TASARSIZ AĞLAR İÇİN BİR GÜVENLİK SİMÜLATÖRÜ

Tuncay YİĞİT*
Sadettin DEMİR**
*Süleyman Demirel Üniversitesi, Mühendislik Mimarlık Fakültesi Bilgisayar Mühendisliği Bölümü
** Süleyman Demirel Üniversitesi, Enformatik Bölümü
tuncay@mmf.sdu.edu.tr, sadettin@sdu.edu.tr

ABSTRACT

In this paper, we examine the include intrusion detection for mobile computing environment. Wireless networks and mobile computing applications has changed the landscape of network security. Firstly, it is known what kind of attack and defence for security of wireless networks. We have developed a simulator for intrusion detection systems (IDS) in the wireless networks and mobile computing application. The simulator has flexible structure and graphical interface. As a result of the study a visual simuator has been obtained that can easily be adapted to the real time application.

Key words: Wireless network, Ad-Hoc network, security,

1. GİRİŞ

Kablosuz ağlar kullanıcıların bilgiye ve servislere konumlarından bağımsız olarak elektronik ortamda erişmelerini sağlayan bir teknolojidir. Kablosuz ağlar temel olarak iki sınıfa ayrılırlar: altyapılı (Infrastructure) ağlar ve tasarsız (Ad-Hoc) ağlar. Altyapılı ağlarda hareketli istasyonlar sabit baz istasyonları ya da erişim noktalarıyla kapsama alanları içerisinde iletişim kurarlar. Hareketli istasyon hareket ederken baz istasyonunun kapsama alanından çıkarsa yeni bir baz istasyonuna bağlanarak iletişime onun üzerinden devam eder. Tasarsız ağlarda ise belli bir altyapı ya da merkezi yönetim söz konusu değildir. Tasarsız ağlar erişim noktası (access point) kullanmadan en az iki kablosuz istasyon tarafından oluşturulur. Tüm istasyonlar (düğümler) hem birbirleriyle iletişim kurarlar hem de paketleri yönlendirirler. Tasarsız ağlar askeri, polis, arama kurtarma, konferans salonu, kampüs, üniversite ve şehir ağlarında kullanılabilirler [1].

Tasarsız ağların çok adımlı ve değişken topolojiye sahip olması, kablosuz ağ ortamından kaynaklanan olumsuzluklar ve düğümlerin hareketli olması çok sayıda problemi ortaya çıkarmıştır. Güvenlik, özellikle güvenliğe duyarlı uygulamalarda tasarsız ağlar için önemli bir konudur[2-5]. Tasarsız ağların altyapısında, merkezi bir denetiminin olmaması gibi karakteristik özellikleri güvenlik politikalarının gerçekleştirilmesinde kısıt olarak karşımıza çıkar. Rasgele ve ani asıllanan kullanıcılar, dolayısıyla dinamik olarak değişen ağ topolojisi güvenlik çözümlerinin de dinamik olmasını gerektirir. Saldırıya açık telsiz ortamda çoklu iletişim ve son derece kısıtlı özkaynaklar ile daha da zorlaşan güvenlik konusu çözülmesi gereken ve hala üzerinde çalışılmakta olan bir sorundur [6].

Bu bildiride, tasarsız ağların güvenliği için geliştirilen simülatör üzerinde durulacaktır ve tartışılmaya çalışılacaktır. Hazırlanan simülatör esnek ve kullanıcı etkileşimli bir yapıya sahiptir ve ağ üzerindeki düğümlerin trafiği izlenebilmektedir. Hazırlanan simülatör ile kablosuz ağlarda güvenlik nedeniyle ağ trafik gözlemlenebilmektedir ve öngörülmeyen ve tanımsız trafik akışı kolayca izlenebilmektedir.

2. TASARSIZ AĞLARDA GÜVENLİK HEDEFLERİ

Tasarsız ağların çok adımlı ve değişken topolojiye sahip olması nedeniyle özellikle güvenliğe duyarlı uygulamalarda için önemli bir konudur. Bu konuda ulaşılması beklenen nitelikler aşağıda verilmiştir [3].

