Siber Güvenlik Deneyleri için Ağ Benzetici ve Ağ Sınama Ortamlarının Kullanımına Dair Ön İnceleme

A Preliminary Study on Using Network Simulation and Network Testbeds for Cyber Security Experiments

Enis Karaarslan
Muğla Sıtkı Koçman Üniversitesi Bilgisayar Mühendisliği Bölümü
enis.karaarslan@mu.edu.tr

Özetçe

Internet altyapısının güvenliği üzerine denemeler ve eğitimler sağlamak için siber güvenlik deneylerinin ve tatbikatlarının yapılması gereklidir. Bu çalışmada, bu deneyler için kullanılabilecek ağ benzetici, öykünüm ve sınama ortamlarının kullanımına dair bir ön inceleme sunulmuştur. Ağ sınama ortamları tanımlanmış; Emulab ve Epic sınama ortamı ayrıntılı olarak tanıtılmıştır. Ağ sınama ortamı kurulması için gereklilikler çalışmada önerilmiştir.

Anahtar Sözcükler: *siber güvenlik deneyi, siber güvenlik tatbikatı, ağ benzetim, ağ sınama ortamları, Emulab*

Abstract

Cyber security experiments and excercises are required in order to provide trainings and practices on security of the internet infrastructure. In this study, a prior review was presented regarding to use network simulation, emulation and testbeds which can be used for these experiments. Network testbeds are defined; Emulab and Epic testbed has been described in detail. Requirements to setup a network testbed are recommended in the study.

Keywords: *cyber security experiment, cyber security excercise, network simulation, network testbed, Emulab*

1 Giriş ve Teorik Çerçeve

Sosyal ağlar, bankacılık, e-devlet uygulamaları, birçok bilgilendirme ve eğlence imkanları ile Internet adını verdiğimiz siber uzay her geçen gün daha yoğun bir şekilde kullanılmaktadır. Siber uzayda, Haziran 2010 istatistiklerine göre 2 milyara yakın Internet kullanıcısı bulunduğu belirtilmektedir [1]. E-devlet uygulamaları bürokrasiyi azaltıp hayatımızı kolaylaştırırken ne yazık ki bazı güvenlik zafiyetlerini/sorunlarını da beraberinde getirmektedir [2]. Bir ülkenin işleyişi, iletişimi gibi birçok hayati süreci Internet altyapısına bağımlı hale gelmektedir.

Devlet ve toplumsal düzenin sağlıklı bir şekilde işlemesi için gerekli olan fiziksel ve sayısal sistemlere kritik altyapılar denir. Bilgi ve iletişim teknolojilerinin kritik altyapıları birbirine bağlamasıyla kritik bilgi altyapıları kavramı ortaya çıkmıştır [3]. Internet, Avrupa ekonomisi ve toplumu için sahip olduğu hayati görevi nedeniyle Avrupa Birliği tarafından Kritik Bilgi Altyapısı (CII) olarak nitelendirilmiştir [4]. Dünya Ekonomik Forumu'nun 2008 yılındaki tahminine göre, önümüzdeki 10 yıl içinde 250 milyar ABD Doları maliyet yaratacak büyük bir Kritik Bilgi Altyapısı aksama olasılığı %10 ile %20 arasındadır. Geçtiğimiz senelerde Estonya, Litvanya, Gürcistan, Burma, Kırgızistan, Güney Kore ve İran'da yaşanan siber saldırılar göz önüne alındığında küresel olarak hazırlık yapılması gerekliliği ortadadır [2, 5].

Kritik altyapıların korunması konusunda çalışmalar yapılması gerekmektedir [3]. Ülkemizde 2008 senesinde ilk siber tatbikat gerçekleşmiş, daha geniş çaptaki bir tatbikat 2011 senesinde uygulanmıştır [6].

