İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

TASARSIZ AĞLARDA SAHİPSİZLİK DURUMUNUN İNCELENMESİ

YÜKSEK LİSANS TEZİ

Müh. Mustafa DAYIOĞLU

Tezin Enstitüye Verildiği Tarih : 08 Mayıs 2006
Tezin Enstitüye Savunulduğu Tarih : 29 Mayıs 2006

Tez Danışmanı : Prof.Dr. Eşref ADALI
Diğer Jüri Üyeleri : Prof.Dr. Coşkun SÖNMEZ (Y.T.Ü)
Yrd.Doç.Dr. D. Turgay ALTILAR

HAZİRAN 2006

ÖNSÖZ

Yüksek lisans tez çalışmam sırasında yardımlarını ve desteklerini eksik etmeyen başta değerli tez danışman hocam Prof. Dr. Eşref ADALI'ya, Bilgisayar Mühendisliği A.B.D'deki öğretim üyelerine ve bölüm sekteremiz Zuhal Yılmazer'a teşekkür ederim.

Mayıs, 2006 **Mustafa DAYIOĞLU**

İÇİNDEKİLER

KISALTMALAR

ANODR **:** Anonymous On Demand Routing
AODV : Ad-Hoc On-Demand Distance Vector
KTAMG : Küme Tabanlı Anomin Mesaj Gönderme
DC-nets : Dining Cryptographer Networks
DSR : Dynamic Source Routing
IDS : Intrusion Detection System
IP : Internet Protocol
ISDN **:** Integrated Services Digital Network
YCEV **:** Yönlendirme Yanıtı
YİS **:** Yönlendirme İsteği
TTL **:** Time to Live
TCP **:** Transmission Control Protocol
URL **:** Uniform Resource Location

TABLO LİSTESİ

Sayfa No

ŞEKİL LİSTESİ

Sayfa No

TASARSIZ AĞLARDA SAHİPSİZLİK DURUMUNUN İNCELENMESİ

ÖZET

Bu çalışmada, gezgin ağlarda sahipsizlik hususları tanımlanıp, sahipsiz sistemler için gerekli güvenlik mekanizmaları oluşturulmuştur. Sahipsizlik herhangi bir küme içerisindeki birbirleriyle haberleşen iki elemanın haberleşme kimliklerinin tanımlanamaması olarak tanımlanmaktadır. İnternet üzerinde sahipsiz e-posta ve web uygulamaları değişik amaçlar için kullanılmaktadır. Bu kavram mobil ağlara daha yeni uyarlanan bir kavramdır. Bu yüzden mobil ağlarda sahipsizliğin garanti edilmesi gerekliliği vardır. Sistemlerde sahipsizliği etkileyen iki tür tehdit vardır. Bu tehdiler sırasıyla pasif ve aktif tehditlerdir. Bu kapsamda pasif tehditlere dirençli anomim sistemler üzerinde yoğunlaşılmıştır. Sahipsiz haberleşen sistemleri oluşturmak için iki farklı güvenlik mekanizması önerilmiştir. İlk olarak önerilen güvenlik mekanizması imgesel yönlendirme yöntemidir. Bu yöntem yüksek hat geçikmeli sistemler için şifreli işlem yükünü azaltmıştır. İkinci yöntem küme tabanlı mesajlaşma düşük hat geçikmesi gerektiren sistemler için sahipsiz iletilişimin güvenliği sağlanmaktadır. Önerilen çözümlerin ardından simulasyon uygulaması gerçekleştirildi. Gerçekleştirilen simulasyon uygulaması önerilen çözümlerin doğruluğunu kanıtlanması açısın iyi sonuçlar vermiştir.

RESEARCHING ANONYMITY CONDITIONS FOR AD HOC NETWORKS

SUMMARY

In this study; Anonymity is defined for mobil networks. Security mechanism is constructed for anonym systems. Anonymity which means hiding identity of one's participation in a communication can be required as a security mechanism in critical networks. In Internet, anonymous e-mail or web applications are used for different purposes. On the other side, wireless adhoc networks are recently adapted to do critical missions in hostile environments. Anonymity must be also guaranteed in these systems. There ara two types of threat for anonym systems. These threats can be counted active and pasive threats. In this study, focused on passive threads for anonym systems. In order to create an anonymous system, new anonymous message sending methods for low delay needed adhoc network applications are designed. Newly designed methods are hoped to require less cryptographic operations and less amount of communication.Two different security mechanisms are proposed for constructing anonym systems. The first proposed security mechanism is route pseudonym method dealt with secure anonym routing. This method propose less cryptographic operation for high delay needed systems. The second method which is cluster based anonym message sending propose provide anonym communication for low delay needed systems. After proposed solutions, the simulation is constructed. The simulation is genarated bu using linux operating system functions and structures such as process, pipes, shared memory and semaphore. The simulation has give a good results to prove assumed solutions.

1. GİRİŞ

Günümüzde tasarsız ağlar bir çok değişik ortamda kritik öneme sahip uygulamalarda kullanılmaktadır. Tasarsız ağlar kolaylıkla dağıtık yapıda mimari oluşturulabildikleriden dolayı, kendi aralarında verileri herhangi sabit yönlendirme olmadan değiş tokuş edebilmektedirler. Günümüzde özellikle birçok askeri uygulamalarda tasarsız ağ uygulaması fikri çeşitli bilgilerin değişik kaynaklardan özellikle kontrollsüz düşman sahalarından toplanmasında bir çok kolaylıklar getirmektedir. Fakat bu tip ortamlarda toplanan bilginin sadece bütünlüğünün ve gizliliğinin sağlanması çoğu zaman yeterli olmamaktadır. Bu tip ortamlarda akış halinde olan bilginin düşman tarafından dinlenmesi veya tespit edilmesi söz konusu olduğundan dolayı taşınan bilginin sahipsizlik özelliğinin; yani bilginin kaynağı ve hedefi ile ilgili kimlik bilgilerinin de gizlenmesi gerekmektedir. Sahipsizlik özelliği sağlanarak gönderilen mesajlar sayesinde bilginin kaynak, hedef kimlik bilgileri ve bilginin aldığı yol gizlenmiş olduğundan bu sayede tasarsız ağı oluşturan ve üzerinde bilginin akışını taşıyan bileşenlerin tespiti zorlaşmaktadır.

Fakat günümüzde kullanılan bir çok tasarsız ağ; ağ trafik analizi yöntemi sayesinde tasarsız ağlarda sahipsizlik özelliği devre dışı bırakılabilmektedir. Bu kapsamda tasarsız ağlarda sahipsizliğin sağlanması için kullanılan mekanizmalar trafik analiz yöntemlerine karşı dirençli olarak tasarlanmalıdır. Ayrıca günümüzdeki gerçekleştirilen bazı çalışmalar tasarsız ağlarda sahipsizlik özelliğinin tasarsız ağlara bazı zayıflıklar getirdiğini göstermektedir. Bu zayıflıklardan en önemlisi; sahipsizlik özelliğine sahip olan tasarsız ağlar hizmet dışı bırakılma saldırılarına karşı dirençsiz kalmaktadırlar. Ayrıca ek bant genişliği gereksinimi ve enerji tüketimi de sahipsizlik mekanizmasına ait bazı zayıflıklara örnek olarak verilebilir. Sonuç olarak tasarlanan sahipsiz tasarsız ağlarda bu tip zayıflıkların hepsinin aynı anda ortadan kaldırılması imkansız gibi gözükmektedir. Bu sebeple sahipsiz tasarsız ağların tasarımı trafik analizine ve hizmet dışı bırakma saldırına karşı direnç, performans, bant genişliği ve enerji tüketimi parametreleri ihtiyaçlar göz önüne alınarak analiz edilerek gerçekleştirilmelidir.

Bu konu ile ilgili literatürde yapılan ilk çalışma sahipsiz olarak yayın mesajları göndermeyi hedefleyen şifreci profesörler (DC-net) [5] çalışması olarak geçmektedir. İkinci ve daha önemli olan çalışma ise karıştırma (Mixes) [6] çalışması olarak isimlendirilmektedir. Karıştırma isimli çalışma sahipsizlik durumunda traffik analizine dirençli çözümler getirmiştir. Sahipsizlik çalışmalarının bir çoğunda oluşturulan çözümler bu iki çalışmayı temel almaktadırlar. Şifreci profesörler çözümünü bir çok açıdan etkin bir çözüm olmadığından gerçek hayattaki uygulamalarda bu çözüm biçimine benzeyen çözümlere pek yer verilmemektedir. Karıştırma çözümü ise birçok uygulamada kullanılmasına rağmen, bu çözüm düşük geçikme gereken sistemlerde sahipsizlik seviyesinin düşürülmesine rağmen çok iyi sonuçlar vermemektedir. Karıştırma fikri özellikle tasarsız ağlara uyarlanmaktadır, fakat bu fikir çok yüksek seviyede şifre işlemi gerektirdiğinden bu tür uygulamalarda çok yüksek iletişim geçikmelerine yol açmaktadır.

Bu çalışmada ilk olarak iki yeni sahipsiz mesaj gönderme yöntemine yer verilecektir. Bu mesajlaşma yöntemleri şifreleme işlemlerini azaltıp, iletişim gecikmesini azaltmayı hedeflemektedir.

Bu çalışma kapsamında Bölüm 2'de sahipsizlik durumu ile ilgili detaylı bilgiye, farklı ağlarda örneğin internet, tasarsız ağlarda vb. sahipsizlik gerekliliklerine değinelecektir. Bölüm 3'te sahipsizlik gerektiren sistemlerle ilgili tehdit modeline değinilecektir. Bölüm 4'te sahipsizlik durumu ile ilgili gerçekleştirilmiş olan literatürde yeralan teorik ve uygulamada gerçekleştirilen çalışmalar gözden geçirilecektir. Bölüm 5'da ise sahipsiz mesaj göndermek için önerilen çözümün detaylarına değinilecektir.

2. ÖN BİLGİ

Bugüne kadar tasarsız ağ ve iletişim teknolojilerinde güvenlik üzerine gerçekleştirilen çalışmaların bir çoğu bilginin gizliliği, bütünlüğü ve iletişim ortamlarında tanımlama ve yetkilendirme hususlarının çözümü için gerçekleştirilmiş olup, bu konularla ilgili çeşitli çözümler oluşturulmasına rağmen sahipsizlik durumu ile ilgili günümüze kadar çok az çalışma gerçekleştirilmiştir.

Sahipsizlik herhangi bir küme içerisindeki birbirleriyle haberleşen iki düğümün haberleşme kimliklerinin tanımlanamaması olarak tarif edilmektedir. Sonuç olarak herhangi bir hizmeti kullanan kullanıcının hizmeti kullanırken kendi kimlik bilgisini açığa çıkartmaması da diğer bir sahipsizlik tarifi olarak ele alınabilir. Bu kısımda "Haberleşme Kimlikleri" olarak ip adresleri, düğümlerin kimlik numaraları vb. gibi ayırdedici özellikler örnek olarak verilebilir. Muhtemel alıcı ve gönderici düğümlerin oluşturuduğu kümeye sahipsizlik kümesi adı verilmektedir. Sahipsiz sistemde sistem dışındaki herhangi bir düğüm, sahipsizlik kümesi içerisindeki iletişimi ayırdedemez, etse de küme içerisindeki hangi iki düğümün haberleştiğini ayırdedemez.

İletilişim sistemlerini dinleyen yada gözlemleyen herhangi kötü niyetli bir düğüm mesajı gönderenin yada mesaj göndericisi-alıcısı ikilisini kritik seviyede mesajların iletişimi açısından öğrenmek isteyebilir. Alıcı sahipsizliği herhangi bir mesajının iletişim esnasında alıcısının kimliğinin belirlenmemesi/tespit edilememesi anlamına gelmektedir. Gönderici sahipsizliği ise herhangi mesajın gönderim esnasında mesajı gönderinin kimliğinin belirlenmemesi anlamına gelmektedir. Yada gönderici-alıcı sahipsizliği mesajın alıcı-göndericisinin arasındaki ilişkinin ortaya çıkarılmaması amacını taşımaktadır. Sonuç olarak farklı tehdit modellerine anominliğinin derecesi ihtiyaçlara göre değişmektedir. Örneğin her hangi bir durumda mesajın alıcı ve göderici ikilisinin gizlenmesi gerekebilirken, başka bir durumda ise bu ikiliden yalnız birisinin gizlenmesi gerekebilmektedir. Ayrıca herhangi bir mesajın gönderici ile

alıcının arasındaki ilişkinin gizlenmesine de mesajın bağlantısızlığı ismi verilmektedir.

Bilgisayar ağları arasındaki iletişimde mesajın kaynak ve hedef adresleri ağ paketlerinin içerisine gömülmektedir. Çeşitli ağ trafiği analizi yöntemleri kullanılarak paketler içerisindeki bilginin elde edilmesi suretiyle mesajlaşan düğümler arasındaki ayırt edici ağ trafiği iletişim örnekleri saldırganlar tarafından elde edilebilmektedir. Zaman bilgisi, iletişim süresi ve iletişim sırasında değiş tokuş edilen verinin miktarı gibi verilerle örnekler arasında iletişim ilişkilerinin oluşturulmasında önemli faydaları bulunmaktadır. Bu sebepten dolayı her nekadar iletişim esansındaki bilginin gizliliğini, bütünlüğü korunsa da bu durum önceki cümlelerde anlatılan sebeplerden dolayı iletişimde kullanılan gizlilik ve bütünlük kriterleri ağ trafiği analizini engelleyememektedir. İletişim halinde bulunan değişik ağlarda sahipsizlik çeşitli yöntemlerle sağlanmaktadır.

İnternet üzerindeki kullanıcılar hangi siteleri, hangi zamanlarda, ne kadar süre ziyaret ettiği gibi bilgileri kimse ile paylaşmak istemeyebilir. İnternet üzerinde bilgi paylaşımı sağlayan şirketler; hangi tür bilgileri, kimlerle paylaştıklarını açıklamak istemeyebilir. Tasarsız ağlarda yer ve hareket bilgilerinin dışarıdan tespit edilebilmesi önemli bir sorun haline gelmiştir. Özellikle askeri uygulamalarda istemcilerin hareket ve yer bilgilerinin düşman tarafından öğrenilmesi çok önemli bir açık olarak karşımıza çıkmaktadır. Bu tip ağlarda birçok yönlendirme mesajları kullanıldığında istemcilerin yada ağ elemanlarının hareket bilgilerinin ortaya çıkarılması çok çok kolaylaşmaktadır. Bu mesajlar sayesinde düğümlerin tespit edilmesi, düğümlerin antenlerinin kapsama alanında bulunan diğer düğümlere olan yolların ve dolayısıyla yer bilgilerinin tespit edilmesi sonucunda düğümler arasında iletilen mesajların izlediği yolların da tespit edilmesi kolaylaşmaktadır. Düşmana ait dinleyici düğümlerin elde ettikleri yol bilgisi ve konum bilgisi sayesinde düğümlerin iletişimde oldukları diğer düğümlere ait bilgilere daha da kolay ulaşılmaktadır.

Tasarsız ağlarda mesaj yollarının dışarıdan öğrenilmesi tasarsız ağ yönlendirme protokollerinin özelliklerinden dolayı çok zor değildir. Tasarsız ağlarda hiçbir düğüm sabit olmadığı için yönlendirme mesajları mesaj yolu üzerindeki tüm düğümlere yönlendirilir. Tasarsız ağlarda en yaygın yönlendirme protokolleri yönlendirme mesajlarını açık olarak yani şifresiz olarak yönlendirmektedir. Bu sebepten dolayı

herhangi kötü niyetli düğümler yönlendirme mesajlarını dinleyerek tüm mesaj yollarını çıkarabilmektedir. Dinamik kaynak yönlendirme (DSR) [2] protokolünde yol bilgileri mesajın içerisinde gönderilmektedir. Kaynak, hedef ve tüm diğer yönlendirme noktaları tek bir yönlendirme mesajı ile elde edilebilmektedir. Tasarsız tasarsız ağlarda kullanılan "On Demand Distance Vector Routing" protokolünde [3], yönlendirme bilgileri yönlendirme tablolarında yer alır, istendiğinde gönderilir. Bu protokol sayesinde tasarsız ağlarda iz takibi dinamik kaynak yönlendirmesi kadar kolay olmasada bu protokol de sorunu tamamen çözmekte yetersiz kalmaktadır. Çünkü birlikte çalışan yada dağıtık yapıda çalışan kötü niyetli dinleyiciler mesajı kaynaktan hedefe doğru dinleyerek mesaj yolunu ortaya çıkarabilirler. Bu sebepten dolayı kötü niyetli dinleyicilerin her türlü ve sınırsız dinleme kabiliyetine sahip olduğu ve dağıtık yapıda çalışabildiği varsayıldığından dolayı bu algortimada tam olarak sahipsizlik durumunun çözümünü sağlayamamaktadır.

Sınırsız dinleme varsayımı; özellikle tasarsız ağ uygulamaları fiziksel olarak kontrol edilmeyen çevrelerde olduğu için çok gerçekçi bir hal almaktadır. Bazı uygulamalarda özellikle askeri olanları örnek verilmesi gerekirse, çoğu askeri tasarsız ağ uygulaması kontrol edilemeyen çevrelerde çalıştırılmaktadır. Bu durumda düşman bu çevrelerdeki ağ trafiğini pasif olarak gözlemleyerek ve herhangi bir şekilde varlığı belli etmeyerek tüm tasarsız iletişimini dinleyerek analiz edebilmektedir. Bu durum özellikle kritik ağ uygulamlarının bu tür kötü niyetli/düşmanların tehditlerine karşı güvenli bir şekilde uyarlanması gereğini ortaya çıkarmaktadır.