Ulaşılabilme Ağ hizmetlerinde, hizmeti veya servisi kesintiye uğratmaya amaçlayan (DoS) saldırılara rağmen, ağın varlığının koruması hedeflenir. DoS saldırıları tasarsız ağların her katmanında gerçekleştirilebilir. Kötü niyetli kullanıcı fiziksel ve MAC katmanlarında ağa mesaj yığarak kanallarda tıkanıklık yaratabilir, ağ katmanında yönlendirme protokolünün çalışmasını aksatarak ağ bağlantısını koparabilir ve daha üst katmanlarda üst düzey hizmetleri servis dışı bırakabilir.

Güvenilirlik Güvenilirlik niteliği bilginin yetkisi olmayan kullanıcılara açılmamasını hedefler. Askeri ya da stratejik bilgiler gibi hassas bilgilerin ağda iletimi güvenilirliği gerektirir. Bu gibi bilgilerin kötü niyetli kullanıcılara sızması güvenilirlik için istenmeyen bir durumdur. Yönlendirme bilgisinin güvenilirliği sızmalara karşı bir önlem olarak kabul edilebilir.

Bütünlük Verinin bütünlüğü korunmalıdır. Gerek fiziksel etkiler gerekse kötü niyetli kullanıcılar tarafından bilinçli olarak yapılan saldırılara rağmen mesajın bütünlüğünün korunması garanti edilmelidir.

Asıllama Ağ içerisinde haberleşilen düğümün iddia ettiği düğüm olup olmadığı sınanmalıdır. Bir düğüm başka bir düğümün yerine geçerek yetkisi olmadığı halde kaynağa erişmemeli ve diğer düğümlerin işleyişine müdahale etmemelidir.

Tasarsız ağlarda katmanların haberleşme protokolleri düğümlerin verilen şartlara uyacağı varsayımı ile tasarlanmıştır. Bu protokoller güvenilmeyen ortamlarda gerçeklenmek istendiğinde bazı düğümler öngörülen kurallara aykırı davranabilir Bu düğümlerin amacı telsiz ortama daha sık erişip diğer düğümlerden daha fazla bilgiye sahip olmak ya da diğer düğümlerin ihtiyacı olan paketleri iletmeyi reddederek güç tasarrufu yapmak olabilir (selfishness) [7].

Kötü niyetli düğümlerin davranışlarının önüne geçebilmek için katmanlı bir güvenlik mekanizması uygulanmalıdır. Tasarsız ağlarda güvenlik önlemleri ağ katmanlarına göre aşağıda verilmiştir[5]:

2.1 Fiziksel Katmanda Güvenlik

Bu katmanda yerleştirilen frekans sekmeli güvenlik mekanizması (FHSM) gibi fiziksel koruma mekanizmaları veri çerçevesinin kaynaktan hedefe ilerlerken dinlenilmesini (eavesdropping), yolunun kesilip durdurulmasını, değiştirilmesini ya da düşürülmesini engelleyebilir.

2.2 Veri Bağı Katmanında Güvenlik

Veri bağı katmanında ağ üzerindeki bilgisayarların çarpışma olmadan medyaya erişimi yönetilir. MAC (Medium Access Control) protokolü ortamın adil olarak paylaşılmasını sağlar.

Bu katmanda yapılacak saldırılarda kötü niyetli düğüm, Ağ Dağıtım Vektörü (Network Allocation Vector)'nün boyutunu değiştirebilir ve komşu düğümlerin boş kalacağı zaman dilimi için büyük sayılar atayabilir. Çerçeveler arası boşlukları (SIFS, DIFS) azaltabilir, küçük geri çekilme değerleri seçebilir [8].

Başarılı bir güvenlik planı olası tüm aldatma şekillerini dikkate almalıdır. En zor sezme görevlerinden biri geri çekilme sayısının değiştirilip değiştirilmediğinin anlaşılmasıdır. Seçilen geri çekilme sayısı rasgele olduğundan herhangi bir düğümün seçtiği küçük geri çekilme değerinin şans eseri mi yoksa kasıtlı mı olduğunun anlaşılması zordur [8].

