SNMPv3 İLE GÜVENLİ AĞ TOPOLOJİ KEŞFİ

Musa BALTA[1] **İbrahim ÖZÇELİK**[2]

[1,2] Bilgisayar Mühendisliği Bölümü

Bilgisayar ve Bilişim Bilimleri Fakültesi

Sakarya Üniversitesi Esentepe Kampüsü 54187 Serdivan / SAKARYA

[1]e-posta: mbalta@sakarya.edu.tr [2]e-posta: ozcelik@sakarya.edu.tr

Anahtar kelimeler: Topoloji Keşfi, Snmpv3

ABSTRACT

This paper's aim is to discover an enterprise network which is created in a virtual enviroment with SNMPv3. An algorithm that is used previously in academic researchs, is redesigned for our topology according to security criterias. Thus, data can collected securely from SNMP devices in network without any data theft.

1.Giriş

Günümüzde kurumsal ağlar, gerek artan kullanıcı sayıları gerekse üzerlerinde çalışan uygulamaların fazlalığı yüzünden daha kompleks ve daha büyük yapılar haline gelmiştirler [1-4]. Büyüyen bu kurumsal ağlardan daha efektif ve verimli bir şekilde yararlanabilmek için en üst düzeyde yönetim ve bakım anlamına gelen ağ yönetim kavramı ortaya çıkmıştır. Ağ yönetimi sistemleri kendi içlerinde güvenlik, topoloji çıkartma, izleme, kontrol, koordinasyon ve planlama gibi birçok özellik barındırırlar. Bu özelliklerin efektif ve verimli bir şekilde kullanılabilmesi için öncelikle kurumsal ağın topoloji keşfinin ve cihazlar arasındaki bağlantıların iyi tespit edilmesi gerekir ki oluşturulacak olan ağ yönetim sistemi, yapılan bu topoloji keşfinin sonuçlarına göre en iyi şekilde tasarlanabilir.

Ağ topolojisi keşfi alanında kullanılan bir çok teknik vardır ve bu alanda bir çok akademik çalışma yapılmıştır. Ağ topolojisi keşfetmede ping, trace-route, DNS (Domain Name System-Alan Adı Sistemi) ve SNMP (Simple Network Management Protocol-Basit Ağ Yönetim Protokolü) gibi birçok teknik vardır [1-4]. Fakat bunlardan sadece SNMP diğerlerine oranla daha iyi ağ performansı sağlar ve sahadaki cihazların kendi aralarındaki bağlantılardan, cihaz tipine kadar tüm ağ bilgisini güvenli ve eksiksiz bir şekilde çekebilir.

Bu bildiride, SNMP' nin güvenlik versiyonu olan SNMPv3 kullanılarak oluşturulan algoritma sayesinde, sanal ortam üzerinde modellenen kurumsal bir ağ alt yapısının topoloji keşfi yapılacaktır. Önerilen algoritma sanal ortam üzerinde çalışacağı için gerçek ortamdan daha kısa sürede icra edilecektir.

2.SNMP (Basit Ağ Yönetim Protokolü)

SNMP, bir çok ağın yönetilmesinde kullanılan basit bir ağ yönetim protokolüdür. Genel itibariyle SNMP 3 yapıdan oluşur; ajan yazılımı (agent), SNMP-sunucusu (SNMP-server) ve bir de SNMP motorunun olduğu ağ yönetim sistemidir. SNMP'nin çalışma mekanizması istek gönderme ve isteğe cevap alma şeklindedir ve bunun için taşıma katmanında UDP protokolünü kullanır [5]. SNMP sayesinde bir cihazdan bilgi alınabileceği gibi, cihazdaki bilgi değiştirilebilir ve cihaza yeni bir yapılandırma uygulanabilir. Örneğin cihaz baştan başlatılabilir, cihaza bir yapılandırma dosyası gönderilebilir ya da cihazdan alınabilir.

