



Savunma ve Güvenlik



İçindekiler

Savunma ve Güvenlik · 6 buluş

ODTÜ-87	Doğrulanabilir Grup Kurulumuna Sahip Hesap Verilebilir Altgrup Çoklu-İmza Şeması	3
ODTÜ-89	Doppler Kayması Temelli Dağıtık Drone Tespit Sistemi	4
ODTÜ-133	İnsansız Hava Araçlarında Yüksek Gürültülü Çok-Kanallı Akustik Veriden Silah Atış Tespiti	5
ODTÜ-145	Sığ Sularda Organik Olmayan Cisim Geçişinin Müonlar ile Tespiti Sistemi	6
ODTÜ-146	Deniz Görev Grubu Hava Savunma Planlama Algoritması	7
ODTÜ-95	Kuantum-Dirençli Kafes-Tabanlı Hesap Verilebilir Altgrup Çoklu-İmza Şeması	8

Doğrulanabilir Grup Kurulumuna Sahip Hesap Verilebilir Altgrup Çoklu-İmza Şeması

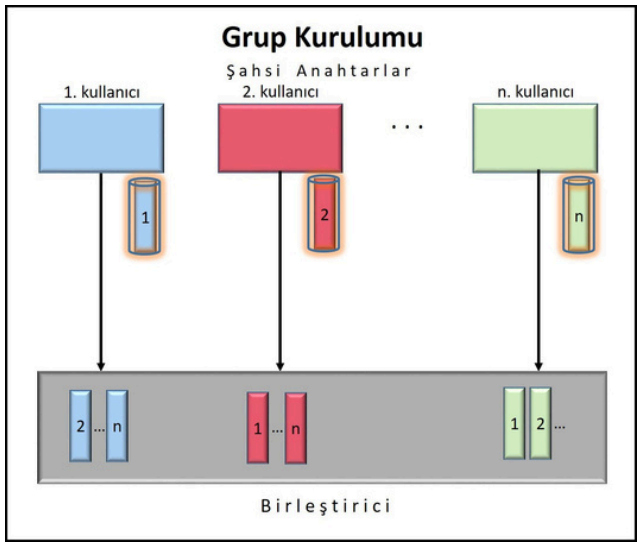
tto.metu.edu.tr
tto@metu.edu.tr

H2C3: Hızlı & Hesap Verilebilir Çoklu İmza-3

Buluş, kendine özgü grup kurulumu sayesinde bilinen eşleme-tabanlı hesap verilebilir imza şemaları içerisinde en hızlı imzalama ve doğrulama ile en küçük imza boyutuna sahiptir.

Avantajlar

Hızlı imzalama: 1 adet eliptik eğri skaler çarpma işlemi gerektirir.
Hızlı doğrulama: 2 adet eliptik eğri ikili lineer eşleme ve n adet eliptik eğri skaler çarpma işlemi gerektirir.
Hesap verilebilirlik: Atılan imzalar cebirsel olarak bağlayıcıdır, imza inkâr edilemez.
Sabit imza boyutu: İmzacı sayısından bağımsız, yalnız 1 adet eliptik eğri grup elemanından oluşur.
Esnek imzacı sayısı: İmzacı sayısı 1'den n'ye kadar olabilir.
(*) n: potansiyel imzacı sayısı



Üretilen imza şahsi açık anahtarlar ve imzacı bilgileri ile doğrulanabilir.

Bir organizasyon adına imza yetkilisi olabilecek potansiyel imzacılar, şahsi anahtarlarıyla müştereken icra ettikleri bir grup kurulumunu müteakiben, elde ettikleri üyelik anahtarlarıyla söz konusu organizasyon adına, hızlı, güvenli ve hesap verilebilir imza atabilmektedirler. Üretilen bu imza, imzacı bilgileri verilen herhangi bir doğrulayıcı tarafından hızlı bir şekilde doğrulanabilmektedir.
Organizasyondaki her potansiyel imza yetkilisi diğerlerinin açık kimliğini şahsi anahtarıyla teker teker imzalayarak birleştiriciye gönderir. Kendi açık kimliği üzerinde oluşturduğu imzayı ise kaydeder. Daha sonra bir mesajı imzalamak istediğinde, şahsi anahtarıyla imzalar ve kaydettiği kimlik imzasını da ekleyerek birleştiriciye gönderir. Birleştirici kendisine gelen imzaları birleştirir. Daha sonra imzacılara ait daha önceden kaydettiği kimlik imzalarını da birleştirerek oluşturduğu imzaya ekler.