2.3 Ağ Katmanında Güvenlik

Tasarsız ağlar üzerinde ağ katmanı protokolleri üzerinden tek sekmeli bağlantı sağlanabildiği gibi, ağ katmanında yol atama ve veri iletimi protokolleri ile çok sayıda sekme üzerine genişletilerek bağlantı sağlanabilir. Kötü niyetli düğümler denetim mesajlarını değiştirerek veya yönlendirme bilgisindeki değerleri çarpıtarak ağ trafiğinin yeniden yönlendirilmesine neden olabilir. Trafiğin yeniden yönlendirilmesi için yapılan hesaplama sırasında yanlış değerliklere sahip yol duyuruları yaparak trafiğin kendi üzerinden geçmesini sağlayabilir.

2.4 Ulaşım Katmanında Güvenlik

Tasarsız ağlarda düğümlerin asıllanması ve yol atama bilgilerinin bütünlüğünün korunarak onaylanması güvenliğin temel yapıtaşlarıdır. Her iki yapıtaşı da uygun anahtarların kullanılmasında bir anahtar yönetim mekanizmasının varlığını gerektirir.

2.5 Uygulama Katmanında Güvenlik

Tasarsız ağların güvenliği, sızmalara karşı şifreleme ve asıllama gibi önlemlerle tam olarak korunamaz. Sistem ikinci bir savunma mekanizmasına ihtiyaç duymaktadır. Saldırı Tespit Sistemi (intrusion detection system) ağdaki şüpheli davranışları algılayıp alarm veren bir yapıdadır. Saldırı Tespit Sistemleri ağı sürekli gözlemleyerek sıra dışı etkinlikleri fark etmeye çalışır. Ağ kaynaklarını hedef alan kötü niyetli faaliyetleri belirleyip cevap veren bu sistem temelde biriktirilmiş denetim bilgilerine dayanır. Bu bilgiler daha sonra kullanılmak üzere belirsiz bir şekilde depolanabildiği gibi bekleyen işlem için geçici olarak da saklanabilir. Bilgilerin nereden ve nasıl toplanacağı, saldırılara nasıl cevap verileceği konfigürasyon ayarları ile denetlenir.

Yönlendirici gibi merkezi denetim noktaları olmayan tasarsız ağlarda saldırı tespit sistemlerinin kullanacağı bilgi o an düğüme giren ve çıkan trafik ile sınırlıdır. Diğer bir anahtar gereksinim de bu sistemlerin kullandığı algoritmaların dağıtılmış olmasıdır. Bir düğümün ağın sadece bir kısmını görebildiği gerçeği de hesaba katılmalıdır. Eğer saldırı tespit sistemlerinin kullandığı algoritmalar işbirliği içinde çalışıyorsa hangi düğümlere güvenileceği şüphelidir. Bu yüzden tasarsız ağlarda sadece dışarıdan gelen saldırılara değil ağın içinden

gelen saldırılara karşı da tedbirli olunması gerekir[3].

