SMTP Protokolü
ve
Spam Mail Problemi

M. Erkan YÜKSEL, Şafak Durukan ODABAŞI

İstanbul Üniversitesi Mühendislik Fakültesi
Bilgisayar Mühendisliği Bölümü

Özet

Bu çalışmada,

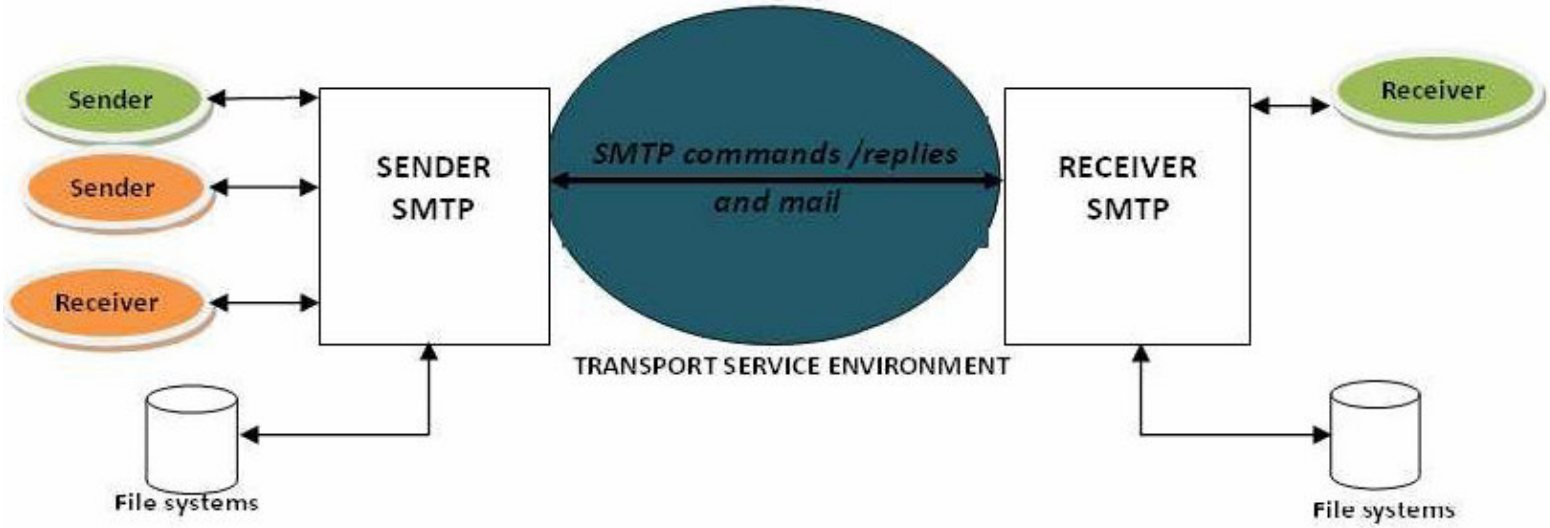
- Antispam/antivirüs programı filtresinden alınan mesaj logları
- DNS blok listesindeki blocklist logları
- Bir mail sunucusunun iç ve dış ağdaki güvenilirlik yapısı

  analiz edilerek

spam göndericilerin davranışları incelenmiştir.

Mevcut Mail Teknolojisi

- İnternet üzerinden email alımı ve iletimi mevcut bir açık standart protokolü kullanılarak gerçekleştirilir: SMTP (Simple Mail Transport Protocol). Mail dağıtımı, bağlantı hostu ile alıcı host arasında bir SMTP işlemini içerir.
- Bir e-mail için, gönderici SMTP sistemi maili internet içine gönderir; alıcı ya da dağıtımcı sistem maili bir taşıma servis ortamından kabul eder ve mail kullanıcı temsilcisine aktarır ya da mail kullanıcı temsilcisinin erişeceği mesaj deposunda saklar.



• SMTP şu iletişim modeline sahiptir: bir kullanıcı mail isteğinin sonucu olarak, gönderici SMTP, alıcı SMTP'ye doğru iki yönlü bir iletim kanalı oluşturur. Alıcı SMTP son hedef olabileceği gibi ara geçişlerden biri de olabilir. Gönderici SMTP, alıcı SMTP'nin yorumlayabileceği ve cevap verebileceği SMTP komutları üretir.