Yönlendirme mesajlarının güvenli hale getirilmesinden sonra, herhangi kötü niyetli kimseler düğümlere ait yer ve hareket bilgilerini elde edemeyecek olmalarına rağmen aynı güvenlik gerekleri yönlendirme mesajları haricinde düğümlerin diğer mesaj değişimleri için de sağlanmalıdır. Özellikle pasif saldırgan; düğümler arası zaman analizi gibi trafik analiz yöntemi kullanarak tasarsız ağ haberleşmesinde kolaylıkla iz takibi yapabilmektedir. Bu sebepten dolayı tasarsız ağlarda mesajların güvenliği için yeni yöntemlerin geliştirilmesine gerek duyulmaktadır.

Tasarsız ağlardaki elamanlar kendilerine ait kısıtlı kapasitedeki enerji pillerini kullanarak geniş coğrafi alanlara yayılabilmektedir. Tasarsız ağ elemanlarında enerji gereksinimi önemli bir yer tuttuğundan tasarsız ağ tasarımlarında enerji

gereksinimleri göz önüne alınmaktadır. Daha önceki paragraflarda anlatıldığı gibi, tasarsız ağlarda sahipsizlik özelliğini sağlamak için çeşitili mekanizmların kullanılması gerekmektedir, bu mekanizmalar tasarsız ağlarda daha çok ve yoğun işlem yapılmasını gerektirmektedir. Bu durum tasarsız ağ elemanlarında yüksek işlemci gerekliliği ve işlem yoğunluğu sebebiyle enerji tüketimini arttırmaktadır. Bu yüzden tasarsız ağlarda sahipsizlik özelliğini sağlayacak tasarımlar yapılırken enerji tüketimide göz önüne alınması gereken önemli faktörlerden biridir. Sahipsizlik özelliğini sağlayan algoritmaların düşük işlemli olması ve işlemci üzerine yük getirmemesi amaçlanmalıdır. Sahipsizlik özelliğini sağlayacak çözümler üretilirken çözümlerin hizmet dışı bırakma saldırılarına karşı etkin olması gerekmektedir. Sonuç olarak oluşturulan çözüm ağ trafik analizlerine karşı dayanıklı, performaslı, hizmet dışı bırakma saldırına direnebilen, düşük bant genişliği ve enerji tüketen olmalıdır.

3. TEHDİT MODELİ

Tasarsız ağlarda sahipsizlik durumu kapsamında tehdit modeli oluşturulmasında temel varsayım olarak kötü niyetli kişilerin tasarsız ağ trafiğini istediği gibi dinleyebilmesidir. Kısaca kötü niyetli kişilerin ağ trafiğini dinlemesi pasif saldırı olarak tanımlanmaktadır. Pasif saldırılar karakteristik olarak aktif saldırılardan farklıdır. Önerilecek modelimizde saldırgan tasarsız ağ elemanlarının yer ve hareket bilgilerini elde edene kadar tasarsız ağ elemalara karşı görünmez yada algılanmaz durumdadır. Saldırgan pasif olarak gerekli bilgileri topladıktan sonra esas saldırılarını gerçekleştirir. Bu sebepten dolayı bu tür saldırı çeşitleri saldırı tespit sistemleri tarafından saldırılar gerçekleştirilene kadar tespit edilememektedir.

Pasif saldırılar dışarıdan veya içeriden gerçekleştirilebilmektedir. Dışarıdan gerçekleştirilen pasif saldırılarda, saldırganın herhangi bir konağı ele geçirmesine gerek yoktur. Bu sebepten dolayı tasarsız ağlarda pasif saldırıları gerçekleştirmek isteyenlerin sadece tasarsız ağların kapsama alanlarında bulunmaları yeterli olduğundan bu tür saldıganların tasarsız ağ trafiğini sınırsız bir şekilde dinlendiği varsayılmaktadır. İçeriden yapılan pasif saldırılarda ise saldırgan herhangi bir alt ağı hedefleyerek o alt ağa ait şifeli yönlendirme bilgilerinin şifresini çözmeye çalışır. Bu sebeplerden bu iki tür saldırı tipi saldırı tespit sistemlerince tespit edilemez.

Bu modelde pasif saldırganlar herhangi bir agresif saldırı tipi göstermemektedirler. Fakat bu durum saldıganların sistem üzerinde herhangi bir mesaj göndermediği anlamına gelmemektedir. Saldırganlar sınırsız bir dinleme kabiliyeti kazanmak için her bir mesajlaşan gönderici-alıcılara ait bulguları analiz etmeli ve bulgular eşleştirmeledir. Eşleştirme işlemi için dinlediği düğümler arasında ek bir haberleşme aktivitesine de ihtiyaç duyulabilmektedir.

4. LİTERATÜR ARAŞTIRMASI

Sahipsizlik çalışmaları literatürde temel olarak iki teorik çalışmaya dayanır. Bu çalışmalar şifreci profesörler ağı (DC-Nets) ve karıştırma (mixes) çalışmalarıdır. Araştırmacılar arasında Karıştırma çalışmaları daha çekidir, bir çok araştırmacı yayınlarını ve uygulamalarını mix fikrinin değişik versiyonları kullanılarak hazırlamıştır. Bu bölümde şifreci profesörler ağı ve karıştırma modelleri gözden geçirilmiştir. Uygulamalarda bu modellerden yararlanılarak oluşturulan ve kullanılan önemli çalışmalara yerverilmiştir. Bu çalışmalar arasında tasarsız ağlarda sahipsizlik çözümleri gözden geçirilmiştir.

4.1 Şifreciler Profesörler Ağı (Dining-Cryptographer Networks)

Şifreci profesörler ağı (DC-Nets) [5]'te temel fikir yayınlanan mesajlarda gönderici sahipsizliğinin sağlanmasıdır. Bu kavramı en basit şekilde açıklamak için bu örnek açıklaycı olacaktır. Yuvarlak bir daire etrafında n adet düğümün yerleştiğini düşünün. Bu düğümler P_1, P_2,.....,P_{n-1},P_n olarak numaralansın. Bu durumda Pi 'nin komşusu P_{i-1} ve P_{i+1} olacaktır. Sonuç olarak elimizde n adet komşu ikili olacaktır. $N_{(h,i)}$ komşu olan P_h, P_i ikililerini temsil etmek için kullanılısa, P_i düğümü $N_{(h,i)}$ ve $N_{(h,j)}$'nin komşu ikilisinin elemanıdır.

Her bir $N_{(h,i)}$ ikilisi kendi aralarında bir adet paylaşacakarı gizli anahtar $b_{(h,i)}$ seçerler. $b_{(h,i)}$ olarak adlandırılan gizli anahtarı yalnızca P_h ve P_i bilmektedir. Sonuç olarak toplam tüm komşu ikililer arasında toplam n adet paylaşılan anahtar olacaktır. Pi olarak sembolleştirilmiş her bir düğüm $b_{(h,i)}$ ve $b_{(i,j)}$ (P_h ve P_j komşulardır) olmak üzere iki adet paylaşılan anahtara sahip olacaktır.

Pi düğümü s_i mesajını sahipsiz olarak gönderebilmek için $v_i = b_{(h,i)} \oplus b_{(i,j)} \oplus s_i$ değerini hesaplamanın sonucunda elde edilen değeri diğer düğümlere gönderir. Hesaplanan v_i değeri tüm düğümler için bilinen değer olmaktadır. Fakat hesaplanan tüm v değerleri tüm düğümler tarafından bilindiğinde,

gönderilecek mesajın varlığı oluşturulan tüm v_i değelerinin XOR'lanması sonucunda elde edilir. XOR işleminin sonucu aşağıdaki gibidir.

$$s = v_1 \oplus \cdots \oplus v_n \quad \textbf{(5.1a)}$$

$$s = (b_{(n,1)} \oplus b_{(1,2)} \oplus s_1) \oplus \cdots \oplus (b_{(n-1,n)} \oplus b_{(n,1)} \oplus s_n) \quad \textbf{(5.1b)}$$

$$s = (b_{(n,1)} \oplus b_{(n,1)} \oplus s_1) \oplus \cdots \oplus (b_{(n-1,n)} \oplus b_{(n-1,n)} \oplus s_n) \quad \textbf{(5.1c)}$$

$$s = s_1 \oplus \cdots \oplus s_n \quad \textbf{(5.1d)}$$

Buradaki varsayıma göre kavram en çok bir düğümün aynı anda tek bir mesaj göndermesi durumda işe yaramaktadır. Eğer aynı zaman diliminde hiç bir düğüm mesaj göndermezse ifadelerden elde edilen değer herzaman sıfır olacaktır. Eğer sadece bir düğüm mesaj gönderirse ifadenin sadeleşmesi sonucunda sadece gönderilecek mesaj elde edilecektir. Bu sayede tüm düğümler sadece bir mesajın gönderildiği durumunda mesajın varlığını tespit edeceklerdir. Bu durumda sadece mesajın varlığı tespit edilecek, fakat mesajı gönderen tespit edilemeyecektir. Bu duruma kısaca gönderici sahipsizliği ismi verilmektedir.

Bu konu ile ilgili önceki paragraflarda verilen örnek en basit durumu ifade etmekteydi. Önceki örnekte düğümler dairesel şekilde dizilmekteydi. Fakat gerçek hayata düğümler dairesel şekide dizilmemektedirler. Çoğunlukla düğümler dairesel olmayan topolojiler oluşturmaktadır. Bu tür durumlarda düğümler kendi içlerinde birbirinden farklı düğümlere farklı şekillerde bağlanabilmektedirler. Bu durumda DC-Nets fikrinin uygulanması bakımından, grafik üzerindeki herhangi bir ayrıt en az iki düğümün birleşmesi sonucu oluşmaktadır. Ayrıtı oluşturan düğümleri Px ve Py olarak adlandırırsak, ayrıtı da Kx,y olarak adlandırabiliriz, aynı zamanda Kx,y ayrıtı Px, Py arasındaki paylaşılan anahtarı ifade etmektedir. Eğer herhangi bir Pi düğümü M mesajını göndermek isterse aşağıdaki ifadeye göre yayın mesajı oluşturur.

$M \otimes \sum$ işaret (i-j) . $K_{i,j}$ ➔ Mesajı gönderen düğümü ifade eder. **(5.2)**

$\forall j$ s.t $\{ P_i, P_j \} \in G$

işaret (a) = 1 eğer a >1, değilse işaret (a) = -1

G: düğüme komşu olan tüm düğümlerin kümesi

Pi haricinceki diğer katılımcılar (Pj) aşağıdaki ifadeyi yayınlar.

$\sum$ işaret (j-k) . $K_{j,k}$ ➔ Mesajı göndermeyen düğümü ifade eder. **(5.3)**

$\forall j$ s.t $\{ P_i, P_j \} \in G$

işaret (a) = 1 eğer a >1, değilse işaret (a) = -1

G: düğüme komşu olan tüm düğümlerin kümesi

Eğer herhangi bir katılımcı mesaj almak isterse, tüm yayın mesajlarını toplar. Mesaj almak isteyen katılımcı bir düğümden (x-y)Kx,y mesajını alırken, diğer düğümdende (y-x)Ky,x mesajını almaktadır. Kx,y = Ky,x olduğundan (x-y)Kx,y + (y-x)Ky,x = 0 olacaktır. Yayın mesajlarının toplamı sonucunda bu tür ifadeler birbirini götüreceğinden sadece M mesajı elde edilecektir. Eğer M mesajı belli bir alıcıya gönderiliyorsa mesaj alıcının açık anahtarı ile şifrelenir, bu durumda mesajı bir çok düğüm elde etmesine karşın sadece bir düğüm açacağından böylece alıcı sahipsizliği sağlanmış olacaktır.

4.1.1 Şifreci Profesörler Ağı (DC-NETS) Çözümünün Eksiklikleri

Şifreci profesörler (DC-Nets) çalışması uygulamada birçok dezavantaja sahiptir. Bunlardan ilki alıcı sahipsizliğinin sağlanması için tüm düğümlerin açık/gizli anahatar ikilisine sahip olması gerekmektedir. Fakat düğüm sayısının çok olduğu ağlarda anahtar dağıtımı ve yönetimi çok zorlaşmaktadır. İkinci dezavantaj olarak; eğer aynı anda iki düğüm mesaj göndermek isterse gönderilen iki mesaj toplanacak ve bunun sonucu olarak gönderilecek mesajların içeriği bozulacaktır. Alıcı düğümler hiç bir zaman mesajı alamayacaklardır. Bu yüzden aynı anda sadece bir adet mesajın

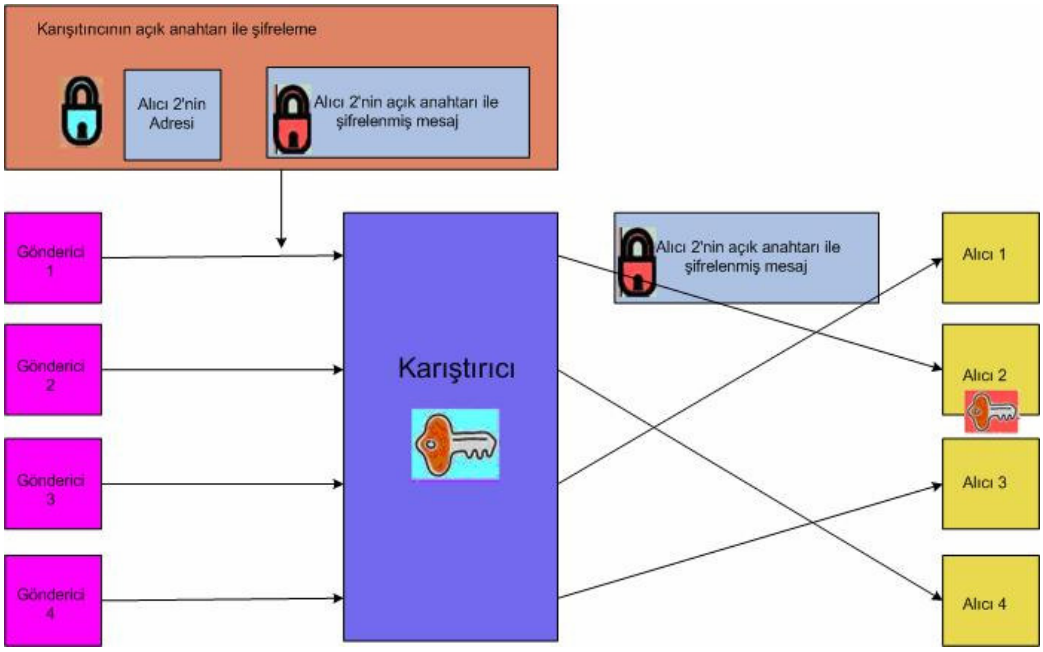
gönderilmesinin garanti altına alınması gerekmektedir. Bu durumda çok önemli bir dezavantaj getirmektedir. Eğer kötü niyetli bir kullanıcı tüm zaman dilimlerinde sisteme gereksiz mesajlar gönderek diğer gönderilen mesajların içeriğinin bolzulması suretiyle sisteme hizmet dışı bırakma saldırısı gerçekleştirmiş olacaktır. Bu tipte servis dışı bırakma saldırılarına karşı üretilen çözümler sistemin verimliliğini etkilemektedir. DC-Nets çalışmasına ait sorunlardan en sonuncusu; eğer mesajı almak isteyen düğüm tüm yayın mesajlarını toplayamazsa yada en az bir adet yayın mesajını kaçırırsa düğüm üzerine yapılan işlem sonucunda ortaya anlamsız içerikte bir mesaj çıkacaktır. Sonuç olarak DC-Nets çok yüksek iletişim güvenilirliğinin olduğu iletişim ortamlarında kullanılmaktadır. Buna örnek olarak halka topolojisinin olduğu iletişim ortamlarımda DC-Nets çözümleri başarı ile çalışmaktadır.

4.2 Karıştırma (Mixes)

Karıştırma (Mixes) [6] gönderici- alıcı sahipsizliğinin sağlanması ve ağ trafiğin analizlerine karşı konulması bakımandan önemli bir fikirdir. Burada gönderici düğüm alıcı düğüme kadar olan f_1, f_2, f_3 ..... f_D ile sembolleştirilen iletici düğümlerin hepsini bilmektedir. İlk olarak gönderici mesajı f_D açık anahtarı ile şifreler. Bunudan sonra da sırasıyla mesaj f_{D-1}, f_{D-2} ... f_2, f_1 açık aanahtarlarıyla şifrelenir. M şifrelenmemiş mesaj, fx ise açık anahtar olarak tanımandığında açık anahtar şifreleme işlemi $E_{fX}(M)$ ile tanımlanmaktadır. Buna göre sırasal şifreleme işleminin yapısı; $E_{fD}(E_{fD-1}\, E_{fD-2}\, (\ldots\ldots E_{f2}\, (E_{f1}(M)))\ldots)$ olarak gösterilmektedir.