Avrupa Birliği Komisyonu'nun Kritik Bilgi Altyapısı Koruma (CIIP) eylem planında [7] ön görüldüğü üzere 2010 yılı içerisinde Siber Avrupa 2010 (Cyber Europe 2010) denemeleri gerçekleştirilmiştir. Geniş çaplı siber saldırılar yaşanması durumunda ne yapılması gerektiği hakkında farkındalık yaratmak üzere çeşitli

etkinlikler gerçekleştirilmiş ve çalışmalar başlatılmıştır [7-9]. Siber Avrupa 2010 etkinlikleri içerisinde Avrupa çapında ilk siber saldırı benzetimi (simulation) gerçekleştirilmiştir [10]. Bu etkinlik Avrupa Ağ Güvenliği Kurumunun (ENISA) koordinasyonu ve Ortak Araştırma Merkezi (JRC)'nin destekleriyle gerçekleşmiştir. Avrupa Birliği çapında siber güvenlik hazırlık denemeleri, Avrupa'nın Dijital Ajandası'nda öngörülen icraatlardır [11]. Yapılan benzetimdeki senaryoda, Avrupa ülkeleri arasındaki Internet bağlantılarının devre dışı kalması veya belirgin bir şekilde kapasitelerinin azalması durumu ele alınmıştır. Saldırı anında Avrupa ülkeleri arasındaki bağlantıların da kullanım dışı olması söz konusudur. Vatandaşlar ve kurumlar, e-devlet uygulamaları gibi kritik çevrimiçi servislere erişimde sorunlar yaşayabilecektir. Sistemlerin servis vermeye devam edebilmesi için etkilenen bağlantılara yönlenen trafiğin farklı bir yoldan yönlendirilmesi gerekmektedir. Bu tür saldırı anlarında üye ülkelerin ortak çalışması gerekecektir [12].

Günümüzde, Internetin dayanıklığı ve esnekliği (resilience) hakkında temel göstergeler, gerçek yaşam vakalarından elde edilmektedir. Oysa ki sıkı yöntembilimler (methodology) kullanarak bilimsel deneyler yapmak; sağlam ve ikna edici kanıtlar elde etmek de mümkündür [4]. Internet'in esnekliği, güvenliği ve istikrarı oluşturulacak deneme ortamlarında araştırılabilir.

Bu çalışmada öncelikle benzetim, öykünüm ve ağ sınama ortamlarının kıyaslaması yapılacaktır. Geçerli ve güvenilir ağ benzetimi sorunu ele alınacaktır. Ağ sınama ortamları tanımlanacak; Emulab tabanlı bir laboratuvarın nasıl çalıştığı ve EPIC altyapısı anlatılacaktır. Araştırma sorusu ve hipotezler ele alınacaktır. Kısıtlama ve sınırlamalar tartışılacaktır. Sınama ortamının kurulmasına dair öneriler verilecektir.

2 Ağ Benzetim, Öykünüm ve Sınama Ortamlarının Kıyaslanması

Benzetimin ağ çalışmalarında kullanımı artmaktadır. Benzetim için aşağıdaki yaklaşımlardan söz etmek mümkündür [13]:

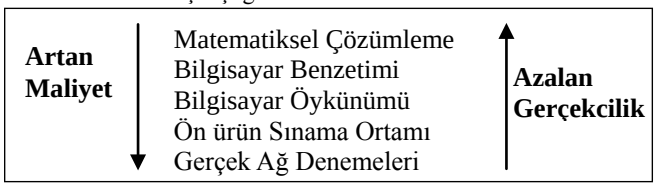
1. Matematiksel çözümleme
2. Bilgisayar benzetimi
3. Bilgisayar öykünümü (emulation)
4. Ön ürün sınama ortamı (prototype testbed)
5. Gerçek ağ denemeleri

Şekil 1'de [13] gösterildiği üzere, gerçek ortamlarda yapılan benzetimler daha gerçekçidir ama maliyetleri de daha fazla olmaktadır [13]. Bilgisayar benzetimlerinin temel artıları aşağıdaki gibidir [14]:

- Tekrarlanabilirlik
- Yanlış ayıklamanın mümkün olması
- Kurulum kolaylığı

Ammar'ın çalışmasında [13] da belirttiği üzere, ağ benzetimlerinin geçerliliği ve güvenilirliği konusunda ciddi tartışmalar yaşanmaktadır. Bu tartışmalar bir alt bölümde ele alınmıştır.

Daha gerçekçi sonuçlar için gerçek donanım üzerinde çalışan öykünüm veya sınama ortamlarının kullanımı söz konusudur.



Şekil-1: Benzetim yaklaşımlarının karşılaştırılması

Sınama ortamlarının kullanımının artma nedenleri aşağıda sıralanmıştır [14]:

- Donanım maliyetlerinin düşmesi
- İşletim sistemi sanallaştırma süreçlerinin yaygınlaştırılması
- Denetim ve yönetim yazılımlarının geliştirilmesidir.