• İletim kanalı kurulduğunda, gönderici SMTP, mailin göndericisini belirten MAIL komutunu yollar. Eğer alıcı SMTP maili almayı kabul ederse, bir OK cevabı yollar. Bunu gönderici SMTP'nin mailin alıcısını içeren RCPT komutunu göndermesi izler. Eğer alıcı SMTP, bu alıcı için maili almayı kabul ederse, OK ile cevap verir; kabul etmezse, tüm mail iletimi için değil sadece bu alıcı için red cevabını döndürür; böylelikle gönderici ve alıcı SMTP'ler aynı kanaldan başka alıcılar için görüşebilirler. Alıcıların başarılı bir şekilde görüşmesi sağlandığında, gönderici SMTP özel bir karakterle sonlanan mail verisi üretir. Mail verisinin başarıyla alınmasından sonra alıcı SMTP OK cevabı döndürür. Bu noktada gönderici SMTP iletim kanalının kapatılması işlemini başlatır.

SPAM PROBLEMİ

- Spam probleminin çevresinde yapılan mevcut çalışma, mail sunucu ve/veya mail istemci tarafındaki spam filtresi uygulamasıdır.
- Spam filtreleme üç metoda dayanır: beyaz listeler, siyah listeler ve e-mail içeriği ya da bunların kombinasyonudur. Mail sunucusunda uygulanan siyah liste filtrelemesi, DNS kara listesinde yayınlanan IP alanına dayanırken, beyaz liste filtrelemesi daha çok istemci tarafında, bir kullanıcının e-mail almasına izin verilen kullanıcı hesaplarına dayanır.

- Spam probleminin çözümü için mevcut email sistemine revizyon yapılmalı ve izin tabanlı bir sisteme dönüştürülmelidir. SMTP e-mail sisteminde tamamen yeni bir protokol uygulanması hem zordur hem de bunun sisteme eklenmesi tüm internet boyunca yeni bir sistemin dağıtılmasının yaratacağı karmaşıklığa neden olur.

Spam ile İlgili Yapılan Çalışmalar

- Spam yollayıcıların global davranışlarının analizi üzerine yapılan çalışmalar, Yüksek Yoğunluklu Spam Yollayıcılar ve Düşük Yoğunluklu Spam Yollayıcılar olarak sınıflandırılmıştır.
- Spam yollayıcı ağı altyapısının varlığı, ağın nasıl genişlediğini ve servis içinde bulunduğunu göstermektedir.
- Yapılan çalışmalar sırasında, spam problemi araştırılmış ve spame karşı mücadelede kullanılacak olan e-mail spam imzasının üretilmesi için botnet tabanlı spam hareketlerinin dağıtılmış karakteristiklerinden yararlanılmıştır.
- Mesaj boyutları, gönderici, alıcı ve mesaj teslim süresi bilgilerini içeren bir mail sunucusu incelenirse, mail sistemleri için kriter olarak kullanılabilecek mail kalıpları üretilebilinir.