Mesaj yolu üzerindeki her düğüm aldığı mesajı kendi gizli anahtarı ile açar, actığı mesajı bir sonraki düğüme yönlendirir. Burada mesaj yolunun ilk düğümü gerçek gönderici, en son düğümü ise alıcı düğümdür. Bundan dolayı aradaki diğer düğümler sadece aldıları mesajı yönlendiren düğümlerden ibarettir. Bu düğümler sadece bir önceki ve sonraki düğüm bilgisine sahiptir. Bu durumda herhangi bir ağ dinleme aktivitesi sonucunda ağı dinleyen kişi mesajlara ait gönderici – alıcı adreslerini dinlemiş olduğu ağın trafiğini analiz etmeden tespit edemez. Özellikle mesajın içeriğinden yola çıkarak ağ trafiğini de analiz ettiğinde ise mesajın gönderici-alıcısına ilişkin çok değerli bilgileri elde edebilir. Bu tür saldırıların veya trafik analizlerinin önüne geçmek için ara düğümler aldıkları mesajları doğrudan ilerideki düğüme yönlendirmezeler. Aradaki düğümler aldıkları mesajları toplayıp, belirli bir

sayıyı bulunca mesajları toplu halde yolladıklarından trafik analizi tipi saldırıların önüne geçilmiş olur. Ayrıca bu tip saldırıların önüne geçmek için düğümlere gelen mesajlar rassal olarak yeniden sıralanıp, yeni sıraya göre düğümden çıkarlar. Bu sayede ağ trafiğini dinleyenler düğüme giren ve çıkan mesajlar arasında ilişki kurup mesajın göndericisi ile alıcısını bulamaz. Özellikle bu yöntem sayesinde sadece pasif saldırıların önüne geçmekten öteye aktif saldırılarında önüne geçilebilmektedir. Çünkü her yönlendirci düğüm yönlendirdiği mesaja ait bir önceki ve sonraki düğümü bilmektedir. Bu şekilde ara düğümlerden herhangi birisi ele geçirilmedikçe mesajın yolunun belirlenmesi mümkün olmamaktadır. Bu yöntem diğer metodlara göre daha aktif yada pasif saldırılara karşın yüksek güvenlik seviyesi sunmasına rağmen, bu yönteminde bir kaç eksikliği bulunmaktadır. Bunlardan birincisi mesajın iletilmesi sırasında her bir yönlendirici düğümde ek geçikmenin ortaya çıkmasıdır. Mesajın iletilmesinde birbirine zıt iki temel parametre ortaya çıkmaktadır. Bu parametreler sırasıyla geçikme ve trafik analizidir. Eğer mesaj iletim sırasında trafik analizi saldırıları en aza indirilmesi gerektiğinde, mesajın geçikmesi artmaktadır. Gecikmenin azaltıldığı durumlarda ise mesaj yolu üzerinde trafik analizi kolaylaşmaktadır. Mesajın iletilmesi sırasında bu iki parametre arasındaki uygun dengenin bulunması gerekmektedir. Fakat burada sistemin güvenliği yada iletişimin güvenliği ön planda olduğu için geçikme her zaman kabul edilebilecek parametrelerden olacaktır. Özellikle geçikme bazı uygulamlar için kabul edilebilir. Bu tip uygulamalara örnek olarak e-posta uygulamasını verilebilir. Bazı uygulamalar gecikmeye karşı duyarlı değildir. Örnek olarak web üzerinde gezinme çoklu ortam uygulamaları vb. geçikmeye karşın duyarlı değildir.



Şekil 4.1: Karıştırma uygulaması

Bu konuda ikinci sorun gönderici ile alıcı arasındaki yolun belirlenmesidir. Yol belirlemede temel olarak farklı iki yöntem kullanılmaktadır. Bu yöntemler sırasıyla "mix-cascade" ve "mix-nets" olarak adlandırılmaktadır. Mix-cascade ağlarda kullanıcı isteği yolu seçmekte özgür değildir. Kullanıcılar mesajı bir düğümden diğer düğüme gönderirken mesajın yolu önceden bellidir. Özellikle bu yöntemin hizmet dışı bırakma saldırılarına karşın zayıflıkları vardır. Özellikle mesaj yolunun üzerinde herhangi bir düğüm devre dışı kaldığında mesajın iletimi engelenmektedir. Bu yöntemde diğer bir dezavantajda saldırganın gönderici düğümle aradaki ilk düğüm arasındaki mesaj gönderimi engellemesidir. [10] Bu durum sistemdeki sahipsizlik seviyesinin düşmesine sebep olmaktadır. Ayrıca mix-cascade kullanıldığında mesaj yolunun yerel olarak düğümlerde bulunması gerekmektedir. Bu düğümlerden herhangi birisinin elegeçirilmesi sonucunda kullanıcılar arasındaki tüm yol bilgileri saldırganın eline geçmektedir. Mix-net yönteminde ise mesaj gönderilmeden mesaj yolu rassal olarak seçilmektedir. Mix-net yönteminde eğer saldırgan ağ trafiğini dinleyebiliyorsa sistem üzerinde kesişim saldırıları [16] gerçekleştirebilir. Kesişim saldırıları özellikle mesaj yolunun kısa olduğu durumlarda çok daha etkili olmaktadır.

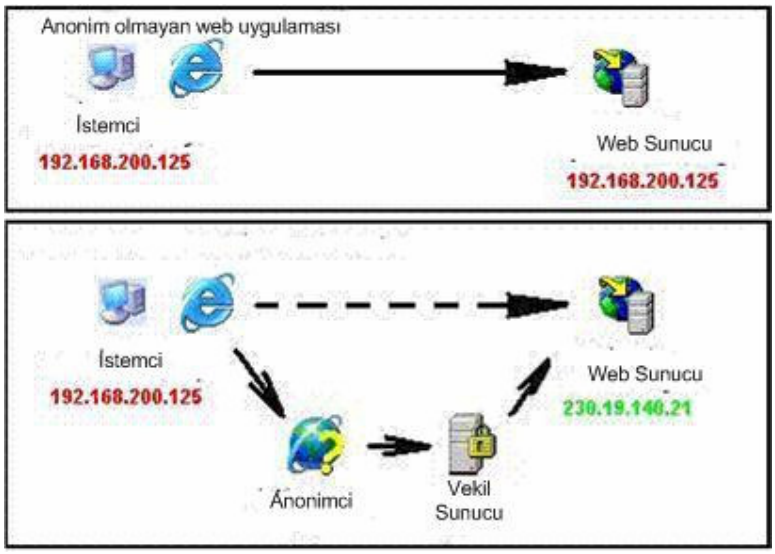
Karıştırma (mixes) fikri ISDN [8] gibi bazı düşük gecikmeli sistemlerde kullanılabildiği gibi, e-posta gibi gecikmeye duyarlı olmayan sistemlerde de kullanılabilmektedir.

4.3 Sahipsiz Uygulamalar

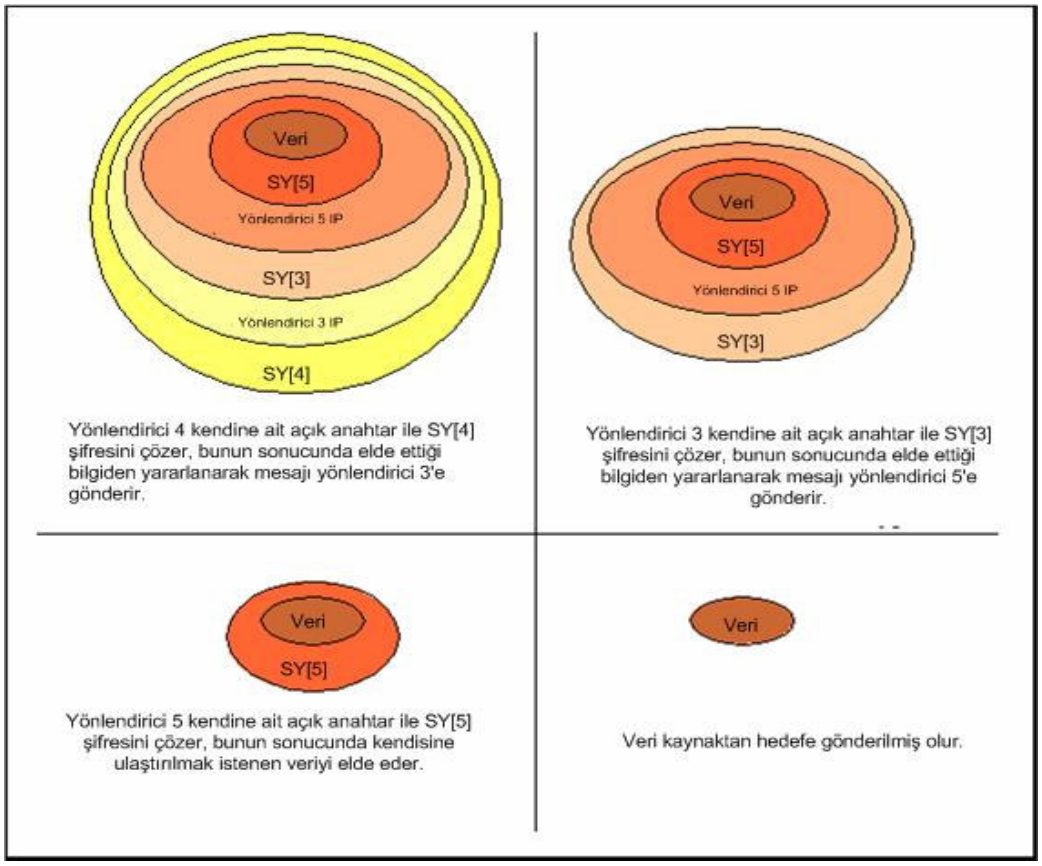
Web erişimi için kullanılan vekil sunucular internet üzerinde web erişimini hızlandıran sistemlerdir. Vekil sunucular kullanıcıların web erişimlerini hızlandırmalarının yanı sıra, web erişimlerinde kısıtlı da olsa sahipsizliği sağlamaktadır. Vekil sunucular kullanıcılardan gelen web isteklerini ön belleklerinde depolayıp, kullanıcılardan gelen URL istekleri internet üzerinden vekil sunucu internet üzerindeki ilgili URL'de bulunan sunucudan talep ederler. Eğer ilgili sunucu üzerindeki URL bulunuyorsa vekil sunucu kendisi üzerinden istekte bulunan istemciye ilgili URL'deki bilgiyi gönderir. Vekil sunucu ilgili URL'den kendi IP adresini kullanarak istekte bulunduğundan internet üzerinde dinleme kabiliyeti olan saldırganlar hiç bir zaman istekte bulunan istemciyi tespit edemezler. Bu sebepten dolayı vekil sunucuları kullanılması gönderici sahipsizliğini sağlamaktadır. Vekil sunucu arkasında bulunan tüm istemcilerde sahipsizlik kümesinin elemanı olmaktadır.

İnternet üzerinde sahipsizlik sadece vekil sunucularla sağlanmamaktadır. Güvenlik duvarları ve yönlendiriciler ağ adres dönüşümünü kullanarak sahipsizliği sağlamaktadırlar. Anonymizer [11] isimli uygulama vekil sunucuda bulunan çalışma modelini kullarak sahipsizliği sağlamaktadır. Buraya kadar verilen örnekler sadece tek vekil sunucu mimarisinin kullanıldığı örneklerden oluşmaktadır. Bir tek vekil sunucudan fazla sunucunun kullanıldığı uygulama örneği olarak katmanlı yönledirme (Onion Routing) [13] örneği verilebilir. Bu örnekte vekil sunucular serisi kullanılmaktadır. 'Onion Routing' uygulaması temel olarak karıştırma fikrini kullanmaktadır. Kısaca kaynak mesaj için yolu belirler, mesajı gerekli şekilde şifreler. Bu örnekte her bir yönlendirici vekil sunucu mesajın şifresini çözer ve ilerideki vekil sunucuya aktarır. Bu uygulama gerçek zamanlı uygulamalarda kullanıldığından geçikme ve mesajların yeniden sıralanması karıştırma ağlara göre farklılık göstermektedir. Onion tipi yönlendiriciler farklı tiplerdeki trafiğin her birini

aynı kanal üzerinden gönderebilme kabiliyetine sahiptir. Sonuç olarak bu uygulamada ağ trafiği analizi yoğun çalışan oninon ağlarda başarılı olamamaktadır.

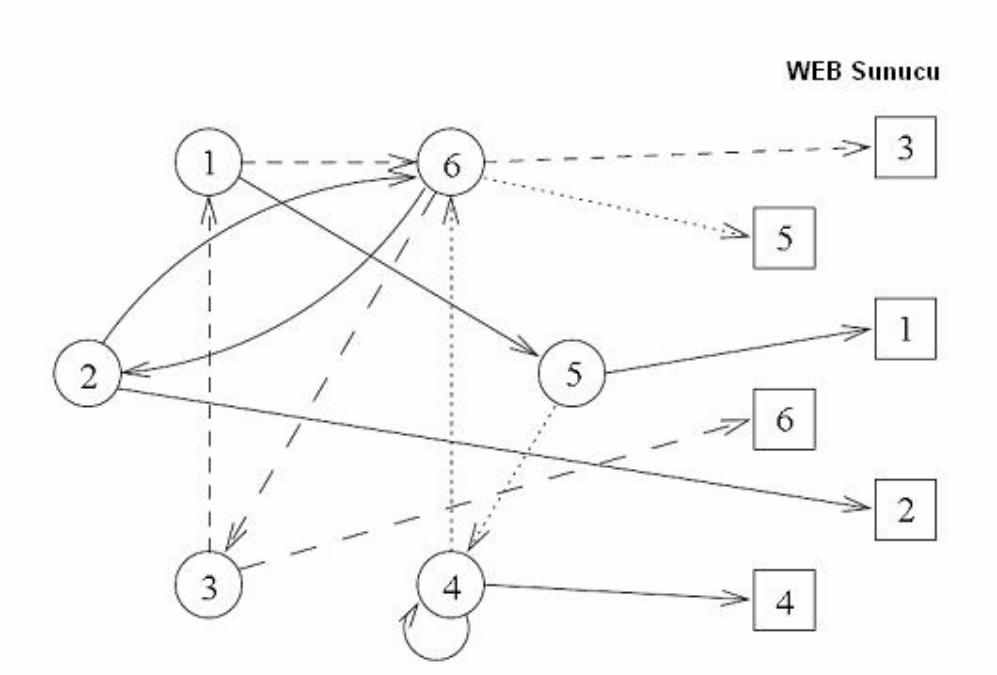


Şekil 4.2: Sahipsiz uygulaması



Şekil 4.3: Katmanlı (Onion routing) yönlendirme yapısı

Crowds [12] sahipsizlik gerektiren uygulamalarda kullanılan diğer bir sistemdir (Şekil 4.4). Sistemin kullanıcıları Crowds kullanıcı grubunu oluştururlar. Web sunucuya grup dışından gelen istekler grup içerisindeki herhangi bir kullanıcıya rassal olarak yönlendirilir. Yeni bir düğüm web sunucuya erişim için iki farklı seçeneğe sahiptir. Bu seçenekler sırasıyla; yeni düğüm sunucuya doğrudan istekte bulunur yada isteğini crowds grubunun içerisindeki her hangi bir düğüme yapar. Yapılan istekler grup içerisindeki herhangi bir düğüm hedefteki web sunucuya isteği gönderene kadar diğer düğümler arasında yönlendirilir. Grup içerisindeki düğümler arasındaki her bir iletişim iletişim halinde olan düğümler arasında kullanılan paylaşılan anahtarla şifrelenir. Grup içerisindeki iletişimi dinleyecek olan lokal dinleyiciler grup içerisindeki düğümler arasındaki iletişimi gözlemleyebilir, fakat grup içerisindeki herhangi bir düğümü ele geçiremedikçe yada ağ trafik analizi yöntemi kullanmadıkça alıcıyı tespit edemez. Grup içerisinde istekleri yönlendiren düğümler gerçek olan istemci olmadığından dolayı gönderici sahipsizliği sağlanmış olacaktır. Bu sistem genel olarak global ağ trafiğinin dinlenmesi veya ağ trafiği analizi durumundaki zaafiyetlere çözüm getirmez.



Şekil 4.4: Kalabalık (Crowds) uygulaması

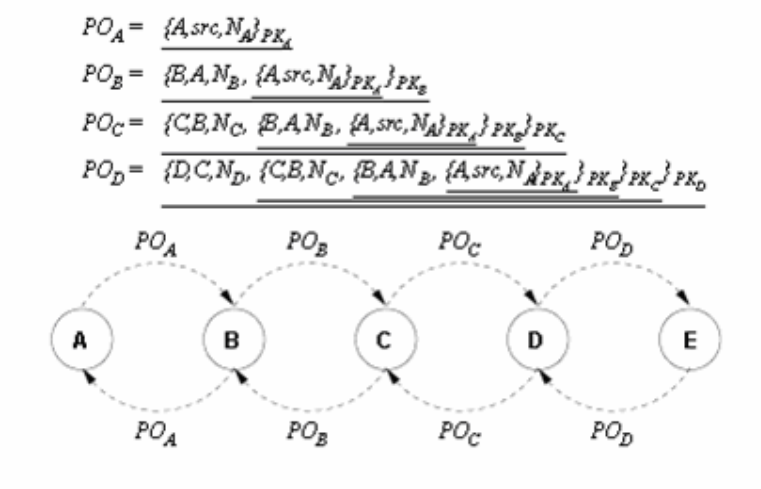
4.4 Tasarsız Ağlarda Sahipsiz Sistemler

Tasarsız ağlarda sahipsizlik çözümlerinin mahremiyetin sağlanması açısından yararları büyüktür. Çünkü her düğüm bu tip ağlarda yönlendirici gibi davranmaktadır. Düğümler arasındaki yönlendirme bilgilerinin değişimi sonucunda oluşan ağ trafiğinde çok değerli bilgiler bulunmaktadır. Kötü niyetli kullanıcılar sistemi dinlerken yönlendirme mesajlarını kullanırlar, bu sayede çok kolay şekilde mahremiyet ve sistem üzerindeki sahipsizlik ihlal edilmiş olacaktır. Sistem üzerinde sahipsizliğin sağlanması için ilk olarak sahipsiz yönlendirme protokollerinin geliştirilmesi gerekmektedir. Bundan sonra mesajlar oluşturulmuş olan sahipsiz yönlendirme protokolüne uygun olarak gönderilmelidir. Bu konu için ANODR (anonymous on demand routing) [18] isimli protokol önerilmiştir. İsteğe bağlı yönlendirme protokollerinde izleme diğer yönlendirme protokollerine çok daha karmaşıktır. Fakat işbirliği halinde olan ağ dinleyicileri tarafından iletişim çok kolay bir şekilde izlenebilmektedir. ANODR yönlendirme mesajlarının katmanlı (onion) yönlendirmeye göre yayınlanması sonucu yönlendirmelerin keşfedilmesi fikrine dayanmaktadır. Katmanlı yönlendirme sisteminde kaynak mesajı mesaj yolu üzerindeki ilk düğümden son düğüme kadar olan tüm düğümlerin açık anahtarına göre sıralı olarak şifrelemektedir. Burada asıl önemli olan husus; tam katmanlı mesaj kaynak düğümde oluşturulur. Kaynak düğümün mesajın izleyeği tüm yol bilgisine sahip olduğu kabul edilir. ANODR isimli yönlendirme protokolünde kaynak düğüm yol bilgisini bilmemektedir. Protokol yönlendirme keşif işlemleri sayesinde yönlendirme bilgilerini bulmaya çalışır. İlk olarak kaynak kapsama alanı içerisindeki düğümlere yönlendirme içerisinde özel bir fonksiyonu içeren yönlendirme mesajlarını yayınlar. Eğer mesajı alan düğüm bu mesajın kendine gelip gelmediğinin farkına mesajın içerisindeki özel fonksiyon sayesinde varır. Eğer bu mesajı alan düğüm mesajın kendisine gelmediğini anlarsa mesajı kendi açık anahtarıyla şifreleyip tekrar yayınlar. Bu durumda herbir yayın işlemi mesaj varışa ulaşana kadar mesaja bir katman daha katacaktır. Varış mesajı aldığında geri dönerek mesaj üzerine her bir katmanı koyan düğümlere gönderir, düğümler aldıkları mesajı kendi kapalı anahtarı ile açarlar ve mesaja yönlendirme bilgilerini girerip diğer düğüme göndereriler. Mesaj bu şekilde kaynak düğümüne kadar ulaşır. Kaynak düğümünde tüm yönlendirme bilgileri derlenerek mesajın varış düğümüne kadar olan yolu gerçek mesaj gönderilmeden evvel belirlenmiş olur. Bu sayede alıcı sahipsizliği yayın

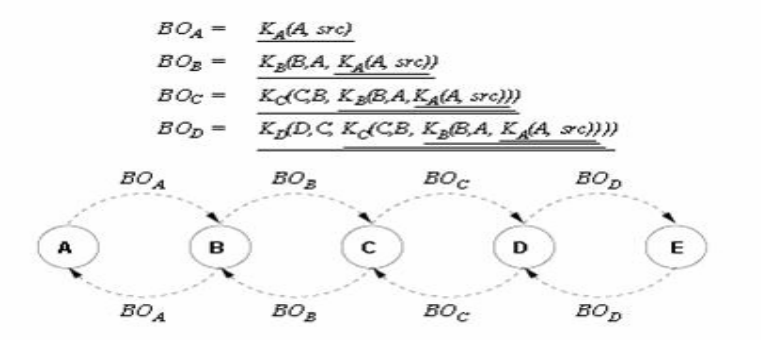
mesajları sayesinde, içerik eşleştirmelerinden korunma ise mesaj şifrelemeleri ve yönlendirme adları sayesinde gerçekleştirilmiş olur.

