AOMDV Protokolünde Black Hole Ataklara Karşı Geliştirilmiş Güvenlik Uygulaması

Sinan TOKLU [1], Aziz AYDIN [2]

[1]Bilgisayar Mühendisliği, Düzce Üniversitesi, Düzce, Türkiye
[2] Akademedya Yazılım, Kocaeli Üniversitesi Teknopark
sinantoklu@duzce.edu.tr, aziz.aydn@hotmail.com
(Geliş/Received:08.12.2016; Kabul/Accepted:03.03.2017)
DOI: 10.17671/gazibtd.309306

Özet- İletişimin büyük kısmını oluşturan kablosuz ağların kullanımı hızlı bir şekilde artmaktadır. Tasarsız ağlar sıklıkla hareketli düğümlerden oluşan alt yapısız kablosuz ağlardır. Tasarsız ağlarda düğümler hem diğer düğümlerle iletişim kurabilir hem de paketleri ileterek yönlendirici görevi üstlenirler. Bu ağlar arama kurtarma, ofis, kampüs, konferans salonu, üniversite ve şehir ağlarında kullanılmaktadırlar. Tasarsız ağlarda düğümlerin hareketli olması, bir altyapının mevcut olmaması, bant genişliğinin ve güç kapasitesinin sınırlı olması bu ağların en önemli sorunlarındandır. Düğümlerin hareketliliği topolojinin hızlı bir şekilde değişmesine ve kurulan yolların bozulmasına neden olmaktadır. Bu çalışmada, ağın güvenliğini bozacak black hole ataklar tasarlayıp, ağın güvenirliğini artıracak güvenlik uygulaması geliştirilmiştir. Çalışmada tasarsız ağlarda kullanılan en güncel protokollerden birisi olan Ad hoc on-demand multipath distance vector (AOMDV) protokolü kullanılmıştır. Bu amaçla, güvenlik uygulamasında senaryolar üretilmiş olup, daha sonra da bu senaryolardan yararlanılarak AOMDV protokolünde güvenlik uygulamasının altyapısı oluşturulmuştur. Çalışmada benzetim aracı olarak Network Simulator (NS 2) programının 2.35 sürümü ve diğer ağ benzetim yazılımları için yardımcı programlar olan tracegraph202, APP-Tool-master grafik yazılımları kullanılmıştır.

Anahtar sözcükler- AOMDV, MANET, Black hole

Implemented Security Application Against Black Hole Attacks in AOMDV Protocol

Abstract- The use of wireless network forming the major part of the communication is increasing rapidly. Ad-hoc networks are typically composed of mobile nodes lower unstructured wireless networks. In ad-hoc network nodes can communicate with other nodes as they undertake the task of the router transmits both packages. These networks are search and rescue, office, campus, conference hall, university and city are used in the network. Be mobile nodes in ad-hoc networking, the absence of infrastructure, limited bandwidth and power capacity of the most important problem of this network. The topology of the nodes mobility leads to deterioration of rapid change and established ways. In this study, the design of black hole attacks to disrupt network security, is a security application that will increase the reliability of the network developed. Most of the current protocols used in networks tasarsiz study, which is one of AOMDV protocol was used. For this purpose, scenarios are being produced in a security application, and then utilizing the aomdv Protocol security in these scenarios the structure of the application has been established. In the study as a simulation tool the network Simulator (ns-2) Version 2.35 of the program, and other network utilities for the simulation software tracegraph202 app-tool-master software was used for graphics.

Keywords- AOMDV, MANET, Black hole

1. GİRİŞ (INTRODUCTION)

Tasarsız ağlar bir grup hareketli ya da hareketsiz düğümün bir araya gelerek oluşturduğu çok adımlı, önceden kurulmuş bir altyapıya sahip olmayan kablosuz ağlardır. Bu ağlardaki düğümler genelde hareketli olmakla beraber sabit düğümler de içerebilirler. Altyapılı ağlardaki gibi bir merkezi bir yönetim bulunmamaktadır. Düğümler hem yönlendirici görevini üstlenmekte hem de diğer düğümlerle iletişim kurmaktadırlar. Ağ altyapısız olduğundan düğümler istedikleri gibi hareket edebilmektedir. Tüm düğümler birbirlerinin kapsama alanında bulunamayacaklarından iletişim çok adımlı olarak yapılmaktadır. Tasarsız ağlar topoloji değişimlerine kolay uyum sağlayabilirler. Herhangi bir düğüm kurulan yoldan çıktığında durum fark edilir ve yeni bir yol kurma süreciyle iletişime kalınan yerden devam edilir. Bu durum gecikmeye sebep olsa da ağ hala iletişime imkan tanımaktadır. Tasarsız ağlardaki düğümlerin güç kaynakları, işlemci kabiliyetleri, saklama kapasiteleri ve bant genişlikleri kısıtlıdır. Güç kaynağının kısıtlı olması düğümlerin kapsama alanlarını sınırlandırmaktadır. Düğümlerin hareketli olması ağırlıklarına sınırlamalar getirmektedir. Bant genişliğinin sınırlı olması da tasarsız ağlarda gönderilecek kontrol mesajlarının sıklığına ve miktarına kısıtlamalar getirmektedir. Tasarsız ağlarda başarılı bir iletişim oluşabilmesi için bu kıt kaynakların etkin olarak kullanılabilmesi gerekmektedir [1].

Tüm uygulama alanlarının yönlendirme protokollerinden kendilerine has istekleri ve ihtiyaçları vardır. Duyarga ağ uygulamaları minimum enerji tüketimi isterken konferans uygulamaları gerçek zamanlı uygulamalar servis kalitesine önem vermektedirler. Tasarsız ağlarda kullanılan iletişim ortamının da -radyo haberleşmesi- kendine has özellikleri vardır. Örneğin, düğümler arasındaki bağlantılar tek yönlü olabilir. Bunun sebebi iki düğümün ileticilerinin güçlerinin farklılığı yüzünden sadece birinin diğerini duyabilmesi ya da ortamdaki gürültü olabilmektedir [2]. Çok adımlı iletişim yapılması hem güçte hem de iletim kapasitesinde yüksek kazançlara yol açmaktadır. Böylece düğümler paketleri çok daha az çıkış gücüyle çok adımda gönderebilmektedirler. Tasarsız ağların daha karmaşık uygulamalarda kullanılmasıyla, servis kalitesine (QoS) olan ihtiyaç artmaktadır. Bu ağların kullanılması ise güvenlik gereksinimlerini ortaya çıkarmıştır. Hareketli ad-hoc ağlarda (Mobile Ad-hoc Networks, MANET) gömülü bir güvenlik tasarımı yer almadığından ataklara karşı savunmasız yapıdadırlar. Dolayısıyla kablosuz kanal hem ağdaki kullanıcılara hem de ağda yer alan kötü niyetli kullanıcılara erişilebilir durumdadır. Güvenlik Ad hoc ağlarda ki en önemli konulardan biridir. Ad hoc ağlardaki en yaygın ataklar ağdan gönderilen paketlerin kötü niyetli düğümler tarafından yok edilmesi ve gelen paketlerde kötü niyetli düğümlerin değişiklik yaparak ağda karışıklığa yol açmasıyla ağın performansının düşürülmesinin hedeflenmesidir. MANET paylaşılan kablosuz ağ ortamı vasıtasıyla hareketli düğümlerin birbiriyle iletişim isteğinde bulunduğu bir yapıya sahiptir [1, 3].

