
GAZİ ÜNİVERSİTESİ
Gazi
1926

V2X İLETİŞİMİNDE KULLANILAN GÜVENLİK TEKNOLOJİLERİ VE TÜRKİYE'DE UYGULANMASI

Gizem ERCEYLAN

YÜKSEK LİSANS TEZİ
BİLİŞİM SİSTEMLERİ ANA BİLİM DALI

GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ

AĞUSTOS 2022

Gizem ERCEYLAN tarafından hazırlanan "V2X İLETİŞİMİNDE KULLANILAN GÜVENLİK TEKNOLOJİLERİ VE TÜRKİYE'DE UYGULANMASI" adlı tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ ile Gazi Üniversitesi Bilişim Sistemleri Ana Bilim Dalında YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Danışman: Prof. Dr. M. Ali AKCAYOL

Bilgisayar Mühendisliği Ana Bilim Dalı, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum. ...……

Başkan: Prof. Dr. M. Fatih DEMİRCİ

Bilgisayar Mühendisliği Ana Bilim Dalı, Ankara Yıldırım Beyazıt Üniversitesi ……...

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum.

Üye: Prof. Dr. Hacer KARACAN

Bilgisayar Mühendisliği Ana Bilim Dalı, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum. ……...

Tez Savunma Tarihi: 04/08/2022

Jüri tarafından kabul edilen bu tezin Yüksek Lisans Tezi olması için gerekli şartları yerine getirdiğini onaylıyorum.

……..……

Prof. Dr. Aslıhan TÜFEKCİ

Bilişim Enstitüsü Müdürü

ETİK BEYAN

Gazi Üniversitesi Bilişim Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Gizem ERCEYLAN

...../……/……

V2X İLETİŞİMİNDE KULLANILAN GÜVENLİK TEKNOLOJİLERİ VE TÜRKİYE'DE UYGULANMASI

(Yüksek Lisans Tezi)

Gizem ERCEYLAN

GAZİ ÜNİVERSİTESİ

BİLİŞİM ENSTİTÜSÜ

Ağustos 2022

ÖZET

Bağlantılı araçlar konum ve yol durumu gibi bilgileri birbirleri ile paylaşarak daha verimli, çevreci ve güvenli bir trafik ortamı oluşmasına katkı sağlamaktadır. Bu iletişimdeki güvenliğin ve gizliliğin korunması ise bağlantılı araçların gelecekte daha yaygın kullanılabilmesi için gerekli olan temel faktörlerden biridir. Bu motivasyon ile bu çalışmada V2X iletişiminde şimdiye kadar kullanılan güvenlik standartları ve sistemleri araştırılmıştır. Açık anahtar altyapısına dayalı güvenlik yapılarında kullanılan mesaj yapıları ve güvenli mesaj iletimi için kullanılan protokoller incelenmiştir. Kimlik doğrulama ve sertifika iptal kontrolü ile ilgili çalışmalar araştırılmıştır. Mevcut kullanımda olan açık anahtar altyapısına dayalı V2X güvenlik sistemleri ile alternatif çözümler sunan V2X güvenlik sistemlerinin avantaj ve dezavantajları incelenmiştir. Açık anahtar altyapısı kullanan sistemlerdeki SİL sunucusu üzerindeki yükü azaltarak araç sertifikalarının iptal kontrolünü sağlayan yarı dağıtık bir sertifika iptal kontrol sistemi önerilmiştir. Önerilen yapı için hazırlanan benzetim sonuçlarında, merkezi SİL sunucusu üzerindeki yükün ortalama %35 azaldığı gözlemlenmiştir. Ayrıca, önerilen yapı sayesinde merkezi sunucu ile araçların haberleşemediği durumlarda güvenli iletişimin devam edebilmesi sağlanmıştır.