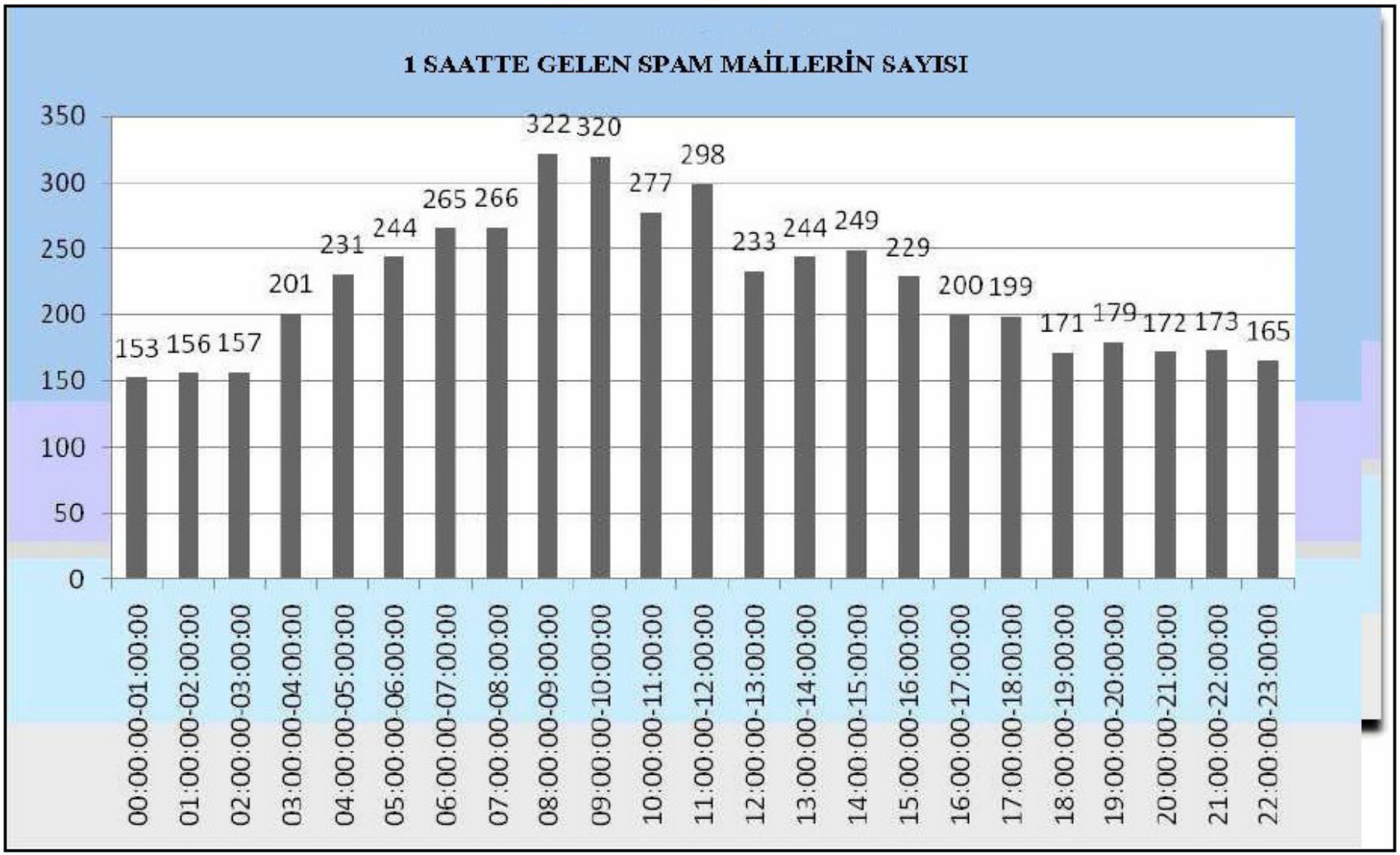
Spam ile İlgili Yapılan Çalışmalar

- SMTP Yol Analizi'ni inceleyen çalışmalarda, mail domainleri ve ilgili IP adreslerinin reddedilme oranını tahmin edecek bir öğrenme algoritması geliştirilmiştir.
- Bu analizlerin temeli, bilinen güvenli mailler ve bilinen spamlerin iletimi için kullanılan yollar bulunmaktadır.
- Bunların dışında, veri madenciliği kullanılarak mesaj iletim uygulamasının nasıl gerçeklendiğini inceleyen çalışmalar da, davranış tabanlı mail analizi için yapılan spam tespitinin bir parçası olabilir.