SNMP cihazdan veri çekeceği zaman daha önceden tanımlanmış olan bazı değerleri kullanarak bu işlemi gerçekleştirir. Bu değerlere yönetim bilgi tabanı (MIB, Management Information Base) değerleri denir ve rakamlarla ifade edilir. Örneğin 1.3.6.1.2.1.1.5.0 değişkeni cihazın sistem adına denk gelmektedir [6,7].Bu yönetim bilgi tabanı değerlerinde ulaşılmak istenen değeri tutan

değişkenlere ise de nesne tanımlayıcısı (OID, Object Identifier) denir. Yönetim bilgi tabanı ve nesne tanımlayıcıların değerleri [8] nolu kaynaklarda bulunmaktadır.

SNMP, ağ güvenliğini sağlarken bazı kriterler kullanır. Bunlardan en önemlileri [8] :

- Kimlik doğrulama: Veri bütünlüğünü sağlar ve verinin kaynağını doğrular.
- Topluluk ismi: Yönetilen cihazlar ve SNMP arasında mesaj iletimi esnasında kullanılan doğrulama parametresidir.
- Şifreleme: SNMP paketlerini şifreler.
- Gizlilik: Ağdaki SNMP paketlerinin içeriğinin gizli tutulması.
- Güvenlik seviyesi: Her SNMP paketi üzerinde kullanılan şifreleme algoritmalarıdır. HMAC MD5, AES veya SHA kullanılır.
- Veri bütünlüğü: Bir mesaj paketi içinde parçalara bölünmemiş veri durumudur.
- SNMP kullanıcısı: SNMP yönetici işlemlerini yapan kullanıcıdır. Ağ yönetim sisteminden gelen SNMP mesajlarına göre ağın durumuyla ilgili değişiklik yapabilir.
- Güvenlik modeli: SNMP ajanı tarafından kullanılan güvenlik stratejisidir. Üç tanedir: SNMPv1, SNMPv2c, SNMPv3.

Bu güvenlik kriterlerini tüm SNMP versiyonları desteklemez. SNMP versiyonlarının güvenlik bazlı karşılaştırmalı tablosu aşağıda verilmiştir.

Tablo 1: SNMP güvenlik modelleri ve seviyeleri [8]

Model	Seviye	Kimlik Doğrulama	Şifreleme
v1	noAuthNo Priv	Topluluk ismi	Yok
v2c	noAuthNo Priv	Topluluk ismi	Yok
v3	noAuthNo Priv	Kullanıcı adı	Yok
v3	authNoPriv	MD5,veya SHA	Yok
v3	authPriv	MD5, veya SHA	DES

SNMPv3, yukarıdaki tabloda görülebileceği gibi güvenlik düzeylerinin hepsini destekleyebildiği için verilerin iletimi esnasında kullanılan şifreleme algoritmaları ile SNMP sorgularının daha güvenli bir şekilde kullanılmasını sağlamaktadır. Böylelikle SNMP paketleri de şifrelenmiş şekilde gideceği için ağ güvenliği sağlanmış olacaktır.

3.Ağ topolojisi keşfi uygulaması

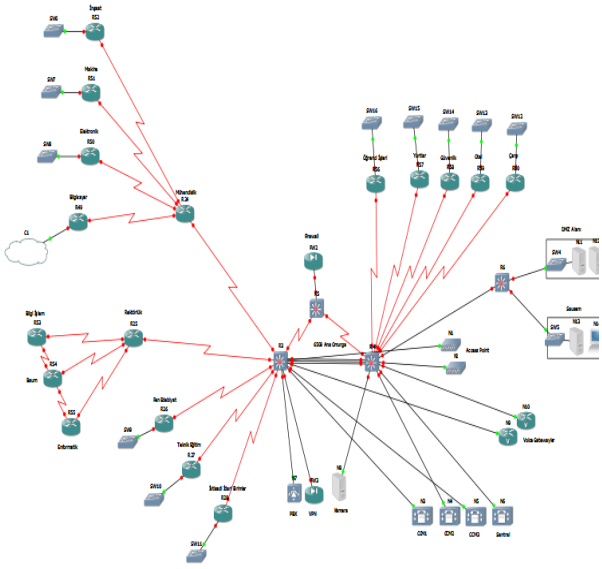
Ağ topoloji keşfi, birçok akademik çalışmaya konu olan geniş ve kapsamlı bir alandır [1-4]. Piyasada gerek ticari gerekse akademik birçok ağ topoloji keşfi yapan uygulamalar mevcuttur [9-10]. Yapılan bu çalışmaların çoğu gerçek ortamlar üzerinde yapılmaktadır. Uygulamamızda ana referans alınan çalışma [1] numaralı çalışmadır. Bu çalışmada da gerçek ortamda SNMPv2c ile sorgulama yapılarak topoloji keşfi yapılmaktadır. Bizim çalışmamızda ise kurumsal bir ağın topolojisi sanal ortamda oluşturularak güvenli bir ortam sunan SNMPv3 ile topoloji keşfi gerçeklenecektir.

