Karaelmas Fen ve Mühendislik Dergisi
Dergi web sayfası: http://fbd.beun.edu.tr
DOI: 10.7212%2Fzkufbd.v8i1.905

Araştırma Makalesi
Geliş tarihi / Received : 14.02.2017
Kabul tarihi / Accepted : 24.04.2017

Kablosuz Ağlarda Çok Katmanlı Güvenlik ve Performansa Etkisi

Multi-Layer Security and Its Impact on Performance in Wireless Networks

Hacı Bayram Karakurt[1*], Cemal Koçak[2], İbrahim Alper Doğru[2]

[1]HAVELSAN, Hava Elektronik Sanayi ve Ticaret A.Ş, Ankara, Türkiye
[2]Gazi Üniversitesi Teknoloji Fakültesi Bilgisayar Mühendisliği, Ankara, Türkiye

Öz

Günümüzde kablosuz ağların kullanımının hızla artması ile birlikte günlük hayatta hemen hemen her alanda kablosuz cihazlar hayatımızın değişmez bir parçası haline gelmiştir. Hızla artan teknolojik gelişmeler ile beraber güvenlik üzerine geliştirilen çözümler devamlı yenilenmek ve yeni çözümlerinde üretilmesi zorunluluğunu doğurmaktadır. Mevcut sistemlerde ağ güvenliği için verilerin ve paketlerin iletilmesi için birçok protokol kullanılmaktadır. Bunlardan en önemlileri IPSec (Internet Protokol Security), WEP (Wireless Equivalent Privacy), WPA (Wireless Proteced Access), RSN (Robust Security Network), ESP (Encapsulated Security Payload), AHP (Authentication Header) protokolleridir. Bu protokollerden bazıları şifreleme, bazıları yetkilendirme, bazıları ise hem şifreleme hem de yetkilendirme seviyesini artıran güvenlik protokolleridir. Bunların yanında güvenlik düzeyini artırmak için güvenlik duvarı, IKE (Internet Key Exchange) gibi farklı yöntemlerde kullanılmaktadır. Bunlara ek olarak VPN (Virtual Private Network)'de internet üzerinden ağlara kontrollü olarak IP tüneli ile bağlanmayı sağlamaktadır. Bütün bu yöntemler hâlâ kablosuz ağlarda tam güvenliği sağlamamaktadır. Bu çalışmada çeşitli kablosuz ağlar için geliştirilen ve çok katmanlı olarak adlandırdığımız sistemler incelenmiş ve güvenliğin üç temel unsuru olan çoklu protokollerin, güvenlik duvarı ve VPN'nin aynı anda kablosuz ağlara uygulanması ile kablosuz ağlarda güvenliğin nasıl arttığı ve bu üç faktörle beraber veri iletiminde ortalama alınan veri trafikleri performanslarının nasıl etkilendiği ortaya konmuştur.

Anahtar Kelimeler: Güvenlik duvarı, Kablosuz ağlar, Mobil güvenlik protokolleri, Mobil uygulama güvenliği, Sanal özel ağ

Abstract

With rapid increasing use of wireless devices, wireless network has become a constant part of our lives in almost every area. After increasing of this technologies, developed solutions have to be updated with new trends and also new security solutions required for security. In existing systems, there are many protocols for transmitting the data and packages via the devices for network security. The most important protocols are IPSec (Internet Protokol Security), WEP (Wireless Equivalent Privacy), WPA (Wireless Proteced Access), RSN (Robust Security Network), ESP (Encapsulated Security Payload) and AHP (Authentication Header). Some of these protocols are encryption, some are authorization, and some are security protocols that increase both encryption and authorization levels. Beside these protocols, there are a lot of different methods like Firewall, IKE (Internet Key Exchange) to increase level of security. In addition, VPN (Virtual Private Network) is also providing IP tunnel to connect with the network over the internet in a controlled manner. All of these methods are still not providing full security on wireless networks. In this essay, we investigate the systems which called multi-layer and applied using three main procedures called protocols, firewall and VPN simultaneously to the wireless networks and find out how this senarious increased security and how affected average receive data traffics.

Keywords: Firewall, Wireless networks, Mobile security protocols, Mobile application security, Virtual private network

1. Giriş

Kablosuz teknolojilerin hayatımıza girmesiyle birlikte birçok cihazda ve uygulamalarda kablosuz ağların kullanımı kaçınılmaz olmuştur. Bu haberleşme bazen yerel bazen de genel olarak internet üzerinden dünyanın bir ucundan bir ucuna gerçekleşebilmektedir. Çizelge 1'de görüldüğü gibi kullanılan cihazlar bazen kişisel olarak bazen de iş amaçlı olarak kritik verileri içermesi nedeniyle daha kritik hale gelebilmektedir.

Öte yandan bu cihazların kullanım amaçları ve alanlarına çizelgeden baktığımızda en çok kişisel olarak kullanımını

*Sorumlu yazarın e-posta adresi: karakurthbayram@gmail.com

Hacı Bayram Karakurt orcid.org/0000-0003-1591-4502
Cemal Koçak orcid.org/0000-0002-8902-0934
İbrahim Alper Doğru orcid.org/0000-0001-9324-7157

Çizelge 1. Kablosuz ağlarda bilgisayarların kullanım amaçları (Bernik and Markelj 2015).

Örnek Sayısı:216	Kullanım	%
Sadece Kişisel	126	58,3
Kişisel Bazen İş Nedeniyle	56	25,9
Hem Kişisel Hem İş Nedeniyle	31	14,4
İş Nedeniyle Bazen Kişisel	1	0,5
Sadece İş Nedeniyle	2	0,9

görmekle birlikte iş hayatında da kullanıldığı görülmektedir. Burada kritik olan aynı anda hem iş hayatında hem de kişisel amaçlı kullanılan cihazlardır. Bu cihazların kullanılması kişisel bilgilerin ele geçirilme ve farklı alanlarda kullanılmasına sebep olmaktadır.

Aynı şekilde internetin ne amaçlı kullanıldığı, girilen web siteleri, gelen e-postaların zararlı olup olmadığını ayırt etme gibi birçok işlev kablosuz cihazlar için büyük öneme sahiptir. Bu araştırmadan çıkan sonuçlar dikkate alındığında öncelikle kullanıcı bazında alınması gereken temel önlemlerin alınması, kullanıcıların eğitilmesi, kablosuz cihazların kullanımında kişisel veriler ile iş cihazı olarak kullanılan cihazların ayırt edilmesi büyük önem taşımaktadır. Ayrıca kullanılacak olan antivirüs programı da bilgilerin güvenliği için hayati önem taşımaktadır (Agasi 2015, Kim vd. 2015, Shukla vd. 2014, Liu vd. 2015).

Kablosuz ağ tipleri incelendiğinde en önemli ağlardan bir tanesi mobil ad-hoc ağlardır (Mobile ad hoc Network-MANET). Bu ağlarda cihazlar olabilecek minimum konfigürasyonla en kısa sürede verilerin iletilmesi amacıyla kurulmuştur (Frigra-İlisia vd. 2013, Palanisamy ve Sakthviel 2015, Singh ve Munjal 2015, Ahmadb et al. 2015). Bunların yanında kablosuz sensör ağları (Wireless Sensor Network-WSN), kablosuz örgü ağları (Wireless Mesh Network-WMN) ve araçsal ad-hoc ağları (Vehicular ad hoc Network-VANET)'ler de diğer kablosuz ağlara örnek ağlardır. Bu ağların yayın olarak kullanımının artması ile birlikte güvenlik sorunları da eş zamanlı olarak artmaktadır. Genel olarak iyi bir ağ tasarımı çoğu zaman güvenlik riskini azaltmaktadır. Ancak ağ tasarımında kullanılan mekan, uzaklık, ağdaki bağlantı sayısı gibi parametreler ağ güvenliğini sağlamak için yetersiz kalmaktadır. Bu nedenle güvenliği artırmak için birçok yöntem ve protokol üretilmiştir.