Bilim Kodu	:	92403
Anahtar Kelimeler	:	Açık anahtar altyapısı (AAA), sertifika iptal listesi (SİL), araçtan her şeye, şifreleme, blokzincir
Sayfa Adedi	:	77
Danışman	:	Prof. Dr. M. Ali AKCAYOL

SECURITY TECHNOLOGIES USED IN V2X COMMUNICATION AND ITS IMPLEMENTATION IN TURKEY

(M. Sc. Thesis)

Gizem ERCEYLAN

GAZİ UNIVERSITY

INFORMATICS INSTITUTE

August 2022

ABSTRACT

Connected vehicles contribute to the creation of a more efficient, environmentally friendly, and safe traffic environment by sharing information such as location and road conditions with each other. Maintaining the security and privacy of this communication is one of the main factors necessary for the more widespread use of connected vehicles in the future. With this motivation, security standards and systems used so far in V2X communication were investigated in this study. Message structures and protocols for secure message transmission are investigated in V2X security structures based on public key infrastructure. Studies on authentication and certificate revocation control have been conducted. The advantages and disadvantages of V2X security systems based on public key infrastructure and V2X security systems that offer alternative solutions have been investigated. A semi-distributed certificate revocation control system is proposed, which provides revocation control of vehicle certificates by reducing the load on the CRL server in systems using the public key infrastructure. In the simulation results, it was observed that the number of requests to the central CRL server decreased by 35% on average. In addition, in cases when the central server and vehicles cannot communicate, vehicles can keep communicating securely due to the semi-distributed structure of the proposed system.

Science Code	:	92403
Key Words	:	Public key infrastructure (PKI), certificate revocation list (CRL), vehicle to everything (V2X), encryption, blockchain
Page Number	:	77
Supervisor	:	Prof. Dr. M. Ali AKCAYOL

TEŞEKKÜR

Bu tez çalışmasının gerçekleştirilmesinde beni yönlendiren ve desteğini esirgemeyen değerli danışman hocam Prof. Dr. M. AKCAYOL'a ve her zaman yanımda olan kıymetli eşim Ali'ye teşekkür ederim.

İÇİNDEKİLER

Sayfa

Sayfa

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

Şekil **Sayfa**

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Simgeler	**Açıklamalar**
GHz	Gigahertz
MHz	Megahertz
msn	Milisaniye
m	Metre
km	Kilometre
km/saat	Kilometre/saat

Kısaltmalar	**Açıklamalar**
AAA	Açık Anahtar Altyapısı
BSM	Temel Güvenlik Mesajları (Basic Safety Message)
CAM	Kooperatif Farkındalık Mesajları (Cooperative Awareness Messages)
C-ITS	Kooperatif Akıllı UlaşımSistemleri (Cooperative Intelligent Transport Systems)
DENM	Merkezi Olmayan Çevre Bildirim Mesajları (Decentralized Environmental Notification Message)
DSRC	Özel Kısa Menzilli İletişim (Dedicated Short Range Communication)
ECU	Elektronik Kontrol Üniteleri (Electronics Control Units)
ETSI	Avrupa Telekomünikasyon Standartları Enstitüsü (European Telecommunications Standards Institute)
IEEE	Elektrik ve Elektronik Mühendisleri Enstitüsü (The Institute of Electrical and Electronics Engineers)
K-AUS	Kooperatif Akıllı Ulaşım Sistemleri

Kısaltmalar	Açıklamalar
OBU	Yerleşik Ünite (On Board Unit)
QoS	Hizmet Kalitesi (Quality of Service)
SAE	Otomotiv Mühendisleri Topluluğu (Society of Automotive Engineers)
SCMS	Güvenlik Yönetim Sistemi (Security Management System)
SDO	Standardizasyon Geliştirme Organizasyonu (Standardization Development Organization)
SİL	Sertifika İptal Listesi
V2X	Araçtan Her Şeye (Vehicle to Everything)
WAVE	Araç Ortamında Kablosuz Erişim (Wireless Access in Vehicular Environment)

1. GİRİŞ

Araçtan Her Şeye (Vehicle to Everything-V2X), araçların diğer araçlar ve trafiği etkileyen diğer cihazlarla haberleşmesini sağlayan iletişim sistemidir. V2X ile yol durumu ile ilgili her türlü bilgi paylaşılarak yol güvenliği artırılmakta, enerji tasarrufu sağlanmaktadır [1]. V2X, trafik verimliliğinin artırılmasını, kaynakların verimli kullanılmasını, trafik kazalarının ve trafiğe bağlı hava kirliliğinin düşürülmesini sağlamaktadır. V2X sayesinde 2025 yılına kadar, trafikte 280 milyon saat daha az sürüş sağlanarak 400,000 ton daha az karbondioksit emisyonu yapılacağı; 260,000 daha az trafik kazası yaşanarak 11,000 daha az hayat kaybının olacağı tahmin edilmektedir [2] .