Bu amaçla bir sonraki bölümde ilk önce modelleme ortamı ile alakalı bilgi, daha sonrasında ise topoloji keşfinde kullanılacak algoritma hakkında bilgi verilecektir.

3.1 Modelleme ortamı

Ağ topolojisinin modellenebilmesi için bir ağ modelleme simülatörü olan GNS3 (Graphical Network Simulator) programı kullanılmıştır. Cisco cihazlarını birebir gerçekleyebilen bir simülatör olduğu için GNS3 seçilmiştir [11]. Uygulama kodunun çalıştırılabilmesi için de VMWARE Workstation sanallaştırma programı üzerinde sanal makine oluşturulup gerekli bağlantılar yapılarak topolojiye ilave edilmiştir [12].

Sanal ortam üzerinde oluşturulan ağ yapısı (Şekil 1), 2 adet ana omurga Cisco 6509 anahtar cihazı etrafında modellenmektedir. Bunlardan birine, bir kurumsal ağın dış servislerini kurum dışı bir ağa (özellikle internete) açan ve ek bir güvenlik katmanı gibi çalışan sivil bölge (DMZ, Demilitarized Zone) alanı, kurum içi ve kurum dışı ağlara güvenli bir şekilde bağlanabilmeyi sağlayan sistem olan sanal özel ağ (VPN, Virtual Private Network) sunucuları, kurum içi iletişimi sağlayan çağrı yöneticileri (call manager) ve erişim noktaları (access point) bağlanmakta, diğer omurga anahtar cihazına ise kurumsal ağın akademik ve idari birimleri bağlanmaktadır.



Şekil 1: Örnek kurumsal bir ağ yapısı

GNS3 programında gerekli konfigürasyonlar (SNMP aktivasyonu, yönlendirici konfigürasyonları, Vlan (Virtual Local Area Network-Sanal Yerel Alan Ağı) konfigürasyonları, vb.) yapıldıktan sonra kurumsal bir ağ yapısının modellenmesi tamamlanır. Uygulama kodunun ve algoritmanın çalışacağı kısım ise VMWARE Workstation programında oluşturulmuş ve Şekil 1'de verilen topolojiye bulut olarak eklenmiştir.

3.2 Önerilen Algoritma

Önerilen bu algoritma, oluşturulan topoloji üzerindeki cihaz tiplerinden, cihazlar arasındaki bağlantıya kadar birçok konuyu ele almaktadır.

Algoritmayı yürütmeye başlamadan önce ağdaki tüm cihazların SNMP konfigürasyonlarının yapılması gerekir. Verilerin güvenli bir şekilde cihazdan okunabilmesi için SNMPv3 kullanılır. Cihaz üzerinde SNMPv3 aktif edilirken aşağıdaki sıra izlenir [5,8]:

- Grup oluşturulur: Tablo 1'deki güvenlik modeli (v3) ve güvenlik düzeyi seçilir. Aşağıdaki komut satırında aynı bölgedeki cihazlar için grup1 isimli grup oluşturmuş olup, güvenlik düzeyi v3 seçilerek bu gruba sadece "read" özelliği atanmıştır.

  snmp-server group grup1 v3 priv read grup1_oku

- Kullanıcı oluşturulur: Gruba eklenecek kullanıcılar güvenlik esaslarına göre oluşturulur. Burada oluşturulan güvenlik kriterleri için kullanıcı doğrulaması için "md5" algoritması, şifreleme için ise de "aes" algoritması kullanılmıştır.

  snmp-server user kullanıcı1 grup1 v3 encrypted auth md5 cisco priv aes 256

- Özellikler atanır: Oluşturulan gruplara "read, write ve notify" özellikleri atanır. Çalışmamız sadece topoloji keşfetme amacında olduğu için "read" komutu kullanılmıştır.

