

EKOĞÜNDEM

BELİRSİZLİKTEN
ÇIKIŞ YOLU:
MİKRO İHRACAT!SİBER GÜVENLİK
YATIRIMLARI TRİLYON
DOLARA KOŞUYOR!COVID-19 'LİDERLİĞİ'
YENİDEN TANIMLADI!ENDÜSTRİ 4.0 ÜRETİM
TESİSLERİNİ DİJİTALLEŞTİRİYOR!STRESTE İSVİÇRE,
MUTLULUKTA FRANSA LİDERİ!HAZİNE VE MALİYE BAKANI BERAT ALBAYRAK
KUR YERİNE ÜRETİME,
SANAYİYE ODAKLANMALIYIZ!RFT ARAŞTIRMA A.Ş. YÖNETİM KURULU BAŞKANI
PROF. DR. SİDDİK YARMANKİŞİYE ÖZEL,
TAM GÜVENİLİR
HABERLEŞME SİSTEMİ:
SYMPES!

SYMPES'in sesin karakteristik özelliğinden faydalanarak sesi bilgi ve enerji fonksiyonlarına ayırarak modelleyen yepyeni bir ses kodlama tekniği olduğuna dikkat çeken RFT Araştırma A.Ş. Yönetim Kurulu Başkanı Prof. Dr. Siddik Yarman, SYMPES'in tamamen milli ve kişiye özel, tam güvenilir bir haberleşme sistemi sunduğunu vurguladı.



RFT ARAŞTIRMA A.Ş. YÖNETİM KURULU BAŞKANI PROF. DR. SİDDİK YARMAN

KİŞİYE ÖZEL, TAM GÜVENİLİR HABERLEŞME SİSTEMİ: SYMPES!

{ SYMPES'in sesin karakteristik özelliğinden faydalanarak sesi bilgi ve enerji fonksiyonlarına ayırarak modelleyen yepyeni bir ses kodlama tekniği olduğuna dikkat çeken RFT Araştırma A.Ş. Yönetim Kurulu Başkanı Prof. Dr. Sıddık Yarman, SYMPES'in tamamen milli ve kişiye özel, tam güvenilir bir haberleşme sistemi sunduğunu vurguladı.

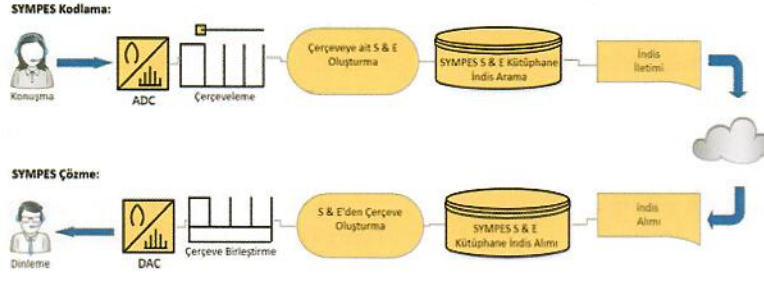
Prof. Dr. Sıddık Yarman, 1974 yılında İstanbul Teknik Üniversitesi, Elektrik-Elektronik Fakültesi, Elektronik Mühendisliği bölümünden mezun oldu. Yüksek Lisansını 1978 yılında Stevens Institute of Technology'de Elektrik Mühendisliği ve Matematik dallarında tamamladı. Doktorasını ise Cornell Üniversitesi Elektrik Mühendisliği, Matematik ve Bilgisayar Bilimleri dallarında 1982 yılında tamamlayan Sıddık Yarman, 1984 yılında Yardımcı Doçent Doktor ünvanı ile Anadolu Üniversitesi, Mühendislik fakültesinde akademik

kariyerini sürdürdü. 1988-1991 yılları arasında STFA-Şirketler Grubu bünyesinde STFA-SAVRONİK (Savunma Elektroniği) firmasının teknik kuruculuğunu üstlendi. Amerika, Avrupa ve Japonya'da uzun süreler Profesör ünvanı ile dersler veren ve araştırmalar yapan Yarman 2004-2018 yılları arasında İstanbul Üniversitesi Mühendislik Fakültesi, Elektrik Elektronik Bölümünün Başkanlığını yürüttü. Ulusal ve uluslararası birçok bilimsel ödüle, 350'den fazla bilimsel makaleye ve haberleşme teknolojileri üzerine projelere ve kitaplara

imza atmış Prof. Dr. Sıddık Yarman ile Teknopark İstanbul kuluçka merkezinde Haziran 2014'te kuruluşunu gerçekleştirdiği RFT Araştırma A.Ş.'nin, bilgi güvenliğinin tekrar tartışıldığı, özellikle de ülkemizin yabancı istihbarat örgütlerince uzun yıllar boyunca dinlendiğine yönelik haberlerin basına yansıdığı bugünlerde, güvenli haberleşme amacına yönelik geliştirdiği ses kodlama sistemi olan SYMPES'i konuştuk.

