Araştırma:

Araştırma Alanları:

- **Ağ güvenliği**
- **Kimlik doğrulama mekanizmaları**
- **Resmi diller: CSP, FDR**
- **Doğrulama, doğrulama ve analiz**
- **Kablosuz algılayıcı ağları**
- **Kimlik doğrulama protokollerinin performans değerlendirmesi ve performansı.**
- **Ağ güvenliği üzerine görüntü işleme tekniklerinin uygulanması**

ARAŞTIRMA İLGİ VE FAALİYETLERİ:

Kimlik doğrulama, herhangi bir kuruluşun BT hizmetlerine gayrı meşru erişim riskini azaltmak için kullanılan temel işlevdir. Kerberos, kimlik doğrulama ve erişim denetimi mekanizmaları için yaygın olarak kullanılan bir kimlik doğrulama protokolüdür.

Kablosuz ağlarda Kerberos kimlik doğrulama protokolünü kullanan güvenlik stratejilerinin geliştirilmesi, Kerberos Anahtar Değişimi protokolü, gecikmeli gecikmeli Kerberos, gecikmeli gecikmeli ve gecikmeli şifre çözme özellikli Kerberos, gecikmeli gecikmeli Kerberos, gecikmeli şifre çözme ve şifre şifreleme özellikleri, temel araştırma ilgi alanlarım arasındadır.

Yalancı güvenli koşullar altında sıklıkla anahtar yenileme ve güvenli anahtar değişimine izin vermek için kimlik doğrulama sunucusunun geçici olarak harici erişim için kapatılması gibi bir dizi araştırma çalışması yayınlanmıştır.

Kimlik doğrulama özelliklerinin yanı sıra Kerberos kimlik doğrulama protokolünün analizi ve doğrulaması için genel bir yaklaşım araştırılmış ve incelenmiştir. Güçlü şifreleme teknikleriyle bir araya getirilen mevcut kimlik doğrulama mekanizmaları ayrıntılı olarak incelenir ve analiz edilir. IEEE 802.1x standardı, IEEE 802.11 kablosuz iletişim ağları da araştırmamın ana bölümlerinden biri olarak kabul edilmektedir.

Kerberos için üç yönlü kimlik doğrulama mekanizmasını geliştirmek için bir kimlik doğrulama protokolü geliştirildi. Sahte güvenli durumlardaki anahtarları dinamik olarak yenilemek, bağlantı / sunucu erişimi için geçici bir kesintiyi gerektirir. Kimlik doğrulama için geliştirilmiş güvenlik sağlamak için bir protokolü açıklayıp analiz ettikten sonra, sistemin performansını düşürmesi açısından maliyeti değerlendirmek için analitik bir yöntem kullanılır.

Şifreleme protokollerini doğrulamak için kullanılan resmi yöntemler, kimlik doğrulama protokollerinin spesifikasyonlarını karşılamasına yardımcı olmak için oluşturulmuştur. Ardışık Süreçleri Haberleşme (CSP) ve Arıza Ayrıştırma Iyileştirme (FDR) denetimi gibi model denetleme teknikleri, çoğu diğer çağdaşlardan daha hızlı protokollerdeki kusurları etkin ve verimli bir şekilde ortaya koymak için kabul görür. Aslında, model denetimi, bir protokol modelinin bileşenleri tarafından erişilebilen tüm devletlerin detaylı bir araştırmasını içerir. Kimlik doğrulama protokollerini açıklayan modellerde, işlemler olarak görülen bileşenler, saldırgan (saldırgan) ve anahtarlar, işaretler, biletler ve sertifikalar gibi kimlik doğrulama parametrelerini içeren ilkelerdir. Araştırmamda, CSP açıklamaları üretmek için otomatik bir nesil araç CASPER kullanılır. Önerilen protokol modelleri, kimlik doğrulama işlemlerinde güvenilen üçüncü kişilere güvenirken, davetsiz misafirlerin yetenekleri olası indüksiyon ve kesintilere dayanmaktadır.

Araştırmamda, saldırganın gelişmiş özelliklere sahip soyut bir tanımını gerçekleştirmek için model denetiminde iki yöntemi birleştirmeyi deniyor. İlgilenilen bir hedef protokol, Kerberos kimlik doğrulama protokolüdür.

Güvenlik mekanizmalarının gücünü arttırma süreci genellikle performans eşiklerini etkiler. Bu gerçeği göz önüne alarak araştırma, etki seviyesini belirlemek için spektral genişleme olarak bilinen ve sonuçta protokol değişikliklerinin performans üzerinde olmasını sağlayacak bir analitik yöntemi benimser. Spektral genişleme devlet araştırmalarına dayanmaktadır. Bu, model patlamanın devlet patlama problemine tabi tutulduğunu ima eder. Değiştirilen protokollerin performans özellikleri mevcut protokollere göre incelenir.