Bu çalışmada tasarsız ağların önemli bir sorunu olan güvenlik konusunda tasarsız ağlardaki güncel protokollerden biri olan AOMDV protokolü kullanılarak, ağda black hole saldırısı oluşturmak ve düğümlerin ağa katılımındaki hız parametreleri dikkate alınarak senaryolar üretip kötü niyetli düğümlere karşı ağda daha iyi performansın elde edilmesi için güvenlik uygulaması geliştirilmiştir. Bölüm 2'de AOMDV protokolü genel olarak anlatılmıştır. Bölüm 3'te ise gerçekleştirilen güvenlik uygulaması anlatılmıştır ve bölüm 4'te ise gerçekleştirilen benzetim ve elde edilen sonuçlar verilmiştir.

2. AOMDV PROTOKOLÜ (AOMDV PROTOCOL)

AOMDV protokolü Destination Sequenced Distance Vector (DSDV) protokolünden temel alınmıştır. AOMDV protokolünde on binlerce dinamik düğümden atlamalar yapılarak bir network sistemi oluşturulabilmektedir. AOMDV protokolünde temel konsept yön bulma süreçlerinde birçok yolun üretilmesi ve hesaplanmasıdır. Bağlantının kopması ve genellikle yanlış yönlendirmelerin gerçekleşmesi dinamik bir yapıya sahip olan AOMDV protokolünde avantaj sağlamaktadır. Yönlendirmede tek yol kullanan Ad Hoc On Demand Distance Vector (AODV) protokolü yönlendirmede herhangi bir yol kullanılmadığında yeni yol arayışına girmektedir. Bu durum her yol bulmada gecikmeye ve ağa yük getirisine neden olmaktadır. AOMDV protokolünde belirtilen verimsizliğin önüne geçmek için çoklu yol kullanılmaktadır[4, 5].

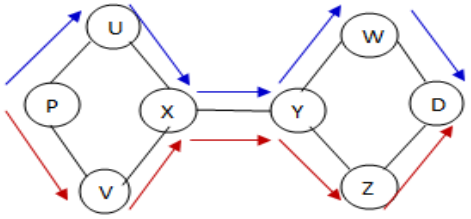
AOMDV protokolünde kaynak düğüm ağa istek paketi (Route Request,RREQ) yayar. Paketi alan ara düğüm yönlendirme tablosunu kontrol eder. Yönlendirme tablosunda hedef düğüme ulaşacak yol bilgisi mevcut ise kaynak düğüme geriye dönük cevap paketi (Route Reply,RREP) paketi gönderir. Hedef düğüme gidecek yol bilgisi yönlendirme tablosunda bulunmuyorsa komşu düğümlere RREQ paketi yaymaya devam edecektir. AODV Protokolünde paketi alan ara düğümde kopya RREQ paketleri oluştuğunda kopya RREQ paketlerden en geç gelen istek paketi göz ardı edilir. Hedef düğüme geç gelen RREQ paketi atılır. AOMDV protokolünde kopya RREQ paketleri atılmaz. Her kopya işlenir. AOMDV protokolünde hedef düğüme gelen paketler işlenmektedir. Gelen paketlerin çoklu olması, hedef düğümden gönderilen yayının diğer düğümlere birden çok yol sunması ve hangi yolların düğümlere ilan edilmesi ve düğümlerin hangi yolları kabul etmesi gerektiği sorusunu

AOMDV protokolünün loop freedom özelliği belirlemektedir [6].

Döngüden kaçınmak için koşullar aşağıda listelenmiştir:

1. Farklı sıra numarası: Hedef düğüme gelen farklı sıra numarasına sahip paketlerden AODV protokolünde olduğu gibi en eski sıra numarasına sahip paket döngüden kaçınmak için atılır.
2. Aynı sıra numarası: Atlama sayısı daha kısa olan yol seçilir. Daha kısa yol bulunmazsa seçilen kısa yoldan başka seçenek bulunmamaktadır.

Hedef düğüme gidecek birden fazla ortak bağlantı bulunması ağda trafik oluşmasına ve tıkanıklığa neden olacaktır. Bundan dolayı ayrık düğüm ve linkler gereklidir. AOMDV protokolünün path disjointness özelliği dikkate alınarak ağın performansı iyileştirilmektedir. Ayrık bağlantı sağlama koşulunun gerçekleşmesi sonraki atlama ve son atlamanın birbirinden farklı olmasına bağlıdır. Şekil 2.1'de P düğümünden D düğümüne giden yolda X düğümü belirtilen koşulu sağlamamaktadır. Bu durumda P-U-X-Y-W-D veya P-V-X-Y-Z-D yollarından biri kullanılacaktır [4, 7].



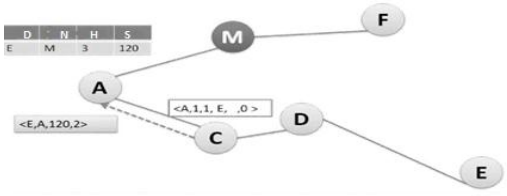
Şekil 2.1. Ayrık bağlantı fikri.(Discrete connection idea)

AOMDV protokolünde çoklu yol sayesinde RREP paketleri tüm düğümlere gönderilmektedir. Ad-hoc ağlarda bağlantı hataları hareketlilik, tıkanıklık, paket çakışmaları, düğüm ya da hop hataları vb. görülebilmektedir. Gönderilen paket yol boyunca bozuk bağlantıya rastladığında hedef düğümden kaynak düğüme doğru RRER paketi yayılır. Yeni bir yol düğümlerin yönlendirme tablolarından tespit edilerek paket akışına devam edilir. Tüm bağlantı yolları bozulduğunda yeni bir yol kurmak gerekecektir. AODV protokolünde bozuk bağlantıya rastlanıldığında ağın kaynaklarını tüketerek yeni bir yol kurma arayışına gidilmektedir. AOMDV çoklu yol sayesinde bulunduğu ağın kaynaklarını daha verimli kullanabilmektedir [8].