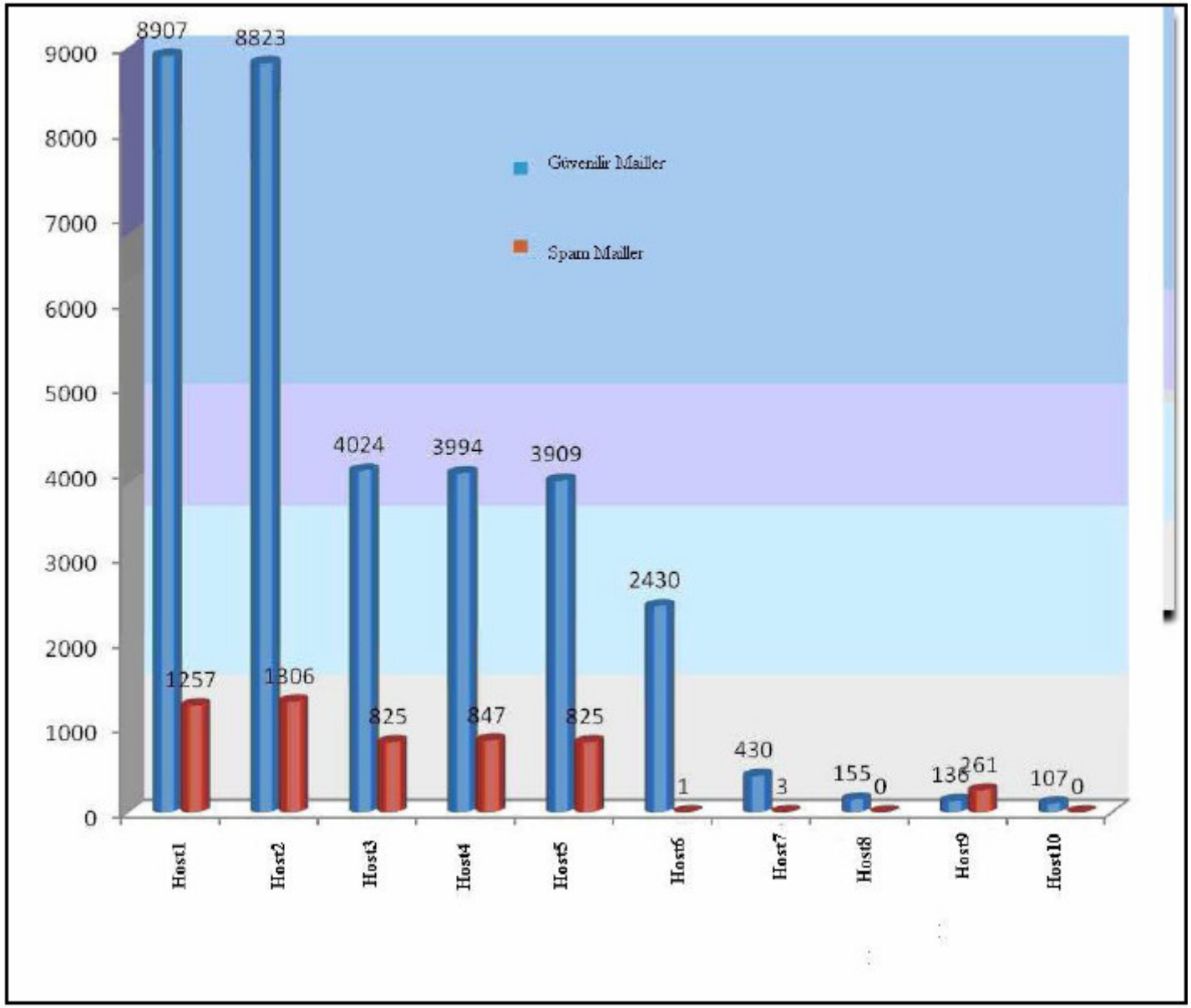
Uygulama

- Bir iç mail sunucusu ve dış mail sunucuları simüle edilerek, sunucların mesaj logları incelenmiştir. E-mail başlıklarından elde edilen veriler analiz edilmiştir. Bu veriler, DNSBL ve anti-spam uygulaması kullanılarak filtrelenmiştir.
- İki adet veri seti ile çalışılmıştır. İlki DNSBL bloklama listesidir. Bu veri, "<ZamanDamgası>, <IP Adresleri>, <OK-REJECT>" bilgilerini içermektedir. OK, IP adresinin DNS kara listesinden (DNSBL) geçtiği anlamına gelmektedir. REJECT ise mailin DNSBL kontrolünden geçemediğini göstermektedir.
- İkinci veri seti, Anti-Spam Filtre veri logu ise, "<ZamanDamgası>, <IP Adresleri>, <HostIsimleri>, <Olasılık–VİRÜS>" bilgilerini kapsamaktadır. DNSBL kontrolünden geçen her mail, mail sunucusunda filtreleme kurallarına uygun olarak 0 ile 1 arasında olasılıklarla işaretlenmek üzere Anti-Spam filtre aracına gönderilir. Eğer mail virüs içeriyorsa VIRUS olarak işaretlenir.
- Spam mailleri, güvenli maillerden ayırmak için, güvenli mail mesajları 0 ve 0.5 arasında olasılıkla işaretlenmiştir. 0.5'den büyük değerlere sahip mailler ise spam olarak belirlenmiştir.
- Mesaj loglarının incelenmesi sonucunda elde edilen veriler tablolar halinde hem iç hem de dış mesaj logları için çizelgelenmiştir.

