Bayesçi Çoklu Değişim Noktası Modeliyle VoIP Ağlarda Saldırı Tespiti
Attack Detection in VOIP Networks Using Bayesian Multiple Change-Point Models

Çağatay Yıldız[1], Taha Yusuf Ceritli[2], Barış Kurt[1], Bülent Sankur[3], Ali Taylan Cemgil[1]
[1]Bilgisayar Mühendisliği Bölümü, Boğaziçi Üniversitesi, İstanbul, Türkiye
{cagatay.yildiz1, baris.kurt, taylan.cemgil}@boun.edu.tr
[2]Hesaplamalı Bilim ve Mühendislik Yüksek Lisans Anabilim Dalı, Boğaziçi Üniversitesi, İstanbul, Türkiye
{yusuf.ceritli}@boun.edu.tr
[3]Elektrik-Elektronik Mühendisliği Bölümü, Boğaziçi Üniversitesi, İstanbul, Türkiye
{bulent.sankur}@boun.edu.tr

***Özetçe* —İnternet üzerinden telefon görüşmesi yapılmasını sağlayan sistemlerde kullanılan protokollerden biri SIP'tir. Günden güne yaygınlaşan SIP ağları DDoS saldırılarının açık hedefi haline gelmiştir. Bu makalede, DDoS saldırılardan doğan sapaklıkları tespit eden bir Bayesçi model sunduk. Model, ağ trafiğini gözlemleyerek saldırı anlarında uyarı vermektedir. Benzetim sistemleri yardımıyla ürettiğimiz veri üzerinde yaptığımız deneylerde modelin başarılı sonuçlar verdiğini gözlemledik.**

Anahtar Kelimeler*—*SIP Ağları, Ağ Saldırısı Tespiti, Çoklu Değişim Noktası Modeli

***Abstract*—One of the most commonly used network protocols in Internet telephony services is SIP. As the popularity of the protocol increases, SIP networks have become targets of DDoS attacks more frequently. In this work, we propose a Bayesian change point model to detect anomalies due to such attacks. The model monitors the network and alarms when a change in the network traffic occurs. We test the model with a data set generated by network traffic and attack simulators.**

Keywords*—*SIP Networks, Network Intrusion Detection, Multiple Change-Point Model

I. GİRİŞ

VoIP (Voice over Internet Protocol), kullanıcılarının internet bağlantıları üzerinden telefon konuşmaları yapmalarına olanak sağlayan bir iletişim teknolojisidir [1]. Yüksek hızlardaki İnternet servislerinin daha ucuza sunulması ve İnternetin hızla yayılması sayesinde VoIP'in popülerliği günden güne artmakta ve bu teknoloji, devre anahtarlamalı telefon ve veri iletişimine güçlü bir alternatif sunmaktadır.

VoIP servislerinin verilmesinde en yaygın olarak kullanılan protokollerden biri SIP'tir (Session Initialization Protocol) [2]. En temelinde SIP, İnternet kullanıcıları arasında bir iletişim oturumunun başlaması için bilgi değiştokuşunu sağlamakta ve kurallarını belirlemekte kullanılır. Kullanıcıların konumlarının, kayıtlı oldukları sunucuların, müsaitlik durumlarının, iletebilecekleri ve kabul edebilecekleri veri tiplerinin takibi ve oturumların başlatılıp sonlandırılması, bu protokolün başlıca sorumlulukları arasındadır.

SIP protokolünü kullanan iletişimin gittikçe yaygınlaşması, bu protokolün sadeliği ve kullanışlılığından kaynaklanmaktadır. Öte yandan, protokolün metin tabanlı olması ve SIP sunucularının İnternet üzerinden erişilebilirliği, sunucuları ve servis kullanıcılarını DoS (Denial of Service) adı verilen saldırıların açık hedefleri haline getirmektedir. DoS saldırıları, kullanıcıların servis almalarını engellemek amacıyla bir bilgisayara ya da onun İnternet bağlantısına yapılan saldırılara verilen genel isimdir [3]. Birden çok bilgisayar aracılığıyla gerçekleştirilen saldırılaraysa DDoS (Distributed Denial of Service) adı verilir.