Kablosuz ağ tipleri için ayrı ayrı güvenlik önlemleri bulunmaktadır. Güvenlik önlemleri için ise ağın çalışma prensibini ve sistemin özelliklerini iyi bilmek gerekmektedir. Kablosuz ağları incelediğimizde örgü ağları (WMN) kablolu bir alt yapısı olmayan ağlardır ve ad-hoc ağlara benzerlik göstermektedir. Ancak ad-hoc ağlara göre daha organize ve alt yapı sağlamlığına sahiptir ve ad-hoc ağların esnekliğine de sahiptir. Düşük maliyetli olan bu ağlar kolayca ölçeklenebilmektedir. Burada bulut bilişim üzerinden birden çok kablosuz yerel alan ağları ile (Wireless Local Area Network–WLAN) zincir oluşturarak veri transferleri gerçekleştirebilmektedir (Badra vd. 2007). Bu ağlarda verilerin güvenliğini sağlamak için sadece veri transferlerine değil bütün olarak WMN ağlarının yapısına gelebilecek ataklara bakmak gerekmektedir. WMN'ler genel olarak MANET'lere benzemelerine rağmen MANET'ten farklı olarak birden fazla arayüzü olan ve birden fazla radyo frekansı olabilen ağ çeşitleridir (Comley vd 2011, Ratheea vd. Sainib 2016). Şekil 1'de de görüldüğü üzere örgü dağıtıcıları ve clientlerinin olduğu erişim noktaları üzerinden veri transferlerinin gerçekleştiği kendi kendini organize eden ağlardır.

WMN ticari amaçlı olarak kullanılmakla beraber daha esnek yapısının olması sebebiyle saldırılara daha açık olarak bilinmektedir. MANET'lerin kullanmış oldukları İnternet servis sağlayıcıları (Internet Servis Provider-ISP) ve internet protokolü (Internet Protocol-IP) WMN'ler tarafından da kullanılmaktadır. Ayrıca WLAN'ların kullanmış oldukları WI-FI protected access'in özelliklerine de sahip olarak güvenliği standart olarak sağlanmaktadır.

Bir diğer kablosuz ağ ise VANET'lerdir. VANET, MANET'in alt gruplarından birini tanımlamak için kullanılan genel olarak taksi, kamyon motosiklet gibi araçların yollarda kurallara ve koşullara uyarak hareket etmelerin amaçlamaktadır. Günümüzde var olan birçok araç kazaları, sürücü hataları gibi vakaları engellemek amacıyla kurulan ağlardır. VANET ağlarda birinci öncelik araçlarda güvenliği artırmaktır. Bu güvenliği sağlarken yolların alt yapısını, hava koşullarını yolların kaç şerit olduğunu vb. bilgileri kullanması ve bu veriler içinde birtakım erişim noktalarında bulunan vericileri kullanması gerekmektedir. Ayrıca VANET ağlar yollarda oluşan hareketlilik nedeniyle kurulamayan kalıcı ağlara yardımcı olarak mesaj ve hizmetler sunmaktadır. VANET'te düğüm noktalarının 802.11p standardına göre iletişim kurmaları beklenir. Mesajlar alıcı kapsam dışındaysa multi-hop kullanılarak iletilecektir. VANET'ler yol güvenliğini artırmak çeşitli sensörler, uyarılar, telemetrik bilgileri kullanarak sürücüleri normal dışı durumlara ve potansiyel tehlikelere karşı uyarmaktadır. VANET'lerde birtakım güvenlik gereksinimleri bulunmaktadır. Bunlar temel olarak bütünlük, gizlilik ve uygunluktur. VANET'lerde acil durum-

lar için, örneğin ambulans, itfaiye araçlarına bilgi aktarımı anlık olmalıdır. Bununla birlikte yaralı ve ölümcül kazalarda veya daha büyük tehlike anlarında anlık acil mesajlar vermelidir. Ek olarak bu ağın trafik kurallarına hakim olması ve ona göre düğümler arasında sinyalleri göndermesi gerekmektedir. Birden fazla problem olduğu durumlarda; örneğin iki tane kaza birden yaşanıyorsa daha önemli olan kazanın sensörler tarafından ayırt ediliyor olması gerekmektedir (Federrath ve Plöbl 2008).

Günümüzde adli tıpta bir takım bilişim uzmanları mobil güvenlikte yeni çözümler üretmek için bir takım çözümler üretme yoluna gitmişlerdir. Genel olarak ilk aşamada ön bilgi toplama yöntemleri bulunmaktadır. Bu yöntemlerden toplama metotları, işletim sistemleri analizi ve edinilen bilgi türleri sınıflandırılarak ilk aşamada mobil tehditlerin analizi yapılmaktadır. Daha sonra tehditler sınıflandırılmaktadır ve bir takım protokollerle (WEB, WPA, IPSec v.s) güvenlik çözümleri sunulmaktadır (Lloret vd. 2014, Aroraa ve Khera 2015, Elezia ve Raufia 2015, Kundu 2015).

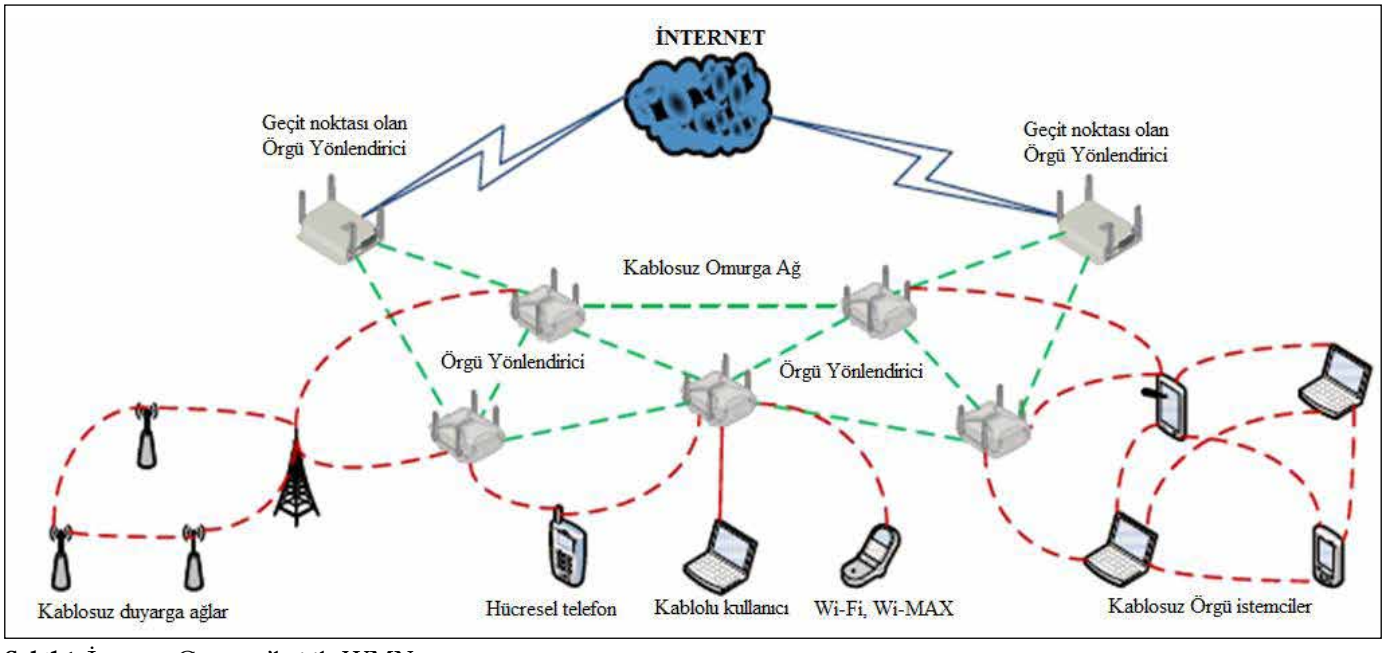
Bütün bu protokoller ve yöntemler bazen tek başına kablosuz ağlarda güvenliği sağlamak için yeterli olmamaktadır. Literatürde bazı çalışmalarda birden fazla protokol, bazı çalışmalarda ise bir protokol farklı yöntem veya bir protokol VPN ile entegre olarak çalışacak şekilde çok katmanlı çözüm yolları sunulmaktadır. Bu makalede de kablosuz ağlarda birden fazla protokolün, bir yöntem ve bir protokolün veya bir protokol ile VPN'in ayrı ayrı uygulandığı güvenlik çözümleri incelenmiş ve bu çok katmanlı güvenliğin performansa olan etkileri incelenmiştir. İkinci bölümde kablosuz ağlarda güvenlik için kullanılan mevcut protokollerden bahsedilmiştir. Üçüncü bölümde ise kablosuz ağlarda güvenlik için çoklu çözüm alternatiflerinden bahsedilmiştir. Dördüncü bölümde bu çoklu katmanlar karşılaştırılmış ve beşinci bölümde ise sonuç ve değerlendirmeler yapılmıştır.

