruyan yöntemin ise ILBC olduğu çıkarılabilir. Şekil 3.12’de gösterilen BER grafiği ses çerçevelerine bakılarak yapılan çıkarım ile doğru orantılıdır. Fakat 6.2 dB’den yüksek SNR seviyelerinde ILBC yönteminden elde edilen BER Uzatılmış MELPe’den elde edilen BER’den daha düşük seviyelere inmiştir. Bunun sebebi ILBC yönteminde kullanılan BCH(462,408,6) blok boyunun Uzatılmış MELPe yöntemindeki BCH(15,5,3) ve Hamming(16,11,1) blok boylarından daha uzun olmasıdır.



ŞEKİL 3.12: Geniş bant BER sonuçları.

Bölüm 4

Sonuç ve Tartışma

Bu çalışmada, telsiz sistemlerinde güvenli ses haberleşmesi için geliştirilmiş SCIP-214.6 protokolünün dar bant modu için yeni bir rahatlatıcı ses yöntemi önerilirken, geniş bant modu için iki farklı faydalı yük çerçevesi oluşturma yöntemi önerilmiştir. Önerdiğimiz yöntemler NATO protokolü ile birlikte benzetim ortamında gerçekleştirilerek ses kalitesi performansları farklı SNR seviyelerindeki PESQ skorları ölçülerek incelenmiştir. Dar bant modunda kriptosenkronizasyon sürekliliğinin sağlanması için kullanılan ASDO mekanizması ses kalitesinde kayba neden olur. Deney sonuçları, önerdiğimiz rahatlatıcı ses yönteminin daha yüksek PESQ skoru sağlayarak ses kalitesini iyileştirdiğini göstermektedir. Geniş bant modunda ise önerilen Üçlü MELPe ve ILBC yöntemlerinin ses kalitesini iyileştirdiği bölgeler kanal koşullarına göre değişiklik göstermektedir. Üçlü MELPe yöntemi 5.5 dB'den düşük SNR seviyelerinde standartta önerilen yöntemle göre her zaman daha iyi ses kalitesi performansı sağlarken iyileştirme oranı %43'e kadar çıkmaktadır. ILBC yöntemi ise standartta önerilen yöntemle göre 5.5 dB'den yüksek SNR seviyeleri için ses kalitesini %30'a kadar artırırken, 5.5 dB'den düşük SNR seviyeleri için %40'a kadar düşürmektedir. Sonuçlar kötü kanal koşullarında Üçlü MELPe yönteminin iyi kanal koşullarında ise ILBC yönteminin kullanılmasının daha uygun olacağını göstermektedir.

Bu çalışmanın devamında mevcut benzetim ortamı kullanılarak farklı SNR seviyelerinde SCIP-214.6 protokolünün güvenli veri haberleşme modlarının performans analizleri gerçekleştirilebilir. Ayrıca protokolün 2.4 Kbps veri iletim hızına sahip dar bant modu için MELPe ses kodlayıcısı 2400 bps yerine 1200 ve 600 bps hızlarında kullanılabilir. Bu sayede ses çerçevesi düşürülmeden ASDO özelliği sağlanırken kanalda kalan boş yerler

hata düzeltme kodlaması için kullanılabilir. Protokolün geniş bant modu için ise daha gelişmiş hata düzeltme kodlaması veya daha gelişmiş ses kodlayıcı yazılımları kullanılabilir. Yapılan çalışmanın gerçek zamanlı uygulaması geliştirilerek HF, VHF ve UHF telsiz sistemlerinde performans testleri yapılabilir.



Kaynakça

- [1] Stefan Paulsen and Tadeus Uhl. Quantifying the Suitability of Reference Signals for the PESQ Algorithm. In *2010 Third International Conference on Communication Theory, Reliability, and Quality of Service*, pages 110–115. IEEE, 2010.
- [2] *Secure Tactical Communication – Interoperability Specification (STaC-IS), Revision 1.1*. NATO, SCIP-214.6, 2020.
- [3] Thomas Moran, David Heide, and Swati Shah. An Overview of the Tactical Secure Voice Cryptographic Interoperability Specification. In *2010-MILCOM 2010 MILITARY COMMUNICATIONS CONFERENCE*, pages 213–218. IEEE, 2010.
- [4] Patrick Shahan, David A Heide, and Aaron E Cohen. Comparison of TSVCIS Voice at 8000 and 12000 BPS versus CVSD at 16000 BPS. In *MILCOM 2012-2012 IEEE Military Communications Conference*, pages 1–4. IEEE, 2012.
- [5] Bradley J Hamilton. SINGARS System Improvement Program (SIP) Specific Radio Improvements. In *Proceedings of the 1996 Tactical Communications Conference. Ensuring Joint Force Superiority in the Information Age*, pages 397–406. IEEE, 1996.
- [6] Anssi Ramo and Henri Toukomaa. On Comparing Speech Quality of Various Narrow and Wideband Speech Codecs. In *Proceedings of the Eighth International Symposium on Signal Processing and Its Applications, 2005.*, volume 2, pages 603–606. IEEE, 2005.
- [7] Søren Vang Andersen, W Bastiaan Kleijn, R Hagen, J Linden, MN Murthi, and J Skoglund. ILBC - A Linear Predictive Coder with Robustness to Packet Losses. In *Speech Coding, 2002, IEEE Workshop Proceedings.*, pages 23–25. IEEE, 2002.