DDoS saldırılarının tespiti ve önlenmesi konusunda literatürde pek çok çalışma bulunmaktadır. Bu yöntemler genellikle başlatılmaya çalışılan ve başarıyla başlatılan oturum sayısı, sunucudan geçen SIP ve RTP (Real-time Transport Protocol) paket sayısı, sunucunun kaynak kullanımı gibi özniteliklerin takibine dayanır [4]. Bu özniteliklerdeki değişikliklere kural tabanlı tepkiler veren, değişikliklerin belirli eşik değerleri aşıp aşmadığını takip eden ya da SIP mesajlarının sonlu durum makinelerindeki sapaklıkları tespit eden ve bu mekanizmalarla saldırı uyarısı veren sistemler mevcuttur [5].

Biz bu çalışmada, DDoS saldırılarının saptanması için bir Bayesçi çoklu değişim noktası modeli geliştirdik. Modelin kalbinde, korunmak istenen SIP sunucusundan sabit bir periyotta toplanacak SIP mesaj verilerinin normal trafik altında ve saldırı anında farklılık göstereceği kabulü yatıyor. Model her yeni gözlemin, bir önceki gözlemle aynı mekanizma tarafından üretilmiş olması olasılığını hesaplıyor. Bu olasılığın düşük olduğu noktalar değişim noktalarını, başka bir deyişle mesaj trafiğinin farklı bir mekanizma tarafından üretildiği ve olası bir saldırının başladığı noktaları, temsil ediyor.

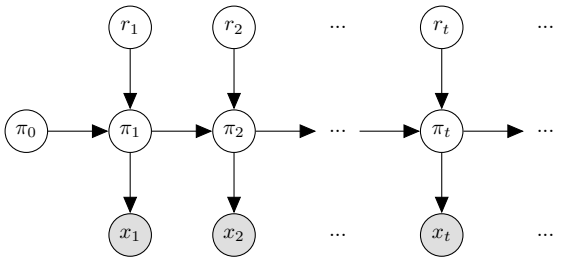
Makalenin ikinci bölümünde geliştirdiğimiz modeli detaylandıracağız ve saldırı tespitinin nasıl yapıldığını anlatacağız. Üçüncü bölümde, kurduğumuz deney ortamını tanımlayacağız. Sonraki bölümde, üretilen benzetim verileri üzerinde yaptığımız deneylerin sonuçlarını yorumlayacağız. Son

978-1-5090-1679-2/16/$31.00

bölümdeyse modelin nasıl geliştirilebileceğini tartışacağız.

II. Model

Bayesçi çoklu değişim noktası modeli, değişken durumlu uzay modellerin(switching state space models) örneklerinden biridir. Çoklu değişim noktası modelinde gözlemler x_t, saklı değişkenler r_t ve π_t ile gösterilir. $r_t \in \{0, 1\}$, t anında rejimin durumunu gösteren bir ayrık değişken, π_t ise r_t'ye koşullu bir Markov zinciridir. Gözlemimiz x_t'nin saklı değişken π_t'ye koşullu olarak üretildiğini eklediğimizde, grafik model Şekil 1'de gösterildiği gibi olmaktadır.



Şekil 1: Çoklu değişim noktası grafik modeli.

t anındaki gözlem x_t'yi, parametresi π_t olan bir katlı terimli (multinomial) dağılımdan örneklenmiş bir rasgele değişken olarak kabul ediyoruz. Bu katlı terimli dağılımın parametresi π sabit olmakla beraber değişim anlarında, yani $r_t = 1$ iken, başka bir değere sabitleniyor. Özetle, kurduğumuz modelin üretici modeli aşağıdaki gibidir:

$$\begin{aligned}
\pi_0 &\sim \mathcal{D}ir(\pi_0; a) \\
r_t &\sim \mathcal{BE}(r_t; p) \\
\pi_t | r_t, \pi_{t-1} &\sim [r_t = 0]\delta(\pi_t - \pi_{t-1}) + [r_t = 1]\mathcal{D}ir(\pi_t; a) \\
x_t | \pi_t &\sim \mathcal{M}(x_t; \pi_t)
\end{aligned}$$