3. GELİŞTİRİLEN TASARSIZ AĞ GÜVENLİK SİMÜLATÖRÜ

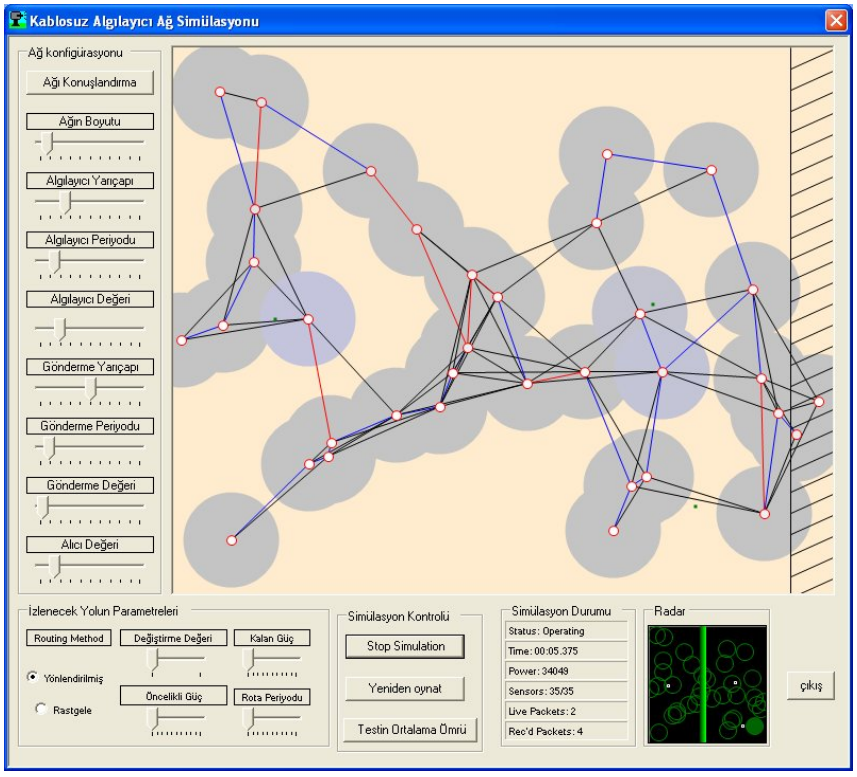
3.1 Simülatörün Tanıtılması

Hazırlanan program kablosuz ağlarda güvenlik nedeniyle trafiği gözlemlemek için tasarlanmıştır ve C# programlama dili kullanılarak gerçekleştirilmiştir. Simülatörün ağ tasarım ara yüzü Şekil 1' de verilmiştir.

Simülatörün çalışma ekranında görüldüğü gibi sağ tarafında bulunan alan ağın tasarlanacağı paneli göstermektedir. "Ağı Konuşlandır" isimli butona tıklandığında, gerekli çizim fonksiyonları çalışmakta ve bu alan içerisinde istenilen büyüklükteki ağ yapısını oluşturmaktadır. Ağın büyüklüğü ve yoğunluğu da, "Ağın Boyutu" isimli nesne ile ayarlanmaktadır. Bu nesne ile programın çalışma anında ağ boyutuna müdahale edilebilmektedir. Ağın boyutunun artması veya azaltılması ile konuşlandırılan ağ içerisinde, düğüm sayısının ve kenar sayısının yoğunluğunu ayarlamaktır. Bu durum Şekil 1'de simülatör programı ile kurulan olası bir ağ için gösterilmektedir.

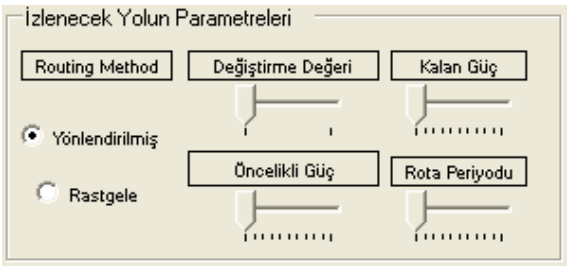
Simülatör için simülasyon kontrol paneli ile simülatör çalıştırılabilmekte, ağ tasarımı yenilenebilmekte ve test için ortalama ömür incelenebilmektedir. Simülatörün çalıştırılması bu panel vasıtasıyla gerçekleştirilmektedir ve panel görünümü Şekil 2'de verilmiştir. Simülasyona Başla butonu programın asıl çalıştırma butonudur ve tasarlanan ağın üzerine rasgele yönlerden saldırılar göndermektedir. Yeniden başlat butonu, ile simülasyon yeniden başlatılabilmektedir. Testin Ortalama Ömrü butonu ile de, farklı bir pencere açarak, kullanıcıya yüzde miktarı olarak okunabilen paketlerin istatistiğini sunmaktadır.