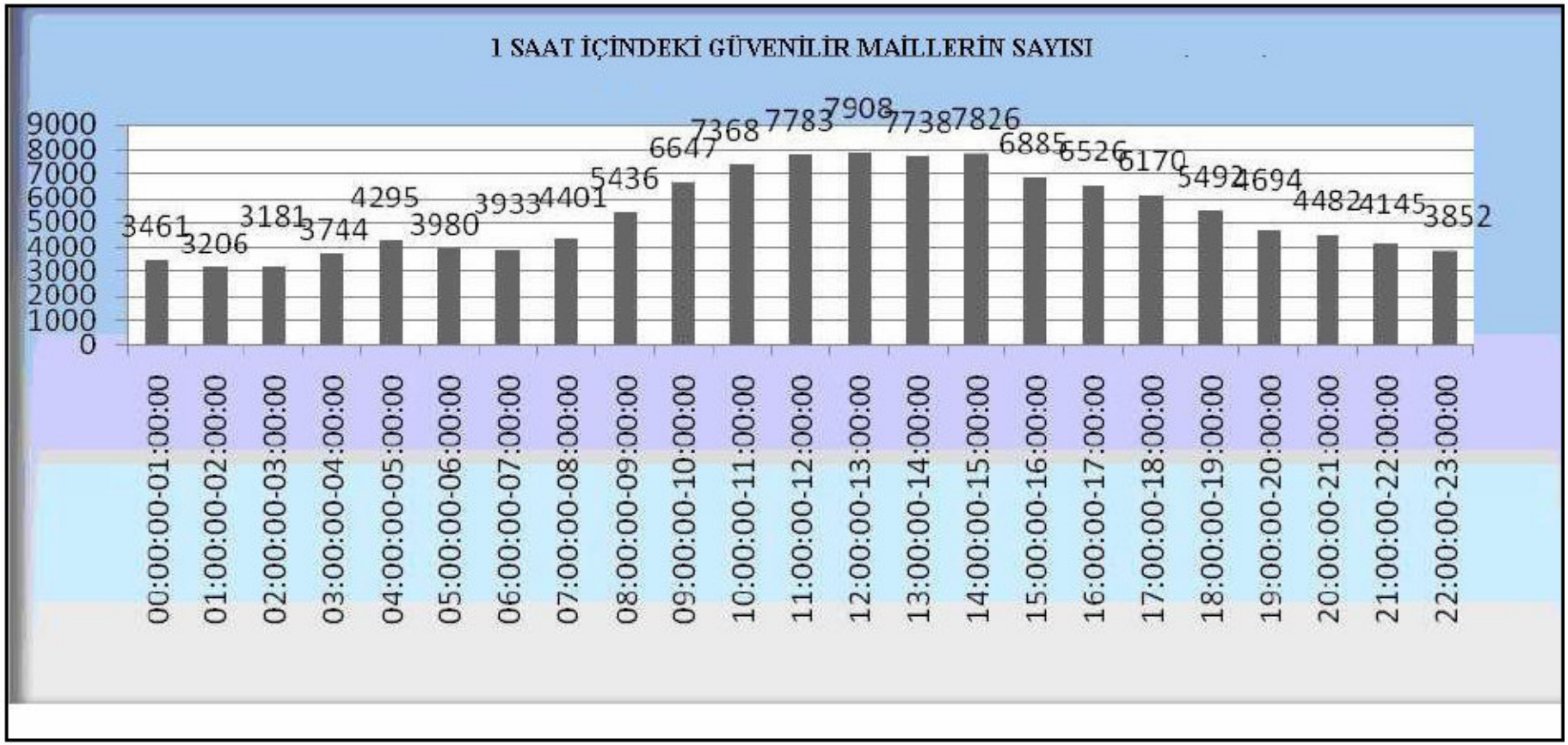
İç mesaj logu için 1 saatte gelen güvenilir maillerin toplam sayısı