2. Gereç ve Yöntem

2.1. Kablosuz Ağlarda Güvenlik İçin Kullanılan Protokoller

Kablosuz ağ çeşitlerinde genel olarak MANET, VANET ve WMN'lerde güvenlik için bir takım protokoller kullanılmaktadır. Kablosuz ağlarda güvenlik için ilk aşamada ağların şifrelenmesi yöntemi geliştirilmiştir. Burada ilk protokol olan WEB'dir. Bu protokolün esas amacı harici saldırılardan sistemi korumaktır. Ancak bu protokol ağa yetkisiz erişimi de engellemektedir. Bunu yaparken kimlik doğrulama bilgi değiştirme ve gizliliği kontrol etmektedir (Coşkun 2008).

WPA'da ise yazılım güncellemesi boyunca oluşabilecek sorunların kaydedilmesi ve küçük ofisler içinde ağ güvenliğini sağlamak gibi amaçları bulunmaktadır. WPA ilk aşamada açık sistem kimlik denetimi yaparak kablosuz erişim noktalarına sinyal gönderir ve daha sonra 802.X standardındaki kullanıcı kimlik denetimi gerçekleştirir (Bandırmalı vd. 2004, Çeken vd. 2008).



Şekil 1. İnternet Gateway'leri ile WMN.

Bir diğer güvenlik protokolü ise RSN"dir. Bu protokolde kullanıcı bir erişim noktasının varlığının fark edilmesi durumunda bu eşirim noktasının anahtarlarını elde eder ve saklar ve bu anahtar bellekte saklanır. WEB, WPA ve RSN protokollerinin karşılaştırılması Çizelge 2'de yer almaktadır.

Bu protokollere ek olarak güvenlik yöntemlerinden bir diğer kullanılan yöntem ise Fonksiyonel Ağ Sanallaştırması (Functional Network Virtualization-NFV) yöntemidir. Günümüzde geliştirilen güvenlik çözümlerine baktığımızda sunulan özellikler genel olarak donanım tabanlıdır ve donanımsal olarakta yeni yapılan tasarımlar, değişiklikler yeni donanımlara ihtiyaç duyulmasına sebep olmaktadır. Bu ihtiyaç maliyet açısından da kurulum, tasarım ve uygulama açısından da bir hayli zor ve pahalıdır. Bu çözümler ayrıca servis kalitesini de garanti etmemektedir. NFV bu alanda en önemli çözümdür (Faheem and Rafigue 2015, Akyildiza, ChunLina and Wangb 2015). Burada birçok donanımsal araçlar, yüksek kaliteli serverlar, ağ düğümleri konsolide edilmektedir. Şekil 2'de görüldüğü gibi NFV herhangi bir veri düzleminde paket işleme ve sabit ve mobil ağ altyapılarını işleme gibi alanlarda uygulanabilir bir alt yapıya sahiptir.

NFV'de bir takım zorluklarla da karşılaşılması mümkündür. Özellikle dağıtık ağlarda bu zorluklarla karşılaşılmaktadır. Birçok internet servisleri, akıllı yapılar (smart grids), akıllı ulaşım sistemler sağlamlığı ve güvenliği garanti altına almak istemektedir. Bu anlamda IP katmanı büyük öneme sahiptir. Ağ operatörleri sanallaştırma yapılırken güvenliğin, esnekliğin ve uygunluğun sağlanmasını istemektedir. Sanal olarak düğümlerin ve diğer birçok oyuncunun fiziksel performansının sanal olarak da sağlanması gerekmektedir. Bunun içinde anormal davranışların tespiti için yeni bir siber-güvenlik mekanizmasına ihtiyaç duyulmaktadır. Derin veri analizleri, davranışsal analizler, zayıf sinyaller, heterojen bilgiler dikkate alınarak yeni bir çözüm sunulmalıdır. Bütün sistemler için IP katmanı ortak olduğundan IP katmanını kontrol etmek gerekmektedir IPSec protokolü zaten bu işlemi gerçekleştirmektedir. IPSec kendi içerisinde framework bulundurmaktadır. IPSec genel olarak bütünlük, gizlilik, tekrar koruma ve bazı saldırılara karşı koruma servislerini sağlamaktadır. Bu protokollere ek olarak ayrıca IPSec'den bağımsız ve kombinasyonlu olarak Doğrulama Başlığı (AH) ve Kapsüllü Güvenlik Yükü (ESP) protokollerini de kullanmaktadır (Kabi 2013).

2.2. Kablosuz Ağlarda Güvenlik İçin Çoklu Çözüm Alternatifleri

Bölüm 2'de bahsedilen bütün bu protokoller fonksiyonel ağ sanallaştırması ve yöntemler kablosuz ağlarda güvenliği sağlamak için tek başına artık yeterli olarak görülmemektedir. Literatürde var olan protokoller ve yöntemler birlikte kullanılarak çok katmanlı güvenlik yapısı oluşturulmaktadır. Bu uygulamalarda güvenlik seviyesi artmasına rağmen diğer performans kriterlerinde ise zaman zaman dezavantajlar oluşturmaktadır. Mevcut protokollerin aynı anda aynı kablosuz ağlarda kullanımı, kullanılan bir protokolle beraber VPN kullanılması veya belli bir protokolle birlikte diğer güvenlik yöntemlerinden bir tanesinin de kullanılması çoklu katman karşılaştırılması ve güvenlik düzeyi için son derece önemlidir.

2.2.1. Çoklu Protokol Kullanımı

Çoklu protokol kullanımında güvenlik seviyesini artırmak için birden fazla protokol birlikte kullanılmıştır. Şekil 3'de yer alan çoklu katmanda IPSec bağımsız ve kombinasyonlu olarak aşağıda yer alan üç protokolü kullanmaktadır. Bu protokoller AH, ESP ile IKE yöntemidir. IPSec, ESP ve AH protokollerini kullanarak hem verileri şifreleyip hem de yetkilendirmeden gelen problemleri önleme adına algoritmayı mimarisine katarak güvenliği daha fazla

Çizelge 2. WEB, WPA ve RSN protokollerinin karşılaştırılması (Bandırmalı, Bayılmış, Demiray Ertürk ve Harmankaya 2004).