Burada $\mathcal{D}ir$, $\mathcal{BE}$ ve $\mathcal{M}$, sırasıyla Dirichlet, Bernoulli ve katlı terimli dağılımları; δ ise Dirac delta fonksiyonunu temsil eder. Gözlemlerimizin $K \geq 1$ boyutlu olduğu durumda bu dağılımlar aşağıdaki formüllerle ifade edilir:

$$\begin{aligned}
\mathcal{D}ir(\pi; a) &= \frac{\Gamma\left(\sum_{i=1}^{K} a_i\right)}{\prod_{i=1}^{K} \Gamma(a_i)} \prod_{i=1}^{K} \pi_i^{a_i - 1} \\
\mathcal{BE}(r; p) &= p^r (1-p)^{(1-r)} \\
\mathcal{M}(x; \pi) &= \frac{\Gamma\left(\left(\sum_{i=1}^{K} x_i\right) + 1\right)}{\prod_{i=1}^{K} \Gamma(x_i + 1)} \prod_{i=1}^{K} \pi_i^{x_i}
\end{aligned}$$

Üretici modeldeki iki parametreden biri olan a, Markov zincirinin sıfırlama parametresidir. Değişim olduğu durumlarda π, parametresi a olan bir Dirichlet dağılımından örneklenen bir rasgele değişkene eşitlenir. Modelin diğer parametresi p ise değişim gerçekleşme ihtimalinin önsel dağılımıdır.

Herhangi bir t anı için değişim noktası tespiti problemi, r_t'nin sonsal dağılımını hesaplamaya karşılık gelir. Bizim problemimizde değişim noktası tespiti gerçek zamanlı yapılacağından problem süzgeçlemeye indirgenir. Yani hesaplamak istediğimiz dağılım $p(r_t|x_{1:t})$'dir. Bu dağılımı π_t üzerinden tümlev alarak bulmak mümkündür:

$$\begin{aligned}
p(r_t|x_{1:t}) &\propto p(r_t, x_{1:t}) \\
&= \int_{\pi_t} p(r_t, \pi_t, x_{1:t}) \qquad (1)
\end{aligned}$$

π_t'nin sürekli olduğu değişken durum uzaylı modellerde r_t'nin küme niceliğinin 2'den büyük olması, çözümün karmaşıklığının t değeriyle üssel hızla artmasına sebep olur [6]. Ancak bizim problemimizde r_t'nin küme niceliği 2'ye eşit olduğundan *İleri Yönlü-Geri Yönlü* algoritmayla(İGA) doğrusal orantılı karmaşıklıkla çıkarım yapmak mümkündür.

İGA'da ileri yönde iletilecek mesajları aşağıdaki gibi tanımlayalım:

$$\alpha_{t|t-1}(r_t, \pi_t) = p(r_t, \pi_t, x_{1:t-1}) \qquad (2)$$
$$\alpha_{t|t}(r_t, \pi_t) = p(r_t, \pi_t, x_{1:t}) \qquad (3)$$

1 numaralı eşitlikte gösterildiği üzere $\alpha_{t|t}(r_t, \pi_t)$ mesajı, hesaplamak istediğimiz dağılımla orantılıdır. Yukarıdaki tanımlara göre ileri özyineleme denklemini şöyle yazabiliriz:

$$\begin{aligned}
\alpha_{t|t}(r_t, \pi_t) &= p(r_t, \pi_t, x_{1:t}) \\
&= \sum_{r_{t-1}} \int_{\pi_{t-1}} d\pi_{t-1} p(r_{t-1:t}, \pi_{t-1:t}, x_{1:t}) \\
&= \sum_{r_{t-1}} \int_{\pi_{t-1}} d\pi_{t-1} p(r_{t-1:t}, \pi_{t-1:t}, x_{1:t-1}) \\
&\quad \times p(x_t|r_t, \pi_t) \\
&= \sum_{r_{t-1}} \int_{\pi_{t-1}} \Big(d\pi_{t-1} \alpha_{t-1|t-1}(r_{t-1}, \pi_{t-1}) \\
&\quad \times p(r_t, \pi_t|r_{t-1}, \pi_{t-1}) \Big) p(x_t|r_t, \pi_t) \qquad (4)
\end{aligned}$$

Ancak sadece ileri yönlü mesajlarla çıkarım yapmak bize kısıtlı bir doğruluk sağlamaktadır. Bu doğruluğu artırmak için L zaman adımı ilerisine kadar olan gözlemleri de kullanabiliriz; diğer bir deyişle, $p(r_t, \pi_t, x_{1:t})$ yerine $p(r_t, \pi_t, x_{1:t+L})$ sonsal dağılımından da yararlanabiliriz. Algoritmanın geri yönlü mesajları

$$\beta_{t|t+1}(r_t, \pi_t) = p(x_{t+1:t+L}|r_t, \pi_t) \qquad (5)$$
$$\beta_{t|t}(r_t, \pi_t) = p(x_{t:t+L}|r_t, \pi_t) \qquad (6)$$