Bilgisayar benzetimleri ve sınama ortamlarının artı

taraflarını birleştirmek ve iki yöntemi birlikte uygulamak da mümkündür. Bilgisayar benzetimleri ile ilinge (topoloji) ölçekleri ve protokol parametreleri belirlenebilir ve sınama ortamlarında daha gerçekçi olarak denenebilir [14]. Şekil 2'de gösterildiği üzere, Ns-3 yazılımı [15] ile bilgisayar benzetimleri ile sınama ortamlarını bir arada kullanmak ve birbirleriyle iletişim kurmalarını sağlamak mümkündür [16].

2.1 Geçerli ve güvenilir ağ benzetimi sorunu

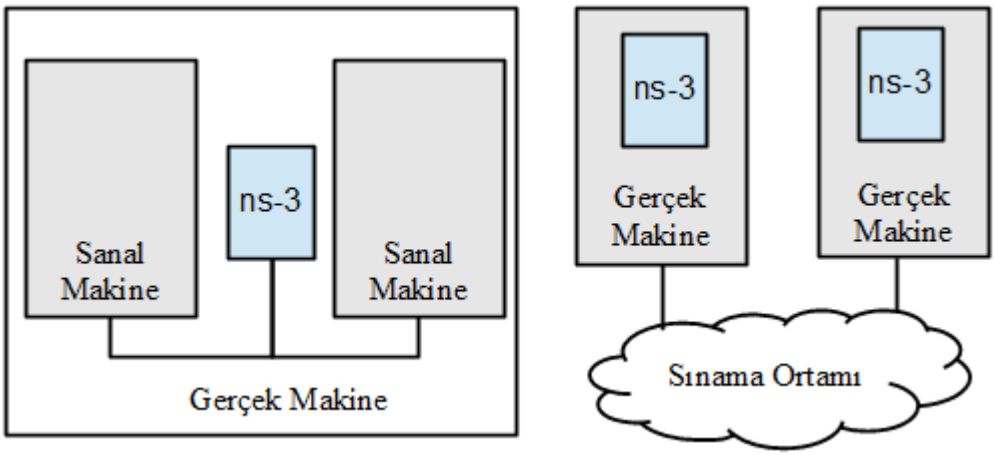
Ağ benzetimlerinin gerçekçiliğinin tartışılma nedenleri olarak aşağıdakileri sıralamak mümkündür [13]:

- Benzetimin ağ araştırmalarında oynadığı rol hakkında ağ toplumunun yeterli bilince sahip olmaması,
- Internet boyutunda ağların benzetimini temel olarak imkansızlaştıran temel sınırlar,
- Gerçekçi ağ modelleri inşa etmede zorluk,
- Benzetim deneylerinin tekrarlanabilir-liği ve geçerliliği için kabul edilebilir standartların eksikliğidir.

Ağ benzetimlerinin kullanılabilmesi için benzetimin güvenilir ve geçerli olduğunun gösterilmesi gerekmektedir. Benzetimlerin daha güvenilir olması için çeşitli çalışmalar yapılmaktadır. Benzetimlerin güvenilirliğini belirleyen ana etmenler olarak aşağıdakileri belirtmek mümkündür [17]:

- Benzetim yazılımının yetenekleri,
- Yazılım doğruluğu,
- Veri doğruluğu,
- Sonuçların doğruluğu,
- Benzetimin doğru bir şekilde kullanılmasıdır.

Yapılan çalışmanın konusu Internet, büyük ağlar ve siber güvenlik olduğunda ise bilgisayar öykünümü ve ön ürün sınama ortamı kullanmak daha anlamlı olabilmektedir. Bu durumda yapılan denemelerin daha gerçekçi olmasını sağlama konusunda çalışılmalıdır.



Şekil-2: Ns-3 ile farklı benzetim ortamlarının birlikte kullanımı

3 Ağ Sınama Ortamları

Ağ sınama ortamları; bilgisayar ve ağ bileşenleri gibi gerçek donanımlardan oluşan öykünüm veya sınama ortamlarıdır. Ağ sınama ortamlarını aşağıdaki şekilde sınıflandırmak mümkündür [18]:

- Küme (Cluster): Ağ simülasyonu tabanlı ve çok sayıda ağ cihazını bir araya getiren deneysel araştırma ortamlarıdır. Örnek olarak Emulab [19], Orbit [20] ve SensLab [21] verilebilir.