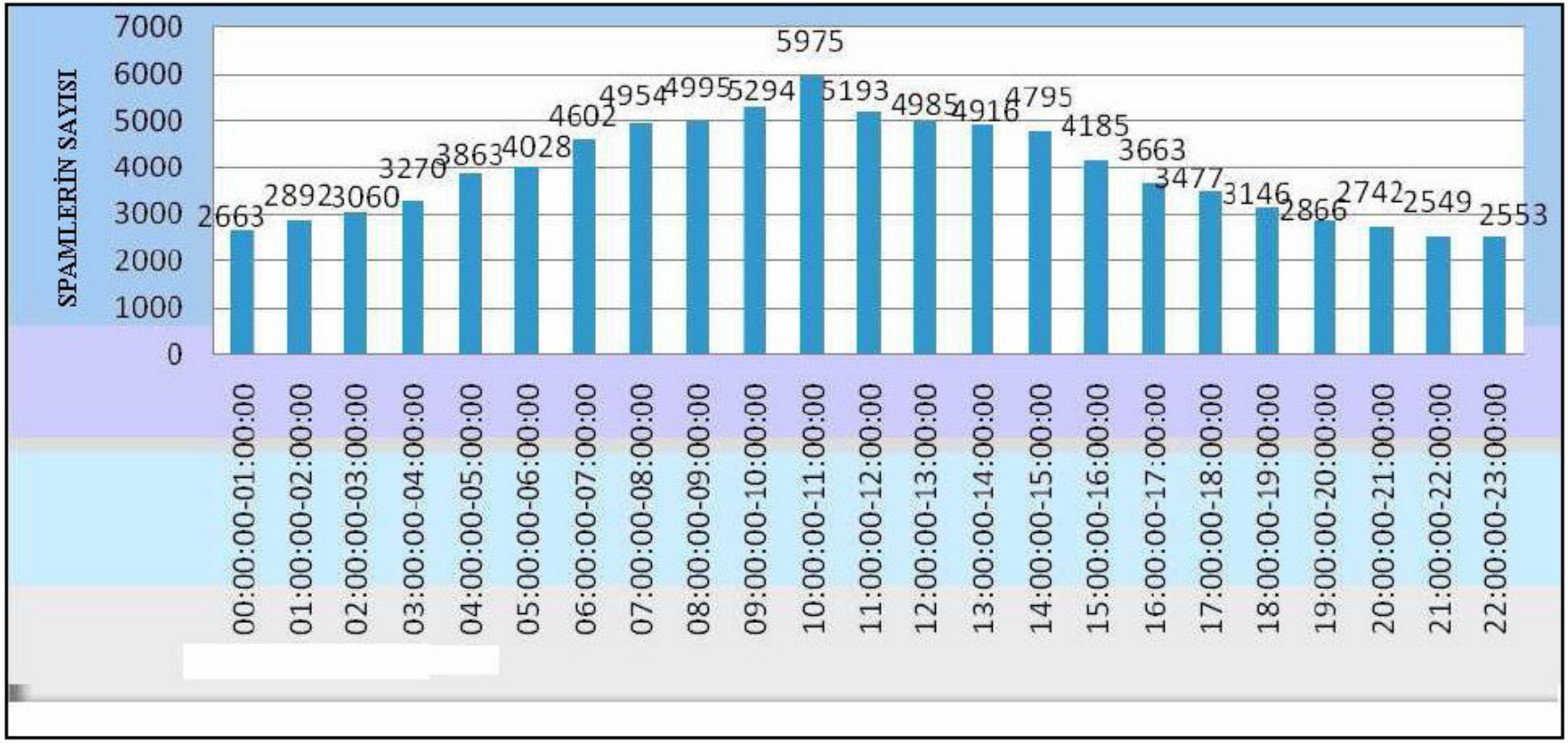
İç mesaj logu için 1 saatte gelen spam maillerin toplam sayısı