Ağ güvenliği amaçları için güçlü şifreleme teknikleriyle birleştirilmiş kimlik doğrulama mekanizmaları kullanılır; Bununla birlikte, yeterli zaman göz önüne alındığında, iyi donanımlı davetsiz misafirler sistem güvenliğini tehlikeye atmakta başarılıdır. Kimlik doğrulama protokolleri, eleştirel olarak analiz edildiğinde genellikle başarısız olur. Protokol arızalarını analiz etmek için resmi yaklaşımlar ortaya çıkmıştır. Bu çalışmada, özellikle iletişim kalıplarının tanımlanması için tasarlanmış soyut bir dil olan İletişimi Arayan Süreçler (CSP) kullanılmaktadır. Sıralamadaki işlevler, doğrulama ve analiz için de kullanılır; bu bilgiler, bazı kritik bilgilerin saldırgan tarafından bulunmadığını

doğrulamaya yardımcı olur. Bunu sağlamak için, her kritik bilgiye bir değer atayarak veya derecelendirerek, ağ içinde oluşturulabilecek tüm kritik bilgilerin belirli bir karakterize edici özelliği olduğunu gösterir. Bu araştırma, sahte güvenlik durumlarında anahtarlar dinamik olarak yenilenirken şifre çözme işlemini zamanlı kimlik doğrulama ile geciktirmeyi birleştiren kimlik doğrulama protokolüne sıralama işlevleri yaklaşımı sunmaktadır.

Geliştirilen tüm modeller için bircok yayın sunulmaktadır.

IEEE 802.11 standardına dayanan kablosuz yerel alan ağları (WLAN'lar), mevcut yerel ağ yapılandırmalarında yaygın şekilde kullanılmaktadır. IEEE 802.11, ağın kapasitesini artıracak çok katmanlı olmayan kanallar sunar. WLAN'ların bozukluklara yatkın olduğuna dair güçlü kanıtlar vardır. Hizmet kalitesini artırmak (QoS) ve WLAN'ların performansını gerçekçi olarak değerlendirmek için sistemlerin kullanılabilirliği göz önüne alınmalıdır. Bu çalışmada, analitik modelleme yaklaşımı kullanarak bir çok kanallı WLAN'ın performans değerlendirmesini inceliyoruz. Mevcut çalışmaların aksine, kritik işlev birimi tarafından tüm kanalların kullanılamamasına neden olan sistemin başarısızlığı düşünülmektedir. Global arızalar olarak yeni bir terim ortaya atıldı. Sistem parametreleri ve minimum negatif olmayan çözüm R'nin yinelemeli bir yöntemle hesaplandığı matris geometrik yöntemi kullanılarak incelenen modellerin çözülmesi mümkündür. Bununla birlikte, spektral genişletme yöntemi, özdeğerler ve özvektörler kullanılarak R'yi çözmek için yinelemeli hesaplamalardan kaçınıldığında bilinen bir alternatiftir. Tam spektral genişleme yöntemi, ortalama kuyruk uzunluğu ve bloke olasılığı gibi performansı ölçmek için kullanılır. Eşanlı denklemlerin çözümünde iteratif iyileştirmeler kullanılır.

Çoğu kablosuz iletişim ve mobil bilgi işlem sisteminin haftada 7 gün, günde 24 saat çalışması bekleniyor. Bununla birlikte, kablosuz iletişim sistemleri başarısızlıkla sonuçlanır. Performans modellemesi ve kablosuz ve mobil sistemlerin değerlendirilmesi son araştırmalar için ilgi çekicidir. Özellikle, gelecek nesil kablosuz ve mobil sistemlerin karmaşıklığı nedeniyle, modelleme ve performans değerlendirmesi, hizmet kalitesine (QoS) ve performans özelliklerine göre mimariyi iyileştirmek için gereklidir. Bu araştırma, kablosuz ortamlarda kablosuz hücresel ağlar için analitik modelleme yaklaşımları kullanan bir performans değerlendirme çerçevesi sunmaktadır. Önerilen modellerde kullanılabilirlik ve hareketlilik sorunları da göz önüne alınmaktadır. Bilinen yaklaşık Markov ödül modeli çözümü ve kesin Spektral genişleme çözüm yaklaşımları düşünüldü. Bloke olasılığı ve ortalama kuyruk uzunluğu gibi önerilen modellerin performans ölçütleri sunulmuştur.

Bu araştırma, sahte güvenli koşullar altında anahtarları dinamik olarak yenileyen Kerberos sunucularının performans değerlendirmesinin modellemesi için geri yayılım sinir ağları kullanan bir ön çerçeve sunmaktadır. Önerilen güvenlik yaklaşımı, performans düşüşüne yol açan bağlantı / sunucu erişimi için geçici kesintiyi içeriyor. Sistemin performans düşüşü açısından maliyeti değerlendirmek için analitik bir yöntem kullanılır. Sunulan model, sistemi tam performans değerlendirmesi için değerlendiriyor. Yenileme sürelerinin etkilerini, zaman arasındaki etkiyi analiz etmek için sayısal sonuçlar sağlanmıştır. Sunucunun yenilenmesi ve arızalarına ek olarak, yapay sinir ağları problem çözme için oldukça farklı bir yaklaşım önermekte ve altıncı nesil bilgi işlem olarak da bilinmektedir. Bu çalışmada iki faz önerilmiştir. İlk aşamada, görüntü ön işleme teknikleri ayrıntılı olarak. İkinci aşamada, performans yayılımı sinir ağları kullanan akıllı bir görüntü işleme sistemi uygulanabilirlik modellemesinin saptanması için uygulanmaktadır.

Geliştirilen tüm modeller için bircok yayın sunulmaktadır.