- Üstüne bindirmeli (overlay) ağlar: Bu tür sınama ortamları, var olan bir ağ üzerine kurulur ve ağ kodları uygulama seviyesinde çalışır. Genellikle yeni iletişim kuralları ve servislerinin denenmesi için kullanılırlar. Dünya genelinde farklı yerlerde mümkün olduğunca fazla uç cihazların sisteme eklenmesini hedeflerler. Örnek olarak Planetlab [22] verilebilir.
- Birlik (federated): Ağ sınama ortamlarının kaynaklarını birleştirmeye çalışan çeşitli girişim ve mimariler bulunmaktadır. Örnek olarak; Amerika'daki girişim GENI [23], Avrupa'daki girişim ONELAB [24] verilebilir.
- Ağ araştırma setleri: Araştırmacıların kendi yerel ağ laboratuvarlarını kurmaları için kullanabilecekleri yazılım ve donanım bileşenleridir.

Örnek sınama ortamlarının temel özellikleri Çizelge 1'de verilmiştir.

Emulab ağ güvenliği ve başarımı konusunda deneyler yapılmasını sağlayan bir ortamdır. Emulab'ın toplam düğüm sayısı net değildir, bazı konumlardaki kurulumlar dış erişime kapalıdır. Araştırmacılara açık olan ve Utah'da bulunan konumdaki Emulab düğüm (node) sayısı çizelgede verilmiştir.

Emulab ve Planetlab, araştırmacıların ücretsiz olarak altyapıdan yararlanmalarını sağlamaktadır. Sistemleri kullanmak için kayıt yaptırarak başvurmak gerekmektedir. Emulab, projenin içeriği gibi bazı kıstaslara göre kullanım izini vermektedir. Planetlab ise araştımacılara 10 dilim kullanma izini vermektedir. Dilim tabanlı kullanım mimarisi [25]'da tanımlanmıştır.

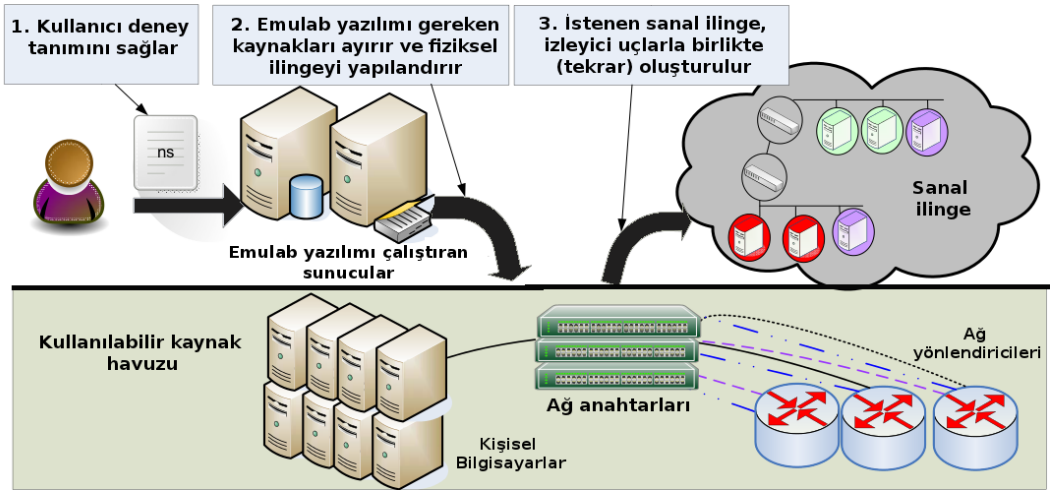
Çizelge-1: Örnek Ağ Sınama Ortamlarının Özellikleri

	İçerik	Birlik	Düğüm	Konum
Emulab	Ağ cihazları, Bilgisayar	Yok	350(+)	38(*)
PlanetLab	Bilgisayar	GENI, Onelab	1160	547
Orbit	Kablosuz Ağ	Yok	400	1
SensLab	Kablosuz Algılayıcı Ağ	Yok	1024	4