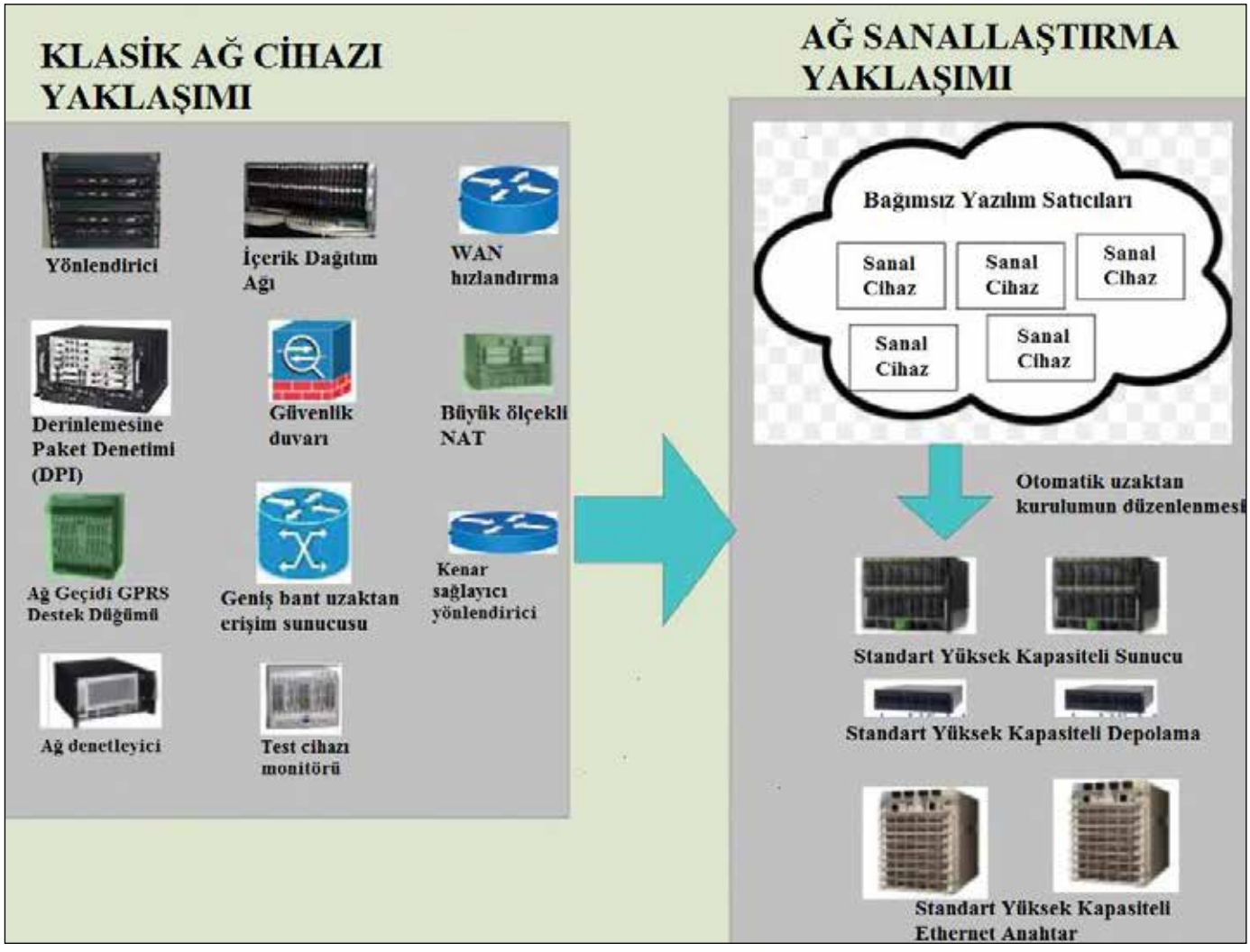
	WEP	WPA	RSN
Şifreleme	RC4 algoritması (Şifreleme yapısı kırılmıştır)	TKIP/RC4 (WEP'in açıklarını kapatıyor)	CCMP/AES CCMP/TKIP
Şifreleme Anahtarı	40 bit	128 bit	128 bit
IV	24 bit	48 bit	48 bit
Anahtar Değişikliği	Anahtar sabittir	Anahtar her oturum, her paket için değişir	Anahtar değişikliğine gerek yoktur
Anahtar Yönetimi	Anahtar yöntemi yoktur	802.1x	802.1x
Asıllama	Zayıf bir yöntem	802.1x EAP	802.1x EAP
Veri Bütünlüğü	ICV	MIC	MIC

artırmaktadır. IPSec protokolü ayrıca mevcut internet ağ alt yapılarıyla Ipv6 içinde kullanılabilmektedir. IPSec protokolü iyi bir çözüm sunmasına rağmen yine de bir takım eksiklikleri bulunmaktadır. Oturum çalma, şifreleme zayıflığı ve erişim kontrolünün kaybedilmesi bunlardan bir kaçıdır. Bunlara ek olarak sunuculara çok sayıda istek göndererek kapasitenin artırılmasını ve bilgisayarın hizmet vermez hale getirilmesini sağlayan Dağıtık Red Servisi (Distributed Denial of Service Attack- DDos) atakları, tekrar ataklar ve komşu düğüm gibi görünüp mesaj değiş tokuşu yapan tünel aldatmacaları IP tabanlı sistemlerdeki IPSec protokolünün güvenlik açığı olarak karşımıza çıkmaktadır. Burada kullanılan AH ve ESP protokolleri bu güvenlik açıklarına çare olmaktadır.

2.2.2 Protokol ve Sanal Ağ Kullanımı

Bir diğer çok katmanlı mimari kullanımında ise mevcut protokollerle birlikte VPN kullanılarak güvenlik düzeyi önemli derecede artırılmaktadır. Sanal ağ kullanımından önce genel olarak güvenlik problemleri ele alınmalı ve güvenlik problemlerini aşabilecek yöntemler önerilmelidir. Örneğin WMN'lerde genel olarak dinamik çalıştıkları ve çok atlamalı ağ oldukları için kendini sık sık güncellemektedir. Bununla birlikte paket transferleri dağıtıcı üzerinden gerçekleştirilirken bir çok atakla karşı karşıya gelmektedir. IEEE802.11s henüz tam olarak standartlaştırılmadığı için de sinyal boğma, dağıtık red servisi, pil tükenme saldırıları, solucan deliği saldırıları, karadelik saldırıları, konumu açıklama saldırıları, kablosuz alt yapı sızdırma, trafiksel saldırılar, kaynakların tükenmesi saldırıları, dövme kurcalama, fiziksel saldırı ve dns bilgi sızdırma gibi saldırı çeşitleri ile sık sık karşılaşılabilmektedir.

Bu ataklar özetle ağ yapısını bozan Erişim Noktası (Access Point-AP)'yi ve düğümlerin mobilitesini hedef alan



Şekil 2. Fonksiyonel Network Sanallaştırması (NFV) (Faheem and Rafigue 2015).

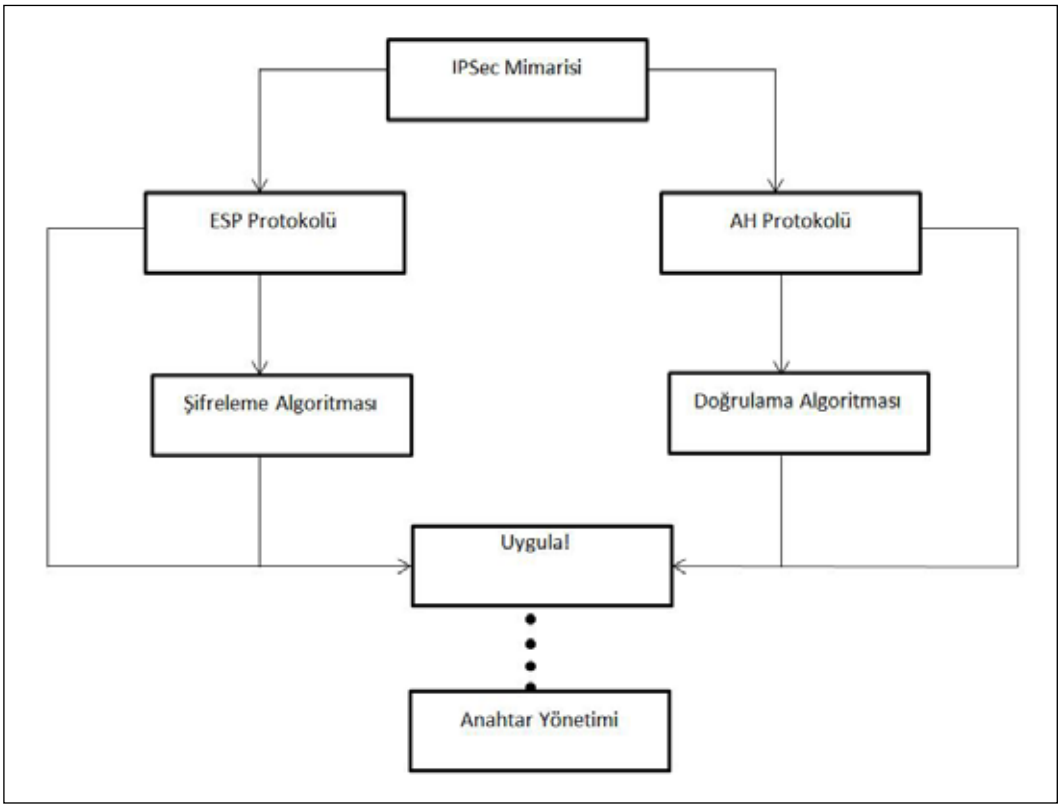
saldırılardır. WMN saldırılarına çözüm olarak üretilen algoritmada trafik mühendisliği kullanılarak aşağıda yer alan akış şemasındaki gibi bir mekanizma oluşturulmuştur. Burada kriptolu frame başlıkları IP protokolünü kullanarak kapsülleme ile önce VPN daha sonrada IPSec protokolü uygulanarak hedef düğüme veriler iletilmektedir (Comley vd. 2011). Şekil 4'de görüldüğü üzere VPN ve IPSec protokolleri aynı anda kullanılarak güvenlik katmanı büyük oranda artırılarak çok katmanlı bir yapı güvenlik yapısı oluşturulmuştur.