AOMDV protokolünde yapılan çalışmalardan bir tanesi öncelikli AOMDV(P-AOMDV) olarak ta adlandırılan yeni bir yönlendirme protokolüdür. Bu protokol otobüs ulaşımı esnasında mobil altyapı kullanılarak beraber işlem yapabilme yeteneği kazandırmıştır. Bu sayede bağlanılabilirlik kayıpların etkisi azaltılmış ve ağın performansı geliştirilmiştir. P-AOMDV kaynak ve hedef arasında bir çok yol bulmakta ve bu işlem sayesinde düğümlerin daha hızlı iletişimine destek vermektedir[9]. Diğer bir çalışmada ise çok yollu yönlendirme protokolü geliştirilmiştir. Alıcı tabanlı AOMDV (RB-AOMDV) olarak adlandırılan bu protokol AOMDV protokolünün güvenirlilik avantajlarını almış ve tekrar kurulum keşif zamanını azaltmıştır. Alıcı düğüm belirli bir zaman aralığında herhangi bir veri paketi alamazsa yol keşfi işleminde olduğunu varsaymaktadır[10].

2.1.Black Hole Atak (Black Hole Attack)

Black hole atak Dos saldırı ataklarının türlerinden biridir. Uydurma yönlendirme bilgisi dağıtır ve üretir. Black hole saldırısında kötü niyetli bir düğüm uydurma yönlendirme bilgilerini gönderir. Kötü niyetli düğüm yönlendirme bilgisinin optimum olduğunu diğer düğümlere yayar. Saldırgan düğüm kaynak düğüme uydurma RREP paketi göndererek hedef düğüme giden daha iyi bir yol olduğunu iddia eder [11]. Hedef düğüme gönderilen RREP paketindeki hedef sıra numarası RREQ paketindeki sıra numarasından daha büyük veya eşit uydurma numarasıdır. Saldırgan kaynak düğümün kendisi üzerinden geçmesi gerektiği bilgisini yayarak ağdaki tüm trafiği yönetmektedir. Şekil 2.2'de RREP paketini alan kaynak düğüm örneği gösterilmiştir [12].



Şekil 2.2. RREP paketini alan kaynak düğüm örneği. (The source node instance that receives the RREP package)

Şekil 2.2'de gösterildiği gibi A kaynak düğümü E hedef düğümüne veri göndermek istemektedir. Kötü niyetli düğümün (M) ağa etkisi tespit edilmiştir. Kaynak düğümde hedef düğüme gidecek yol bilgisi bulunmadığından, tüm komşu düğümlere RREQ paketi yayacaktır [13]. Gönderilecek RREQ paketinin yapısı aşağıdaki bilgilerden oluşmaktadır. Kaynak düğümün adresi, kaynak düğümün adresi, broadcast numarası, hedef düğümün adresi, hedef sıra numarası ve atlama sayısından oluşmaktadır. Kaynak düğüm RREQ paketini gönderdiğinde oluşacak RREQ paket içeriği <A,1,1,E, ,0> yapısında olacaktır. Paketi alan komşu düğümler (C,M) yönlendirme tablolarını kontrol edeceklerdir. C düğümü yönlendirme tablosunu kontrol ederek, E'ye giden bir yol olduğunu belirlerse geriye dönük A düğümüne RREP paketi gönderecektir. Hedef düğüme giden yol bilgisi yönlendirme tablosunda mevcut değilse kaynak düğümden gelen bilgiyi yönlendirme tablosuna kaydedecektir. Komşu düğümlere istek paketi yaymaya devam edecektir.

Kötü niyetli düğüm paketi aldığında hedef düğüm bilgisinin kendisinde bulunduğu uydurma bilgisini kaynak düğüme RREP paketini göndererek belirtir. Kötü niyetli düğüm hedef düğüme kendisi üzerinden gidildiğinde daha az atlama sayısıyla ulaşabileceğini, RREP paketini kaynak düğüme göndererek, kaynak düğümden iletilen verinin kendisi üzerinden geçmesini istemektedir. Kaynak düğüme gönderilecek RREP paket yapısı hedef düğümün adresi, gelecek düğümün adresi, atlama sayısı ve hedef düğümün sıra numarasından oluşmaktadır. RREP paket içeriği <E,M,120,2> belirtildiği gibi olacaktır [14]. Kaynak düğüm RREP bilgisini aldıktan sonra veriyi M düğümüne gönderecektir. M düğümüne gelen paketler kaybolacaktır. Kötü niyetli düğüm amacına ulaşacaktır.
Bu alanda yapılan çalışmalardan bir tanesinde hiyerarşik kablosuz algılayıcı ağlar için farklı tipteki sinkhole düğümlerin belirlenmesi için yeni bir yaklaşım sunulmuştur. Bu yaklaşımda hiyerarşik kablosuz algılayıcı ağlar bir çok kümelere bölünmüştür ve her küme güçlü bir küme başına sahiptir. Bu küme başı görevinde olan düğümler kendi kümelerinde sinkhole atağı yapan düğümlerin belirlenmesi işlevini yerine getirmektedirler[15]. Diğer bir çalışmada ise Blackhole ve Grayhole atakların belirlenmesi için yeni bir mekanizma önerilmiştir. Bu mekanizma normal AODV yönlendirme protokolünün ve Watchdog mekanizmasının modifikasyonundan sonra çalışmaktadır. Bu mekanizmada düğüm veya herhangi bir yolun güvenirlilik seviyesinin tanımlanması için renk planını kullanmaktadır[16].

3. ÖNERİLEN YÖNTEM İLE AOMDV UYGULAMASI (AOMDV APPLICATION WITH THE PROPOSED METHOD)

Bu çalışmada kötü niyetli düğümlerin ağdaki saldırısının tüm ağı etkilemesinin azaltılması, dinamik yapıdaki düğümlerin belirli hızlarla ağa katılımının sağlanması, ağ kaynaklarının verimsiz kullanımını azaltan güvenlik tasarımı uygulaması amaçlanmış ve gerçekleştirilmiştir. Çalışmada ağdaki veri akışını bozabilecek düğümlerin ağ topolojisindeki karmaşıklık düzeyi incelenerek atakların etkisini azaltmaya dönük güvenlik uygulaması önerilmiştir.