3.1 Emulab

Emulab emülasyon sınama ortamı [26], Emulab yazılımını çalıştıran 2 sunucudan ve deneyde kullanılabilecek öğeleri (kişisel bilgisayarlar veya sanal makinalar, ağ anahtarı ve yönlendiricisi gibi ağ cihazları) içeren bir kullanılabilir kaynak havuzundan oluşur. Emulab deneyinde uç olarak kullanılabilecek cihazlar kişisel bilgisayarlar olabildiği gibi, sunucular içerisinde tanımlanmış sanal makinalar da olabilir. Her uç cihazın en az 2 adet ağ arabirimi olmalıdır. Bunlardan bir adedi Emulab sistemi içerisindeki iç iletişim için kullanılacak ve yönetim için ayrılmış denetim ağı (control network) olarak adlandırılan özel sanal ağa (VLAN) dahil olacaktır. Diğer ağ arabirimleri deneyde kullanılacak ve kurulacak ilingeye (topoloji) göre farklı sanal ağlara dahil olabilecektir. Emulab yazılımı Cisco, HP gibi ağ anahtarlarını ve hangi uçların hangi cihaza takıldığını SNMP aracılığı ile tanımakta ve gerekli sanal ağ ayarlarını özdevimli olarak yapabilmektedir.

Emulab tabanlı bir sınama ortamında deney başlatmak için gereken temel adımlar Şekil 3'de gösterilmiştir.



Şekil-3: Emulab tabanlı bir sınama ortamında deney başlatmak için gereken temel adımlar

Deney tanımlamaları, Emulab yapılandırma betiğinde genişletilmiş Ns-2 dilinde yazılır. Seçilen senaryoya göre fiziksel kaynaklar kullanılarak sanal bir ilinge oluşturulmaktadır. Bu süreçte; ağ anahtarlarında gereken değişiklikler yapılmakta, ilingedeki uç cihazlarını temsil edecek kişisel bilgisayarlara gerekli işletim sistemi ve şablon tanımlarında var olan yazılımlar da özdenimli olarak kurulmaktadır.

Emulab ortamının; tekrar edilebilirlik, ölçeklenebilirlik ve deneylerin denetlenebilirliği gibi artıları vardır.

3.2 EPIC Altyapısı

Avrupa Komisyonu Ortak Araştırma Merkezi EC JRC (Joint Research Center) ISPC (Institute for the Protection and Security of the Citizen) Enstitüsü'nde EPIC (Experimental Platform for Internet Contingencies) adında Internet riskleri için deneysel bir ortam kullanılmaktadır. Bu deneysel ortam ile ilgili ayrıntılı teknik rapor için bkz. [27].

Yapılan doktora sonrası çalışma kapsamında EPIC altyapısı üzerinde çeşitli çalışmalar gerçekleştirilmiştir. EPIC altyapısı Emulab tabanlıdır. Bu altyapıya erişim sadece enstitüdeki laboratuvardan verilmektedir. Laboratuvarda araştırmacıya sağlanan kişisel bilgisayar üzerinden EPIC altyapısına ulaşılıp deneyler yapılabilmektedir. EPIC sistemi aşağıdaki alt birimlerden oluşmaktadır [28]:

1. Laboratuvar Ortamı: Denemeler için var olan kaynaklar; Sunucular, kişisel bilgisayarlar, ağ yönlendiricileri (router) ve ağ anahtarları (switch)
2. Emulab yazılımı ile kurulumun denenmesi,
3. Saldırıların gerçekleştirilmesi: Özelleştirilmiş tfn2k aracı [29], Scapy [30] veya benzeri araçların kullanılmasıyla DOS ve/veya DDOS saldırıların gerçekleştirilmesi,
4. Veri Toplama: Ağ trafiği izlerinin (trace) tcpdump [31] ile toplanması, ajan yazılımların gönderdiği bilgilerle Zabbix yazılımı kullanılarak deney ağının izlenmesi,
5. Veri Çözümlemesi: Tcpdump izlerini tcpts (tcp time stamp – zaman damgası) değerleri veya benzer yazılımlarla ayrıştırılması (parse),
6. Arka Plan Trafiği: Gerçek trafik izlerini tekrar oynatmak, iperf [32] benzeri yazılımlarla yapay ağ trafiği yaratılmasıdır.