Diğer yandan OPNET benzetim aracı kullanılarak güvenlik seviyesinde yapılan analizlerde de hem protokol hem de VPN kullanılması durumunda güvenlik düzeyi belirgin bir şekilde artış göstermiştir (Çakır ve Kaptan 2009, Akbaş ve Gümüşkaya 2010, Akbaş ve Gümüşkaya 2011, Chu and Lea 2008). MPLS (Multi-Protocol Label Switching) denilen ve WMN'lere has olan yöntem 802.11i'ye göre daha güvenli olmakla beraber VPN ve IPSEC protokolleri kullanılmasına göre daha az güvenli olduğu tespiti yapılmıştır. TE(Traffic Engineering) üzerinden gerçekleştirilen senaryoda da MPLS in yalnız kullanımı MPLS'in VPN ile kullanımı ve hem VPN hemde IPSec protokolünün kullanımının gerçekleştirildiği birde 802.11i'nin kullanılmış olduğu dört senaryo Şekil 5'de görüldüğü gibi karşılaştırılmıştır. Buna göre kullanılan düğümler erişim noktaları da sabit tutulduğunda atlama sayısı en fazla olanın hem VPN hem de IPSec'in kullanıldığı senaryo olduğu görülmektedir. Daha sonra VPN daha sonra MPLS ve en sonda 802.11i'nin atlama sayısı olduğu görülmektedir. Bu da göstermektedir ki atlama sayısı fazla olan VPN ve IPSec'li senaryo daha fazla atağa maruz kalmıştır ki paketler kendilerini korumak adına atlama sayılarını artırmışlardır (Şekil 5).

Sonuç olarak geliştirilen bu yöntemde mevcut paketlerin iletilmesi aşamasında standart yöntemlerin kullanılması ile birlikte VPN ve IPSec protokollerinin beraber kullanıldığı yöntemler çok daha verimli ve güvenli olarak saldırılara karşı savunma sistemi için geliştirilmiştir.

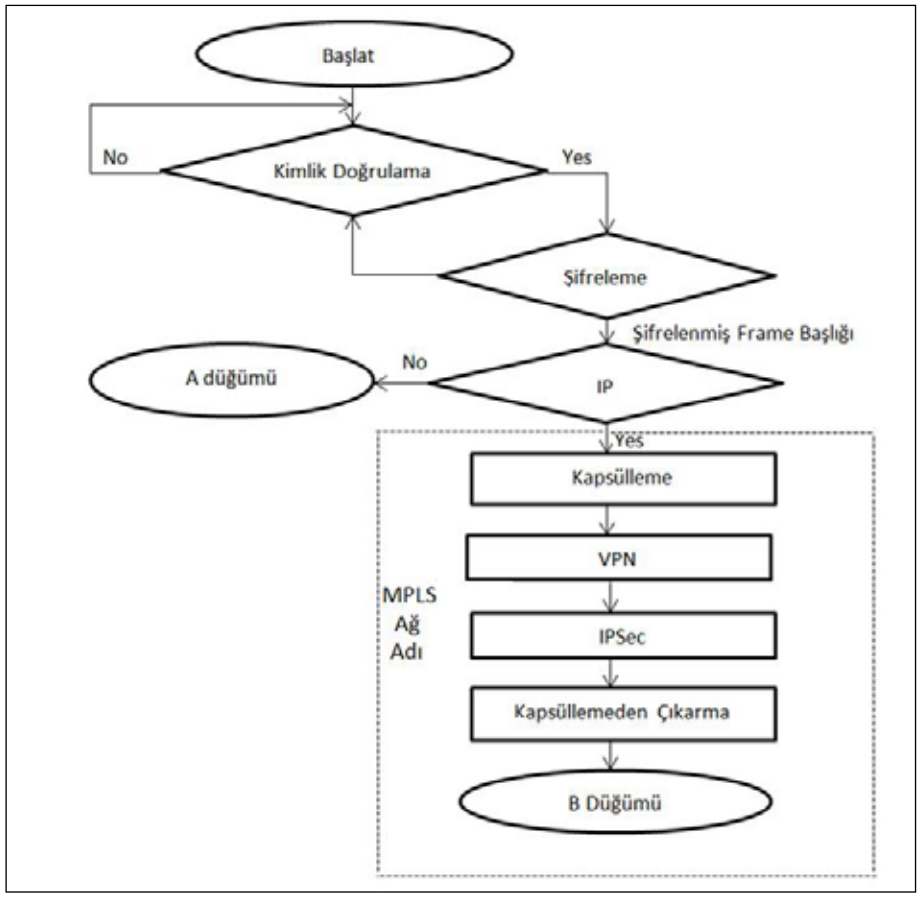
2.2.3. Protokol ve Mimari Değişimi

Birçok kablosuz ağ iletişiminde ise karşılaşılan güvenlik problemlerinde birden fazla katmanlı protokol kullanımı yerine yöntem ve sistemlerde değişiklikler yapılarak mevcut protokollerle birlikte güvenlik seviyesi artırılmaktadır. Örneğin VANET'ler için yeni bir çözüm yolu olarak hesaplama ve bant genişliğini ön planda tutan bir yaklaşım geliştirilmiştir. Burada yol güvenliğini ilgilendiren durumlarda asimetrik kriptografi ile birlikte Ortak Anahtar Altyapısı (Public Key Infrastructure-PKI), diğer tüm mesajlar için ise

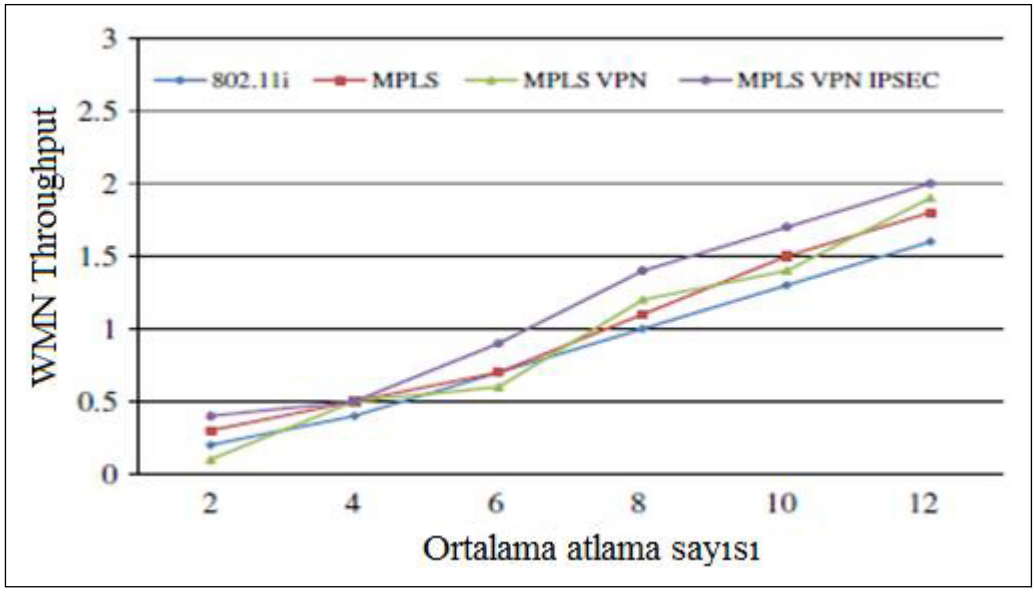


Şekil 3. IPSec, ESP ve AH çok katmanlı protokol uygulaması (Faheem and Rafigue 2015).

(özellikle periyodik olarak gönderilen telemetrik mesajlar gibi) daha hızlı ve daha güvenli (Narayanan, Padmavathi and Sujithra 2013) olduğundan simetrik kriptografi ile Şekil 6'da görüldüğü gibi korunmaktadır. VANET Asimetrik kısmı ele alındığında PKI ile birlikte araca ait bir kimlik Araç Kimliği (Vehicle-related identities-VRI) ile kullanılmak üzere sertifika sağlanması gerekmektedir. Sertifikalar ise devlet tarafından yetkilendirilmiş Hükümet Yetkisi(Governmental Transportation Authority-GTA) sertifika yetkilileri Sertifika yetkisi(certification authority–



Şekil 4. Trafik mühendisliği yöntemi (Muagilim vd. 2011).



Şekil 5. Güvenlik katmanı karşılaştırılması (Muagilim, Loo and Comley 2011).