AOMDV protokolünde black hole atağını gerçekleştirebilmek için ağa kötü niyetli düğüm eklenmiştir. Kötü niyetli düğümün ağa etkisi incelenmiştir. Kötü niyetli düğüm üzerinden yol kurulmuş, bu yol üzerinden geçen paketler atılmıştır. Kötü niyetli düğüm bunu yapmak için hedefe gidecek yolun kendisi üzerinden daha az atlama sayısıyla ve daha büyük sıra numarasıyla komşu düğümlere yanlış cevap olarak göndermektedir. Komşu düğümlerden gelen paketler kötü niyetli düğüm tarafından atılmaktadır. Diğer kablosuz yönlendirme protokolleri olan DSDV, AODV, DSR, HWMP vb. black hole saldırısına açıktır [17].

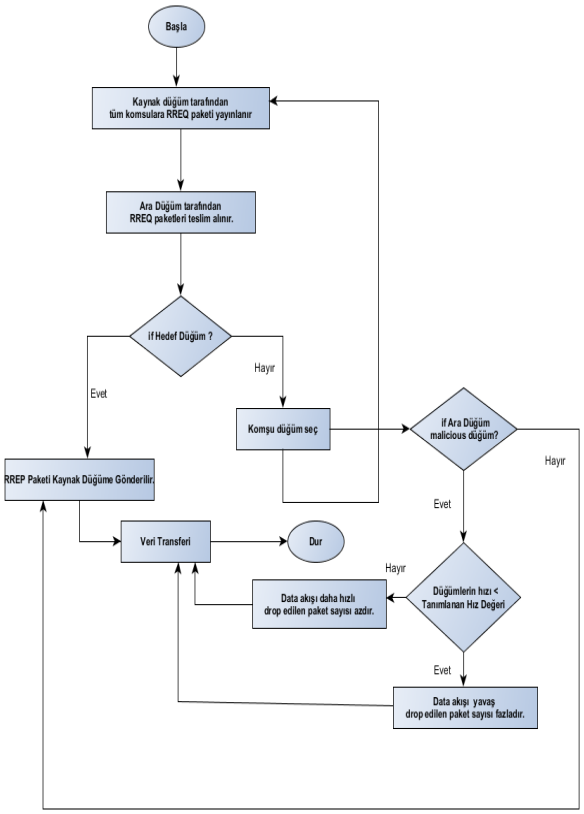
AOMDV protokolünde kötü niyetli düğümün davranışının ağın performansını düşürmesi ve ağdaki veri akışını bozması, dolayısıyla paket kaybının artmasını engellemek için güvenlik uygulaması geliştirilmiştir. Düğümlerin ağa katılımında hareket özelliklerini kullanarak konumlanması ağın performansını artırmaktadır. Düğümlerin ağa belirli hızlarla katılımında kaynak düğümün komşu düğümlere istek paketi göndermeleri, paketleri alan komşu düğümlerin yönlendirme tablolarını güncellemesi ve hedef düğüme gidecek yol bilgisi cevabı yer alan düğümlerin kaynak düğüme cevap paketini göndermesiyle veri akışı başlamaktadır. Kötü niyetli düğümün ağdaki davranışı incelendiğinde düğümlerin ağa katılımında belirli hızlarla yer almaları ve hedef düğüme gidecek sahte yönlendirme bilgisini kaynak düğüme kolayca gönderebildiği görülmektedir [18]. Ağda düşük hızla konumlanan düğümler kötü niyetli düğümün paketleri kaybetmesine neden olmaktadır. Düğümlerin hız parametrelerinin artırılması ağda kurulacak yapının belirsizliği dolayısıyla kötü niyetli düğümlerin sahte yol bilgisi göndermelerini zorlaştırmaktadır.

AOMDV protokolünde çoklu yol kullanıldığından hedef düğüme giden yollardan birisi bozulduğunda hedef düğüme ulaşan diğer yollar üzerinden veri akışı devam etmektedir. AOMDV protokolünün bu yapısı ağda yeni bir yol kurma arayışı için zaman harcamaması düğümlerin ağda konumlanmasının, kötü niyetli düğümün davranışının hız parametresi üzerinde değerlendirebilmekteyiz. Düğümlerin ağa katılım hız değerleri kontrol edilerek zaman aşımı maksimum hız değeri düğümlerin eşik değeri olarak tanımlanmaktadır. Eşik değere yaklaşan düğümlerin ağa katılma hızlarının eşik değere yaklaşması kötü niyetli düğümün ağdaki paket kaybına etkisini azaltmaktadır [19,20]. AOMDV protokolü güvenlik tasarım yapısında tanımlanan hız değeri üzerinden ortaya çıkan akış diyagramı Şekil 3.1'de gösterilmiştir. Akış diyagramında tanımlanan hız değeri en yüksek atlama hız değeri olarak belirlenmiştir. Düğümlerin ağa katılım hız değerleri kontrol edilerek zaman aşımı maksimum hız değerini düğümlerin eşik değeri olarak tanımlamaktayız. Eşik değere yaklaşan düğümlerin ağa katılma hızlarının eşik değere yaklaşması kötü niyetli düğümün ağdaki paket kaybına etkisini azaltmaktadır. Eşik atlama hız değeri aşağıda tanımlanmaktadır.

lb = En düşük atlama (0.2 m/s NS2.)
ub = En yüksek atlama (105 m/s NS2 [21].)

Şekil 3.1'de gösterildiği gibi kaynak düğüm tüm komşu düğümlere paket yollamakta ve bu gönderilen paketler ara düğüm tarafından alınmaktadır. Eğer gönderilen paket hedefte ise ulaştığı bilgisi kaynak düğüme gönderilmektedir. Gönderilen paket hedef düğümde değil ise komşu düğümlerden birisini seçer ve gelen paketi ona yönlendirir. Bu yeni ara düğüm kötü niyetli bir

düğüm ise ve düğümlerin hızı tanımlanan hız değerinden büyük olursa veri akışı hızlı olur ve atılan paket sayısı azalmaktadır. Fakat düğümlerin hızı tanımlanan hız değerinden küçük olursa bu durumda veri akışı yavaşlamakta ve atılan paket sayısı artmaktadır.