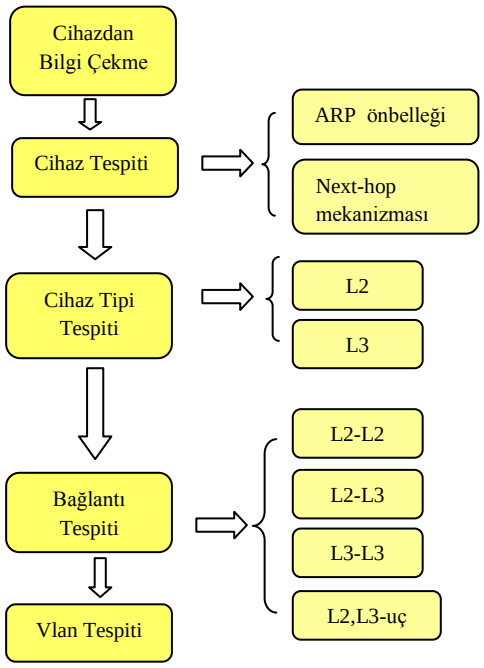
  snmp-server view izle system included

- VPN kullanıcıları için gerekli ayarlamalar yapılır. Oluşturulan gruplara "context ve match" parametreleri kullanılarak bir içerik tanımlanmalıdır.

Gerekli ayarlamalar yapıldıktan sonra algoritma çalıştırılmaya hazırdır. Daha öncede ifade edildiği gibi SNMP protokolü istek gönderme ve isteğe cevap şeklinde çalışır [4]. Cihazın sistem bilgisi, üzerindeki yönlendirme tablosu, mac adres tablosu, cihaz üzerinden geçen paket sayısı gibi cihazla ilgili tüm bilgiler MIB denen değerlerle ifade edilir. Yani cihazdan ilgili veri çekileceği zaman o veriyle alakalı olan MIB değeri sorgunun sonuna eklenir.

Algoritma da, cihazlardan dönen bu SNMP MIB değerlerine göre oluşturulmuş ve algoritmanın her aşamasında yapılan işleme göre MIB değerleri kullanılmıştır.

Uygulama için önerilen algoritma aşağıda verilmiştir. Bu algoritma, GNS3 modelleme programının anahtar cihazlar (switch) ve mantıksal topolojilerdeki bazı özellikleri desteklememesinden dolayı, [1] numaralı çalışmada önerilen algoritmanın özelleştirilmiş halidir:



Şekil 2: Önerilen Algoritma

Algoritmanın adımları:

- **Cihazdan bilgi çekme**: Sanal ortam üzerinde ağ topolojisi oluşturulduktan sonra cihazlar üzerinde konfigürasyon yapılır, daha sonra bu cihazlara SNMP sorgusu gönderilerek bilgi çekilir.

- **Cihaz tespiti**: ARP önbellek kayıtları ve Next-hop mekanizması kullanılarak, cihazlar üzerinden "ipNetToMediaNetAddress" ve "ipRouteNextHop" değerleri çekilir [13,14].

- **Cihaz tipi tespiti**: Cihazdan çekilen "sysServices" değerine göre cihazın L2 veya L3 cihaz olduğuna karar verilir.

- **Bağlantı tespiti**: Cihazlardan dönen ip ve mac adres eşleştirmeleri sonucunda aradaki bağlantının L2 bağlantı veya L3 bağlantı olduğuna karar verilir.

- **Vlan tespiti**: Cihazlardan dönen "Cisco-VTP-MIB" değeri kullanılarak vlan numarası ve ismi tespit edilir [15].

3.3 Uygulama geliştirme ortamları

Uygulama java programlama diliyle yazılmaktadır. Veritabanı olarak MySql kullanılmaktadır. SNMP kütüphanesi için Advent Net Java API'leri kullanılmaktadır [16]. Topoloji keşfinden sonra topoloji çıktısının grafiksel olarak görüntülenebilmesi için Java'nın grafik kütüphanelerinden JGraphT kullanılmaktadır [17].