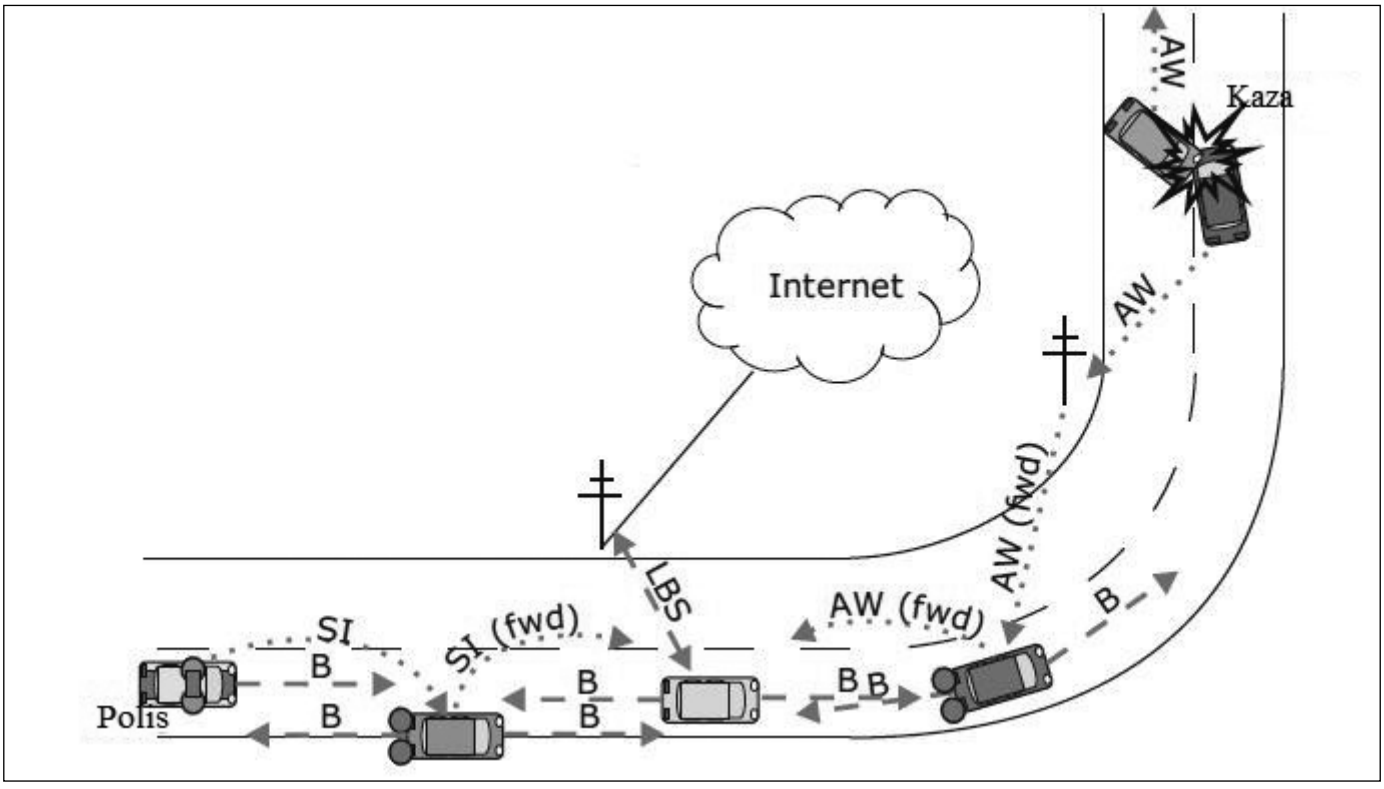
CA) sağlanmalıdır. Gerçek-zamanlı olarak işlenmesine engel olunmaması amacıyla DoS dahil olmak üzere bütün gerçekleşebilecek bütün ataklara karşı önceden önlemlerin alınması gerekmektedir (Berger 2013, Afifi vd. 2016, Barrero vd. 2016). VANET mesajları anlık işlenmesi gereken yol güvenliği ve sürüş şartlarını ilgilendiren mesajlar olduğu için önerilen güvenlik altyapısı hesaplama ve bant genişliği için verimli olmalıdır (Federrath ve Plöbl 2008).

Ağın performansı ve gizlilik gereksinimleri göz önüne alındığında bütün iletileri imzalamak gerekli değildir. İşte bu sebeple Coğrafi olarak Dağıtık Çalışan (Geographically Distributed Trusted Third Parties–GTTPs), kendi bölgesinde mesajların şifrelenmesi ve kimlik doğrulamayı sağlayan düğümler kullanılmalıdır. GTTPs belli bir coğrafi alanın dışından gelen ağlara karşı daha güvenli olan ve dış ağlara erişimi engelleyen bölgesel bir yöntemdir. Ülkeler ana hatlarıyla araçları ilk tanımlamayı net bir şekilde yukarıda belirtildiği gibi uygun sertifikasyonlarla yapmalıdır. Öte yandan tanımlamalar yapılırken uygun prosedürlerle gerek yetkili kurumlar gerek aracın satışının gerçekleştiği servisler ve GTA ile birlikte aracın sahibinin yer aldığı aşağıdaki şekilde görülen prosedürlerin yapılması bu ağın çalışması açısından kritik öneme sahiptir (Federrath ve Plöbl 2008).

Kablosuz ağlarda buradan yola çıkarak mevcut protokollerin yanında yeni yöntemlerinde eklenmesi özellikle VANET tipi ağ iletişimi için kaçınılmaz olduğu sonucu ortaya konmuştur. VANET güvenlik altyapısının oluşturulması için ne tür bir altyapı kullanılması gerektiği mesaj bütünlüğü ve güvenliğin gerekliliği tartışmalarından sonra asimetrik ve simetrik kriptolar ile donanımı irdelemeye dayanıklı cihazlar ile bir altyapı sistemi yeni yöntem olarak ortaya çıkmıştır.

2.3. Yeni Tasarımda Çok Katmanlı Güvenlik

Yapılan çalışmalar ele alındığında birçok ağ iletişim yönteminde mevcut protokoller ve yöntemlerin yeterli olmadığı görülmüştür. Güvenlik seviyesini artırmak adına bazen birden fazla protokol bazen mevcut protokollere ek olarak VPN kullanılması veya bazen mevcut protokollerden yeni bir yöntemin var olması gerekliliği üzerine birçok çalışma yapılmıştır. Kablosuz ağın görevine ve kapasitesine göre ağ katmanlarında bazen birden fazla protokol, bazen VPN ve protokol, bazen de mevcut protokollere yeni bir yöntem eklenilmesi güvenlik seviyesini artırmaktadır. Bu seçimde ise güvenlik ön planda tutulmakla beraber paket iletimlerinde meydana gelebilecek yavaşlamalar, alınan ve gönderilen veri trafiğinin azalmasının önüne geçilmesi gerekmektedir.

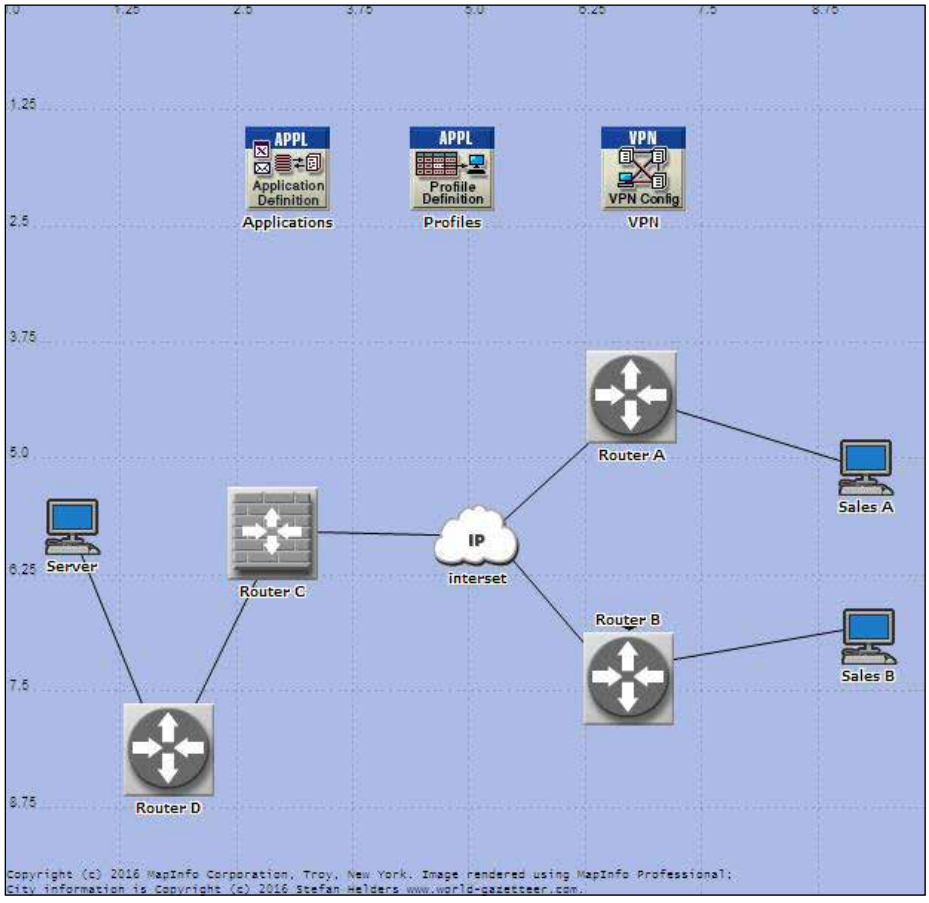


Şekil 6. VANET farklı mesaj kullanım yöntemi (Federrath and Plöbl 2008).