Tablo 4.1: Değişkenler tablosu

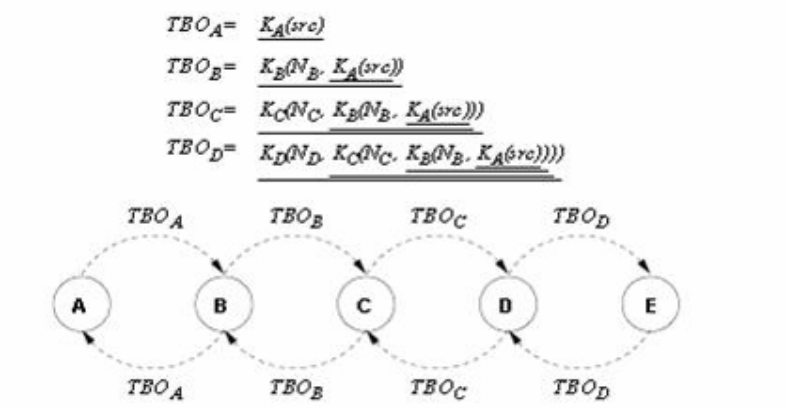
PK_A	Node A's public key	K_A	An encryption key only known by node A
SK_A	Node A's private key corresponding to PK_A	K_{AB}	An encryption key shared by node A and B
$\{M\}_{PK_A}$	Encrypting/verifying message M using public key PK_A	N_A, N_A^i	Nonce or nonces chosen by node A
$[M]_{SK_A}$	Decrypting/signing message M using private key SK_A	RREQ	Route Discovery Request Packet
$K(M)$	Encrypting/decrypting message M using symmetric key K	RREP	Route Discovery Reply Packet
src	a special tag denoting the source	RERR	Route Maintenance Error Packet
$dest$	a special tag denoting the destination	,	concatenation of appropriately formatted bit strings



Şekil 4.5: Açık anahtar şifresi kullanılarak yönlendirme keşfi



Şekil 4.6: Soğan yapısı kullanılarak yönlendirme keşfi



Şekil 4.7: Arka kapı fonkisyonu kullanılarak yönlendirme keşfi

5. ÖNERİLER

5.1 Tasarım Ölçütleri

Sahipsiz iletişimde, ilk olarak mesaj içerisinde açık olarak giden kaynak ve varış başlık bilgileri mutlaka mesaj içerisinden çıkarılmalıdır. Bu sayede mesajın dış kaynak tarafından dinlendiğinde mesajdaki kaynak ve varış bilgilerinin ele geçirilmesi önlenmiş olacaktır. İkinci olarak mesaj yolu üzerinde her bir gönderici düğümün mesaj için önceki ve sonraki düğüm bilgilerini her hangi ek yönlendirme bilgisine ihtiyaç duymadan bilmesi gerekmektedir. Fakat mesaj mesaj yolu üzerindeki tüm düğümlerin saldırganlar tarafından ele geçirilmesi durumunda mesaj için sahipsizlik ortadan kalkacaktır. Bu iki kriter katmanlı yapı (Onion Structure") olarak karıştırma (mixes) çözümünde ele alınmıştır, bu kısımla ilgili geniş açıklamaya literatür taraması kısmında yer verilmiştir. Üçünü olarak sahipsiz sistemler; ağ trafiğini dinleyenlerin trafik analizlerine karşı dirençli olmalıdır. Bu durum karşında yapılabilecek basit çözümlerden biri mesajları şifrelemektir.

Tasarsız ağ iletilşiminde herhangi bir ağ düğümü gönderici, alıcı veya yönlendirici düğüm olabilmektedir. Bir düğüme tüm giren ve çıkan mesajların içeriklerinin gözlemlendiği varsayımı altında, eğer bir mesaj bir düğüme girip diğer o düğümden çıkmışsa düğüm o mesaj için yönlendirici düğüm olarak adlandırılmaktadır. Genelde bir çok mesaj bir düğüme giriş yapar, girdiği gibi de o düğümden yönlendirilmektedir. Eğer saldırdan yönlendirici düğümlerde giren ve çıkan mesajlar için eşleştirme yapabilirse, saldırgan herhangi bir mesajı varış düğümüne kadar izleyebilecektir.

Ağ iletişiminde herhangi bir ağ düğümü gönderici, alıcı yada yönlendirici düğüm olabilmektedir. Ağ iletişiminde tüm mesajların içeriğinde bakılmaksızın ağ düğümüne girdiğini ve aynı şekilde çıktığı varsayılırsak; bu düğüm yönlendirici düğüm olarak adlandırılmaktadır. Genelde bir çok mesaj bir düğüme gidiği gibi aynı

zaman diliminden de o düğümden ayrılmaktadır. Eğer herhangi bir saldırgan tüm yönlendiricilere giren ve çıkan mesajlar arasında ilişki kurabilirse istediği mesajı varış adresine kadar takip edebilme kabiliyetine sahip olur. Sonuç olarak yönlendirici düğüme giren mesaj o düğümden çıkmadığında o düğüm varış düğümüdür. Bu sebepten gerçekleştirilecek tasarım bu durumlarda mesajın nereden nereye gittiğini dışarından kötü niyetli kişilerin öğrenebilmesini engellemelidir.

Mesajların eşleştirilmesi mesajın içeriğine veya zaman ilişkisine göre gerçekleştirilebilmektedir. Aynı içeriğe sahip mesajlarda mesajın boyu içerik eşleştirmesini kolaylaştırmaktadır. Bunun önüne geçmek için mesajları içeriğine dolgu mesajlar konarak tüm mesajlarının boyununu aynı düzeye getirerek bunun üzerine mesajları şifrelemek mesajlar için içerik eşletirmesini zorlaştırmakta ve saldırgaların bu tür yöntemleri kullanmasını caydırmaktadır. Mesajların eşleştirilmesinde mesajın zaman damgası diğer bir belirteçtir. Özellikle bir düğüme gelen mesaj ile aynı mesajın o düğümden ayrılması çok yakın zaman aralıklarında olduğu için mesaj eşleştirilmesinde zaman damgası kullanılmaktadır. Eğer yönlendirici düğüm kendine gelen mesajların geliş sırasının aksine mesajları düzenli olmadan mesaj iletimini değiştirebilirse saldırganın mesajını zaman damgası aracılığıyla mesajın izlemesinin önüne geçilmiş olacaktır. Kısaca bu işleme karıştırma (mixing) işlemi adı verilmektedir. Bu yöntem ağ iletişiminde paket gecikmesine yol açabilmektedir. Bu sebepten dolayı rassal olarak tuzak mesajlar göndermek diğer mesajları beklemekten daha iyi bir çözüm olabilmektedir.

Saldırganların pasif dinleme saldırıları gerçekleştirmelerinin yanı sıra aktif saldırıları da gerçekleştirme seçenekleri de vardır. Pasif saldırılar karşısında sisteminin direnç kazanması saldırganların aktif mesaj seli saldırıları gerçekleştirmesine sebep olmaktadır. Örnek olarak her hangi bir saldırgan mesajların dağıtıldığı ve mesaj sıralarını karıştıran düğüme n-1 adet mesaj gönderebilir. Karıştırıcı düğüm n adet mesajın gelmesini bekler ve gelen bu mesajları uygun varış noktalarına göndermek için rassal olarak dağıtır. Sonuç olarak saldırdan n-1 adet mesajı karıştırıcı düğüme gönderdiği için mesajların nerelere gideceğini de bilmektedir. Eğer saldırgan karıştırıcı düğümün çıkışını dinlerse, bu n mesaj içerisinde bulunan bir adet gerçek mesajında nereye gideceğini tespit etmiş olacaktır. Bu tip saldırıların önüne geçmek için sistemdeki kullanıcıların gönderdiği mesajın kimlik doğrulmasını yapması gerekmektedir. Burada mesaj kimlik doğrulamasının anlamı izin verilen bir hizmet

ve ağ trafiği için kontrol edilmesidir. Özellikle web karıştırma [16] uygulamasında çeşitli tür imzalar kullanılmaktadır. Bu tür imzalar sayesinde kullanıcılar kendilerinin kimliklerini karıştırıcı düğümlere sahipsiz olarak kanıtladığından dolayı mesaj seli türü saldırılar etkili olamamaktadır.

Normal tasarsız ağlarda, saldırganlar kullanıcıların sonlu zaman periyodu ağ trafiği örnekleri sayesinde sistemdeki kullanıcıların kimliklerini ortaya çıkarabilirler. Bu sebepten dolayı belirli bir zaman periyodunda gözlemlenen örneklerin artması sayesinde sistemdeki sahipsizlik derecesini düşürebilmektedir. Bu tip saldırılar genel olarak kesişim saldırıları olarak adlandırılmaktadır. Özellikle mükemmel bir sahipsiz sistemin bu tip saldırılara karşın dirençli olması gerekmektedir. Bu tip saldırılarda saldırganlar genel olarak gerçek gönderici ve alıcı kimliklerini tespit etmeyi amaçlamazlar, sadece sistem üzerinde sahipsizlik kümesini indirgemeyi amaçlarlar. Yapılan araştırmalardan elde edilen yayınlarda sahipsiz sistemlerde bu tip saldırılara karşı henüz etkin bir çözüm bulunamamıştır.

Düşük hat geçikmesi gereken sistemlerde; içerik eşleştirmesi saldırıları ve fiziksel düğümün ele geçirilme direnci tasarım kriterlerinin elemanları olarak seçilmektedir. Bu kapsamda zamanlama analizleri, sel ve kesişim saldırıları için tasarım kriterleri olarak ele alınmazlar. Bu kapsamdaki araştırmalar genelde internet uygulamaları (web uygulamaları) kapsamında sahipsiz sistem oluşturumak için gerçekleştirilir. Ancak internet uygulamalarında global dinlenme tehdidi sahipsiz sistem tasarımı için önemli bir sorun olarak düşünülmez. Bunun yanında tasarsız ağlarda global dinleme sahipsiz sistemler için oluşturulacak tehdit modelinin en önemli elementidir. Çünkü sensor ağ düğümleri fiziksel güvenlikten uzak olarak yabancı/düşman çevrelerde konumlandırılmıştır. Saldıganlar tüm iletişim hatlarını karşı sensör düğümler kullanarak dinleyebilirler.

Tasarsız sahipsiz ağların önem derecelerine göre konum bilgisi ve düğümlerin hareket bilgileri dış dünyadan gelen saldırganlar için çok önemlidir. Sahibi olmayan sistemlerde mesaj yolların takip edilmesiyle; birbirleri arasında kordineli olarak çalışan karşı/düşman düğümler mesajı gönderen ve alan düğümlerin yer bilgilerini elde edebilir. Yer bilgilerini tanımlarken yönlendirme yollarındaki değişikliklerin takibi saldırganlar için önemli bilgi kaynağı oluşturur. Saldırgan düğümler mesaj

alış/verişi içerinde olan takip edilemeyen yönlendirme şemalarını kullanan düğümlerin hareket bilgilerini de elde edebilir.

Sahipsiz ağlar ağ trafiğini izleyen pasif saldırılara karşı ve ağ iletişimi kapsamında yapılabilecek aktif saldırılara karşı ağı korumaktadır. Sahipsiz sistemler saldırganların sistemi meşgul eden yada sistemi çalışmaz hale getiren iletişim isteklerine karşın ek güvenlik fonksiyonlarına ihtiyaç duymaktadır. Bundan dolayı gerçek zamanlı çalışan ortamlarda sadece sistemin gözlemlenmesi veya dinlenmesi sonucunda ortaya çıkacak pasif saldırıları önlemek amacıyla bir model oluşturmak yeterli olmayacaktır. Oluşturulacak model sadece pasif saldırıları önleyebileceği gibi aynı zamanda aktif saldırılarıda önleyebilecek model olmalıdır. Bu kapsamda sahipsizliğin uygulandığı ağlarda hizmet dışı bırakma saldırılarına karşın sistem üzerinde anormallik analizine dayanan saldırı tespit sistemi yönteminin kullanılmasında fayda vardır. Ağ üzerindeki anormallik analizinde ağ üzerindeki normal ağ trafiği davranışı belirlenir, bu davranışın dışında olan ağ trafikleri sistemlere yapılan saldırı olarak algılanır ve gerekli önlemler alınır.

Sahipsizlik durumunun çözümünde sistemin durumunu etkileyebilecek bir çok parametre mevcuttur. Sistemin sahipsizliği sağlanmasında bu parametrelerden birisinin ön plana çıkması diğer paramaretyi arka plana itebilmektedir. Bu parametreler kısaca trafik analizi direnci, performans, hizmet dışı saldırılarına dayanıklılık, bant genişliği ve enerji sarfiyatı olarak sıralanabilmektedir. Örnek olarak vermek gerekirse sistemde trafik analizi direncinin arttırılması amaçlandığında sistemde hizmet dışı bırakma saldırılarına karşı zayıflıklar ortya çıkabiliyor. Trafik analizine direnç, performans ve enerji tüketimi parametreleri "İmgesel Yönlendirme" ve "Küme Tabanlı Sahipsiz Mesaj Gönderimi" çözümlerinde ele alınacaktır.

Tüm tasarsız ağlarda temel olarak iki temel ağ trafiği çeşidi mevcuttur. Bunlardan birincisi yönlendirme işlemi ile ilişkili olan ağ trafiğidir, bu trafik çeşidi düğümler arasında yönlendirme bilgilerinin taşınması, korunması ve paylaşılmasına olanak sağlar. İkinci tip trafik ise sahipsiz ağlarda uç noktaların haberleşmesi sırasında kullanılan mesajın içine gömülü yönlendirme bilgisine göre yönlendirilen mesaj trafiğidir. Sonuç tasarsız ağlarda sahipsizliğin sağlaması için her iki trafiğe ilişkin çözüm geliştirilmesi gerekmektedir.

Bu kapsamda önerilen ileriki bölümlerde değinilen imgesel yönlendirme yöntemi yönlendirme trafiğinin isteğe bağlı olarak ve sahipsiz olarak yönlendirilmesi ile ilgilidir. Gerçek mesajlardaki sahipsizlik karıştırma fikri ile garanti edilmektedir. Ancak imgesel yönlendirme ve karıştırma fikrinin birleşmesi ile oluşan çözüm karıştırma fikrindeki çok yüksek iletişim gecikmelerinden dolayı gerçek zamanlı olmayan sistemler için çözüm olabilmektedir. Bu kıstın olmasına rağmen imgesel yönlendirme yöntemi akademik yayınlarda tanımlanan benzer sistemlerin tersine bu yöntem sistemde aşırı derecede şifreleme işlem yükü bulunmamaktadır. KTAMG yöntemi yüksek derecede tasarsız ve düşük iletişim gecikmeleri gereken sistemler için önerilmiştir. Bu yöntem sayesinde isteğe bağlı yönlendirme yapılmaksızın farklı bir yönlendirme seçeneği önerilmiştir. Önerilen yönlendirme seçeneği özellikle karıştırma fikrindeki gibi çok fazla işlem gücü gerektirmeyeceğinden gerçek zamanlı sistemler için kullanılması uygun olacaktır.