Şekil 3.1. Güvenlik uygulaması akış diyagramı.(Flow diagram of safety application)

3.1. Benzetim (Simulation)

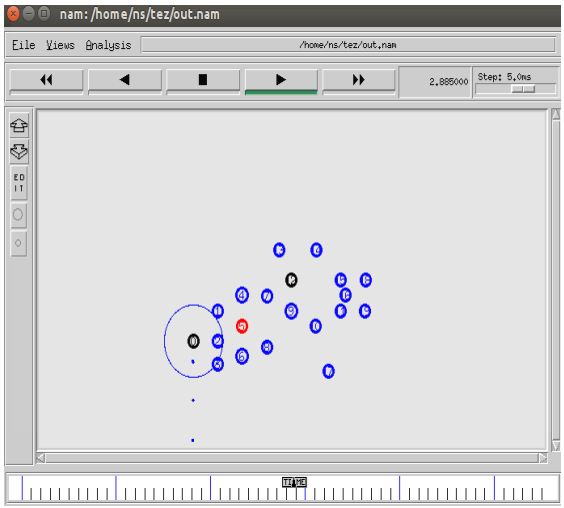
Gerçekleştirilen uygulamanın benzetim aracı olarak Network Simulator (NS 2) programının 2.35 sürümü kullanılmıştır. NS kullanılmasının sebebi kullanıcılara çok sayıda fonksiyon sunması, kablosuz ağları desteklemesi ve açık kaynak kodlu olduğundan protokol eklemeye, mevcut protokolleri değiştirmeye imkân vermesidir. NS 2 kablolu ve kablosuz ağ araştırmalarında kullanılan nesneye dayalı bir ayrık olay benzetim aracıdır.

3.1.1. Benzetim Senaryoları (Simulation Scenarios)

Protokollerin performanslarının karşılaştırılması için 2 farklı senaryo, 6 farklı hareket modeline göre benzetim yapılmıştır. Tüm senaryolarda hareketli düğümler aynı atlama hızlarıyla alana rastgele dağıtılmıştır.

Tcl dosyalarımız düğümlerin ağa katılımındaki hız değerleri dikkate alınarak oluşturulmuştur. Dosyalarımızda kötü niyetli düğümlerin ağa katılım hızı diğer düğümlerin hızlarıyla eş değer olarak belirlenmektedir. Düğümlerin ağa değişken hız tanımlarıyla katıldıklarında ağın performansını hangi ölçüde etkilediği benzetim aracıyla tespit edilmiştir. Senaryolarımızda atlama hızları artan bir şekilde devam etmektedir. Senaryolarda tanımlanan hız değerleri maksimum hız değeri ve minimum hız değeri aralığında belirlenmektedir. Senaryo1 de tanımlanan atlama hızı değerini u1, senaryo 2 de tanımlanan hız değerini u2 belirtilmiştir. Güvenlik uygulaması senaryomuzda ağda yer alan beş numaralı düğüm kötü niyetli düğüm olarak belirlenmiştir. Kötü niyetli düğümün ağda görünmesi için düğüm farklı bir renkte tanımlanmıştır.

Düğümlerin ağdaki davranışları iki hareket senaryosu üzerinden incelenmiştir. Hareket modellerinde kaynak düğümden hedef düğüme giden yollar değişmektedir. İki farklı hareket senaryosunda hedef düğümler değişkenlik göstermektedir. Ağa değişken atlama hızlarıyla katılan düğümlerin atlama hızlarında artış gerçekleştiğinde kötü niyetli düğümün ağdaki performansının etkisi benzetim aracıyla tespit edilmektedir. Şekil 3.2'de senaryolar için kullanılan topoloji gösterilmiştir.



Şekil 3.2. Senaryolar için kullanılan topoloji (Topology used for scenarios)

Şekil 3.2'de gösterilen topolojide ilk hareket modeli için 20 hareketli düğüm oluşturulmaktadır. Topoloji 700 X 700 m'lik bir alana kurulmuştur. Benzetim süresi 60 saniyedir. Hedef düğüm 12. düğüm olarak belirlenmiştir. İkinci hareket modeli 20 hareketli düğümden oluşmaktadır. Topoloji 800 X 800 m'lik bir alana kurulmuştur. Benzetim süresi 60 saniyedir. Hedef düğüm 17. düğüm olarak belirlenmiştir. Üçüncü hareket modeli 20 hareketli düğümden oluşmaktadır. Topoloji 1000*1000 m'lik bir alana kurulmuştur. Benzetim süresi 60 saniyedir. Hedef düğüm 19. düğüm olarak belirlenmiştir. Kaynak ve hedef düğüm aynı renklerde ve kötü niyetli düğüm farklı renkte tanımlanmıştır.

Hareketli düğümler "random waypoint" modeline göre hareket etmektedirler. NS 2 aracının düğüm hareket üreteci "setdest" kullanılarak düğümlerin hareketlerini belirten hareket dosyaları oluşturulmuştur[8]. Hareket dosyası üretilirken ilgili senaryonun hareketli düğüm sayısı, maksimum hızı, benzetim süresi (60s), duraklama süresi ve topolojinin koordinatları verilmektedir. Benzetimde kullanılacak rastlantısal trafik bağlantıları NS 2 aracının trafik senaryo üreteci "cbrgen" ile üretilmektedir. Her senaryo için kullanılan trafik parametreleri ve senaryolarda kullanılan genel parametreler Çizelge 3.1'de gösterilmiştir.

Çizelge 3.1. Benzetim parametreleri (Simulation parameters)

	Senaryo 1	**Senaryo 2**
Düğüm sayısı	20	20
Trafik tipi	CBR	CBR
Seed	1	1
Paket boyutu	512 Byte	512 Byte
Simülasyon süresi	60 s	60 s

3.1.2. Performans Kriterleri (Performance Criteria)

Ağa katılım ve hızları değişken olan düğümlerin katılım hızları ve varış noktalarına göre oluşturulan senaryoların kötü niyetli düğümün ağdaki performansının AOMDV protokolünde karşılaştırılması için aşağıdaki kriterler değerlendirilmiştir.

- Düşürülen paket miktarı: Kaynaklar tarafından üretilen veri paketi sayısının kötü niyetli düğüm tarafından düşürülmesidir. İletiminin verimi, düşürülen paket miktarı ve sonuç itibariyle kullanılan yönlendirme protokolünün güvenilirliği hakkında bilgi sağlamaktadır.

- Ortalama gecikme: Gecikme bir veri paketinin varış tarafından alındığı zamandan paketin kaynak tarafından üretildiği zamanın çıkarılmasıyla elde edilmektedir. Gecikme, kuyrukta beklemeden, MAC seviyesindeki gecikmeden, iletim ve yayılım gecikmelerinden oluşmaktadır. Gecikme servis kalitesi için önemli bir parametre olduğundan kullanılan yönlendirme protokolünün güvenilirliği hakkında bilgi sağlamaktadır.