Deney ağını izlemek için kullanılan Zabbix yazılımı [33], ileri seviyede izleme, uyarı ve

görselleştirme imkanlarını ölçeklenebilir ve özdevinimli bir şekilde sunmaktadır. Uygulamada, öncelikle Zabbix sunucusunun bir şablonu oluşturulmuştur. Denetlenmek istenilen cihazların üzerinde Zabbix ajan (agent) yazılımları çalışmaktadır. Zabbix sunucusu ayrı bir uç cihaz olarak ayrı bir deneyde çalışmakta ve deney ağında herhangi bir karışıklığa yol açmamak için denetim ağı üzerinden ajan yazılımları ile iletişim kurmaktadır.

4 Araştırma Sorusu ve Hipotezler

Bir benzetim veya sınama ortamının gerçeğe yakın sonuçlar döndürebilmesi için neler yapılması ve nasıl düzenlenmesi gerektiği de ayrıntılı olarak araştırılmalıdır. Benzetim sonuçlarının gerçekçi olabilmesi için öncelikle kullanılan rastsal sayı üreteçlerinin rastsallığı sağlanmalıdır. Rastsallık hem şifreleme protokollerinde hem de benzetimde önemli bir etmendir [34].

Tamamen denetlenebilir bir deneme ortamında tekrarlanabilir deneylerin icrasının nasıl sağlanacağı da araştırılmalıdır. Böylece başka parametrelerin değerleri değiştirilerek denemeler sağlıklı bir şekilde yapılabilecektir.

Bir siber güvenlik deneyini gerçekçi kılmak için kaç uç noktaya ihtiyaç olduğu ve eldeki laboratuvar imkanları ile ne kadarının uygulanabileceğinin belirlenmesi gereklidir.

Internet altyapısının gerçekçi ağ ilingelerinin (topology) ve koşulların (örneğin WAN bağlantılarının gecikme ve kayıp özelliklerinin) yeniden verimli bir şekilde oluşturulmasının nasıl sağlanacağı araştırılmalıdır.
Yönlendirme protokollerinin esnek olarak çalışması, örneğin saldırı durumunda başka bir rotayı kısa bir sürede belirleyebilmesi için yapılandırmanın nasıl olması gerektiği de belirlenmelidir.

Böyle bir sınama ortamının siber güvenlik tatbikatları gibi eğitim ve hazırlık faaliyetleri için nasıl geliştirilebileceği ve etkin kullanılabileceği üzerine de çalışılmalıdır.

5 Kısıtlama ve Sınırlamalar

Bilgisayar benzetimlerinde, benzeti-mi yapılan uç bilgisayar sayısı arttıkça özellikle bellek sorunu yaşanmaktadır. Ns-3 yazılımının diğer benzetim yazılımlarından daha iyi bellek ve işlemci kullandığı Weingartner ve arkadaşlarının çalışmasında [35] gösterilmiştir. Yine de bu tür benzetim yazılımlarında on binlerce uç bilgisayarının benzetimini yapmak etkin olmamaktadır. Bu durumda kullanılan yazılımları iyileştirmek bir çözüm olmakla beraber yetmeyecektir. Benzetimin birden fazla cihazda dağıtık çalışması daha etkin bir çözüm olacaktır.

Bilgisayar benzetimini birden fazla makinede dağıtık çalışmasında ve sınama ortamları kullanımında ağ arabirim (Örn. ethernet) kartının ve işletim sisteminin sınırları da belirleyici etmenler olacaktır. Kullanılacak ethernet kartının sürücüsünün aygıt yoklayıcısı (device polling) özelliğini desteklemesi ve TCP/IP boşaltma motoru (offload engine) desteğinin olması sınama ortamındaki ağ başarımını arttıracaktır. Ayrıca, FreeBSD gibi TCP/IP yığını SMP sistemlerde daha verimli çalışacak şekilde iyileştirilmiş işletim sistemlerinin kullanılması ve üzerinde tampon bellekleri olan, yüksek paket trafikleri için iyileştirilmiş sunucu seviyesi ethernet kartlarının tercih edilmesi daha iyi başarımlar sağlayacaktır.

6 Sınama Ortamının Kurulmasına Dair Öneriler

Sınama ortamı için kullanılabilecek farklı yazılım araçları Sieterlis ve Masera'nın çalışmasında [36] ayrıntılı olarak ele alınmıştır. Emulab ve Planetlab, bir sınama ortamı kurmak için gerekli yazılımları ve belgeleri sağlamaktadır. Sınama laboratuvarında kurulacak saldırı ve ağ izleme programlarının özgür yazılımlardan seçilmesi önerilmektedir. Böyle yapılması durumunda herhangi bir yazılım maliyeti olmayacaktır.