5.2 İmgesel Yönlendirme Yöntemi

İçerik eşleştirmelerine karşı mesajın yolu üzerindeki her bir düğümde içeriğinin değiştirilerek dışarıdaki herhangi bir dinleyici tarafından düğümlere giren ve düğümlerden çıkan mesajlar arasında ilişkinin kurulamaması sağlanır. Özellikle soğan yapısı ismi verilen yapıda mesajın düğümler arasında yer değiştirmesinde mesajların şifrelenmesi ya da şifreleme katmanlarının oluşturulması sayesinde bu tür koruma mekanizması sağlamaktadır. Kaynak düğüm göndereceği düğüme kadar olan tüm yol için yönlendirme bilgisini şifreleyerek katmanlı olarak mesajın içerisinde gömer ve herhangi bir yönlendirici düğüm sadece bir katmana ait yönlendirme bilgisini çözebilir. Eğer bu düğüm saldırgan tarafından ele geçirilse bile, saldırgan mesajın sadece bir katmanına ait bilgiyi çözebilir ve bu bilgiden de sadece ileriki düğümün bilgisi elde edilebilmekte, mesajın tüm yol bilgisi elde edilememektedir. Sonuç olarak bu yöntem tüm mesaj yolu üzerindeki düğümlerin saldırgan tarafından ele geçirilmediği sürece düğüm ele geçirme saldırılarına karşı dirençlidir. ANODR sistemleri isteğe bağlı yönlendirmeler için soğan yapısı kavramını kullanırlar. Bu yöntem içerisinde arka kapı fonksiyonu bulunan mesaj yayını işlemini kullanmaktadır. Fakat bu yapının gerçeklenmesi çok fazla sayıda işlem gerektirdiğinden bu yapı çok fazla desteklenmez. İçerik eşleştirmeleri mekanizmaları genelde yayın mesajlarından faydalanmaktadır. Çünkü bu yöntemde her bir

yönlendirme isteği yayın mesajları sayesinde gerçekleştiğinden bu istekler tüm düğümler tarafından elde edilmektedir. Bu sayede tüm ortamı dinleyen birisi tüm düğümlere giden mesajları mesajın kime gittiğinin önemi olmadan elde edebilmektedir. Sonuç olarak çok şifreleme katmanı yapısı yayın yapısı kullanıldığında içerik eşleştirmelerine karşın korumasızdır. Bu tür saldırıların önüne geçmek için soğan yapısına gerek duyulmadan imgesel yönlendirme fikri alternatif çözüm olarak verilmiştir.

Yönlendirme keşfi sırasında, gönderici düğüm < YİS, sırnum, trvar, N> formatında yayın mesajı gönderir. Burada **YİS** yönlendirme isteği mesajının tipini, **sırnum** global olarak verilen sıra numarasını, **trvar** sadece varış düğümü tarafından açılabilecek şifreli arka kapı fonksiyonunu, N ise yerel olarak verilen rastsal imgeyi ifade eder. Sahipsiz olarak yönlendirme keşfi şu şekilde gerçekleşir.

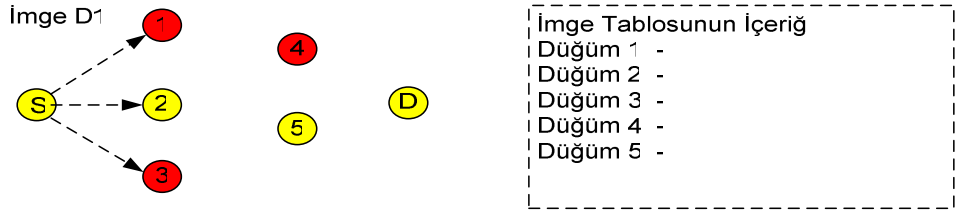
1. YİS Fazı: Başlangıç olarak gönderici YİS mesajlarını komşu düğümlere yayınlarlar. Bir düğüm YİS mesajını aldığında, mesajın sıra numarasını kontrol eder. Eğer daha önce aynı sıra numarasına ait mesaj almışsa mesajı çöpe atar. Eğer almamışsa aldığı mesaj ile ilgili yeni bir yerel rastsal imge üretir, eski rastsal imgeyi yenisiyle değiştirir ve diğer komşu düğümlere yayınlar. Bu safhada yönlendirici düğüm yayın işlemi ile ilgili bazı bilgileri tutar. Bu bilgiler sıra numarası, eski ve yeni imgeler, mesajın trvar kısmı ve YİS mesajlarının gelecek safhada gerçekten yönlendirme cevabı verilip verilmediğini belirten kontrol bitidir. Kontrol biti ilk olarak oluşturulduğunda 0 değeri verilir.

2. YCEV Fazı: Eğer bir düğüm YİS mesajı alırsa, düğüm mesajın içerisindeki arka kapı fonksiyonunu açmaya çalışır. Eğer başarılı olursa bu düğüm bir YCEV yönlendirme mesajı oluşturur. Bu mesajın formatı <YCEV, sıraNo, prvar, N> şeklindedir. Bu mesaj formatında sıraNo alınan YİS mesajının sıra numarası, prvar ile arka kapı fonksiyonunun açıldığının ispatıdır. N ise ilgili YİS mesajından elde edilen imgedir. Yönlendirici düğümler herhangi bir YCEV mesajı aldıklarında imge girişinin değerini bulmaya çalışırlar. Bu değer depolanan ilgili arka kapı fonksiyonun değeri ile karşılaştırılır. Eğer karşılaştırılan değerler uygun ise ilgili kontrol bitinin değeri 0'dan 1 olarak değiştirilir. Sonuç olarak bu girdi varış tarafından onaylanır. Bu yolla yönlendirme belirleme işleminin bir aşaması tamamlanır. Bundan sonra yönlendirici düğüm içerisinde onaylanan yeni imgenin olduğu yeni bir YCEV mesajı

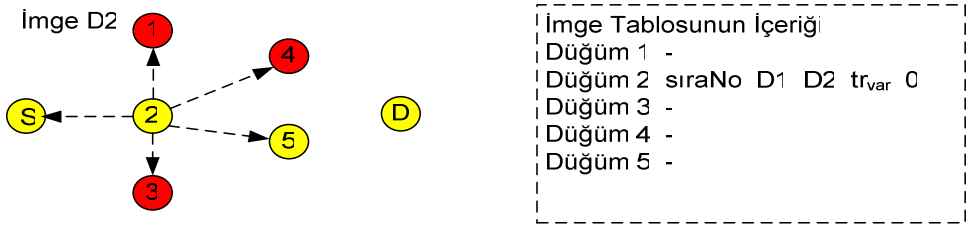
oluşturur. Yeni oluşturulan mesaj diğer düğümlere yayınlanır. Benzer aşamalar YCEV mesajının gönderici düğüm tarafından alınmasına kadar gerçekleştirilir.

Şekil 5.1'den Şekil 5.9'a kadar alternatif çözüm aşama gösterilmektedir. İlk olarak, kaynak mesajı N_1 imgesiyle yayınlar. (Şekil 5.1) Yayın mesajını alan tüm düğümler kendilerinde bulunan imge tablolarında sıra numarası ve mesaj imgesinin özelliklerini içeren yeni giriş oluştururlar. Mesajı alan düğümler bu mesajı aldıktan yeni bir imge değerleri oluşturur ve oluşturulan imgeleri tablolarına ekledikten sonra yeni imgeli mesaj olarak diğer düğümlere yayınlarlar. (Şekil 5.2- Şekil 5.9). Şekillerde tüm düğümlere ait imge tablolarının durumları ve imgelerin özellikleri belirtilmiştir.

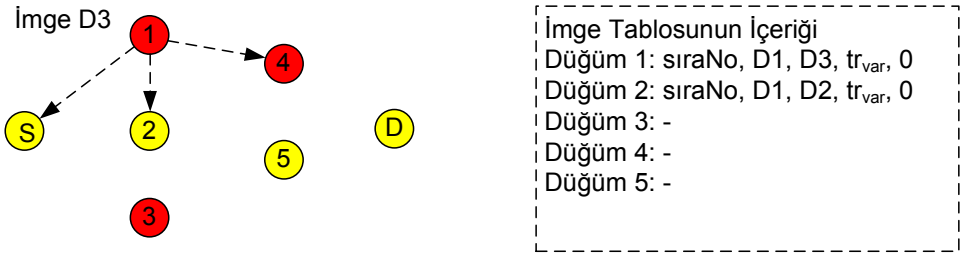
Mesajı varış düğümüne ulaştıktan sonra, varış düğümü karşılık gelen YİS mesajına ilişkin içerisinde imge değerinin ve arka kapı fonksiyonundaki bilginin doğrulanmasının bir YCEV mesajı üretir ve bu mesajı yerel olarak yayınlar. YCEV mesajını alan düğümler mesajın sıra numarasına göre imge tablosunda mesajı ararlar. Mesajın sıra numarası tablodaki kayıtlarla eşleştirildiğinde düğüm YİS isteğine karşı gelen YCEV mesajının gerçekliğini onaylar. Bundan sonra kontrol biti "1" değerine çekilir. (Şekil 5.7- Şekil 5.9). Bu değer çekme işlemi gönderici ile alıcı arasında sanal yönlendirme oluşturulana kadar devam eder.



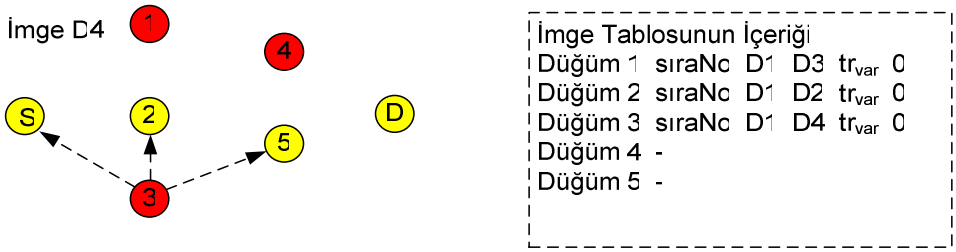
Şekil 5.1: Kaynak düğümden İmge 1 yönlendirme isteği yayını



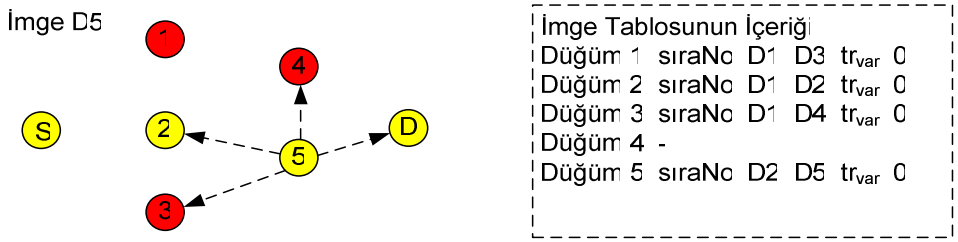
Şekil 5.2: Düğüm 2'den İmge 2 yönlendirme isteği yayını



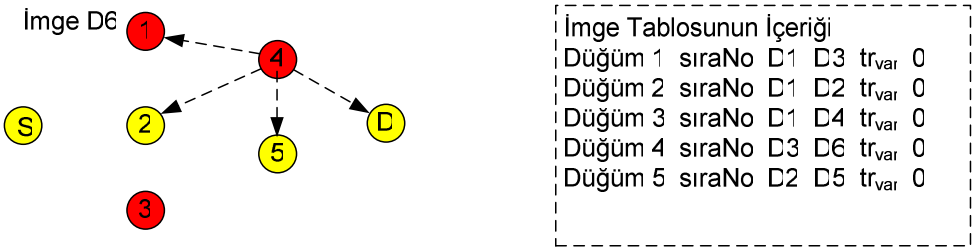
Şekil 5.3: Düğüm 1'den İmge 3 yönlendirme isteği yayını



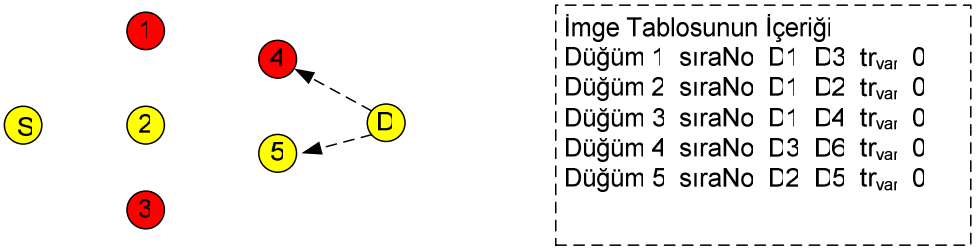
Şekil 5.4: Düğüm 3'den İmge 4 yönlendirme isteği yayını



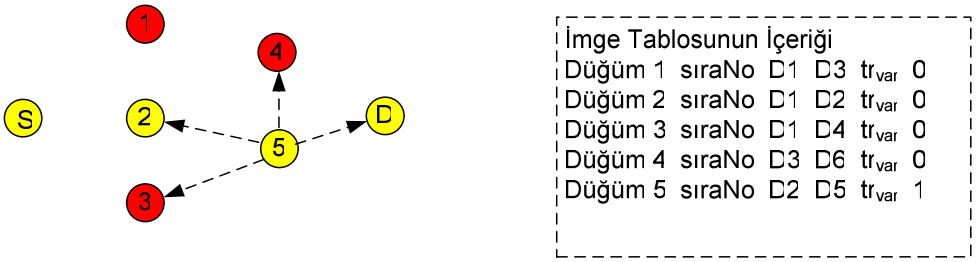
Şekil 5.5: Düğüm 5'den İmge 5 yönlendirme isteği yayını



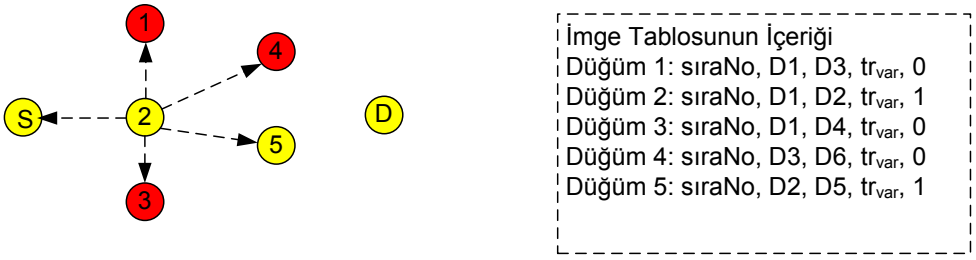
Şekil 5.6: Düğüm 4'den İmge 6 yönlendirme isteği yayını



Şekil 5.7: Varış Düğümünden İmge 5 yönlendirme cevabı yayını



Şekil 5.8: Düğüm 5'den İmge 2 yönlendirme cevabı yayını



Şekil 5.9: Düğüm 2'den İmge 1 yönlendirme cevabı yayını

Bu çözümde söz edilen sistemde ANODR sistemi ile karşılaştırıldığında çok fazla iş gücü gerektiren açık anahtar işlemleri bulunmamaktadır. Bu sistem ek tablolalar kullandığından depolama karmaşıklığı artmaktadır. Fakat bu dezavantajın etkisi önceden belirlenmiş zaman aşımı değerleri ile azaltılabilmektedir. Örneğin YİS aşamasında, her bir düğümün oluşturulduğu her bir yayın mesajı için değeri "0" olan kontrol biti girilmektedir. Yönlendirme cevaplarının gelmediği makul bir zaman için zaman aşımı değeri belirlendiğinde bu giriş sona ermektedir. Bu örnekte önerilen metoda göre her bir iletişim için tekbir yönlendirme bulunmaktadır. Fakat hat

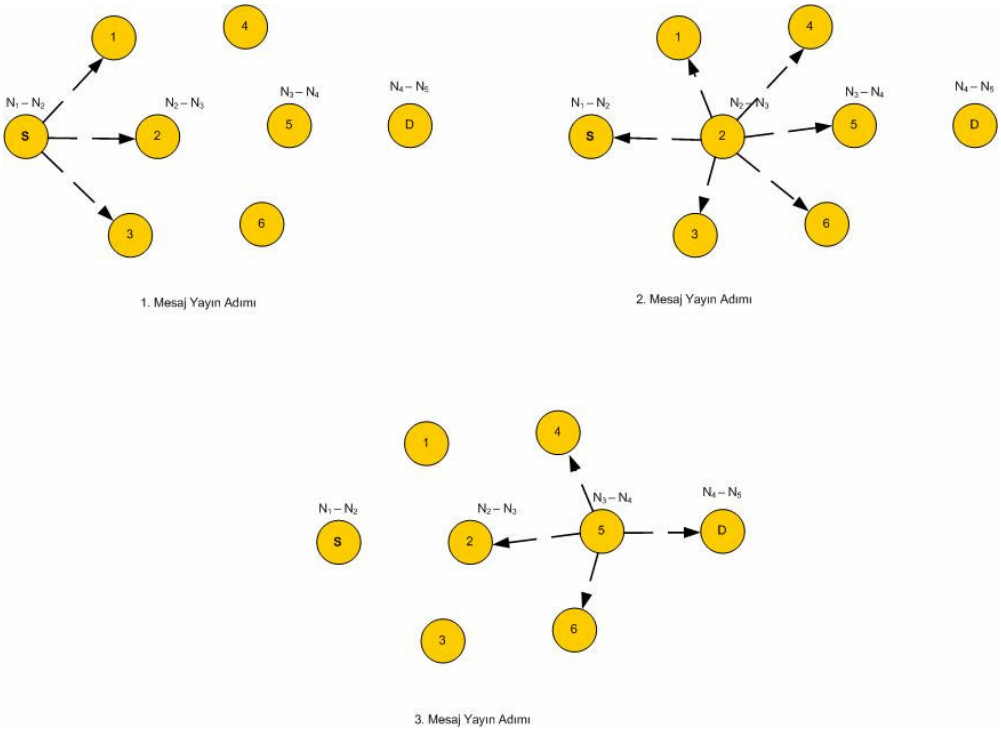
kesilmesi durumunda yeni bir yönlendirmelere ihtiyaç olduğundan bir iletişim için birden fazla yönlendirme bulunabilir.