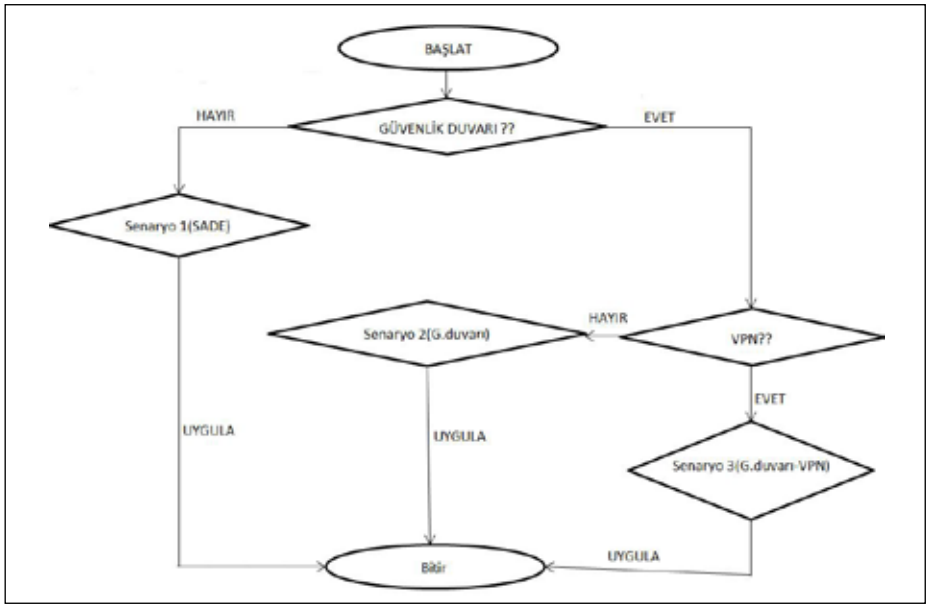
2.3.1 Çok Katmanlı Güvenlikte Önerilen Tasarım

(Aboelela 2008) tarafından yazılan kitaptaki laboratuvar çalışmasını baz alarak yapmış olduğumuz üç temel senaryodan oluşan yeni bir uygulama tasarımı Şekil 7'deki gibi gerçekleştirilmiştir.

Şekil 8'de görülen birinci senaryoda herhangi bir güvenlik seviyesi bulunmamaktadır. İkinci senaryoda ise sadece güvenlik duvarı uygulanarak tasarım gerçekleştirilmiştir. Son senaryoda ise hem güvenlik duvarı hem de VPN sanal özel ağ kullanılmıştır.



Şekil 7. Yeni tasarım elemanları (Aboelela 2008).



Şekil 8. Çoklu katman tasarımı.

Yeni modelde protokol, VPN ve yöntem olarak güvenlik duvarı ayrı ayrı senaryolarda kullanılarak güvenlik seviyesini artışı görülmüş ve ayrıca performans ölçütü olarak da literatürde çok sık kullanılan alınan veri trafiği byte/saniye cinsinden hesaplanarak bu yöntemdeki farklı senaryoların performansa olan etkisi incelenmiştir. İncelenenen senaryoda veri tabanı ve Metin Transfer Protokolü (Hyper-Text Transfer Protocol-http) iletiminde yer alan alınan ortalama veri trafiği incelenmiştir.

2.3.2.Yeni Tasarımda Güvenlik ve Performans Karşılaştırmaları

Çizelge 3'de görüldüğü üzere çoklu katmanlarda hem çoklu protokol kullanımı hem protokol ve VPN kullanımı hem de yöntem eklemeleri güvenliği kesin bir şekilde artırmıştır. Güvenlik duvarı veri tabanı için alınan veri trafiğini sıfırlamaktadır. VPN ise güvenlik seviyesini artırmasına rağmen alınan veri trafiğini azaltmaktadır. Güvenlik duvarı ve sanal ağın kullanılmadığı sade tasarımda ise veri tabanı için alınan veri trafiği en yüksektir ancak güvenlik en alt seviyededir.

Çizelge 4'de görülen Http iletişiminde ise VPN ve güvenlik duvarının kullanılması performansı olumlu etkilemektedir. Http iletişiminde güvenlik duvarının uygulandığı ve sade tasarımda alınan veri trafiği açısından aynı seyirde ve yaklaşık olarak aynı olarak görülmektedir.

Çoklu katmanlarda hem çoklu protokol kullanımı hem protokol ve VPN kullanımı hem de yöntem eklemeleri güvenliği kesin bir şekilde artırmıştır. IPSec, ESP ve AH protokollerini kullanarak hem verileri şifreleyip hem de yetkilendirme ile güvenlikteki temel iki problemi aynı

Çizelge 3 . Veri tabanı iletiminde ortalama alınan veri trafiği senaryo karşılaştırmaları.

Veri Tabanı İletiminde Ortalama Alınan Veri Trafiği			
Zaman (Dakika)	**Senaryo 1 ortalama alınan veri trafiği (byte/saniye)**	**Senaryo 2 ortalama alınan veri trafiği (byte/saniye)**	**Senaryo 3 ortalama alınan veri trafiği (byte/saniye)**
1	0	0	0
2	4,1	0	0,1
3	3	0	2,7
4	2,1	0	4,2
5	7	0	3,9
6	9	0	3,1
7	7	0	2,7
8	8,3	0	2,6
9	8,4	0	3,1
10	8,8	0	4

Çizelge 4. Http iletiminde ortalama alınan veri trafiği senaryo karşılaştırmaları.

Http İletiminde Ortalama Alınan Veri Trafiği			
Zaman (Dakika)	**Senaryo 1 ortalama alınan veri trafiği (byte/saniye)**	**Senaryo 2 ortalama alınan veri trafiği (byte/saniye)**	**Senaryo 3 ortalama alınan veri trafiği (byte/saniye)**
1	0	0	0
2	13,1	13,1	15
3	8,2	8,2	10
4	6	6	7
5	5,2	5,2	5,8
6	4	4	4,5
7	3,6	3,6	4
8	3	3	3,2
9	2,8	2,8	6
10	2,7	2,7	5,1

anda aşılmasını sağlanmıştır. VPN ve IPSec protokolleri aynı anda kullanılarak güvenlik katmanı ve güvenlik yapısı güçlendirilmiştir. MANET'lerde sunulan yeni yöntemde ise kriptolama ile birlikte yasal zeminde güvenlik protokolü eklenilmesi yeni bir yöntem ve güçlü güvenlik altyapısı oluşturmuştur. Yeni senaryoda ise güvenlik duvarı ve sanal özel ağlar kullanılarak güvenlik seviyelerinin veri tabanı ve http iletiminde alınan veri trafiğini nasıl etkilediği üzerine çalışma yapılarak, güvenlik seviyesinin artması durumunda alınan veri trafiğinin azaldığını ve performansı negatif etkilediği gözlemlenmiştir.