Doppler Kayması Temelli Dağıtık Drone Tespit Sistemi

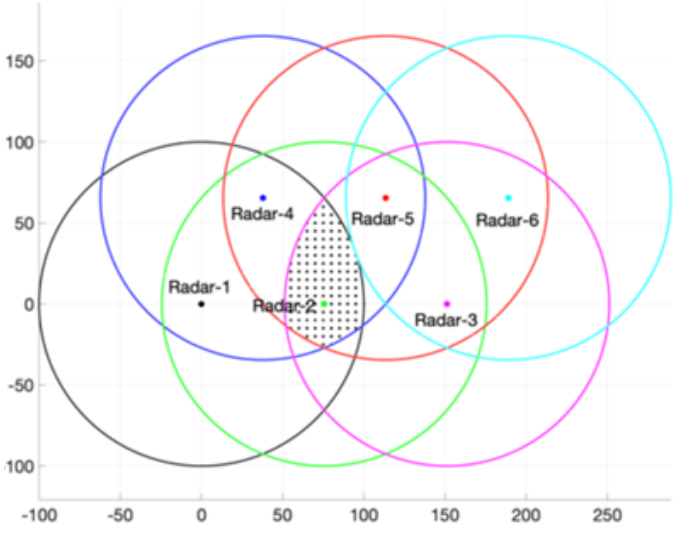
tto.metu.edu.tr
tto@metu.edu.tr

Dağıtık Drone Tespit Sistemi

Yoğun hedef ortamlarında da çalışabilen drone tespit sistemi teknolojisidir. Bu teknoloji drone pervanelerinin hareketinden kaynaklanan Micro-Doppler işaretlerin tespitine ve diğer hedeflerin filtrelenmesi prensibine dayanmaktadır.

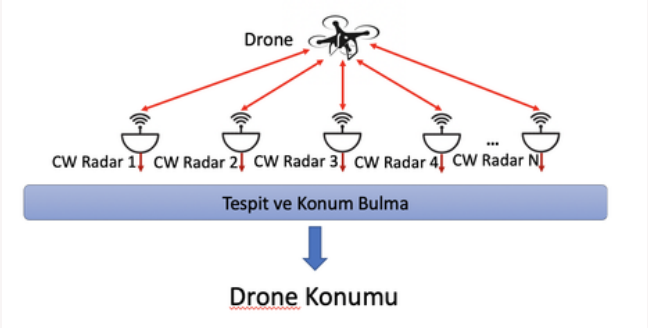
Avantajlar

Maliyet etkin: Kısıtlı radar kapsama alanlarında maliyet etkin
Ölçeklenebilir: Sistem mimarisi, gözetleme yapılacak bölgeye göre ölçeklenebilir
Kademeli performans etkilenmesi: Dağıtık yapıda çok sayıdaki radar kullanımı ile yüksek güvenilirlik
Kolay yerleşim: Büyük bir radar yerine küçük çok sayıdaki radar ile sistem yerleşim kolaylığı
Yoğun ortamda çalışabilme: Hedef yoğun ortamda doğrudan drone işaretlerine özel filtre kullanımı ile tespit kolaylığı



Özellikle şehir ortamı gibi radar kapsama alanı kısıtlı, hedef yoğun ortamlarda radar temelli drone tespiti.

Drone tespiti için günümüzde çeşitli yaklaşımlar bulunmaktadır. Radar ile drone tespiti de bu çözümlerden birisidir. Radar kapsama alanı kısıtlı, hedef yoğun ortamlarda klasik radarların drone tespiti için kullanımı maliyet ve performans etkin çözümler sunamayabilir. Buluş, dağıtık, düşük güçlü ve maliyetli radar çözümü tanımlamaktadır. Bu teknik drone'ların dağıtık yapıdaki radar verilerinin birleştirilerek tespitini ve konumlandırmasını sağlamaktadır. Dağıtık yapıdaki radar yaklaşımı ile kısıtlı radar kapsama alanları olan bölgelerde uygun radar yerleşimi ile kör bölgelerin oluşması engellenebilmektedir.