4. BENZETİM SONUÇLARI (SIMULATION RESULTS)

Bu bölümde önerilen 2 senaryonun ağa farklı katılım hızlarıyla yer almalarının kötü niyetli düğüm karşısındaki performansları benzetim sonuçlarına göre karşılaştırılmaktadır. Her senaryo için 2 farklı ağa katılım hızlarıyla oluşturulan ve kaynak düğümden hedef düğüme giden farklı yollar kullanılarak 6 farklı hareket modeline göre benzetim yapılmıştır.

4.1.Düşürülen Paket Miktarı (Dropped Package Amount)

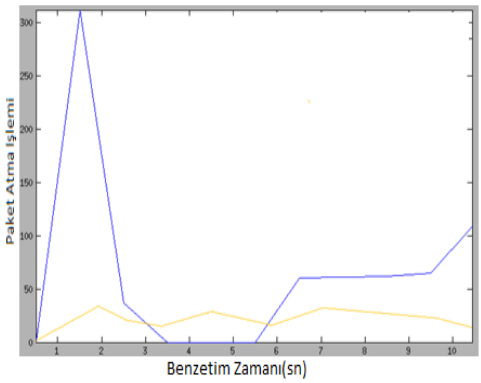
Şekil 4.1'de a'da gösterildiği gibi Senaryo 1-1 hareket modelinde 707 paket düşürülmüştür. Senaryo 2-1 hareket modelinde 204 paket düşürülmüştür. Kaynak düğüm 0. düğüm hedef düğüm 12.düğüm olarak belirlenmiştir. b'de ise düğümler Senaryo 1-2 hareket modelinde 692 paket düşürülmüştür. Senaryo 2-2 hareket modelinde 265 paket düşürülmüştür. Kaynak düğüm 0. düğüm hedef düğüm 17.düğüm olarak belirlenmiştir. c'de gösterilen grafikte ise Senaryo 1-3 hareket modelinde düğümlerden 769 paket düşürülmüştür. Senaryo 2-3 hareket modelinde 355 paket düşürülmüştür. Kaynak düğüm 0. düğüm hedef düğüm 19.düğüm olarak belirlenmiştir. Elde edilen sonuçlara bakıldığında düğümlerin farklı topolojilerde ağda değişken katılım hızlarıyla yer aldıklarında, ağa katılım hızının yüksek olması kötü niyetli düğümün paket atmasını zorlaştırmaktadır. Bu durum ağdaki paket kaybını azaltmakta ve ağın performansını artırmaktadır. Çizelge 3.2'de düşürülen paket miktarı tablo halinde gösterilmektedir.

Çizelge 3.2. Düşürülen paket miktarı (*Dropped Package Amount*)

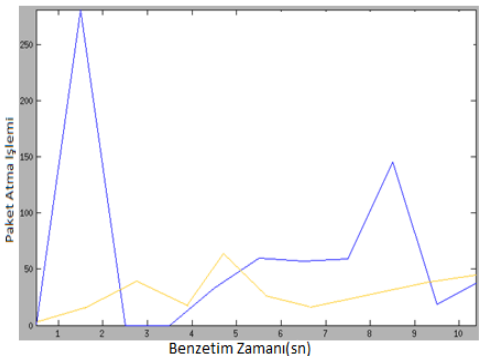
Senaryolar	**Düşürülen paket miktarı**	**(Kaynak – Hedef) Düğüm**
Senaryo 1-1	707	0-12
Senaryo 2-1	204	0-12
Senaryo 1-2	692	0-17
Senaryo 2-2	265	0-17
Senaryo 1-3	769	0-19
Senaryo 2-3	355	0-19

4.2.Ortalama Gecikme (Average Delay)

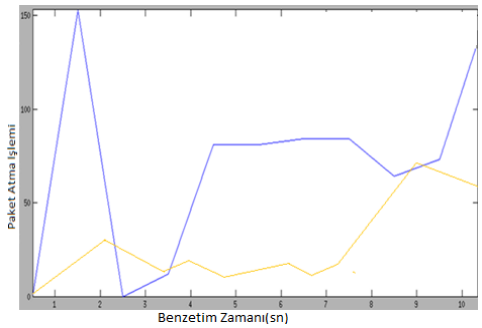
Şekil 4.2'de senaryo 1'de düğümlerin ağa u1 katılım hızıyla katıldıklarında ortalama gecikme gösterilmektedir. Şekil 4.2 a'da gösterildiği gibi Senaryo 1-1 hareket modelinde ortalama gecikme 9873.62 ms'dir. Kaynak düğüm 0.düğüm hedef düğüm 12.düğüm olarak belirlenmiştir. b'de senaryo 1'de düğümlerin ağa belirlenen katılım hızıyla katıldıklarında ortalama gecikme gösterilmektedir. Kaynak düğüm 0. düğüm hedef düğüm 17.düğüm olarak belirlenmiştir. Senaryo 1-2 hareket modelinde ortalama gecikme 9275.3 ms'dir. c'de senaryo 1'de düğümlerin ağa belirlenen katılım hızıyla katıldıklarında ortalama gecikme gösterilmektedir.



a) Senaryo 1-1 ve Senaryo 2-1



b) Senaryo 1-2 ve Senaryo 2-2

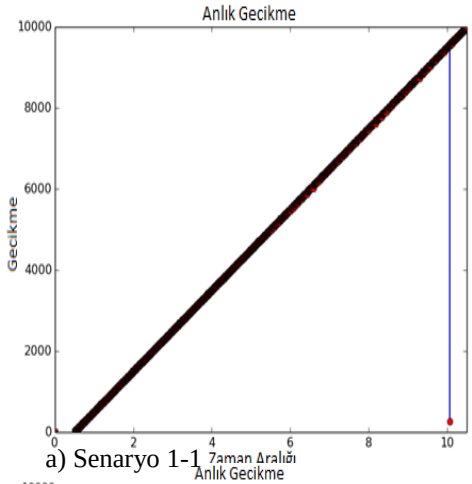


c) Senaryo 1-3 ve Senaryo 2-3

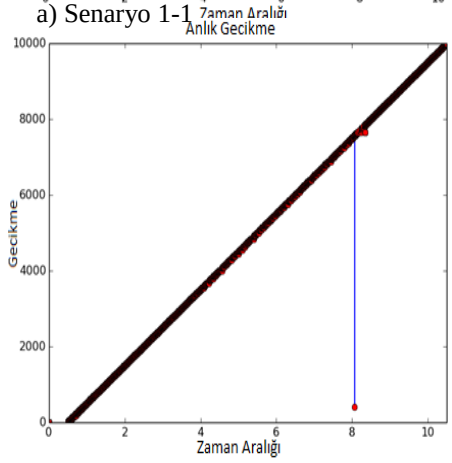
Şekil 4.1. İki Senaryonun Paket Düşürme Grafiği. (Package Dropped Chart of Two Scenarios.)