Yine simülatör için Şekil 3 de İzlenecek yolun parametreleri paneli verilmiştir. Bu panelde de, çalışma aşamasında rasgele olarak gönderilecek saldırıların parametreleri ayarlanmaktadır. Saldırıların yönü, hızı vb. bazı özellikleri bu panel yardımıyla ayarlanabilmektedir. Tasarım aşamasında planlanarak, ana formun en altına yerleştirilen bir diğer panel de, Simülasyon Durumu isimli paneldir ve Şekil 4 de bu panel verilmiştir. Bu panelde de, kullanıcı tasarladığı ağa ve gönderdiği rasgele saldırılara geri bildirim alabilmektedir. Okunabilen veya okunamayan paketler, algılayıcı reseptörler, zaman ve durum gibi pek çok bilgi, programın çalışması aşamasında bu panelde görülebilmektedir.

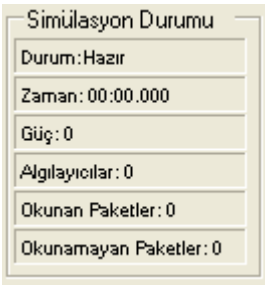


Şekil 1. Kablosuz ağ simülatörü ana tasarım ekranı

Şekil 2. Simülasyon kontrol paneli



Şekil 3. İzlenecek Yolun Parametreleri paneli

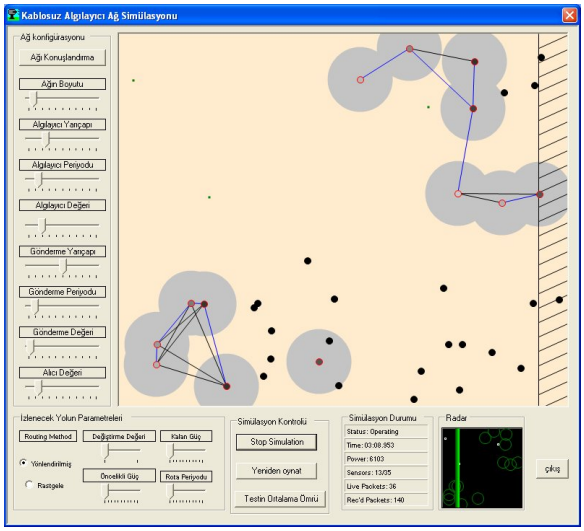


Şekil 4. Simülasyon durum paneli

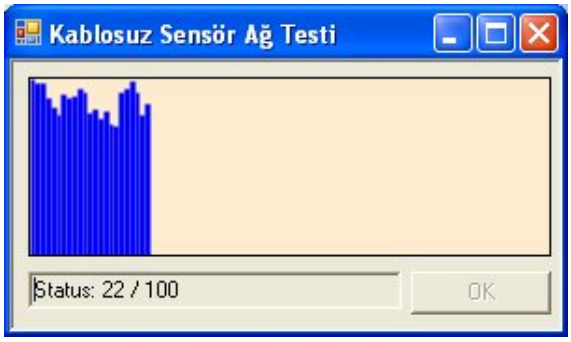
3.1 Simülatörün Çalıştırılması

Simülatörün çalıştırılıp kullanılabilmesi için, öncelikle ağın tasarlanması gerekmektedir. "Ağı Konuşlandır" isimli butona tıklandığında, ağ tasarlanacaktır ve çalışmaya hazır hale gelecektir. "Simülasyonu Başlat" isimli buton ile simülatör çalışmaya başlayacak ve simülatörün çalışması aşamasında, radar panelinde ağdaki düğümlerin bir benzetimi sunulmuştur. Radar paneli ile hangi ağ düğümlerinin, zarar gördüğü belirtilmektedir. Bir süre sonra, ondan fazla saldırıya maruz kalmış düğüm pasif hale gelecek ve devre dışı kalacaktır. Şekil 5'de pasif hale geçen düğümler, koyu siyah birer nokta haline dönecektir. Şekil 5'deki küçük yeşil karecikler ise simülasyon dahilindeki saldırıları göstermektedir. Simülasyon bittiğinde ise, "Simülasyon Durumu" isimli panelde son durum kullanıcıya sunulacaktır.