şeklinde tanımlandığında geri yöndeki özyineleme denklemi

$$\begin{aligned}
\beta_{t|t}(r_t, \pi_t) &= p(x_{t:t+L}|r_t, \pi_t) \\
&= \sum_{r_{t+1}} \int_{\pi_{t+1}} d\pi_{t+1} p(x_{t:t+L}, \pi_{t+1}, r_{t+1}|r_t, \pi_t) \\
&= \sum_{r_{t+1}} \int_{\pi_{t+1}} d\pi_{t+1} p(x_{t+1:t+L}, \pi_{t+1}, r_{t+1}|r_t, \pi_t) \\
&\quad \times p(x_t|r_t, \pi_t) \\
&= \sum_{r_{t+1}} \int_{\pi_{t+1}} \Big(d\pi_{t+1} \beta_{t+1|t+1}(r_{t+1}, \pi_{t+1}) \\
&\quad \times p(r_{t+1}, \pi_{t+1}|\pi_t, r_t) \Big) p(x_t|r_t, \pi_t) \qquad (7)
\end{aligned}$$

L adım geri yönlü özyinelemeden sonra $p(r_t, \pi_t, x_{1:t+L})$ sonsal dağılımı ileri ve geri yönlü mesajların çarpımı cinsinden

Parametreler		K	B	F	BaB	BiB	T
Trafik Şiddeti	Saldırı Şiddeti						
Düşük	Düşük	0.81	0.65	0.72	1	0.3	0.2
Düşük	Yüksek	0.87	0.83	0.84	1	0.65	0.45
Yüksek	Düşük	0.94	0.8	0.86	1	0.6	0.35
Yüksek	Yüksek	0.93	0.9	0.91	1	0.8	0.43

Tablo I: Sentetik veri üzerindeki sonuçlar

yazılabilir:

$$\begin{aligned} p(r_t, \pi_t, x_{1:t+L}) &= p(r_t, \pi_t, x_{1:t}) p(x_{t+1:t+L} | r_t, \pi_t) \\ &= \alpha_{t|t}(r_t, \pi_t) \beta_{t|t+1}(r_t, \pi_t) \end{aligned}$$

III. Deneyler

Önceki bölümde detaylarını sunduğumuz modelin nihai amacı SIP sunucularına yapılan saldırıların tespiti olduğundan, modeli besleyecek veriler korunması istenen sunucudan toplanmalıdır. Bu prototip çalışmada DDoS saldırılarının sunucu tarafında yoğun bir ağ trafiği yaratacağı düşüncesine dayanarak, sunucudan birim zamanda geçen 28 farklı tipte SIP mesajını saydık. Bu mesajlar, istemler ve cevaplar olarak iki kategori altındadır:

- İstemler: Register, Invite, Subscribe, Notify, Options, Ack, Bye, Cancel, Prack, Publish, Info, Refer, Message, Update
- Cevaplar: 100, 180, 183, 200, 400, 401, 403, 404, 405, 481, 486, 487, 500, 603

Benzetim verilerinin üretimi için bir SIP sunucusu, sunucu üzerindeki ağ trafiğini üretecek ve (trafikle eşzamanlı) saldırıları gerçekleştirecek birer araç kullandık. Sunucu olarak Asterisk tabanlı Trixbox [7] sistemini tercih ettik. Trafik verisini üretmek için sunucuya kayıtlı kullanıcıları SIP protokolü kullanarak ve belirli bir olasılık modeli dahilinde gerçek zamanlı olarak birbirleriyle konuşturan bir benzetim birimi kullandık [8]. Son olarak, saldırı benzetimlerini gerçekleştirmek için NETAŞ tarafından geliştirilen NOVA V-Spy adlı araçtan faydalandık [9].