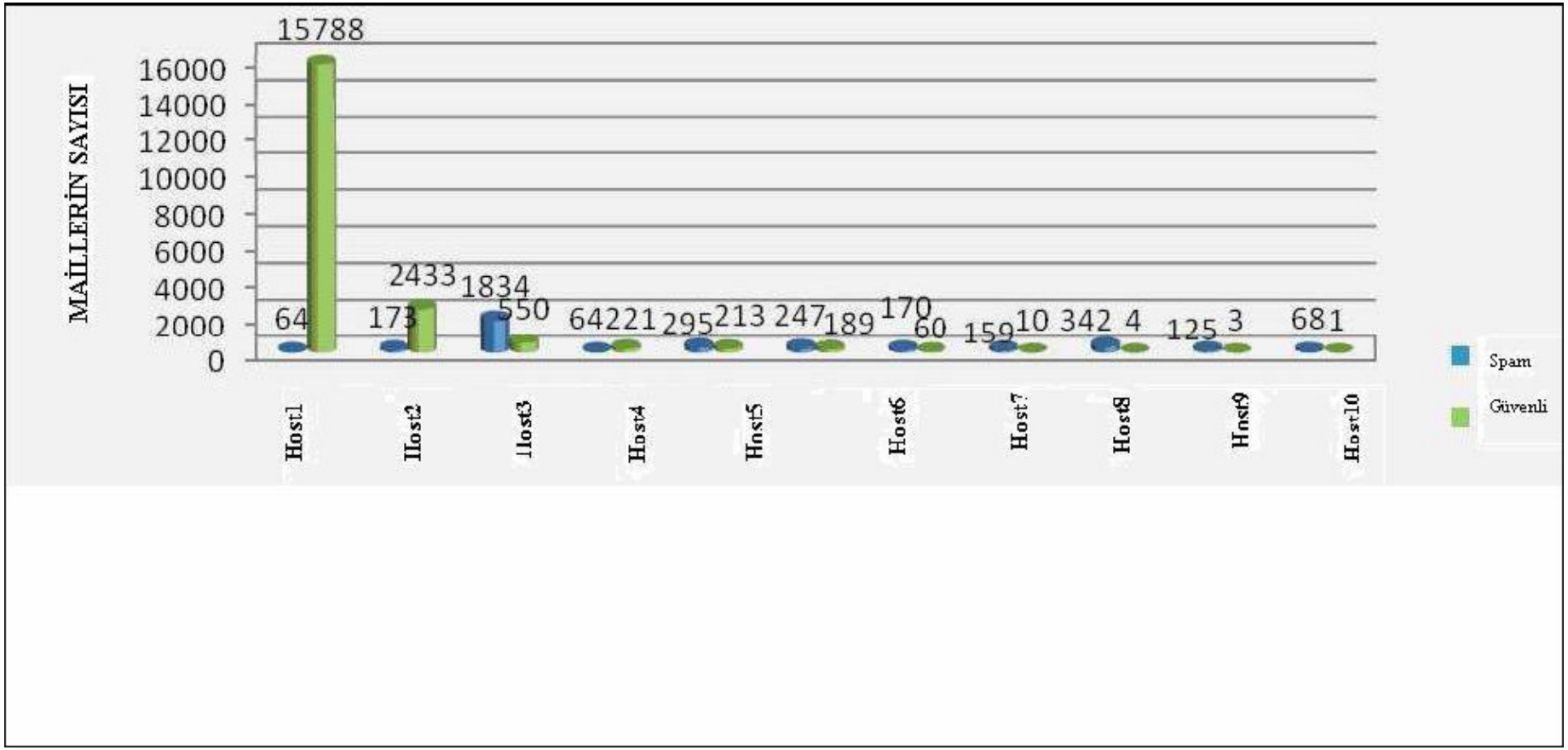
İç mesaj logu için en meşgul 10 sunucu ve maillerin dağılımı



Dış mesaj logu için 1 saatte gelen güvenilir maillerin toplam sayısı



Dış mesaj logu için 1 saatte gelen spam maillerin toplam sayısı



İç mesaj logu için 1 saatte gelen spam maillerin toplam sayısı

Sonuç

- Saatler arasında mail aktivitesinin yüksek olduğu zamanlarda, spam hareketliliği de artmaktadır. Aynı sunucudan gelen güvenli ve spam mailler arasında güvenilir maillerin sayısının çok olduğu görülmüştür.,
- İç mail sunucusundan 1 saat içinde alınan güvenilir maillerin ortalama sayısı 1440 iken, ortalama spam mail sayısı 222 olarak gözlenmiştir.
- Elde edilen sonuçlar, spam aktiviteleri hakkında aydınlatıcı olmaktadır. Hem iç hem de dış sunuculardan gelen mailere göre, alınan mail sayısıyla beraber spam mail sayısı da artmaktadır ve bu değer gece yarısından önce tepe noktasına ulaşmaktadır.
- Spam mailler hem iç hem de dış sunuculardan gelmektedir. Bu esnada birçok mail DNSBL'in kontrolünden tespit edilmeden geçmeyi başarmıştır. Bu durum dinamik IP adreslerinin kullanımı veya spam üreticilerin bot makineler üzerinde çalışmaları ve buna bağlı olarak DNSBL filtrelemeden kaçabilmeleriyle açıklanabilir.
- Verinin analizi sonucu, spam mailler filtrelendiğinde, spam yollayıcıların, spam mail göndermeye devam ettikleri; yani filtrelemenin spam yollayıcıları durduramadığı ve bazı spamlerin doğal olarak yayıldıkları gözlenmiştir.