ODTÜ-89

İnsansız Hava Araçlarında Yüksek Gürültülü Çok-Kanallı Akustik Veriden Silah Atış Tespiti

tto.metu.edu.tr
tto@metu.edu.tr

Drone üzerinde gürültüye dirençli silah atış tespiti

Avantajlar

Mikrofon dizisi yakınındaki gürültü yerine, uzak silah atış seslerini ön plana çıkarabilmesi

Ön bilgi olmadan farklı silah çeşitlerine ve durağan olmayan drone gürültülerine adaptif olması

Hem zaman hem frekans açısından yüksek çözünürlük, farklı sinyallere odaklanabilmesi

Farklı mikrofon dizisi büyüklüklerini ve geometrilerini destekleyebilme

Gerçek zamanlı işleme için düşük hesaplama karmaşıklığı

Dizideki bazı mikrofonlarda arıza olsa bile çalışabilme

Atış konumlandırma için farklı namlu sesi ve şok dalgalarının değişken drone gürültüsüne rağmen adaptif tespiti ve iyileştirilmesi

Çoklu sensör verisinin hemfikirliğini kullanarak, yüksek gürültü altında olay / silah atışı tespitini adaptif şekilde yapabilmesi

Yeni ortaya atılan dizi korelasyon haritası sinyallerin öz-korelasyonuna dayanmaktadır. Adaptif kısım, bilinen CWT analizinin ölçeklerinin özel bir belirlenme şeklidir.

Sığ Sularda Organik Olmayan Cisim Geçişinin Müonlar İle Tespiti Sistemi

tto.metu.edu.tr
tto@metu.edu.tr

Emins

Düşük hatalı alarm ile muadillerinde olmayan şekilde, organik cisimleri görmemektedir.

Avantajlar

Düşük hata payı ile tespit.

Organik olan cisimlerin (örnek yunus sürüsü) EMİNS tarafından görülmeyecek olması.

Pasif bir sistem olması.

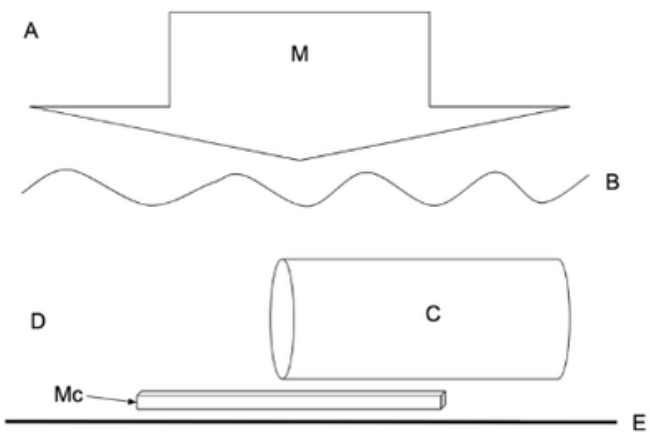
Cismin teşhisi için gerekebilecek, cismin uzunluğu, çapı ve hızı gibi parametrelerin ölçülebilmesi.

70 metre deniz derinliğine kadar sistemin kurulabilmesi.

Boğazlar gibi sığ sularda gizli denizaltı geçişleri için uyarı sistemi olarak kullanılabilir.

Buluş konusu, sığ sularda, sualtında veya su yüzeyinde duran veya hareket eden organik olmayan cisimlerin (örneğin denizaltı) geçişinin ve/veya varlığının tespiti için sualtında tabana veya bir platforma yerleştirilen müon akısı ölçüm cihazı ve anlık müon akısında cismin varlığı ile gerçekleşen azalma sonucunda canlı alarm verecek sistem ile ilgilidir.

Suyun içine girebilen yüksek enerjili kozmik kaynaklı müonların, çeliğin yüksek durdurma gücü dolayısıyla, sayılarının azalmasının tespiti mümkündür.



A. Atmosfer

B. Deniz, okyanus, boğaz, nehir veya doğal veya yapay göl yüzeyi

C. Organik olmayan cisim, örneğin denizaltı

D. Deniz, okyanus, boğaz, nehir veya doğal veya yapay göl

E. Deniz, okyanus, boğaz, nehir veya doğal veya yapay göl tabanı

M. Atmosferik müon akısı

Mc. Müon akısı ölçüm cihazı

Deniz Görev Grubu Hava Savunma Planlama Algoritması

tto.metu.edu.tr
tto@metu.edu.tr

NADP Algoritması

Buluş gerçek zamanlı kullanabilecek şekilde kısa sürede ve etkili çözüm üretebilen bir algoritmadır.