Yukarıdaki araçlarla hazırladığımız deney ortamı iki değişkenle kontrol edilmektedir:

- **Ağ Trafik Şiddeti:** Benzetim sisteminin birim zamanda ürettiği paket sayısına bağlı olan bir ikili değişken (düşük/yüksek)
- **Saldırı Şiddeti:** Saldırı aracının birim zamanda ürettiği paket sayısına bağlı olarak 2 değer alabilen bir değişken (düşük/yüksek)

Sıraladığımız değişkenlerin 4 farklı kombinasyonu bulunmaktadır ve her bir kombinasyon, farklı birer deney ortamına karşılık gelmektedir. Her bir deney ortamında NOVA V-Spy'ın üretebildiği 5 farklı DDoS saldırısını (Invite, Register, Options, Cancel, Bye) gerçekleştirdik. Her bir DDoS saldırısını, paketleri monoton ve dalgalı olmak üzere iki düzende üreterek yineledik. Düşük trafik şiddetinde 30, yüksek trafik şiddetinde 25 saldırı gerçekleştirdik. Her bir saldırı, başlangıç ve bitiş anlarında ağ trafiğinde önemli değişikliklere sahip olacağından ürettiğimiz veride toplam 110 değişim noktası bulunmaktadır.

Saldırı tespiti edici bir sistemin en temel iki başarım ölçütü saldırıları tespit etme ve doğru alarm verme oranlarıdır. Bu nedenle sistemin performansını kesinlik ve bulma oranıyla ölçtük:

$$\begin{aligned} \text{Kesinlik (K)} &= \frac{\text{Doğru alarmlar}}{\text{Doğru alarmlar + Yanlış alarmlar}} \\ \text{Bulma Oranı (B)} &= \frac{\text{Doğru alarmlar}}{\text{Tüm gerçek alarmlar}} \\ \text{F Ölçütü (F)} &= 2 \times \frac{K \times B}{K + B} \end{aligned}$$

İyi bir saldırı tespit yönteminde yukarıdaki değerlerin 1'e yakın çıkmasını bekleriz. Bu ölçütlere ilave olarak modelin saldırıları ne hızla tespit ettiğini göstermek için zaman duyarlılığını(T) tanımladık:

$$\text{T} = \frac{\text{Doğru alarmların gecikmelerinin toplamı}}{\text{Doğru alarm sayısı}}$$

Modelimizin yukarıda tanımlanan deney düzeneklerindeki performansı, Tablo I'de gösterilmiştir. Tablo I, modelin verdiği alarmlar ve saldırıların gerçekleştirildiği anlar doğrultusunda hesaplanan kesinlik, bulma oranı, F ölçütü ve zaman duyarlılığını göstermektedir. Tablodaki *BaB* ve *BiB* sütunları, sırasıyla saldırılarının başlangıç ve bitiş anlarının bulma oranlarına karşılık gelmektedir. Gerçekleşmesinden sonraki beş saniye içerisinde modelin alarm tepkisi verdiği saldırıları "tespit edilmiş", bu sürenin 5 saniyeden fazla olduğu saldırıları "ıskalanmış" olarak kaydettik.

IV. Sonuçlar ve Vargılar

Tablo I'deki en dikkat çekici nokta, denediğimiz tüm saldırı ve ağ trafiği parametreleri altında saldırı başlangıçlarının %100 başarımla saptanabilmesidir (bkz. BaB başlıklı sütun). Bu da DDoS saldırılarını saptayan bir sistemin sahip olması gereken en temel niteliklerden biridir. Öte yandan benzer başarım oranını saldırı bitiş anları için gözlemleyememekteyiz. Bu husus veri üreten modelinin özelliğinden kaynaklanmaktadır: Saldırı bitiş anlarında trafik değişimleri saldırı başlangıçlarına göre daha yumuşaktır ve bu da değişim noktası tespitini güçleştirmektedir.

Dikkat çekici başka bir sonuç, saldırı şiddetini artırmanın hem kesinlik hem de bulma oranı ölçütlerinde iyileşmeye yol açmasıdır. Beklenebileceği gibi şiddetin yüksek olduğu saldırılar (düşük şiddettekilere göre) ağ trafiğinde daha bariz bir değişime yol açar ve bu da değişim noktası tespitini kolaylaştırır.

Tablonun son sütunu, saldırıların ortalama kaç saniye gecikmeyle tespit edildiğini göstermektedir. Tabloya bakarak trafik ya da saldırı şiddetindeki değişikliklerin gecikme üzerinde ihmal edilebilir bir etkisi olduğunu söyleyebiliriz. İlaveten, kurduğumuz deney ortamı sunucu üzerinde 1 saniye boyunca toplanan verilerin modele girdi olarak iletilmesine izin vermektedir. Bu da tablodaki değerlerin kabul edilebilirliğini işaret eder.