Çizelge 3.3. Ortalama gecikme (*Average Delay*)

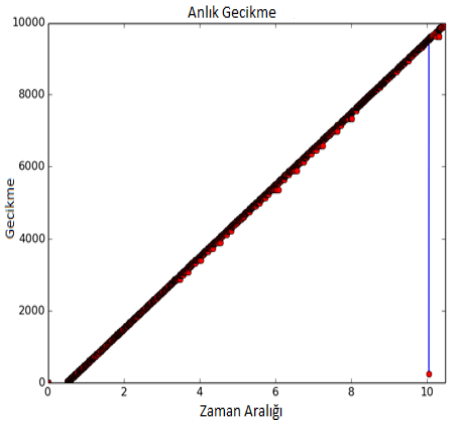
Senaryolar	**Ortalama gecikme**	**(Kaynak – Hedef) Düğüm**
Senaryo 1-1	9873.62 ms	0-12
Senaryo 2-1	6726.43 ms	0-12
Senaryo 1-2	9275.3 ms	0-17
Senaryo 2-2	7034.08 ms	0-17
Senaryo 1-3	9943.79 ms	0-19
Senaryo 2-3	7050.09 ms	0-19



a) Senaryo 1-1



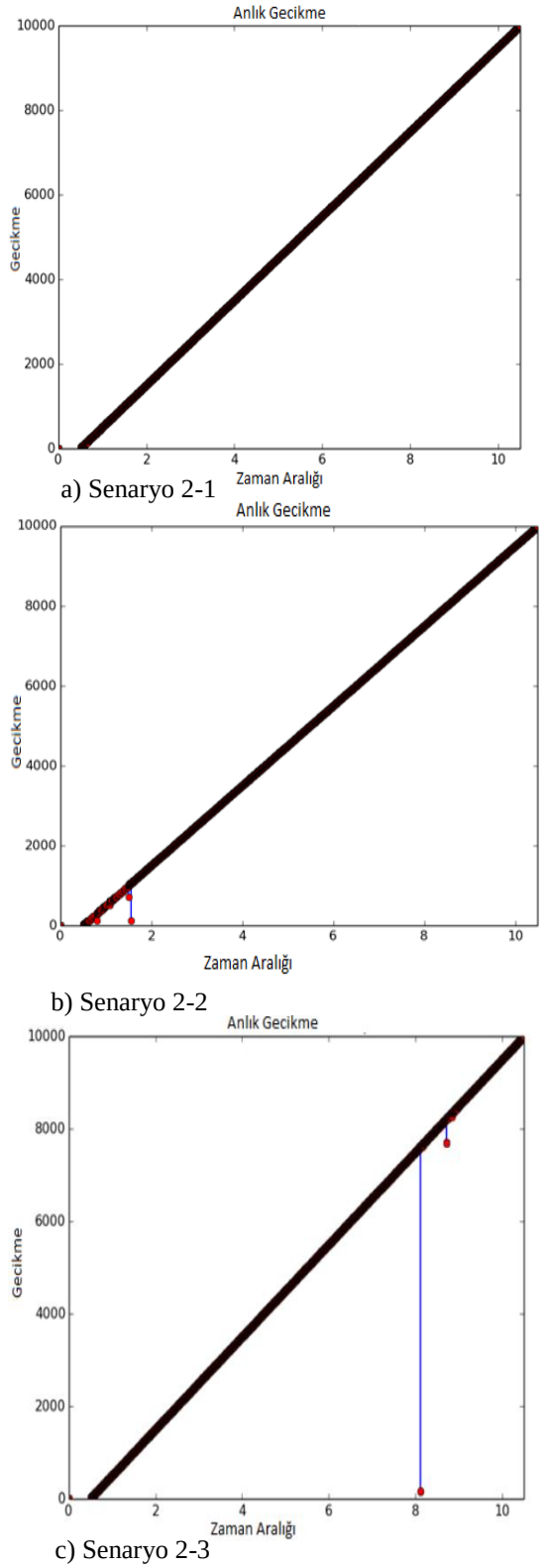
b) Senaryo 1-2



c) Senaryo 1-3

Şekil 4.2. Senaryo 1 ortalama gecikme süreleri. (Scenario 1 average delay times)

Kaynak düğüm 0. düğüm hedef düğüm 19.düğüm olarak belirlenmiştir. Senaryo 1-3 hareket modelinde ortalama gecikme 9943.79 ms'dir. Çizelge 3.3'de elde edilen ortalama gecikme tablo halinde sunulmaktadır. Şekil 4.3'de senaryo 2'de düğümlerin ağa u2 katılım hızıyla katıldıklarında ortalama gecikme gösterilmektedir.



Şekil 4.3. Senaryo 2 ortalama gecikme süreleri. (Scenario 2 average delay times.)

Şekil 4.3 a'da Senaryo 2-1 hareket modelinde ağa belirlenen katılım hızıyla katıldıklarında ortalama gecikme 6726.43 ms dir. Kaynak düğüm 0. düğüm hedef düğüm 12.düğüm olarak belirlenmiştir. b'de senaryo 2'de düğümlerin ağa belirlenen katılım hızıyla katıldıklarında ortalama gecikme gösterilmektedir. Kaynak düğüm 0. düğüm hedef düğüm 17.düğüm olarak belirlenmiştir. Senaryo 2-2 hareket modelinde ortalama gecikme 7034.08 ms' dir. c'de ise senaryo 2'de düğümlerin ağa belirlenen katılım hızıyla katıldıklarında ortalama gecikme gösterilmektedir. Kaynak düğüm 0. düğüm hedef düğüm 19.düğüm olarak belirlenmiştir. Senaryo 2-3 hareket modelinde ortalama gecikme 7050.09 ms' dir.