- [8] S Andersen, A Duric, H Astrom, R Hagen, W Kleijn, and J Linden. RFC3951: Internet Low Bit Rate Codec (iLBC). *Network Working Group*, 2004.
- [9] Sergey N Kirillov and Alexander A Lisnichuk. Analysis of Narrow-Band Interference Effect on Cognitive Radio Systems Based on Synthesized Four-Position Radio Signals. In *2018 XIV International Scientific-Technical Conference on Actual Problems of Electronics Instrument Engineering (APEIE)*, pages 50–54. IEEE, 2018.
- [10] SCIP Signaling Plan, Revision 3.6 (SCIP-210). <http://www.iad.gov/SecurePhone/openDoc.cfm?akQb5p/JiNIei0GEuy9TBg==>. Accessed: 2020-05-22.
- [11] John M Alvermann, Michael T Kurdziel, and William N Furman. The Secure Communication Interoperability Protocol (SCIP) over an HF Radio Channel. In *MILCOM 2006-2006 IEEE Military Communications conference*, pages 1–4. IEEE, 2006.
- [12] John M Alvermann and Michael T Kurdziel. The Secure Communication Interoperability Protocol (SCIP) over a VHF/UHF Radio Channel. In *MILCOM 2008-2008 IEEE Military Communications Conference*, pages 1–6. IEEE, 2008.
- [13] Valeriu Ionescu, Ion Sima, Adrian-Viorel Diaconu, and Valentin Stan. Security Communications Interoperability Protocol Implementation. In *2012 9th International Conference on Communications (COMM)*, pages 327–330. IEEE, 2012.
- [14] US DoD. MIL-STD-3005. *Department of Defense Telecommunications Systems Standard*, 1999.
- [15] Edward J Daniel and Keith A Teague. Performance of FNBDT and Low Rate Voice (MELP) over Packet Networks. In *Conference Record of Thirty-Fifth Asilomar Conference on Signals, Systems and Computers (Cat. No. 01CH37256)*, volume 2, pages 1568–1572. IEEE, 2001.
- [16] Amit Kumar Panda, Shahbaz Sarik, and Abhishek Awasthi. FPGA Implementation of Encoder for (15, k) Binary BCH Code Using VHDL and Performance Comparison for Multiple Error Correction Control. In *2012 International Conference on Communication Systems and Network Technologies*, pages 780–784. IEEE, 2012.
- [17] Tongsheng Zhang and Qun Ding. Design of (15, 11) Hamming Code Encoding and Decoding System Based on FPGA. In *2011 First International Conference*

- on Instrumentation, Measurement, Computer, Communication and Control*, pages 704–707. IEEE, 2011.
- [18] ITUT Rec. P. 862.1: Mapping Function for Transforming P. 862 Raw Result Scores to MOS-LQO. *International Telecommunication Union, Geneva*, 24, 2003.
- [19] Frederick H Raab, Robert Caverly, Richard Campbell, Murat Eron, James B Hecht, Arturo Mediano, Daniel P Myer, and John LB Walker. HF, VHF, and UHF Systems and Technology. *IEEE Transactions on Microwave Theory and Techniques*, 50(3): 888–899, 2002.
- [20] Kristina V Tatarinova and Vineamin E Zakharov. Search on the Normal Wave Amplitude Change for HF-Waves Propagating in the Ionosphere. In *2019 Russian Open Conference on Radio Wave Propagation (RWP)*, volume 1, pages 504–506. IEEE, 2019.
- [21] Stuart G Farquhar, Andrew J Baynham, and AE Talbot. BLOS Communications Technologies for the Deep Battle—a UK Perspective. In *MILCOM 2000 Proceedings. 21st Century Military Communications. Architectures and Technologies for Information Superiority (Cat. No. 00CH37155)*, volume 1, pages 40–44. IEEE, 2000.
- [22] István Z Kovács, Patrick CF Eggers, and Kim Olesen. Radio Channel Characterisation for Forest Environments in the VHF and UHF Frequency Bands. In *Gateway to 21st Century Communications Village. VTC 1999-Fall. IEEE VTS 50th Vehicular Technology Conference (Cat. No. 99CH36324)*, volume 3, pages 1387–1391. IEEE, 1999.
- [23] R Decesari. Developmental VHF/UHF Radio Communications Techniques for Submersible Systems. In *OCEANS’80*, pages 434–439. IEEE, 1980.
- [24] Emanuel Costa, Marco Aurélio Nunes da Silva, and Markus Liniger. Prediction of Diffraction Effects due to Irregular Terrain on Radio Wave Propagation in the VHF and UHF Bands. In *2011 XXXth URSI General Assembly and Scientific Symposium*, pages 1–4. IEEE, 2011.
- [25] Naoto Kogo and Tetsuomi Ikeda. Antenna Performance of Push-to-Talk Transceiver in VHF and UHF Bands Considering Impedance Matching. In *2013 International Symposium on Electromagnetic Theory*, pages 358–361. IEEE, 2013.