Hocam, öncelikle SYMPES'in temelinde yatan bilimsel çalışmalarınızı ve bu tekniği geliştirmenizin temel motivasyonunu öğrenmek istiyoruz...

Türkiye'de 1990'lı yıllarda Başbakanlık'ta güvenlik işlerinden sorumlu baş müşavirlik görevinde bulundum. Turgut Özal, Süleyman Demirel, Tansu Çiler, Necmettin Erbakan, Mesut Yılmaz ve Bülent Ecevit'in başbakanlıkları döneminde hizmet verdim. Sayın Recep Tayyip Erdoğan'ın döneminde de çok ciddi katkılarımız oldu; hem akademisyen olarak hem iş adamı olarak birçok çalışmada yer aldım. Başbakanlık Güvenlik İşlerinden Sorumlu Teknik Baş Müşaviri iken görevimiz yeni gelişmekte olan cep telefonları ile haberleşmeyi güvenli hale getirmektir. Uzun yıllar TÜBİTAK'ta ciddi bir ekiple birlikte çalıştık. Ülkemiz için ilk defa Milli Kripto Haberleşme altyapısını TÜBİTAK Elektronik Ünitesi başlatmıştı. Daha sonra yine devletimizin isteği üzerine rahmetli Turgut Özal'ın Başbakanlığı döneminde Anadolu Üniversitesi'nde göreve başlamıştım. Daha sonra oradaki çalışmalarımızı genişlettik. Bugün işletmiş olduğumuz çalışmalarla Savronik adlı bir şirket kurduk. Biz teknik felsefesini; Sezai Türkeş ve Fevzi Akkaya ise sermayesini karşıladı ve Savronik kurulmuş oldu. Bizim o zamanlar tabi iş tecrübemiz yoktu. TÜBİTAK'tan arkadaşım kripto yazılımları geliştiren Prof. Dr. Fuat İnce, Cornell Üniversitesi'nden arkadaşım Kemal Kumcu ve kardeşim Faruk Yarman ile birlikte çok sağlam mühendislik ekibi oluşturduk. Savronik



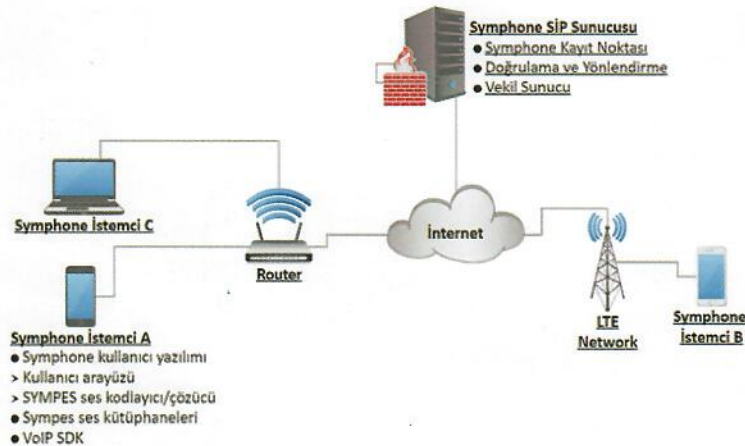
içerisinde ilk milli özel kriptoları da yaptık. Yine aynı dönemde rahmetli İstanbul Üniversitesi Mühendislik Fakültesi Dekanı Profesör Ergül Tütüncüoğlu hocamız ve Boğaziçi