Sonraki çalışma olarak, sanal ortam üzerinde oluşturulan kurumsal ağın içersinde kaç adet L2, L3 cihazın olduğu, bu cihazlar arasında hangi bağlantı türlerinin olduğu, oluşturulan Vlan (Sanal yerel ağ) isimleri ve numaraları belirlenip, topolojinin grafiksel olarak şeması çıkarılacaktır.

4.Sonuçlar

Bu çalışmada kurumsal bir ağ yapısının topoloji keşfinde gerçek bir ortam üzerinde çalışmak yerine fiziksel ortamdaki sıkıntılarla karşılaşmamak için sanal bir ortam üzerinde bir çalışma yapılmıştır. Sanal ortam için GNS3 ve VMWARE programları kullanılmış, bu programlar üzerinde gerekli konfigürasyonlar yapılmış ve güvenli bir ortam sunan SNMPv3 kullanılarak örnek bir kurumsal ağ yapısı oluşturulmuştur. Topoloji keşfi için daha önceden yapılan birçok akademik ve ticari uygulamada kullanılan teknikler göz önüne alınarak bir algoritma önerilmiştir. Bu algoritmanın uygulama geliştirme ortamları başlığı altında verilen araçlarla gerçeklenmesi sonraki çalışma olarak hedeflenmiştir. Bu hedefin gerçeklenmesi ile önerilen algoritmanın farklı topolojiler üzerinde çalıştırılmasına ve çıkan sonuçlara bağlı olarak topolojiler arasında performans testleri yapılmasına da imkan tanıyacağı sonuç olarak öngörülmüştür.

5. Teşekkür

Bu çalışma SAÜ Bilimsel Araştırma Projeleri Komisyonu tarafından desteklenmiştir. (Proje no: 2011-50-01-072)

6. Kaynakça

1.Pandey S. , Choi M. , Won Y. ,Hong J. , SNMP-based enterprise IP network topology discovery,In International Journal of Network Management 2011; Volume 21, Issue 3, May 2011, Pages: 169–184

2. Siamwalla R, Sharma R, Keshav S. *Discovering internet topology*. Technical report, Cornell University, May 1999.

3. Breitbart Y, Garofalakis M, Jai B, Martin C, Rastogi R, Silberschatz A. Topology discovery in heterogeneous IP networks:the NetInventory system. *IEEE/ACM Transactions on Networking* 2004; **12**(3): 401–414.

4. Lowekamp B, O'Hallaron DR, Gross TR. Topology discovery for large Ethernet networks. In *ACM SIGCOMM*, San Diego, CA, August 2001; 237–248.

5.http://www.dell.com/content/topics/global.aspx/power/en/ps2q03_maah?c=us&1=en&cs=555 [Ziyaret Tarihi: 25.07.2011]

6. JIZONG LI, WEB-based Network Monitoring Using SNMP, CGI and CORBA, in University of Manitoba, August 1999, 6:10-14:22.

7. E. MELLQUIST, SNMP++: An Object-Oriented Approach to Developing Network Management Applications, Prentice Hall PTR, 1997; 5:10:20-28

8.http://www.cisco.com/en/US/docs/ios/12_0t/12_0t3/feature/guide/Snmp3.html [Ziyaret Tarihi: 15.07.2011]

9. http://nmap.org/book/man.html [Ziyaret Tarihi: 16.07.2011]

10.http://www.paessler.com/manuals/prtg8/quick_start_guide.htm [Ziyaret Tarihi: 16.07.2011]

11.http://www.gns3.net/documentation [Ziyaret Tarihi: 25.06.2011]

12. http://www.vmware.com/support/pubs/[Ziyaret Tarihi: 25.06.2011]

13. Cisco. SNMP community string indexing. http://www.cisco.com/en/US/tech/tk648/tk362/techn

ologies_tech_note09186a00801576ff.shtml [Ziyaret Tarihi: 27.07.2011].

14. Bierman A, Jones K. Physical topology MIB. *IETF RFC-2922*, September 2000.

15.CISCO-VTP-MIB http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a00801576ff.shtml [Ziyaret Tarihi: 05.07.2011].

16. AdventNet. AdventNet SNMP API. http://snmp.adventnet.com/[Ziyaret Tarihi: 01.07.2011].

17. JGraphT. Implementation and source code. http://jgrapht.sourceforge.net[ZiyaretTarihi:02.07.2011]