5.3 Küme Tabanlı Sahipsiz Mesaj Gönderme Yöntemi

Bu yöntem yüksek derecede tasarsız ve düşük iletişim gecikmeleri gereken sistemler için önerilmiştir. Bu yöntem sayesinde isteğe bağlı yönlendirme yapılmaksızın farklı bir yönlendirme seçeneği önerilmiştir. Önerilen yönlendirme seçeneği özellikle karıştırma fikrindeki gibi çok fazla işlem gücü gerektirmeyeceğinden gerçek zamanlı sistemler için kullanılması uygun olacaktır.

Önceki bölümde söz edilen imgesel yönlendirme çözümünde ve ANODR metodunda yönlendirmelerin sahipsiz olarak keşfedilmesi deneniyordu. Keşfedilmesi safhasının tamamlanmasının ardından, uygun olan yönlendirme bilgisi imgesel yönlendirme olarak her bir düğüme gömülüyordu. Fakat gerçek mesaj imge altyapısı kullanılarak sahipsiz olarak gönderilmelidir. ANODR keşif aşamasına benzer yerel yayın metodunu tercih eder. Şekil 5.10 'de belirtilen ağ topolojisi buna örnek olarak verilmektedir. Şekil 5.10 'de kaynak düğümden varış düğüme mesaj gönderilmesi aşamasında keşif adımları gösterilmektedir. Bu kapsamda uygun imgesel bilgi mesaj yolu üzerindeki her düğümde gösterilir. Kaynak düğümü S mesajı içine gömülen imge N_2 değeri ile birlikte yayınlanmaktadır. Tablosunda ilgili değerim karşılığı bulunan düğüm aldığı mesajı tekrar yeni imge değeri N_3 ile yayınlar. Bu şekilde sırasal mesaj yayın işlemi mesaj varış düğüme gelinceye kadar devam eder. İmge değerlerinin karşılığı olmayan yayın mesajlar çöpe atılır. Fakat tüm sistemi dinleyen birisi yayın mesajlarının çöpe atıldığı veya yayın mesajlarının tekrar yayınlandığı düğümlerin oluşturduğu yolu gözleyebilmektedir. Bu durumda örneğin K mesajı sırasıyla 1,2 ve 3 no'lu düğümlere gönderdi. Bundan sonraki adımda düğüm 1 ve 3 mesajı çöpe attı, fakat düğüm 2 mesajı yeniden yayınladı. Biraz akıllı olan dinleyici kolaylıkla 2. düğümün gideceği düğümü tahmin edebilir. Bu tür ağ trafiği analizlerinin çöpe atılacak mesajlar çöpe atılmadan yeninden yayınlanırsa önüne geçilebilir. Bu metot gereksiz bir yayın trafiği oluşturmakta, bu durumda düğümlerin enerji tüketimlerinin artması sorununu beraberinde getirmektedir. Bu tip analizlerden diğer bir kaçınma yolu ise her bir düğümde mesajların karıştırıcı uygulamaların çalıştırılmasıdır. Bu durumda kaynak ile varış düğümü arasında yüksek mesaj

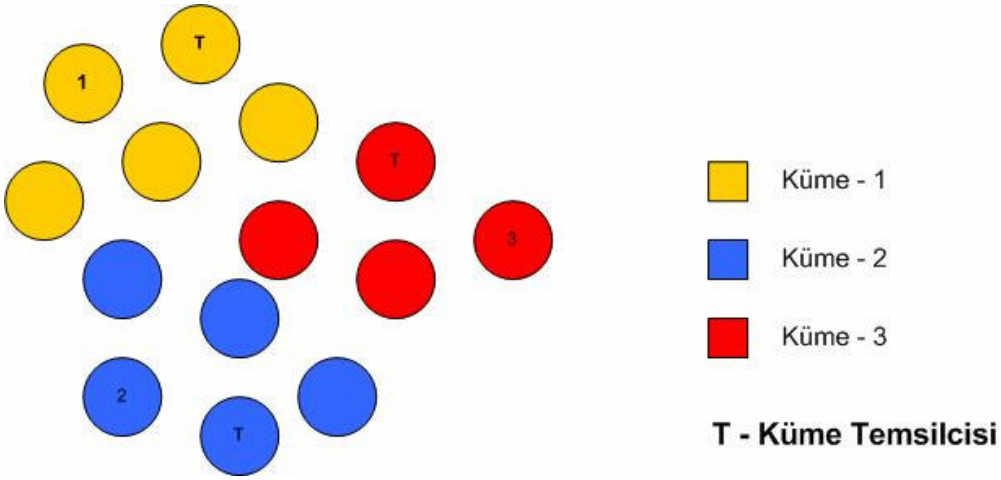
gecikmelerini beraberinde getirmektedir. Özellikle gerçek zamanlı uygulamalarda bu yol etkin olmamaktadır. Sonuç olarak mesajların karıştırılması çok yüksek gecikme getirmekte fakat düğümler üzerindeki işlem yükü azalmaktadır. Bunun sonucunda düğümlerin enerji sarfiyatı azalmaktadır.



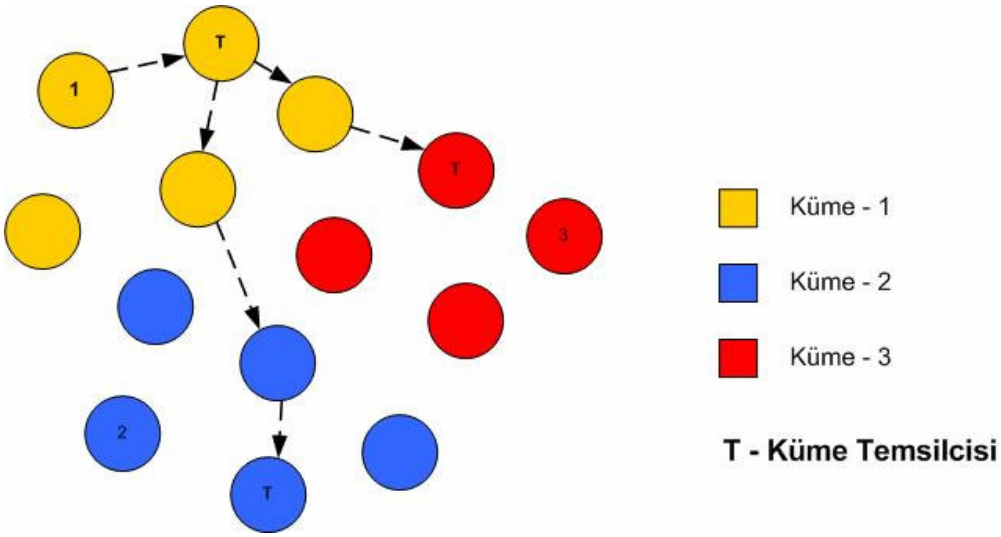
Şekil 5.10: İmge anaçatısı üzerinden mesaj gönderme

Bu çalışmada düşük hat gecikmesi gerektiren sistemlerde sahipsiz mesaj göndermede KTAMG isimli metottan söz edilecektir. Bu metot kısa zaman aralıklarında makul miktarda ek yayın mesajları sayesinde sahipsiz mesaj göndermeyi tanımlamaktadır. Bu metotta düğümler kümeleri oluşturmaktaydı. Bu küme içerisinde bu küme içerisinde bir adet temsilci düğüm Şekil 5.11 bulunmaktadır. Bu metotta tüm ağ düğümleri kümelere ayrılmış olarak kabul edilmektedir. Sistem içinde her bir düğümün bir kümeye ait olduğunu ve küme içerisinde de bir düğümün temsilci olarak seçildiğini garanti eder. Eğer bir düğüm farklı kümedeki diğer bir düğüme mesaj göndermek Şekil 5.11 isterse mesaj ilk olarak o kümenin içerisindeki temsilci düğüme gönderilir. Bu aşamadan sonra temsilci düğüm bu mesajı diğer kümelerin temsilci düğümlerine gönderir Şekil 5.12 Bu düğümler aldıkları mesajı yerel olarak kendi kümlerinin içerisinde bulunan düğümlere yayınlarlar. Özellikle global arka kapı fonksiyonu mesajın içerisine gömüldüğünden doğru varış eksiksiz olarak tespit

edilebilir. Bu metot mesajların yayınlanmasında sonsuz mesaja ıraksanmaması için TCP protokolündeki zaman aşımı (TTL) kavramını da kullanmaktadır. Temsilci düğüm kümedeki düğümlerin sayısına göre göndereceği mesaja bir TTL değeri atamaktadır. Küme içerisindeki bir düğüm mesaj aldığında mesajın içerisinde bulunan TTL değerini azaltarak yeninden yayınlar. Eğe mesajdaki TTL değeri sıfır olunca mesaj çöpe atılır. Örnek bir TTL kavramına Şekil 5.13'de yer verilmiştir. Burada temsilci düğüm TTL değerini iki olarak seçip mesajı yayınlamaktadır. Mesajı alan düğümler bu değeri bir azaltarak mesajı tekrar yayınlamaktadır. Geriye kalan düğümler mesajı aldıklarında TTL değeri sıfır olduğu bu işlem sonlanmaktadır.

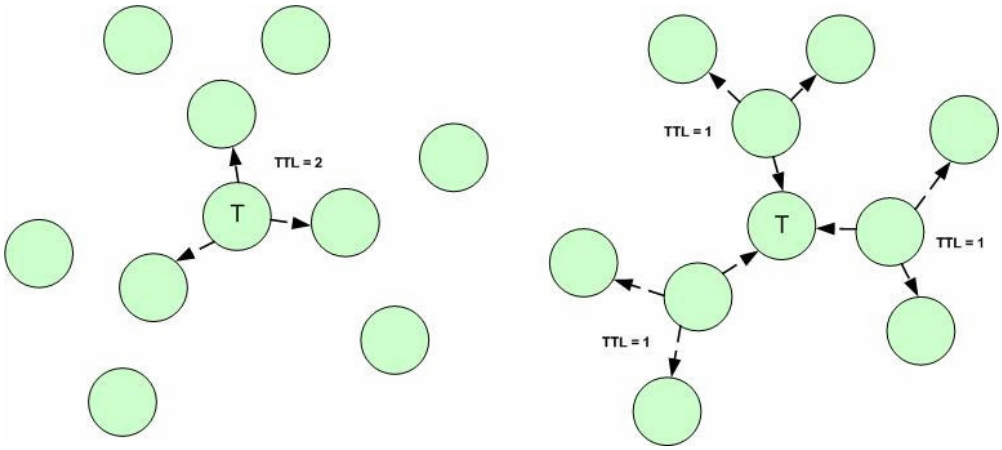


Şekil 5.11: Küme topolojisi



Şekil 5.12: Kümeler arasında mesaj yayınlanması

Tüm ağı dinleyen birisi ağ üzerindeki her bir düğüme giden mesajı görebilmektedir. Fakat asla mesajın gerçek alıcısını tespit edememektedir. Kümeler arası iletişimde ek olara isteğe bağlı yönlendirmeye keşif aşamalarına ihtiyaç duyulmamaktadır. Bunun sebebi bu iletişimlerin temsilci düğümler arasında olması ve her bir düğüm arasında başlangıçta belirtilen belirlenen sabit yönlendirmeden kaynaklanmaktadır. Yönlendirmelerin korumasına temsilci düğümler arasında ağ topolojisinin değişimi ya da düğümlerdeki gücün bitmesinde ihtiyaç duyulmaktadır. Temsilci düğümler küme üyelerinden gelen tüm ağ trafiğini aktarırlar. Bu tip düğümler pil ömrü uzun düğümler arasından seçilmektedir. Temsilci düğümler arasındaki ağ yönlendirme paketlerinin dinlenmesi dinleyici önemli bir bilgi kaynağı değildir. Bunun sebebi ise sistemin temsilci düğümlerin gerçek gönderici veya alıcı olmadığınım bilmesinde kaynaklanmaktadır. Bu düğümler sadece kümeler arasında yönlendirici düğüm olarak görev yapmaktadırlar.



Şekil 5.13: TTL Mekanizmasının işleyişi

Bu metodun en büyük getirisi düğümlerin içerisinde mesaj karıştırma işleminin yapılamamasının sağlanmasıdır. Özellikle düşük gecikme gerektiren sistemlerde bu metot birçok avantaj getirmektedir. ANODR sisteminin aksine bu sistemde daha az yayın mesajının üretilmesidir. Bu sistem sayesinde çoklu yayın mesajlarının tüm düğümler yerine sadece temsilci düğümlere gönderilmesiyle sistemin kazandığı sahipsizlik derecesine göre daha az seviyede enerji tüketilmektedir. Temsilci düğümler farklı topolojilerde akıllıca seçildiğinde sistemi dinleyenlerin dinleme kabiliyetleri ya da dinlendiklerinde çıkarım yapma kabiliyetleri azalmaktadır. KTAMG metodunun diğer bir getirisi de yayım mesajları işlemlerinde mesajların

sonlanması için herhangi bir sonlandırma mekanizmasının varlığıdır. Özellikle yönlendirme keşfi aşamasında ANODR sistem yayın mesajlarının sonlandırılması için herhangi bir etkide bulunmamaktadır. En son avantaj ise isteğe bağlı yönlendirmede yönlendirme keşfi aşamasına gerek olmamasıdır.

Bu sistemin avantajları olduğu kadar da dezavantajları da bulunmaktadır. İlk olarak sistem üzerinde kümeleme işlemlerinin gerçekleştirilmesi gerekmektedir. Özellikle küme elemanlarını ve temsilcilerini belirleme sisteme ek işlem yükü getirmektedir. İkinci olarak; düğümler içerisinden pil ömrü yüksek olan ürünler küme temsilcisi olarak kullanılmaktadır. Bu yüzden küme temsilcileri kümeler arasında iletişim açısından öneme sahiptir. Bu yüzden küme temsilcileri hizmet dışı bırakma saldırıları ile karşı karşıyadır. Başarılı hizmet dışı bırakma saldırısı ya da herhangi bir düğümde olan arıza sistem üzerindeki diğer kümelerin bu küme elemanları ile iletişim kuramaması sorununu beraberinde getirmektedir. Bu sebepten bu tür sistemlerde hat kesintisinin tespit edilip, temsilci düğümler arasında yönlendirmenin korunması ve alternatif iletişim yollarının bulunması gereklidir. Özellikle bu sistemlerde yönlendirmelerin korunması mutlaka göz önüne alınması gereken bir durumdur. Özellikle bu tip sistemlerde temsilci düğümlerin devre dışı kalması durumunda daha da gerekli olmaktadır. Eğer temsilci düğüm devre dışı kaldığı durumda sistem mutlaka alternatif yol bulmak zorundadır.

5.4 Önerilen Çözümlere İlişkin Uygulamalar

Bu bölümde İmgesel Yönlendirme Yöntemi ve Küme Tabablı Mesajlaşma Yöntemelerine ilişkin simulasyon uygulamalarına yer verilmiştir. Gerçekeşletirilen simukasyonlada her iki çözüm yolu için aynı simulasyon mimarisi kullanılmıştır. Bu sayede önerilen çözümlerin birbirileriye karşılaştırılabilmesi amaçlanmıştır.

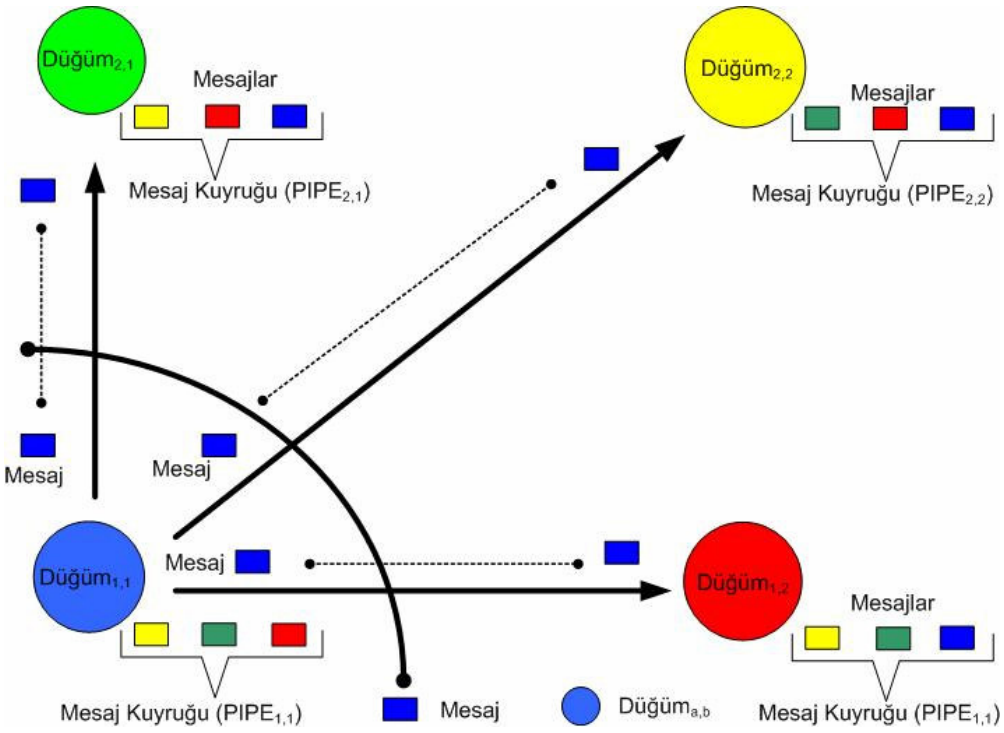
Gerçekleştirilen simulasyonlarda önerilen çözümlerin gerçek ortama uygun olarak denenmesi sağlanmıştır. Bu kapsamda Linux işletim sisteminin süreç (process), mesaj kuyruğu (pipe) , paylaşılan alan ve semafor yapıları kullanılmıştır. Simulasyon uygulaması çalışmasıdaki mesaj kuyruğu ve süreç yapıları önerilen çözümlerdeki algoritmalara ilişkin yapıların gerçekleştirilmesinde, paylaşılan alan ve semafor yapıları ise simulasyon uygulamasına ilişkin istatistiksel verilerin toplanması ve işlenmesi amacıyla kullanılmıştır.