Üniversitesi'nden rahmetli Prof. Dr. Ömer Cerit ile oluşturduğumuz bir ekiple cep telefonlarına takılan çok özel kriptolu çipler geliştirdik, testlerini yaptık. Bunları hayata geçirdikten sonra acaba konuşmalarımızı kriptosuz olarak güvenli hale getirebilir miyiz? sorusu gündeme geldi. Benim çocukluğumda mahalleden yakın arkadaşım, hepinizin çok iyi tanıdığı rahmetli gazeteci Savaş Ay gırtlak kanserine yakalandığında bana "Benim konuşma problemime çözüm bul. Ben yine eskisi gibi kendi sesimle gümbür gümbür program yapmak istiyorum" dedi. Ben o sıralarda İstanbul Üniversitesi'nde hiç kimsenin erişemeyeceği kriptosuz güvenli haberleşme altyapısını geliştirmek üzerinde araştırma yapıyordum. Savaş'ın eski orijinal kayıtlarından sesini inceledim. Bir matematik ses modeli kurdum. Kurmuş olduğum modele SYMPES adını verdim. Bu modelin oluşturulmasında birçok doktora öğrencimin de muazzam emekleri, katkıları var. Hepsini sağ olsunlar, var olsunlar. SYMPES'i geliştirmek için çalışmalarımızı yürüttüğümüz dönemde maalesef Savaş Ay'ı kaybettik. O zaman gerçek zamanlı telefon konuşmalarında sesi doğru ve hızlı bir şekilde iletecek modeli oluşturmaya odaklandım ve 2014 yılında Teknopark İstanbul'da RFT Araştırma Anonim Şirketini kurdum.

Peki, RFT, SYMPES'i nasıl geliştirdi?

SYMPES'i gerçek zamanlı olarak çalıştırma kararını aldıktan sonra TÜBİTAK'ta ilk milli kripto yazılımları geliştiren arkadaşlarımın da içinde olduğu bir

mühendislik ekibi oluşturduk. Bir Amerika gezim sonrasında keşfettiğim yeni yaklaşımla SYMPES'i gerçek zamanlı tabana oturtmayı başardık. Çözümü önce PC'lerde çalıştırdık. Buna ilişkin bir patent aldık. Ortak bir TÜBİTAK projesi kapsamında STM Firmasıyla



PC'lerde çalışan bir versiyonun uygulamasını yaptık. Daha sonra ürünün ticarileşmesi çalışmalarına ağırlık verip, Türkiye'de güvenli haberleşme ihtiyacı duyan kurumların hizmetine sunma çalışmalarına başladık. Türkiye'de de bunu Genel Kurmay Başkanlığı'na anlattık. Arkasından Savunma Sanayi Müsteşarımız değerli hocamız Prof. Dr. İsmail Demir'e anlattık.

Peki, biraz da SYMPES'in teknik özelliklerini konuşalım... SYMPES Ses Kodlama Modeli nedir? Ne tür özelliklere sahiptir?

SYMPES, sesin karakteristik özelliğinden faydalananak sesi bilgi ve enerji fonksiyonlarına ayırarak modelleyen yepyeni bir ses kodlama tekniğidir. Tamamen milli, yerli ve özgün üründür. Rekabetçi ses kalitesi, kendiliğinden güvenli ses iletişimi, düşük gecikme (latency) süresi, esnek teknik özellikler ve kapalı kullanıcı grubu uygulamaları sunar.

Modellemenin temelinde IP tabanlı muhabere sistemlerinde standart kodlayıcılardan (codec) farklı olarak, ses verisinin kendisi gönderilmeden, sese ait indis değerlerinin haberleşme ortamında iletilmesi yer almaktadır. Bu sayede, sistemin doğal yapısı gereği

güvenli haberleşme alt yapısı sunulur. Kendi başına bir kriptoloji algoritması olmamakla birlikte SYMPES, kendiliğinden bir kriptolojik altyapıya sahiptir.

SYMPES haberleşmesinde hattaki veriler gerçek ses verilerine doğrudan bağlı değildir. İletişim hattına sadece indisler verilir. İndislerin sesleri temsil etmesi 65536 ! değişik biçimde olabilir. ($65536 ! > 10^{1000}$)

İlk aşamada bir kereye mahsus olarak e (envelope: bilgi) ve s (signature: enerji) veri tabanlarını oluşturmak gerekmektedir. Bu işlem için dilimizde kullanılan sesleri tanımlayan hece ve kelimelerden çok sayıda örnek alınır. Bu örnekler, SYMPES veri tabanı oluşturma algoritması kullanılarak e ve s veri tabanlarına dönüştürülür ve kaydedilir. Daha sonra en yakın komşu algoritmaları kullanılarak tekrarlamalar azaltılır ve veri tabanları sıkıştırılmış olur.