Emulab web üzerinden erişim için gerekli imkanları sağlamaktadır. Bu nedenle, kurulacak laboratuvarın fiziksel yerinden çok, bu konuda araştıma yapacak kişilere internet üzerinden her zaman erişilebilir olmasının sağlanması

önemlidir.

Kurulacak sınama ortamının sağlıklı çalışması için teknik desteğe ihtiyaç olacaktır. Konusunda yetkin bir teknik ekiple, bu sistemdeki cihazların sağlıklı bir şekilde çalışır ve üzerinde çalışan yazılımların her zaman güncel olmasının sağlanması mümkündür.

7 Sonuçlar ve Öneriler

E-devlet gibi birçok çevrimiçi servisin devreye girmesi ile günlük hayat her geçen gün Internet'e daha bağımlı hale gelmektedir. Ulusal bilgi kaynaklarının güvenliğinin sağlanması için çalışmalar yapılması gerekmektedir.

Siber güvenlik ve siber savaşlar geleceğin en önemli konuları olmaya adaydır. Siber saldırılar ve siber terörizm olaylarındaki artış da özellikle ulusal bilgi kaynaklarının güvenliğini tehdit eder durumdadır. Bir ülkenin e-devlet ve bilgi sistemlerinin çalışmasını engellemek için; yönlendirme ve DNS hizmetlerinin aksamasına veya yanlış çalışmasına yol açacak saldırılar sanıldığı kadar zor değildir. Bu tür saldırılar geçmişte de yaşanmış ve Estonya gibi ülkelerde ciddi ekonomik ve toplumsal sonuçlara yol açmıştır [3]. Bu tür saldırılara karşı hazırlıklı olmamız gerekmektedir [6].

Internet'in esnekliği, güvenliği ve istikrarının araştırılması deneme ortamlarının oluşturulması ile mümkündür. Daha gelişmiş siber güvenlik tatbikatlarının ve deneylerinin gerçekleştirilebilmesi için bilimsel araştırmaların yapılması gerekmektedir. Benzetimlerin senaryo karmaşıklığı, boyut ve gerçekçiliğini arttırmak için deneme sınama ortamlarının nasıl kullanılabileceği konusunda ayrıntılı araştırmaların gerçekleştirilmesi gerekmektedir. Ayrıca eğitim için de bu süreçlerin kullanımı mümkündür.

EMULAB benzeri bir sınama ortamı altyapısının ülkemizde de kurulması ve araştırmacıların erişimine açılmasıyla siber güvenlik konusunda araştırma ve eğitimin daha iyi yapılabilmesi mümkün olabilecektir.

Teşekkür

Bu çalışmada, Enis Karaarslan TÜBİTAK tarafından 2219 Yurtdışı Doktora Sonrası Araştırma Burs Programı kapsamında desteklenmiştir.

8 Kaynakça

[1] Internet Usage Statistics, 10.03.2011 tarihinde erişildi, http://internetworldstats.com/stats.htm

[2] **Emre B.**, İnternet Güvenliğinin Tarihçesi, Tübitak BİLGEM dergisi, Cilt 3, Sayı:5, 2011

[3] **Karabacak B.**, Kritik Altyapılar, Dünya ve Türkiye Özeti, Tübitak BİLGEM dergisi, Cilt 3, Sayı:5, 2011

[4] Internet stability and security, 17.02.2011 tarihinde erişildi, http://sta.jrc.ec.europa.eu/index.php/internet-stability-and-security

[5] Protecting Europe from large scale cyber-attacks and disruptions, 17.02.2011 tarihinde erişildi, http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_organised_crime/si0010_en.htm

[6] Tübitak BİLGEM Siber Güvenlik Tatbikatı, 22.02.2011 tarihinde erişildi, http://www.uekae.tubitak.gov.tr/home.do?ot=5&rt=&sid=0&pid=0&cid=8322

[7] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection - "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" {SEC(2009) 399} {SEC(2009) 400} http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52009DC0149:EN:NOT

[8] Towards the first pan-european exercise on Critical ICT Infrastructure Protection,

ENISA Quarterly Review Vol. 6, No. 2, June 2010; http://www.enisa.europa.eu/publications/eqr/issues/eqr-q2-2010-vol.-6-no.-2