- [26] Tiantian Li and Zhigang Zhang. Analysis and Design of HF Radio Noise Measurement Antennas considering Directivity and Polarization. In *2019 IEEE 9th International Conference on Electronics Information and Emergency Communication (ICEIEC)*, pages 483–486. IEEE, 2019.
- [27] Andriy Zalizovski, Yuri Yampolski, Alexander Koloskov, Sergey Kashcheyev, and Bogdan Gavrylyk. Response of Parameters of HF Signals at the Long Radio Paths on Solar Activity. In *2019 URSI Asia-Pacific Radio Science Conference (AP-RASC)*, pages 1–1. IEEE, 2019.
- [28] Dobro Blazhevski, Adrijan Bozhinovski, Biljana Stojchevska, and Veno Pachovski. Modes of Operation of the AES Algorithm. 2013.
- [29] Syed Jahanzeb Hussain Pirzada, Abid Murtaza, Tongge Xu, and Liu Jianwei. Initialization Vector Generation for AES-CTR Algorithm to Increase Cipher-text Randomness. In *2019 2nd International Conference on Information Systems and Computer Aided Education (ICISCAE)*, pages 138–142. IEEE, 2019.
- [30] William Wesley Peterson and Daniel T Brown. Cyclic Codes for Error Detection. *Proceedings of the IRE*, 49(1):228–235, 1961.
- [31] Noor Najeeb Qaqos. Optimized FPGA Implementation of the CRC Using Parallel Pipelining Architecture. In *2019 International Conference on Advanced Science and Engineering (ICOASE)*, pages 46–51. IEEE, 2019.
- [32] Jonathan R Engdahl and Dukki Chung. Fast Parallel CRC Implementation in Software. In *2014 14th International Conference on Control, Automation and Systems (ICCAS 2014)*, pages 546–550. IEEE, 2014.
- [33] NATO Interoperable Narrow Band Voice Coder. STANAG 4591 C3 (Edition 1)-The 600 bit/s, 1200 bit/s, 2400 bit/s. *NSA/1025 C*, 3, 2008.
- [34] Alan V McCree and Thomas P Barnwell. A Mixed Excitation LPC Vocoder Model for Low Bit Rate Speech Coding. *IEEE Transactions on Speech and audio Processing*, 3(4):242–250, 1995.
- [35] US DoD. MELP Analog-to-Digital Conversion of Voice by 2400 bit/second Mixed-Excitation Linear Prediction [J]. *Department of Defense Telecommunications System Standard*.

- [36] MELPe - Enhanced Mixed Excitation Linear Predictive. <https://melpe.org/>. Accessed: 2020-05-22.
- [37] MD Street. Future NATO Narrow Band Voice Coder (Stanag 4591) Selection Process (Phase Two). Technical report, NC3A Technical Note 912, 2002.
- [38] Suzi Seroja Sarnin, Nani Fadzlina Nairn, and Wan Nor Syafizan W Muhamad. Performance Evaluation of Phase Shift Keying Modulation Technique Using BCH Code, Cyclic Code and Hamming Code Through AWGN Channel Model in Communication System. In *The 3rd International Conference on Information Sciences and Interaction Sciences*, pages 60–65. IEEE, 2010.
- [39] Alexis Hocquenghem. Codes Correcteurs D’erreurs. *Chiffres*, 2(2):147–56, 1959.
- [40] Raj Chandra Bose and Dwijendra K Ray-Chaudhuri. On a Class of Error Correcting Binary Group Codes. *Information and control*, 3(1):68–79, 1960.
- [41] ITU-T Recommendation. Perceptual Evaluation of Speech Quality (PESQ): An Objective Method for End-to-End Speech Quality Assessment of Narrow-Band Telephone Networks and Speech Codecs. *Rec. ITU-T P. 862*, 2001.
- [42] Antony W Rix, John G Beerends, Michael P Hollier, and Andries P Hekstra. Perceptual Evaluation of Speech Quality (PESQ) - A New Method for Speech Quality Assessment of Telephone Networks and Codecs. In *2001 IEEE International Conference on Acoustics, Speech, and Signal Processing. Proceedings (Cat. No. 01CH37221)*, volume 2, pages 749–752. IEEE, 2001.
- [43] Tingxiao Yang. The Algorithms of Speech Recognition: programming and simulating in MATLAB, 2012.
- [44] EH Rothauser. IEEE Recommended Practice for Speech Quality Measurements. *IEEE Trans. on Audio and Electroacoustics*, 17:225–246, 1969.