Derin Öğrenme Teknolojileri Kullanarak Dağıtık Hizmet Dışı Bırakma Saldırılarının Tespit Edilmesi

Ferhat Özgür Çatak, Ahmet Fatih Mustaçoğlu

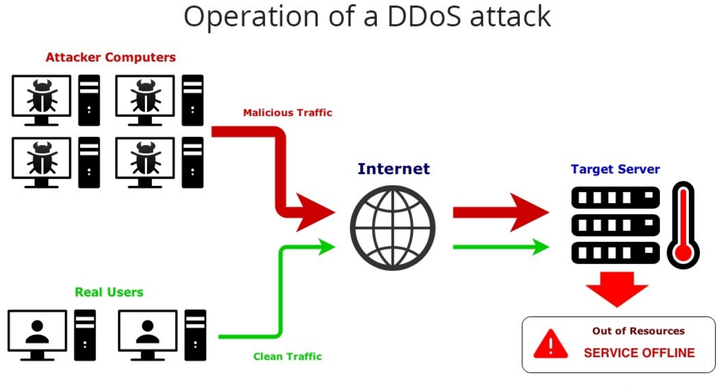
TÜBİTAK BİLGEM Siber Güvenlik Enstitüsü

Amaçlar

- Kurumsal sistemlerde kötü amaçlı ağ trafiğinin miktarı artmaktadır.
  - *botnet*, *fuzzer*, *shellcode*
- Günlük operasyonları tehdit etmesi sebebiyle oldukça önemli bir konu haline gelmiştir.
  - Erişilebilirliğe saldırmayı hedefleyen dağıtık hizmet dışı bırakma saldırıları, hizmete bağlanması gereken meşru kullanıcılar için hizmetlere erişimi engellemeyi amaçlamaktadırlar.
- *Ağ akış modellerine* dayalı derin öğrenme yöntem ve teknolojileri tabanlı *ağ trafiği sınıflandırma modeli* önerilmektedir.
- Sınıflandırma performansını artırmaya yönelik olarak derin yapay sinir ağlarına dayalı model kullanılmıştır.

Giriş

- Dağıtık hizmet dışı bırakma saldırıları (Distributed denial of service - DDoS): Kurban sistemin kaynaklarını tüketmeyei hedefleyen saldırılardır.
- Kaynaklar: *ağ*, *disk*, *işlemci*, *memory*



Şekil 1: Bir DDoS Saldırısı.

https://www.scudlayer.com/en/ddos-attacks/

Veri Kümesi

Normal aktiviteler ve saldırı davranışlarını içeren ağ trafiği PCAP dosya formatında kayıt edilmiştir.

Saldırılar

- *Fuzzers*
- *DoS*
- *Recon.*
- *Analysis*
- *Exploits*
- *Shellcode*
- *Backdoors*
- *Normal*
- *Worms*

Veri kümesinde yer alan kayıtların *normal* ve *saldırı* dağılımları:

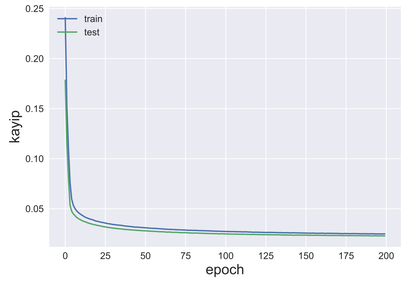
Tablo 1: Veri kümesinde bulunan nitelikler.

Trafik	Toplam kayıt
Normal	37000
Saldırı	45332

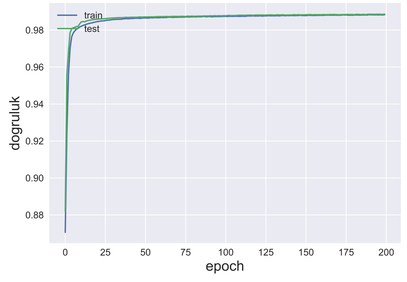
Teknolojiler

- Keras
- Theano
- Pandas
- Scikit-learn

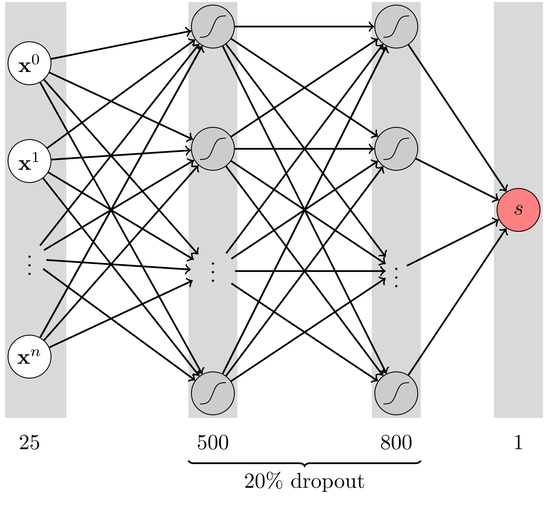
Eğitim Aşamaları



Şekil 2: Modelin iterasyon kayip değerleri.



Şekil 3: Modelin iterasyon doğrulukları.



Şekil 4: Sınıflandırma modeli.

Bulgular

Tablo 2: Kullanılan altyapılar.

Platform	CPU	Memory
Quadro 1000M	96 CUDA cores @ 1 GHz	16 GB
Intel i7-600	4 Çekirdek @ 4 GHz	16 GB

Tablo 3: Modelin değerlendirme sonuçları.

Sınıf	Kesinlik	Duyarlık	F_1	Doğruluk
Normal	0.99	0.99	0.99	0.9889
Saldırı	0.95	0.96	0.96	0.9889

Tablo 4: İşlem Süresi.

Platform	Eğitim (sn)
Quadro 1000M	3516,21
Intel i7-600	10601,42

Sonuçlar

Önerilen yöntemin yüksek boyutlu siber güvenlik alanında kullanılan veri kümelerine uygulanabilir olduğu gösterilmiştir. Bu yöntem kullanılarak zararlı ağ trafiğinin algılanmasında kaynak IP adresi gibi yanıltıcı alanlara bakılmadan, gelen paketler içerisinde yer alan büyüklük, varış süresi, yük boyutu gibi sunucuya gelen isteklerin niteliklerine bakılarak model oluşturmaktadır. Bu sebeple paketler üzerinde saldırganlar tarafında IP, MAC adres sahteciliği gibi yöntemlerden etkilenmemektedir.

İletişim

- Dr. Ferhat Özgür Çatak: ozgur.catak@tubitak.gov.tr
- Dr. Ahmet Fatih Mustaçoğlu: afatih.mustacoglu@tubitak.gov.tr