Önerilen çözümlerde tasarsız ağlarda bulunan düğümler arasında sahipsiz haberleşmenin sağlanması üzerine durulmuştu. Bu kapsamdaki simulasyon uygulaması çalışmasında gerçek hayatta tasarsız ağlar üzerinde bulunan düğümler uygulamada birer süreç olarak ifade edilmiştir. Tasarsız ağ düğümleri arasındaki habeleşme ise IPC (inter process commincation) olarak simulasyon uygulamasına aktarılmıştır. Örnek olarak simulasyon uygulamasındaki bir düğüm diğer bir düğüme paket göndermesi gerekiyorsa bu durum simulasyon uygulamasında süreçlerin birbirleriyle haberleşmesi şeklinde gerçekleştirilmiştir. Bu sayede simulasyon uygulamasına ilişkin elde edilen veriler gerçek hayat uygulamasındaki verilelerle uyumluluk sağlamaktadır.

Simulasyon uygulamasının temelinde iki temel yapı mevcuttur. Bunlardan birincisi ağ düğümleri önceki paragrafta bu yapılar işletim sistemi süreçleriyle karşılandı. Diğeri ise mesaj kuyruklarıdır. Mesaj kuyrukları ise linux işletim sistemi altında bulunan PIPE isimli yapı kullanılarak gerçeklenmiştir. Bu uygulamada her bir süreçe bir adet o sürece ait pipe atanmıştır. Bu sayede süreçlerin birbiriyle haberleşmesi gerektiği durumda bir süreç diğer sürecin pipe yapısına mesaj göndermektedir. Pipe yapısı işletim sistemi üzerindeki dosya yapısına benzemektedir. Dosya yapısına göre farkları sırasıyla; bu yapıya gelen mesajlar bilgisayarın belleğinde bulunmakta ve fiziksel olarak disk üzerine kayıt edilmemekte, diğeri ise bu yapıya gelen mesajlar ilgili süreç tarafından okunduğunda okunan mesajlar bu yapı üzerinden silinmektedir. Ayrıca PIPE yapısı aynı zamanda kuyruk yapısı olduğundan bu yapıya ilk gelen mesaj ilk sırada çıkar yada okunur, en son gelen mesaj en son çıkar. Bu sebepten dolayı PIPE yapısı genel olarak düğümler üzerindeki kuyruk yapılarıyla özdeştirler.

İmgesel Yönlendirme ve Küme Tabanlı Mesaj Gönderme yöntemi temel olarak düğümlerin mesajları yayınlmasına temeline dayanmaktadır. Düğümler tarafından yayınlanan mesajları alan diğer düğümler aldıkları mesajın durumuna göre mesaji diğer düğümlere yayınlarlar. Şekil 5.14'te düğümlerin önerilen yöntemlerde hangi şekilde yayın mesajı gönderildiği belirtilmektedir. Bu şekilde Düğüm$_{1,1}$ diğer komşu yada iletişim içerisinde bulunabileceği düğümlere yayın mesajı göndermek istemektedir. Bu durumda Düğüm$_{1,1}$ mesajı yayınlar, uygulmada belirtilen ağ tasarsız ağ olduğu için yayınlanan mesajı, mesajı yayınlayan düğümün kapsama alanı içerisindeki Düğüm$_{1,2}$ Düğüm$_{2,1}$ Düğüm$_{2,2}$ almaktadır. Yayın mesajı, yayın mesajı

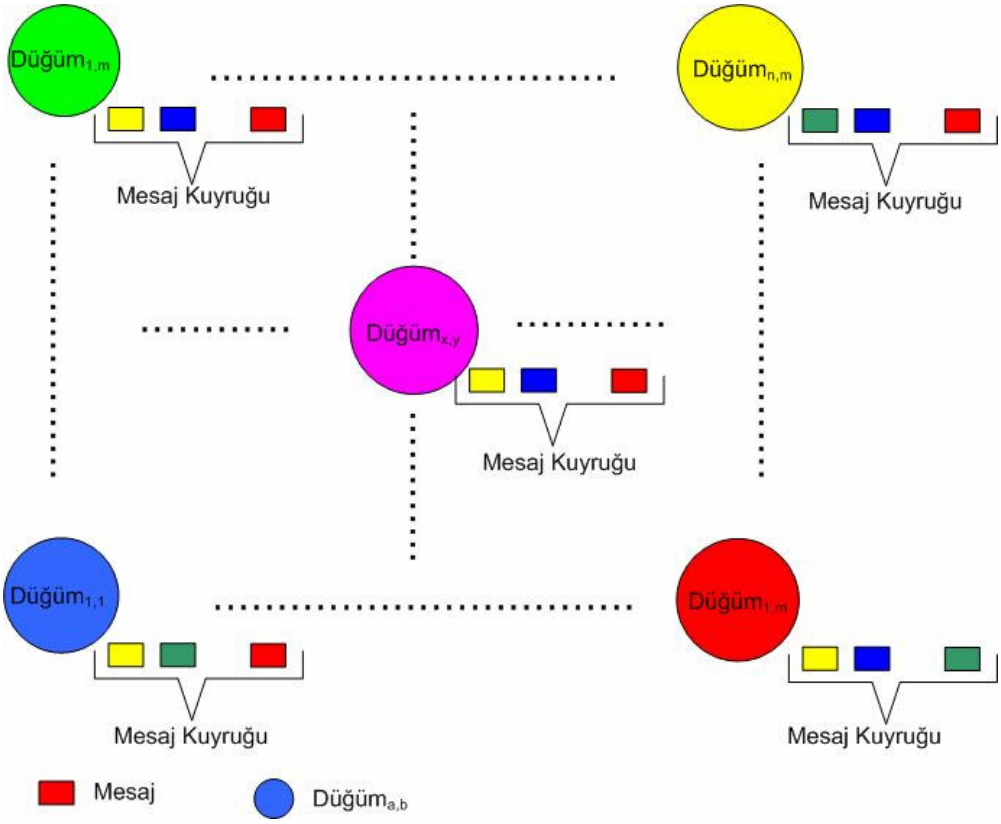
alacak olan düğümlerin mesaj kuyruklarına gelmektedir. Bu düğümlerin mesaj kuyruklarında diğer düğümlerden gelen diğer mesajlar da bulunmaktadır. Şekil 5.14'te gönderilen mesaj mavi renkle belirtilmiştir. Bu durumda mesajı alan diğer düğümler şekle göre mesajı kuyruklarında başka mesajlarda olduğu için aldıkları mesajı mesaj kuyruğunun sonuna kaydederler. Bu kapsamdaki simulasyon uygulamasında düğümler tarafından gönderilen mesajlar ilgili düğümü tanımlayan sürece atanmış olan PIPE yapısı içerisinde mesaj kuyruğuna alınmaktadır. Simulasyon uygulamasında mesaj kuyruğunun boyu ile ilgili herhangi bir kısıt getirilmemiştir.



Şekil 5.14: Düğümlerin yayın mesajlarını göndermesi

Bu çalışma kapsamında oluşturulan benzetim uygulamasında tasarsız ağ düğümlerinin düzlemsel olarak yayıldığı varsayılmıştır. Normal olarak tasarsız ağların bulunduğu ortamlar göz önüne alındığında 1500x300 m'lik alanda yaklaşık 50 adet düğümün var olduğu kabul edilmektedir[18]. Bu kapsamda geliştirilmiş olan benzetim uygulamasında en fazla 400 adet düğüm benzetime dahil edilebilmektedir. Bu durum göz önüne alındığında gerçekleştirilen benzetim 1500x2400m'lik alanı yaklaşık 3,6 Km^2 alanının benzetimi gerçekleştirilebilmektedir. Bu alanda gerçekleştirilmiş çalışmalar incelendiğin benzetim için kullanılan düğüm sayısının 50

civarında olduğu gözlemlenmiştir[18]. Gerçekleştirilen benzetime ilişkim mimari topoloji Şekil 5.15'de belirtilmiştir. Oluşturulan topolojide düğümler düzlemsel olara eşit aralıklarda dizilmiştir. Bu kapsamda gerçekleştirilen benzetim çalışmasında kaynak düğüm ile varış düğümü en uçtaki düğümlerden ve aralarındaki uzaklığın en fazla olduğu düğümlerden seçilmiştir. Bu çalışmada kaynak düğüm Düğüm$_{1,1}$ varış düğümü ise Düğüm$_{n,n}$ olarak kabul edilmiştir.

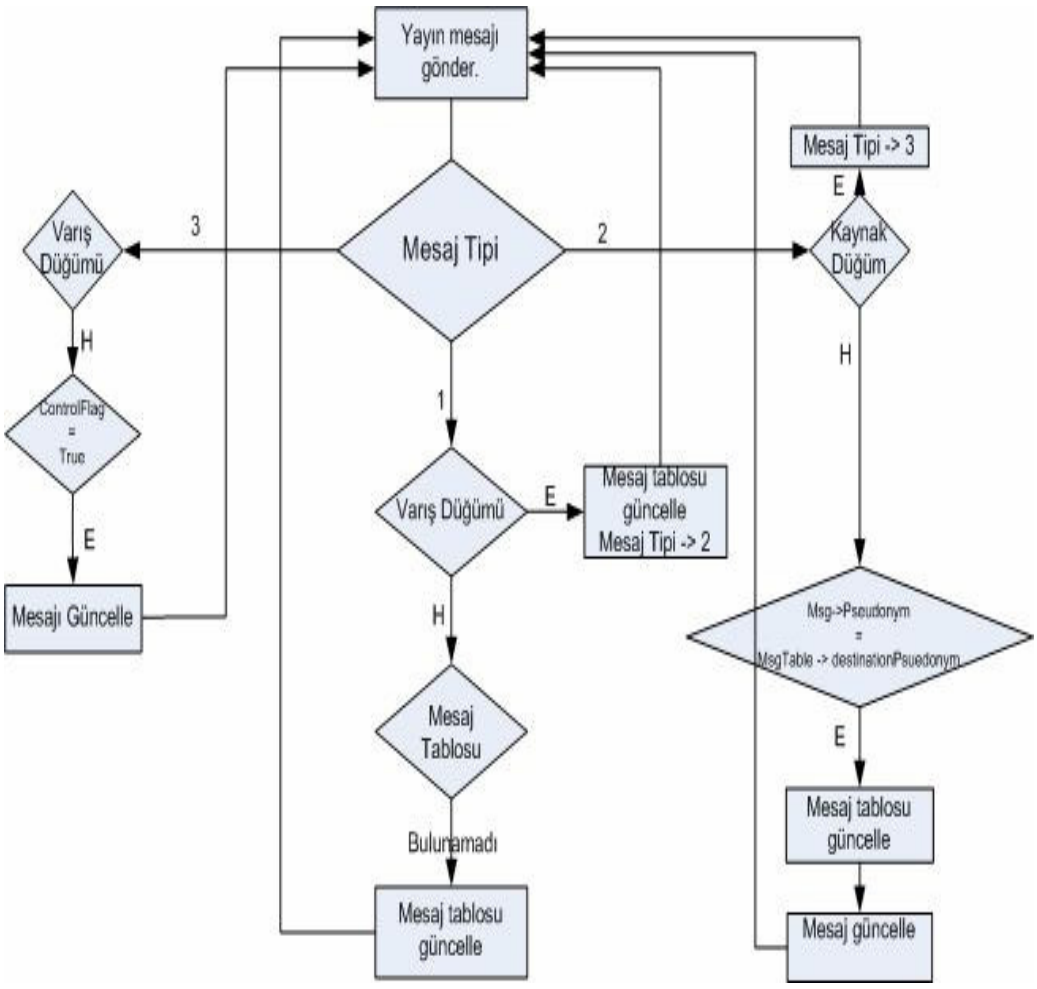


Şekil 5.15: Simulasyon uygulaması topolojisi

5.4.1 İmgesel Yönlendirme Yöntemi Uygulaması

İmgesel Yönlendirme Yöntemi üç farklı aşamadan oluşmaktadır. Bu aşamalar yönlendirme isteği, yönlendirme cevabı ve mesaj gönderme aşamalarıdır. Yönlendirme isteği aşaması kaynak düğüm tarafından oluşturulan ve varış düğümüne kadar olan tüm düğümlerin taranak imgesel yönlendirme tablolarının oluşturulduğu adımdır. Bu adım yönlendirme isteği mesajının varış düğüme gitmesi ile son bulmaktadır. Bu aşamdan sonra varış düğümünden yönlendirme isteği mesajına

cevap olarak yönlendirme cevabı mesajı gönderilir. Bu aşamda varıştan kaynağa doğru ilgili düğümlerde mesaj iletimi sırasında mesajın yönlendirileceği düğümlerde ilgili ilgili kontrol bit'leri bir olarak atanır. Varış düğümünden yönlendirme cevabı mesajı kaynak düğüme geldiğinde yönlendirme keşfi aşaması sona ermiş olur. Bundan sonra kaynak ile varış arasında mesajlaşma gerçekleştirilir. Mesajlaşma aşamasında kaynak düğüm mesajları komşu düğümlerine yayınlar, komşu düğümlerde mesajları kendilerinin komşu düğümlerine yayınlar. Bir düğüme gelen mesajın yayınlanmasının temel kural ise o düğüm üzerinde bulunan mesaj tablosunda ilgili kontrol bitinin değerinin '1' olması gerekliliğidir. Uygulama çalışmasında yönlendirme isteği mesajlarına ilişkin mesaj tipi '1', yönlendirme cevaplarına ilişkin mesaj tipi '2' ve mesaj iletişimine ilişkin mesaj tipi '3' olarak belirlenmiştir. İmgesel Yönlendirme Yöntemi ile ilgili simulasyonun akışı Şekil 5.16'de belirtilmiştir.



Şekil 5.16: İmgesel Yönlendirme yöntemi akış diyagramı

İmgesel yönlendirme yöntemi ile ilgili uygulamada üç farklı veri tipi kullanılmıştır. Bunlar sırasıyla Tablo 5.1, Tablo 5.2 ve Tablo 5.3'te ayrıntılı olarak açıklanmıştır. İmgesel Yönlendirme Yöntemi, bu çalışmada ANODR yöntemine alternatif yöntem olarak ;sunulmuştu. Bu yöntem sayesinde ANODR'deki bir çok yönlendirme düğümlerinin belirlenmesi aşamasındaki bir çok şifreli işlemde tasarruf sağlanmaktadır.Fakat bu yöntemde ANODR yönteminden farklı olarak düğümde messaageTable isimli bir tablo tutulmaktadır. Bu tablo sayesinde düğüm üzerinde geçen mesajlar ve mesaj tiplerine göre sahipsiz yönlendirme bilgileri tutulmaktadır. Bu durumda düğüm üzerinden yayınlanan her bir mesaj için ek olarak 20 byte bellek alanı tutulması gerekmektedir. Örnek olarak sistemde her bir düğümün aynı anda farklı sıra numaralı bin adet mesajı işlediğini düşünürsek düğümde bu amaç için oluşturulan mesaj tablosunun boyutu 20 K Byte düzeyinde olacaktır. Bu değer ise günümüz koşullarında üretilen cihazlar için çok düşük kaynak gerektirmektedir.

Tablo 5.1: Düğüm değişkeni (node)

Değişken Tipi : node		
Değişken İsmi	**Tipi**	**Açıklama**
X	İnt	Düğümün X eksenindeki koordinatını belirtir..
Y	İnt	Düğümün Y eksenindeki koordinatını belirtir.
sourceNode	İnt	Düğümün kaynak düğüm olduğunu belirtir. Sadece simulasyon uygulamasında kullanılır.
trDest	İnt	Sadece varış düğümünün bildiği değer. Bu sayede hem yönlendirme cevap aşaması başlar, hemde mesajlaşma esnasında mesajın kaynak düğüm tarafından alınması sağlanır.

Tablo 5.2: Değişken tablosu (message)

Değişken Tipi : messsage		
Değişken İsmi	**Tipi**	**Açıklama**
messageType	int	Mesaj tipini belirler.
seequenceNumber	int	Mesajın id'sini belirler, bu sayede aynı tip mesaj bir düğümden iki kez geçmez.
messagePseudonym	int	Mesajı işleyen ve yayınlayan düğüme özel değer , bu değer sayesinde yönlendirme cevap aşaması oluşturulur.
TrDest	int	Sadece varış düğümünün bildiği değer. Bu sayede hem yönlendirme cevap aşaması başlar, hemde mesajlaşma esnasında mesajın kaynak düğüm tarafından alınması sağlanır.
Distance	int	Kaynak düğümden mesaj çıkarıldığında 0 değeri verilir. Mesaj düğümler arasında yayınlanırken ilgili düğüm uzaklıkları bu değere eklenir. Sonuçta mesaj varacağı düğüme geldiğinde kaynak – varış uzaklığı hesaplanmış olur.

Tablo 5.3: Değişken tablosu (messageTable)

Değişken Tipi : messsageTable		
Değişken İsmi	**Tipi**	Açıklama
messageType	int	Mesaj tipini belirler.
sequenceNumber	int	Mesajın id'sini belirler, bu sayede aynı tip mesaj bir düğümden iki kez geçmez. Düğüme gelen mesaj bu değerle karşılaştırılır.
sourcePseudonym	int	Düğüme gelen mesaja ait imge değerini belirtir. Bu sayede yönlendirme cevabı aşamasında
destinationPseudonym	int	Düğümden yayınlanan mesaj için düğümün vermiş olduğu imge değeridir.
ControlFlag	int	Yönlendirme mesajı cevap aşamasında gelen mesajın imge değeri ile mesaj tablosundaki varışa ait imge değerinin eşit olduğu durumda bu değişkenin değeri '1' olur. Bu sayede mesaj gönderimi esnasında yönlendirme düğümleri belirlenmiş olur.
*routeMessage	int *	Uygulamaya ilişkin istatistiksel veri toplanması için kullanılmaktadır. Yönlendirme isteği aşamasında topolojide mesajların ziyaret ettiği düğümlerin sayısı belirlemek için kullanılır. Tüm düğümlere ilişkin süreçlerin erişebileceği paylaşılan bellek alanı olarak tanımlanmıştır.