Avantajlar

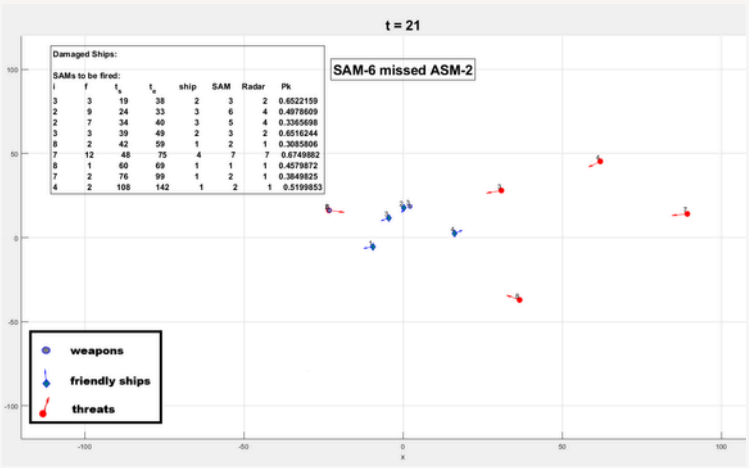
Gerçek zamanlı ve etkili (optimuma yakın) çözümler elde edilebilmesi

Platformların hayatta kalma olasılıklarının artırılması

Savunma kaynaklarının verimli kullanılması

Çözüm yaklaşımının ölçeklenebilir olması

Algoritmanın kolaylıkla oluşturulabilir olması



Deniz görev grubu hava savunma planlaması kapsamında angajman çizelgeleme ve gemi rotalama kararlarını sağlama

Buluş, Deniz Hava Savunma Planlama (NADP) Algoritması, deniz görev grubu platformlarını hava tehditlerinden etkin bir şekilde korumak amacıyla savaş yönetim sistemlerinde kullanılmak üzere geliştirilmiş bir çözüm yaklaşımını içermektedir.

NADP algoritması, deniz hava savunma planlamasını optimize eden ve otomatikleştiren bir algoritmadır. Algoritma, gemilerin manevra kararlarını, tehditlere karşı silah ve sensörlerin atanmasını ve zamanlamasını içeren savunma kaynaklarının çok kısa sürede planlanmasını kapsar.

Kuantum-Dirençli Kafes-Tabanlı Hesap Verilebilir Altgrup Çoklu-İmza Şeması

tto.metu.edu.tr
tto@metu.edu.tr

Kuantum-Dirençli ASM Şeması (vMS2)

Literatürdeki ilk kuantum-dirençli Hesap Verilebilir Altgrup Çoklu-İmza (ASM) şemasıdır; kafes tabanlı yapısıyla kuantum bilgisayarlara karşı güvenlik sağlar.

Avantajlar

Kuantum-dirençlilik: Mevcut ASM şemalarının sunmadığı kuantum bilgisayar güvenliği sağlar.
Hesap verebilirlik: İmzayı atan her alt grup üyesinin kimliği doğrulanabilir.
Esnek imzacı sayısı: Sabit eşik gerektirmez; herhangi bir alt grup birlikte imza atabilir.
Geniş uygulama alanı: Finans, kimlik doğrulama, e-oylama, blokzincir ve askeri sistemlerde kullanılabilir.
Standart uyumlu temel: NIST PQC finalisti Dilithium'un genişlemesi olan MS2 üzerine kuruludur.

Dijital imzayı kuantum-dirençli platforma taşıyan ilk ASM çözümü.

Mevcut klasik ASM şemaları (DLP/DHP tabanlı) kuantum bilgisayarlara karşı savunmasızdır. vMS2, MS2 çoklu-imza şemasını Doğrulanabilir Sır Paylaşımı (VSS) ve Rejection Sampling protokolüyle genişletir.
Grup kurulum safhasında her kullanıcı gizli anahtarını temel alan rastgele bir polinom seçer; üyelik anahtarları VSS aracılığıyla paylaşılır. İmza üretiminde üyelik anahtarı kullanılarak hesap verebilirlik sağlanır. Güvenlik, Module-LWE ve Module-SIS varsayımlarına dayanır.