SYMPES'in geleneksel kriptolu haberleşmeden farkı nedir?

Yazılı kriptolojik haberleşmede, karakterler kullanılır. Karakter sayısı 128 (7 bit) veya 256 (8 bit) olsa da bunlardan çoğu pratikte kullanılmaz. Sadece 32 harf



(büyük ve küçük) ve bazı semboller kullanılır. Kripto algoritmaları 128 (256) karakteri çeşitli algoritmalar çerçevesinde karıştırır, evirir, çevirir ve şifrelemiş olur. Kriptolojide dildeki yapı çok önemlidir. Çünkü dillerde büyük oranda "redundancy", yani karakterler arasında kuvvetli ilişkiler vardır. Harflerin dağılımı, tekli, ikili, üçlü vb. iyi bilinir. (Örneğin Türkçede en çok "e" harfi sonra "a" harfi kullanılır. İngilizcede "q" harfinden sonra daima "u" gelir. En çok rastlanılan üçlü Türkçede "bir", İngilizcede "the" kelimeleridir. Bu özelliği cep telefonlarımızda bilgisayarda yazı yazarken görürüz. Yazacağımız kelime bir iki harf sonra tahmin edilir.)

Kriptoanaliz yapan taraf (kriptoanalist) şifreli mesajı kırmak için dillerin bu özelliğini kullanarak, bu 100 kadar karakteri ve onun kombinasyonlarını arayıp çekip çıkarmaya, bulmaya çalışır. Algoritma bilgisi, özellikle dil bilgisi ve frekans analizi burada esas olur.

SYMPES algoritmasında ise durum çok farklıdır. Karakter sayısı 65536'dır (100 kadar değil). Bu 65536 vektör, doğal dillerdeki gibi bir yapıya sahip değildir. Kıırma girişimlerinde doğal dillerdeki gibi frekans analizleri yapılamaz. Ama gene de hatta iletilen vektörlerin, araya giren bir karşıt tarafından izlendiğinde rassal (random) görünmesi gerekir ki frekans analizi benzeri yöntemler işe yaramasın. SYMPES çalışmalarımızda bu amaçla iletişimde histogramlar incelenmiş ve "uniform" görünen bir dağılım için rassallaştırma ("randomize" etme) sağlanmıştır.

SYMPES'in kullanım alanları hakkında bilgi verebilir misiniz?

SYMPES mobil telefonlarda, masaüstü ve dizüstü bilgisayarlarda, tabletlerde, telsizlerde ve VoIP haberleşmesinde kullanılabilir. İsteğe göre uyarılma ve düzenleme yapılabilir.

Güncel uygulamalarınız var mı?

Symphone, SYMPES Ses Kodlayıcı tabanlı bir internet üzerinden ses aktarımı (VoIP) uygulamasıdır. Kullanıcılara güvenilir haberleşme yanında yüksek ses kalitesi ve bant genişliğine göre özgün çözüm sunar. Şu anda Android uygulaması hazırlanmış olup geliştirilmektedir. iOS uygulamasında da çalışmalar tamamlanmak üzeredir. Öte yandan SYMPES, L2 bandında çalışan Savronik telsizlerine entegre edilmiştir. Aslında bu uygulama her türlü akıllı elektronik donanım üzerinde çalıştırılabilir.

Son olarak SYMPES'in ticari geleceğini de konuşalım... Neler söylemek istersiniz?

Bu projenin geçmişinde 30 yıllık bilimsel çalışma birikimi ve keşifler var. Günümüzün teknolojik



olanaklarıyla dinlenemeyecek, kriptosu çözilemeyecek haberleşme sistemi ve donanımı yoktur. Ancak SYMPES temel özellikleri itibarıyla dinlenemez, tam güvenli ve bir anlamda kişiye özel bir haberleşme teknolojisidir. İçinde bulunduğumuz dünya şartlarını dikkate aldığımızda önceliğimiz bu teknolojiyi Cumhurbaşkanlığımızın önderliğinde devletimizin hizmetine sunmaktır. Bununla beraber farklı kullanıcı ihtiyaçlarına özel olarak uyarlanabilen özellikteki SYMPES Ses Kodlama Algoritması bir çok dost ülkenin, ulusal ve uluslararası ticari kuruluşlar ve özel kullanıcı guruplarının kullanımına da sunulabilir.