6. SONUÇLAR (CONCLUSIONS)

Tasarsız ağlarda gömülü bir güvenlik tasarımı yer almadığından ataklara karşı savunmasız yapıdadır. Tasarsız ağların değişken topolojiye sahip olması, düğümlerin hareketli olması ve kablosuz ağ ortamından kaynaklanan olumsuzluklar birçok soruna neden olmaktadır. Dolayısıyla kablosuz kanal hem ağdaki kullanıcılara hem de ağda yer alan kötü niyetli kullanıcılara erişilebilir durumdadır. Tasarsız ağlarda düğümlerin hareketliliği ve topolojinin değişken olması yönlendirme işlemini bu ağların önemli problemlerinden biri kılmaktadır. Bu çalışmada güncel protokollerden AOMDV protokolü kullanılarak, Dos atak türlerinden Black hole saldırısı ağdaki güvenliği bozacak şekilde oluşturulmuştur. Düğümlerin ağa katılım hızları değerlendirilmiştir. Çalışmamızda maksimum hız değeri eşik değer olarak belirlenmektedir. Gerçekleştirdiğimiz benzetim senaryolarında düğümlerin ağa katılım hızlarında artış gerçekleştiğinde kötü niyetli düğümün daha az paket düşürdüğü ve ağdaki ortalama gecikmenin azaldığı elde edilen sonuçlarda gösterilmiştir.

Kötü niyetli düğümün davranışının ağın performansını düşürmesi ve ağdaki veri akışını bozması dolayısıyla paket kaybının artmasını engellemek için düğümlerin ağa katılım hızları artırılmıştır. Farklı topolojilerdeki ağ ortamlarında bulunan düğümlerin özellikle hareketli düğümlerin hedef noktalara veya hareket halinde iken hızlı davranmaları ağa yapılan saldırıların etkisini önemli ölçüde azaltmaktadır.

Tasarsız ağlarda topolojinin ağda değişkenlik göstermesi ve kaynakların sınırlı olması güvenlik uygulamalarının ortaya çıkmasını gerekli kılmaktadır. Topolojide oluşturulan Black hole saldırılarıyla ağın verimliliğinin benzetiminin yapılabildiği, ağa katılım hızlarında değişkenlik gerçekleştiğinde Black hole ataklara karşı düğümlerin direnç gösterdiği, düşürülen paket miktarları ve gecikmelerle tespit edilmiştir. Çalışmada tasarsız ağlarda saldırılara karşı dirençli olan güvenlik uygulamalarına ihtiyacın devam ettiği tespit edilmiştir.

KAYNAKLAR (REFERENCES)

[1] Nevatia, Y., "Ad-Hoc Routing for USARSim", Networks and Distributed Systems Seminar, 2007.

[2] Jani, P.V. "Security within AdHoc Networking," Position Paper, PAMPAS Workshop, 2002.

[3] Gorantala, K. "Routing Protocols in Mobile Ad-hoc Networks", Master Thesis, UMEA University, 2006.

[4] Gupta, P. ve Pandey, S. "Performance Analysis of AOMDV and AODV Routing Protocol in MANET", International Journal of Advanced Research in Computer Science and Software Engineering,vol.5(11), 2015.

[5] Charles E. P. ve Elizabeth M. R. "Ad hoc on-demand distance vector routing", July 2003.

[6] Tiwari, A. ve Verma, N. " A Novel Scheme for Intrusion Detection & Anticipation of Black Hole & Gray Hole Attacks In AODV Based MANET using ZED", International Journal Of Engineering And Computer Science ISSN:2319-7242 vol.3(5), 5744-5751, 2014.

[7] Kurosawa, S. ve Nakayama, H. ve Kato, N. ve Jamalipour, A. ve Nemoto, Y. "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method". International Journal of Network Security, vol.5(3), 338–346, 2007.

[8] Zonglin, L. ve Guangming, H. ve Xingmiao, Y. " Spatial Correlation Detection of DDoS attack", International Conference on Communication, Circuits and System (ICCCAS 2009), 304-308, 2009.

[9] Alves, J. ve Wille, ECG., "P-AOMDV: An improved routing protocol for V2V communication based on public transport backbones", Transactıons on Emerging Telecommunications Technologies, vol:27(12), 1653-1663,2016.

[10] Al-Nahari, A., Mohamad, MM.,"Receiver-Based Ad Hoc On Demand Multipath Routing Protocol for Mobile Ad Hoc Networks", PLOS ONE, vol:11(6), 2016.

[11] Agrawal, S. ve Jain, S. ve Sharma, S. "A Survey of Routing Attacks and Security Measures in Mobile Ad-hoc Networks", Journal of Computing, vol.3(1), 2011.

[12] Revathi, B. ve Geetha, D. "A Survey of Cooperative Black and Gray hole Attack in MANET", International Journal of C.S. And Management Research ,vol 1(2) , September 2012.

[13] Gupta, H. ve Shrivastav, S. ve Sharma, S. "Detecting the DOS Attacks in AOMDV Using AOMDV-IDS Routing", International Conference on Computational Intelligence and Communication Networks, 2013.

[14] Wang, K. ve Chen, J. ve Zhou, H. ve Qin, Y. "Content-Centric Networking: Efect of Content Cachingon Mitigating DoS Attack", International Journal of Computer Science Issue, vol.9, 43-52, 2012.

[15] Wazid, M.,Das, AK., Kumari, S. ve Khan, MK., "Design of sinkhole node detection mechanism for hierarchical wireless sensor networks", Security and Communication Networks, vol:9(17), 45964614, 2016.

[16] Khanna, N. ve Sharma, P.,"Mitigating Blackhole and Grayhole Attack in MANET using Enhanced AODV with TLTB Mechanism", International Journal of Future Generation Communication and Networking, vol:9(8),129-140, 2016.

[17] Chadha, M. ve Joon R., ve Sandeep, "Simulation and Comparison of AODV, DSR and AOMDV Routing Protocols in MANETs", International Journal of Soft Computing and Engineering (IJSCE), vol 2(3), 2231-2307, 2012.

[18] Bhalaji, N. ve Shanmugam, A. "A Trust Based Model to Mitigate Black Hole Attacks in DSR Based Manet", European Journal of Scientific Research ISSN 1450-216X, vol.50(1), 6-15, 2011.

[19]Ahmed, M. ve Md. Hussain, A. "Performance of an IDS in an Adhoc Network under Black Hole and Gray Hole attacks" published in IEEE, 2014.

[20] Chen H.L. ve Lee C.H., "Two Hops Backup Routing Protocol in Mobile Ad Hoc Networks",11th International Conference on Parallel and Distributed Systems Workshops (ICPADS'05), 600-604, 2005.

[21] Internet: http://www.isi.edu/nsnam/ns/tutorial/, 2016.