[9] CYBER EUROPE 2010 - First Ever Pan-European Exercise on Large Scale ICT Incidents, ENISA Quarterly Review Vol. 6, No. 4, December 2010, http://www.enisa.europa.eu/publications/eqr/issues/eqr-q4-2010-vol.-7-no.-4

[10] European Commission, Digital Agenda: cyber-security experts test defences in first pan-European simulation, 2010, http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1459&format=HTML&aged=0&language=EN&guiLanguage=en

[11] Digital Agenda for Europe: key initiatives, 17.02.2011 tarihinde erişildi, http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/200&format=HTML&aged=0&language=EN&guiLanguage=en

[12] JRC poster for "CYBER EUROPE 2010", 17.02.2011 tarihinde erişildi, http://sta.jrc.ec.europa.eu/pdf/scni/publications/cyber-europe-2010-a3size.pdf

[13] **Ammar, M.**, 2005, Why We STILL Don't Know How to Simulate Networks. 13th IEEE International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems, 179-179. IEEE. doi: 10.1109/MASCOTS.2005.76. http://www.cc.gatech.edu/%7Eammar/presentations/ANSS/ANSS-KEY_files/frame.htm

[14] **Lacage M.**, NS-3 Trilogy yaz okulu konuşmaları, 2009, http://www.nsnam.org/tutorials/trilogy-summer-school.pdf

[15] The ns-3 network simulator, 17.02.2011 tarihinde erişildi, http://www.nsnam.org

[16] **Henderson T., Lacage M.**, ns-3 tutorial, 2009, http://www.nsnam.org/workshops/wns3-2009/ns-3-tutorial-part-1.pdf

[17] **Muessig, P., Laack, D., Wrobleski, J.** (2001). An integrated approach to evaluating simulation credibility. Citeseer. Retrieved February 16, 2011, from http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA405051

[18] Report of nsf workshop on network research testbeds, National Science Foundation, (2002), http://www-net.cs.umass.edu/testbed_workshop/testbed_workshop_report_final.pdf

[19] Emulab-Network Emulation Testbed, http://www.emulab.net/

[20] ORBIT, 17.02.2011 tarihinde erişildi, http://www.orbit-lab.org/

[21] Senslab, http://www.senslab.info/

[22] Planetlab, 17.02.2011 tarihinde erişildi, http://www.planet-lab.org/

[23] GENI, Exploring Networks of the Future, http://www.geni.net/

[24] Onelab, Future Internet Testbeds, http://www.onelab.eu/

[25] Slice-Based Facility Architecture(v0.8), 2007, http://www.cs.princeton.edu/~llp/arch_abridged.pdf

[26] **E. Eide, L. Stoller, J. Lepreau**., 2007, An experimentation workbench for replayable networking research. In 4th USENIX Symposium on Networked Systems Design & Implementation, pages 215-228.

[27] **Siaterlis, C., Masera, M.**, 2010, The development of the Internet resilience laboratory at IPSC, JRC Technical Report 57145. Office. Retrieved from http://sta.jrc.ec.europa.eu/pdf/scni/publications/report_57145.pdf

[28] EPIC Description Leaflet, 17.02.2011 tarihinde erişildi, http://sta.jrc.ec.europa.eu/pdf/scni/publications/LAB_poster_epic_A3.pdf

[29] Tribe Flood Network 2000 (TFN2K),

http://packetstormsecurity.com/distributed/tfn2k.tgz

[30] Scapy, http://www.secdev.org/projects/scapy/

[31] Tcpdump & Libpcap, http://www.tcpdump.org/

[32] iperf, http://iperf.sourceforge.net/

[33] Zabbix, http://www.zabbix.com

[34] **Karaarslan E.**, 2001, Büyük ölçekli rastsal ve asal sayı üretimi, Ege Üniversitesi Fen Bilimleri Ensitütüsü Yüksek Lisans Tezi, Tez no: 113994,

[35] **Weingartner, E., Vom Lehn, H., Wehrle, K.**, 2009, A Performance Comparison of Recent Network Simulators. 2009 IEEE International Conference on Communications, 1-5. IEEE. doi: 10.1109/ICC.2009.5198

[36] **Siaterlis C., Masera M.**, 2010, A survey of software tools for the creation of networked testbeds, International Journal On Advances in Security, ISSN. 1942-2636, vol. 4, No. 1-2, pp.1-12