Tablo 5.3: (Devam) Değişken tablosu (messageTable)

Değişken Tipi : messsageTable		
Değişken İsmi	**Tipi**	Açıklama
*reverseRouteMessage	int *	Uygulamaya ilişkin istatistiksel veri toplanması için kullanılmaktadır. Yönlendirme cevabı aşamasında topolojide mesajların ziyaret ettiği düğümlerin sayısı belirlemek için kullanılır. Tüm düğümlere ilişkin süreçlerin erişebileceği paylaşılan bellek alanı olarak tanımlanmıştır.
*messageSend	int *	Uygulamaya ilişkin istatistiksel veri toplanması için kullanılmaktadır. Yönlendirmenin belirlendikten sonra mesaj gönderme aşamasında topolojide mesajların ziyaret ettiği düğümlerin sayısı belirlemek için kullanılır. Tüm düğümlere ilişkin süreçlerin erişebileceği paylaşılan bellek alanı olarak tanımlanmıştır.
RouteState	int	Uygulamanın yönlendirme isteği durumunda olduğunu belirtir.
reverseRouteState	int	Uygulamanın yönlendirme cevabı durumunda olduğunu belirtir.
mesageSendState	int	Uygulamanın mesaj gönderme durumunda olduğunu belirtir.

Anomim olarak mesajlaşılan bir ağda ne kadar çok yayın mesajı trafiği olursa bu ağı dışarıdan dinleyen kimselerin bu ağdaki mesaj akışlarını eşleştirmeleri zorlaşmaktadır. Bununla beraber sahipsiz haberleşmede nekadar çok yayın mesajı oluşursa ağ üzerindeki cihazların güç tüketimleri de o nispette artar.

Tablo 5.4 ve Tablo 5.5 'de kapsama alanlarına göre yayın mesajları gösterilmiştir. Anomim olarak haberleşen sistemlerde düğümlerin kapsama alanı arttırıldığında kapsama alanı arttırılan düğümler daha çok düğümle haberleşeceği için kapsama alanı arttırılan tablolardaki yayın mesaj sayıları artmıştır. Fakat yayın mesajlarının sayısınının artmasına rağmen kaynakla varış düğümü arasındaki uzaklık çok büyük oranda değişmemekte ve uzaklığın sabit kaldığı yada çok az azaldığı görülmektedir. Azalma miktarının da kapasama alanındaki artış kadar olduğu gözlemlenmektedir.

Tablo 5.4: Yayın mesajı sayıları (Düğüm kapasama alanı dört birim)

Düğüm Sayısı	Yayın Mesajı Sayısı (YIS)	Yayın Mesajı Sayısı (YCEV)	Yayın Mesajı Sayısı (MSEND)	Mesaj Uzaklığı
100	3372	75	167	20
144	5084	107	143	23
256	9796	163	199	33
400	16092	219	255	43

Tablo 5.5: Yayın mesajı sayıları (Düğüm kapasama alanı sekiz birim)

Düğüm Sayısı	Yayın Mesajı Sayısı (YIS)	Yayın Mesajı Sayısı (YCEV)	Yayın Mesajı Sayısı (MSEND)	Mesaj Uzaklığı
100	8223	137	259	18
144	14196	168	290	20
256	30848	274	503	29
400	53834	380	502	38

Sahipsiz olarak haberleşen sistemlerde sistemin sahipsizliği varış düğümünden kaynak düğümüne mesaj gönderilirken mesajın geçmiş olduğu düğüm sayısının sistemdeki toplam düğüm sayısına oranı sistemdeki sahipsizlik derecesini vermektedir. Tablo 5.6 ve Tablo 5.7 'de belirtildiği üzere düğümlerin kapsama alanı arttırıldığında sistemin anomimlik derecesinin arttığı gözlemlenmiştir. Ayrıca tablolardan gözlemlemen duruma göre yönlendirme isteği sırasında sistemdeki sahipsizliğin derecesi neredeyse bire yakın çıkmaktadır. Fakat yönlendirme cevabı ve mesaj aşamaları sırasında sistemdeki sahipsizlik düşmekte ve sistem tam olarak sahipsiz bir hal alamamaktadır. Ayrıca sahipsiz mesajlaşan düğümlerin sayıları arttırıldığı sistemde sahipsizliğin düştüğü gözlemlenmektedir.

Tablo 5.6: Ziyaret edilen düğüm sayısı (Dört birim)

Düğümlerin Kapsama Alanı = 4 Birim			
Düğüm Sayısı	**Ziyaret Edilen Düğüm Sayısı (YIS)**	**Ziyaret Edilen Düğüm Sayısı (YCEV)**	**Ziyaret Edilen Düğüm Sayısı (MSEND)**
100	99	29	64
144	144	69	83
256	255	87	114
400	400	121	151

Tablo 5.7: Ziyaret edilen düğüm sayısı (Sekiz birim)

Düğümlerin Kapsama Alanı = 8 Birim			
Düğüm Sayısı	**Ziyaret Edilen Düğüm Sayısı (YIS)**	**Ziyaret Edilen Düğüm Sayısı (YCEV)**	**Ziyaret Edilen Düğüm Sayısı (MSEND)**
100	99	50	90
144	143	72	122
256	255	162	226
400	399	195	256

5.4.2 Küme Tabanlı Mesaj Gönderme Yöntemi Uygulaması

Küme Tabanlı Mesajlaşma Yöntemi uygulaması teme olarak iki aşamadan oluşmaktadır. Bu aşamalardan ilki mesajın kaynak düğümünden temsilci düğümlere gönderilmesi, ikincisi ise temsilci düğümün kapsama alanı içerisinde mesajın yayın yoluyla varış düğüme gönderilmesidir. Bu yöntemde sahipsiz sistemler içerisinde mesajın sonsuz olarak yayılmaması için mesaja kaynak düğümünden çıkarken TTL (time-to-live) değeri atanmaktadır. Bu değer mesajın herbir yayınlanmasında bir

azaltılmaktadır. Bu değerin 0 olduğu durumda ise mesaj çöpe atılır, yani yayınlanmaz.

Küme tabanlı mesaj gönderme yöntemi ile ilgili uygulamada üç farklı veri tipi kullanılmıştır. Bunlar sırasıyla Tablo 5.8, Tablo 5.9'da ayrıntılı olarak açıklanmıştır. Küme tabanlı mesaj gönderme, bu çalışmada yayın yöntemine alternatif yöntem olarak ;sunulmuştur..Fakat bu yöntemde yayın yönteminden farklı olarak düğümde messaageTable isimli bir tablo tutulmaktadır. Bu tablo sayesinde düğüm üzerinde geçen mesajları sıra numaraları tutulmaktadır. Bu durumda düğüm üzerinden yayınlanan her bir mesaj için ek olarak 4 byte bellek alanı tutulması gerekmektedir. Örnek olarak sistemde her bir düğümün aynı anda farklı sıra numaralı bin adet mesajı işlediğini düşünürsek düğümde bu amaç için oluşturulan mesaj tablosunun boyutu 4 K Byte düzeyinde olacaktır. Bu değer ise günümüz koşullarında üretilen cihazlar için çok düşük kaynak gerektirmektedir.

Tablo 5.8: Değişken tablosu (Mesaj Tablosu)

Değişken Tipi : messsageTable		
Değişken İsmi	**Tipi**	**Açıklama**
sequenceNumber	İnt	Mesajın id'sini belirler, bu sayede aynı tip mesaj bir düğümden iki kez geçmez. Düğüme gelen mesaj bu değerle karşılaştırılır.

Tablo 5.9: Değişken Tipi (Mesaj)

Değişken Tipi : messsage		
Değişken İsmi	**Tipi**	**Açıklama**
seequenceNumber	İnt	Mesajın id'sini belirler, bu sayede aynı tip mesaj bir düğümden iki kez geçmez.
TrDest	İnt	Sadece varış düğümünün bildiği değer. Bu sayede hem yönlendirme cevap aşaması başlar, hemde mesajlaşma esnasında mesajın kaynak düğüm tarafından alınması sağlanır.

Tablo 5.9: (Devamı) Değişken Tipi (Mesaj)

Değişken Tipi : messsage		
Değişken İsmi	**Tipi**	**Açıklama**
Distance	İnt	Kaynak düğümden mesaj çıkarıldığında 0 değeri verilir. Mesaj düğümler arasında yayınlanırken ilgili düğüm uzaklıkları bu değere eklenir. Sonuçta mesaj varacağı düğüme geldiğinde kaynak – varış uzaklığı hesaplanmış olur.
TimeToLive	İnt	Düğüm mesajı yayınladığında mesajın bu değeri bir azaltılır. Eğer düğüme gelen mesaj

Tablo 5.10: Düğüm değişkeni (node)

Değişken Tipi : node		
Değişken İsmi	**Tipi**	**Açıklama**
X	İnt	Düğümün X eksenindeki koordinatını belirtir..
Y	İnt	Düğümün Y eksenindeki koordinatını belirtir.
represantativeNode	İnt	Düğümün temsilci düğüm olduğunu gösterir.
sourceNode	İnt	Düğümün kaynak düğüm olduğunu belirtir. Sadece simulasyon uygulamasında kullanılır.
trDest	İnt	Sadece varış düğümünün bildiği değer. Bu sayede hem yönlendirme cevap aşaması başlar, hemde mesajlaşma esnasında mesajın kaynak düğüm tarafından alınması sağlanır.

Tablo 5.11: Temsilci düğüm sayısı (Bir adet)

Temsilci Düğüm Sayısı (Bir Adet)				
Düğüm Sayısı	**Yayın Mesajı Sayısı**	**HOP Sayısı**	**Ziyaret Edilen Düğüm Sayısı**	**Mesaj Uzaklığı**
100	3245	5	98	17
144	5038	6	142	20
256	9801	8	255	28
400	16049	10	398	36

Tablo 5.11 ve Tablo 5.12'de belirtildiği üzere sistemde temsilci düğümlerin sayısı arttırıldığında sistemin anomimlik derecesinin değişmediği gözlemlenmiştir. Ayrıca bu yöntemde temsilci düğümlerin sayılarının arttırılmasının sistemin sahipsizliği üzerinde etkisi bulunmamaktadır. Bu yöntemde mesaj gönderim sırasında sistemin sahipsizliği bire yakın değerlerde çıkmaktadır. Sistemde temsilci düğümlerin arttırılması durumunda yayın mesajlarının sayısında ve kaynak ile varış arasızndaki yolun uzaklığında azalma gözlemlenmiştir. Ayrıca bu yöntemde varış ile kaynak arasındaki uzaklık imgesel yönlendirme yöntemine göre çok daha azdır. Bu sebepten dolayı hat geçikmesi de daha az olmaktadır.

Tablo 5.12: Temsilci düğüm sayısı (Dört Adet)

Temsilci Düğüm Sayısı (Dört Adet)				
Düğüm Sayısı	**Yayın Mesajı Sayısı**	**HOP Sayısı (Temsilci alan içerisinde)**	**Ziyaret Edilen Düğüm Sayısı**	**Mesaj Uzaklığı**
100	1450	3	98	4+6
144	2617	3	143	11+4
256	6267	5	254	16+5
400	11600	6	399	23+6

6. SONUÇLAR VE TARTIŞMA

Bu kapsamda önerilen iki yöntem değişik ağ topolojilerine göre karşılaştırılmıştır. Düşük hat gecikmesi gereken sistemlerde KTAMG yöntemi başarılı sonuçlar vermiştir. Bu yöntemle varış ile düğüm arasındaki uzaklık imgesel yönlendirme yöntemine göre çok daha az çıkmaktadır. Fakat bu yöntem mesaj gönderim esnasında yayın mesajları imgesel yönlendirme yöntemine göre çok daha fazladır. İmgesel yönlendirme yöntemi mesaj gönderim esnasında daha az sayıda yayın mesajı isteyen sistemlerde kullanılması gerekmektedir. Hat gecikmesinin önemli olmadığı sistemlerde ise imgesel yönlendirme yöntemi işlem karmaşasını ciddi bir şekilde azaltmaktadır.

Tablo 6.1: Önerilen yöntemlerin karşılaştırılması

Yöntemlerin Karşılaştırılması				
Düğüm Sayısı	**Küme Tabanlı Mesaj Gönderim**		**İmgesel Yönlendirme**	
	Yayın Mesajı Sayısı	**Mesaj Uzaklığı**	**Yayın Mesajı Sayısı (MSEND)**	**Mesaj Uzaklığı**
100	3245	17	167	20
144	5038	20	143	23
256	9801	28	199	33
400	16049	36	255	43

KAYNAKLAR

[1] **Raymond, J.-F.**, 2000. Traffic Analysis: Protocols, attacks, design issues and open problems. In Proc. Workshop on Design Issues in Anonymity and Unobservability, ICSI TR-00-011, Berkeley, CA, USA, (25-26 July 2000), s. 7-26

[2] **John, D. B., Maltz, D.A.**, 1996. Dynamic Source Routing in Ad Hoc Wireless Networks. Mobile Computing, , volume 353, 153-181

[3] **Perkins, C. E., Royer, E.M.,** 1999. Ad-Hoc On-Demand Distance Vector Routing. In IEEE WMCSA '99, s 90-100

[4] **Back, A., Moller, U., Stiglic, A.**, 2001. Traffic Analysis Attacks and Trade-Offs in Anonymity Providing Systems. In Proceedings of Information Hiding Workshop (IH 2001), Pittsburgh (2001), s 245-257

[5] **Chaum, D.**, 1998. The Dining Cryptographers Problem: Unconditional Sender and Receipent Untraceability. In Journal of Cryptology 1, s 65-75

[6] **Chaum, D.**, 1981. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms ,Communications of the Associations for Computing Machinery 24, 2 , s 84-88

[7] **Pfitzmann, A., Pfitzmann, B.**, 1986. Networks Without User Observability-Design Options. In Eurocrypt 85, Springer-Verlag, Berlin (1986), s 245-253

[8] **Pfitzmann, A., Pfitzmann, B., and Waidner, M.**, 1991**.** ISDN-Mixes: Untraceable Communication with Very Small Bandwith Overhead. In GI/ITG Conference: Communication in Distributed Systems, Mannheim (Şubat 1991), s 451-463

[9] **Danezis, G.,** 2003. MIX-networks with Restricted Routes. In the Proceedings of Privacy Enhancing Technologies Workshop

[10] **Berthold, O., Pfitzman, A., and Standtke, R.**, 2000. The Disadvantages of Free MIX Routes and How to Overcome Them. In the Proceedings of Privacy Enhancing Technologies Workshop on Design Issues in Anonymity and Unobservability, Temmuz 2000, s 30-45

[11] **Anonymizer**, www.anonymizer.com

[12] **Reiter, M. K., and Rubin, A.D.**, 1999. Anonymous Web Transactions with Crowds. In Communications of the ACM 42, 2, Şubat. 1999, s 32-48

[13] **Reed, M. G., Syverson, P.F., Goldschlag, D.M.**, 1998. Anonymous Connections and Onion Routing. In IEEE Journal on Selected Areas in Communications 16 (4), Mayıs 1998, s 482-494

[14] **Shields, C., Levine, B.N.**, 2000. A Protocol for Anonymous Communication Over the Internet. In Proceedings of the 7th ACM Conference on Computer and Communications Security, Athens, Greece, Kasım 2000, s 33-42

[15] **Berthold, O., Federrath, H., Kohntopp,** 2002**. M.** Project "Anonymity and Unobservability in the Internet". Infrastructure Security Conference (InfraSec), Springer

[16] **Berthold, O., Federrath, H., Kopsel, S.**, 2000. Web MIXes: A System for Anonymous and Unobservable Internet Access. In H. Federrath, editor, Designing Privacy Enhancing Technologies; Workshop on Design Issue in Anonymity and Unobservability. Springer-Verlag,

[17] **Kong, J., Hong, X., Gerla, M.**, 2003. An Anonymous On Demand Routing Protocol with Untraceable Routes for Mobile Ad-hoc Networks, Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking & Computing, s 291-302

[18] **Boukerche A, El-khatib K, XU L, Kobra L,** 2004. A Novel Solution For Achieving Anonymity In Wireless Ad Hoc Networks, In Proceedings of the 1st ACM International Workshop on Performance Evaluation Of Wireless Ad Hoc, Sensor, And Ubiquitous Networks, s 30–38.

[19] **Jiejun K, Xiaoyan H, Sanadidi, M.Y., Gerla, M.,** 2005**.** Mobile Ad Hoc Networks Need Efficient Anonymous Routing, Proceedings. 10th IEEE Symposium On Computers And Communications.

[20] **Lefevre K, Dewitt D, Ramakrihnan D,** 2006. Multidimensional K-Anonymity, IEEE International Conference On Data Engineering

[21] **Seys S, Preneel B,** 2006. Anonymous Routing Protocol for Mobile Ad hoc Networks, 20th IEEE International Comminications

[21] **PapamitiratosP.,** 2006. Secure ad hoc Networking Consumer Communications and Networking Conference, s. 10-14

ÖZGEÇMİŞ

Mustafa DAYIOĞLU; 23 Temmuz 1978 yılında İstanbul'da doğmuştur. Lise eğitimini 1995 yılında İstanbul Atatürk Fen Lisesinde tamamlamıştır. Lisans eğitiminde 2001 yılında İstanbul Teknik Üniversitesi Elektrik – Elektronik Fakültesi Kontrol ve Bilgisayar Mühendisliği ve 2004 yılında İşletme Fakültesi İşletme Mühendisliği bölümlerinden mezun olmuştur. Eğitim hayatına halen İstanbul Teknik Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Yüksek Lisans programında devam ettirmektedir. Ayrıca 2001 yılından beri TÜBİTAK – Ulusal Elektronik Kriptoloji Araştırma Enstitüsünde Uzman Araştırmacı olarak çalışmaktadır.