Gerçek dünya senaryosunda kullanıcıların gün içindeki belli periyotlara bağlı bir ağ trafiğini yaratmaları beklenir. Bu durumu test etmek için, düşük ve yüksek trafik şiddetinde üretilen veri kümelerini birleştirdik. Modelin bu birleşik veri

kümelerini tespit ettiği ve edemediği değişim noktalarında bir değişiklik meydana gelmezken yanlış alarm sayısı 11'den 13'e yükseldi.

İGA'nın geri yönde özyineleme bölümünde kullanılan L değerindeki değişikliklerin modelin performansını nasıl etkilediğini inceledik. L değerinin çok büyük seçilmesi, başarımı iyileştirmezken işlem sayısını artırdığından kullanışlı değildir, küçük seçilmesi ise saptama başarımını düşürmektedir. Bu açılardan deneylerimizde L için 10 değerinin uygun olduğunu gördük.

Modeli test etmek için kullandığımız sentetik veri, SIP sunucusundan geçen paketlerden elde edilmiştir. Ancak her saldırının paket trafiğinde kolaylıkla fark edilebilir değişiklere yol açacağını söylemek doğru olmaz. Modelin bu gibi durumlarda da saldırıları tespit edebilmesi için, saldırıya işaret edebilecek başka tür verilere (örneğin SIP sunucusunun işletim sistemi istatistikleri) bakmak yerinde olacaktır. Bu ve benzeri çabaların, model başarımını artıracağını bekleyebiliriz.

V. Gelecek Çalışmalar

Bu çalışmada anlatılan model üzerinde pek çok irdeleme yapmak mümkündür. Model parametreleri r_t ve π_t'nin çevrimiçi öğrenilmesi bunlardan biridir. Buna ilaveten, grafik model üzerinde değişiklikler yapabiliriz. Örneğin, değişim noktalarının birbirlerinden bağımsız şekilde modellenmesi yerine r_t saklı değişkenlerini bir Markov zinciri kuracak gibi de düşünebiliriz. Ayrıca modeldeki saklı katman sayısını artırmak da mümkündür. İlave bir katman, ağ trafiğindeki periyodik değişimleri takip etmek üzere modellenebilir.

Modeldeki saklı değişken π_t, herhangi bir t anı için veriyi ürettiğini düşündüğümüz mekanizmanın parametrelerine karşılık geldiğinden benzer ağ trafiklerinin benzer π_t değerleri tarafından üretilmesini bekleyebiliriz. Dolayısıyla π_t parametrelerinin sahip olduğu değere bakarak, herhangi iki andaki saldırıların aynı olup olmadıkları hakkında fikir yürütebiliriz. Bir ileri aşama olarak değişik saldırıların π_t değerlerinden bir katalog meydana getirip yeni bir saldırının tipini hızla tahmin etmeyi düşünebiliriz.

VI. Bilgilendirme

Bu proje Boğaziçi Üniversitesi-NETAŞ ortak çalışması olup TEYDEB 3140701 nolu "Anomali Tespit ve Önlemede Öğrenen Sistem Mimarisi ile Birlikte Kalite Artırıcı ve Yüksek Hizmet Devamlılığı Sağlayan Zengin Servislerin VOIP Güvenlik Duvarı Ürününde Gerçekleştirilmesi" projesi kapsamında geliştirilmiştir. NOVA V-Gate ve NOVA V-Spy, NOVA Siber Güvenlik'in tescilli ticari ürünleridir.

Kaynakça

[1] www.us-cert.gov/sites/default/files/publications/understanding_voip.pdf

[2] H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler, J. Rosenberg, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[3] https://www.us-cert.gov/ncas/tips/ST04-015

[4] S. Ehlert, D.Geneiatakis, T. Magedanz, "Survey of network security systems to counter SIP-based denial-of-service attacks", Journal of Computers & Security, 225-243, 2010

[5] E. Y. Chen, "Detecting DoS attacks on SIP systems", 1st IEEE Workshop on VoIP Management and Security, 53-58, 2006.

[6] D. Barber, T.Cemgil, "Graphical models for time-series", Signal Processing Magazine, IEEE, 2010.

[7] http://www.fonality.com/trixbox

[8] B. Kurt, Ç. Yıldız, T. Y. Ceritli, M. Yamaç, M. Semerci, B. Sankur, A. T. Cemgil, "Olasılıksal SIP Ağı Benzetim Sistemi", 24. IEEE Sinyal İşleme ve İletişim Uygulamaları Kurultayı (Sunulacak), 2016.

[9] http://novacybersecurity.com/nova-vspy.html