3. Sonuç

Kablosuz ağlarda çeşitli haberleşme yöntemlerinde uygulanan mevcut protokoller ile birlikte sanal özel ağ ve yöntemler bulunmaktadır. Ancak kablosuz cihazların kullanımının hızlı bir şekilde artması ile birlikte mevcut protokoller ve yöntemler güvenlik için yeterli olmamaktadır. Bu nedenle kablosuz ağ çeşidine göre kullanılan birçok protokolün geliştirilmesi veya bu protokollere yeni yöntemler eklenilmesi kaçınılmazdır. Bu makalede literatürde yapılan çalışmalarda yeni yöntem, yeni protokol veya yeni sanal özel ağlar yerine mevcut protokol ve yöntemlerin aynı anda kombinasyonlu ve uygun mimari ile kullanılması üzerine yapılan çalışmalar incelenmiştir ve bu yapıların performansa olan etkileri aktarılmıştır. Kullanılan her protokolün kendi özelliğine göre aldığı güvenlik önlemi aynı ağda birden fazla fonksiyonel güvenlik katmanı oluşturarak güçlü alt yapıya sahip yeni güvenlik yöntemleri türetilmiştir.

Yapılan yeni tasarımda ise çalışmalar sınıflandırılarak temel olarak üç çeşit çok katmanlı güvenlik sınıfı oluşturulmuştur. Bu çalışmalarda tasarımda güvenlik duvarı ve sanal özel ağlar kullanılarak güvenlik seviyelerinin veri tabanı ve http iletiminde alınan veri trafiğini nasıl etkilediği, güvenlik seviyesinin artması durumunda alınan veri trafiğinin azaldığını ve performansı negatif etkilediği gözlemlenmiştir. Bu nedenle çok katmanlı güvenlik tasarımı uygulanırken güvenlik dışındaki performans ölçütlerinin değişim gösterdiği ve negatif etkilendiği göz önünde bulundurularak çalışmalar gerçekleştirilmelidir. Yapılacak çalışmalarda hem hızlı hem de güvenli kablosuz ağlar için, çoklu katmanlı güvenlik tasarımlarında aynı işlevi gören protokol alt yapı işlevlerinin elimine edilmesi sağlanmalıdır.

4. Kaynaklar

Aboelela, E. 2008. Network Simulation Experiments Manual. *Univ. Massachusetts/Dartmouth.* Edition 2.

Afifi, H., Ibrahim, AW., Marot, M., Said, AM. 2016. Modeling Interactive Real-Time Applications in VANETs with Performance Evaluation. *Comput. Networks.,* 16: 1389-1286.

Ahmadb, R., Azni A., Hayaatib NF., Hazwania., HNoha ZAM., 2015. Systematic Review for Network Survivability Analysis in MANETS. *Procedia - Social Behav. Sci*., 195: 1872 – 1881.

Agasi, O. 2015. Encapsulating mobile security. *Comp.. Fraud Sec.*., 6: 10-12.

Akbaş, D., **Gümüşkaya, H. 2010.** Bir kurumsal Ağın Güvenlik Yapılarının Modellenmesi. *Bilgisayar Müh. Bölümü* Haliç Üniv., İstanbul Türkiye.

Akbaş D., Gümüşkaya, H. 2011. Real and OPNET modeling and analysis of an enterprise network and its security structures. *Procedia Comput. Science*.**,** 3: 1038-1042.

Akyildiz, IF., Chun Lina, S., Wangb, P. 2015. Wirelesssoftware-definednetworks(W-SDNs)and network function virtualization (NFV) for 5G cellular systems: An overview and qualitative evaluation. *Comput. Networks.,* 93: 66–79.

Aroraa, A., Khera, A. 2015. Wi-Fi Enabled Personal Computer Network Monitoring System Using Smart Phone With Enhanced Security Measures. *Procedia Comput. Science.,* Cilt 70: 114 – 122.

Badra, M., Hajjeh İ., Urien, P., 2007. Flexible And Fast Security Solution For Wireless LAN. *Persasive Mobile Comput*., 3: 1-14.

Bandırmalı, N., Bayılmış, C., Demiray, HE., Ertürk, İ. Harmankaya, AO. 2004. Kablosuz Ağlarda Güvenlik Protokollerinin Karşılaştırmalı İncelenmesi. *Kocaeli Üniversitesi, Mühendislik Fakültesi Enform. Bölümü.* Kocaeli, Türkiye.

Bandırmalı, N., Ertürk, İ., Çeken, C., Bayılmış, C. 2008. Yüksek Riskli Kablosuz Algılayıcı Ağlarda Güvenlik ve Şifreleme Uygulaması. *2.Ağ ve Bilgi Güvenliği Ulusal Sempozyumu.,* 216-220.

Barrero, F., García-Campos, JM., García, JS., Reina, DG. Toral, SL. 2016. An evaluation methodology for reliable simulation based studies of routing protocols in VANETs. *Sim. Model. Prac. Theory*., 66: 139–165.

Berger, T. 2013. Whittenton N. Mobile Ad Hoc Network of Waterborne Enhanced Maritime Security. *MTS.* 40:4.

Bernik, I., Markelj, B. 2015. Safe use of mobile devices arises from knowing the threats. *J. Information Sec. App.,* 20: 84-89.

Çakır, C., Kaptan, H. 2009. VoIP Teknolojilerinde Opnet Tabanlı Güvenlik Uygulaması. *Bilişim Tek. Derg*.**,** 2: 3.

Chu j., Lea C. 2008. A restorable MPLS-based hose-model VPN network. *Comput. Networks.,*51: 4836–4848.

Comley, R., Loo, K., Muagilim, OE. 2011. Wireless mesh network security: A traffic engineering management approach. *J. Network Comput. App*., 34: 478-491.

Coşkun, İ., Demircioğlu, S., Gezer M., Odabaş, C., Pehlivan, İ. 2008. Kablosuz Ağ Şifreleme Yöntemlerinin Karşılaştırılması. *2.Ağ ve Bilgi Güvenliği Ulusal Sempozyumu.,* 193-197.

Elezia, M., Raufia, B. 2015. Conception of Virtual Private Networks using IPsec suite of protocols, comparative analysis of distributed database queries using different IPsec modes of encryption. *Procedia - Social and Behavioral Sciences***.,** 195: 1938– 1948.

Faheem, K., Rafigue, K. 2015. Securing 4G/5G wireless networks., *Comput. Fraud and Sec***.,** 8-12.

Federrath, H., Plöbl, K. 2008. A Privacy Aware and Efficient Security Infrastructure for Vehicular Ad Hoc Networks. *Comput. Standart & Interfaces***.,** 30: 390-397.

Frigura-İliasa, F., Mulec, G., Vasiu, R. 2013. Distributed flow controller for mobile ad-hoc networks. *8th IEEE International Symposium on Applied Intelligence and Inform*.

Harmankaya, AO., Demiray, HE., Ertürk, İ., Bayılmış, C., Bandırmalı, N. 2008. Kablosuz Ağlarda Güvenlik Protokollerinin Karşılaştırmalı İncelenmesi. *2.Ağ ve Bilgi Güvenliği Ulusal Sempozyumu.,* 51-57.

Kabi, A. 2013. IEEE 802.11 Securing in Mobile Wireless Networks. *Australian College Kuawit.,* 978: 1-4.

Kim, DW., Yan, P., Zhang, J. 2015. Detecting fake anti-virus software distribution Webpages. *Comp. Sec.,* 49: 95-106.

Kundu, A. 2015. Mitigation of Storage Covert Channels in IPSec for QoS Aware Applications. *Procedia Comput.. Science*., 54: 102–107.

Liu, J., Ren, J., Xu, Y. 2015. Investigation of dynamics of a virus–antivirus model in complex network. *Physica A.,* 421: 533-540.

Lloret J., Modares, H., Moravejosharieh A., Salleh, R. 2014. A survey of secure protocols in Mobile IPv6. *J. Network Comput. App***.,** 39: 351-368.

Munjal. A., Singh, YN. 2015. Review of stateful address auto configuration protocols in MANETs. *Ad. Hoc. Network.,* 33: 257-268.

Narayanan S., Padmavathi G., Sujithra M. 2013. Mobile Device Data Security: A Cyrptographic Approach by Outsourcing Mobile data to Cloud. *Procedia Comput. Science.,* 47: 480-485.

Palanisamy GV., Sakthivel, M. 2015. Enhancement of accuracy metrics for energy levels in MANETs. *Comput. Elect. Engineering***.,** 48: 100-108.

Ratheea, G., Sainib, H. 2016. A Fast Handoff Technique in Wireless Mesh Network (FHT for WMN). *Procedia Comput. Sci.*, 79: 722 – 728.

Shukla, JB., Shukla, P., Singh G., Tripathi, A. 2014. Modeling and analysis of the effects of antivirus software on an infected computer network. *Applied Math. Com***.,** 227: 11-18.