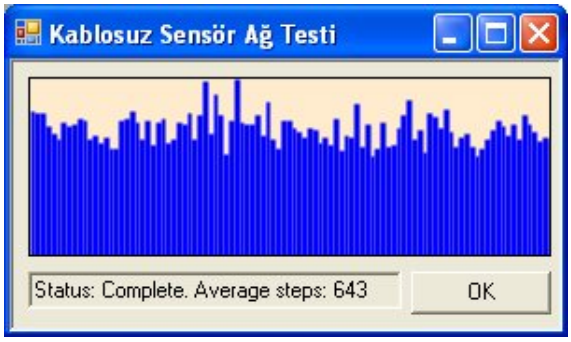
Testin Ortalama Ömrü isimli buton, ağda o anki durum hakkında bilgi vermektedir. Simülatörün çalışması aşamasında ve çalışma sonrasında test ortalama ömrü grafikleri sırasıyla Şekil 6 ve şekil 7 de verilmiştir.



Şekil 5. Programın çalışması esnasında bazı düğümlerin pasif hale geçmiş görünümü



Şekil 6. Testin Ortalama Ömrü isimli pencere (Çalışma Anında)



Şekil 7. Testin Ortalama Ömrü isimli pencere (Çalışma Sonunda)

4. SONUÇLAR

Kablosuz ağlar son yıllarda uygulama ve kullanım kolaylığı gibi nedenlerden dolayı hızlı bir gelişim göstermiş ve bilgisayar ağları konusunda kendisine ciddi bir yer edinmiştir. Kablosuz ağların bir alt uygulaması olan tasarsız ağlar ise sabit bir baz istasyonu veya erişim noktası içermediğinden askeri uygulamalar gibi tamamen mobilize olması gereken uygulamalarda öne çıkmaktadır. Bu uygulamalarda ise güvenlik konusunun ne denli önemli olduğu da aşikardır. Hazırlanan simülatör esnek ve kullanıcı etkileşimli bir yapıya sahiptir ve ağ üzerindeki düğümlerin trafiği izlenebilmektedir. Hazırlanan simülatör ile kablosuz ağlarda güvenlik nedeniyle ağ trafik gözlemlenebilmektedir ve öngörülmeyen ve tanımsız trafik akışı kolayca izlenebilmektedir. Bu noktadan sonraki adım ise bu simülasyon programının gerçek hayata uygulanması olacaktır. Bu simülasyon programı temel alınarak gerçek uygulamalar üzerinde çalışabilecek, trafiği izleyebilecek ve böylelikle saldırıları tespit edebilecek bir yazılım geliştirilmesi amaçlanmaktadır.

KAYNAKLAR

[1] William Stallings, "Wireless Communications and Networking", Prentice Hall, 2002.

[2] E. Akten, B. Örencik, " Tasarsız Ağlarda Dağıtık Anahtar Yönetim Sistemi", Ağ ve Bilgi Güvenliği Ulusal Semp. (ABG 2005),İstanbul, 9-11 Haziran, 2005, s. 60-64.

[3] Frank Stajano, Ross Anderson, "The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks, Security Protocols", 7th International Workshop Proceedings, Lecture Notes in Computer Science, 1999. p:1-11

[4] Lidong Zhou, Zygmunt J. Haas, "Securing Ad Hoc Networks", IEEE Networks Special Issue on Network Security November/December, 1999, p:24-30.

[5] H Yang, H Y. Luo, F Ye, S W. Lu, and L Zhang, "Security in mobile ad hoc networks: Challenges and solutions" IEEE Wireless Communications. 11 (1), 2004, p:38-47.

[6] K. Sanzgiri, D. LaFlamme, B. Dahill, B. N. Levine, C. Shields, E. M. Belding-Royer, "Authenticated routing for ad hoc Networks", IEEE Journal on Selected Areas in Communications, Vol. 23, No. 3, March 2005, p:598- 610.

[7] Refik Molva and Pietro Michiardi, "Security in Ad hoc Networks", Proceedings PWC 2003, September 2003.

[8] Alvaro A. Cárdenas, Svetlana Radosavac, John S. Baras, "Ad hoc networks: Detection and prevention of MAC layer misbehavior in ad hoc Networks", Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor Networks, October 2004, p:17-22.