Bu çalışmada V2X iletişiminde mesaj güvenliğini sağlamak için kullanılan yöntemler ile ilgili araştırma yapılmıştır. Hücresel tabanlı, IEEE 802.11p tabanlı ya da hibrit V2X yapılarının kullanıldığı görülmüştür. Hücresel tabanlı V2X sistemleri umut vaat eden bir yapı olmakla birlikte IEEE 802.11p'ye dayanan sistemlerin mevcut kullanımda olduğu ve erken dönemlerde standartlaştırıldığı görülmüştür [3]. Bu bilgilerden yola çıkarak IEEE 802.11p tabanlı V2X sistemleri için oluşturulan V2X güvenlik modelleri üzerinde durulmuştur.

V2X iletişimine uygun, mesaj bütünlüğü, kimlik doğrulama ve gizliliği sağlayacak verimli bir V2X güvenlik yapısının geliştirilmesi büyük önem taşımaktadır. Literatürde asimetrik anahtarlama [4], simetrik anahtarlama [5] ve blokzincir yapısı kullanılan [6, 7] V2X güvenlik sistem tasarımlarının yapıldığı görülmektedir.

V2X iletişim güvenliği için simetrik anahtarlama yönteminin kullanıldığı yapılarda simetrik anahtarlamanın kıyasla daha düşük hesaplama yükü nedeniyle işlem süresi düşmektedir. Fakat, gizli anahtarın iletişim halinde olan taraflara ulaştırılması sisteme ek maliyet getirmektedir. Araç gizliliği sağlanırken kötü niyetli araçların tespit edilmesindeki zorluk, bu sistemin ana dezavantajıdır.

Hiyerarşik düzen üzerine oturtulmuş merkezi yapıların getirdiği dezavantajlar, dağıtık yapısı sayesinde blokzincir tabanlı V2X güvenlik sistemlerinde bulunmamaktadır. Bu yapıdaki zorluk ise V2X iletişimine uygun hızda işlem kaydı yapılabilmesini sağlayacak mutabakat

mekanizmalarının belirlenmesidir. Blokzincirin V2X sistemlerinde kullanımının zaman içinde yaygınlaşması beklenen bir sonuç olacaktır.

V2X iletişim güvenliği için en sık kullanılan yöntemin Açık Anahtar Altyapısı (AAA) yönteminin olduğu görülmektedir. Institute of Electrical and Electronics Engineers (IEEE) ve European Telecommunications Standards Institute (ETSI) tarafından oluşturulmuş V2X standartları, asimetrik anahtarlamanın kullanıldığı AAA üzerine kurulmuştur [8, 9]. Asimetrik anahtarlama tabanlı V2X güvenlik sistemlerindeki sertifika iptal kontrolünün geliştirilmesi gereken karmaşık bir süreç olduğu göze çarpmaktadır. Bu yapıdaki en büyük problem, tehlikeli ya da yasadışı varlıkların V2X iletişimine dahil olmasıdır. Güvenli bir V2X sisteminde yasadışı, kötü niyetli veya özel anahtarı tehlikeye düşmüş araçların sertifikalarının iptal edilmesi önemlidir. Geçmiş çalışmalarda sertifika iptal kontrolünün, Sertifika İptal Listesi (SİL) adı verilen listeler ile yapıldığı görülmektedir [10]. Mevcut standartlarda kullanılan SİL kullanımı ölçeklenebilirlik açısından zayıftır ve araç sayısının yüksek olduğu ağlarda kabul edilemez bir gecikmeye neden olmaktadır. İkinci önemli problem ise mesaj doğrulaması ve araç kimlik doğrulaması yapılırken aynı zamanda araçların gizliliğinin korunabildiği verimli bir yapının tasarlanabilmesidir. Böyle bir yapının yaratılabilmesi için takma isim (pseudonym) sertifikası kullanımı, grup imzalama [11, 12] ve halka imzalama [13] gibi imzalama metotlarının kullanıldığı görülmektedir. Standartlarda önerilen, takma isim sertifikalarının ömrünün kısa olması SİL'lerin boyutunun kısa sürede artmasına sebep olmaktadır [14]. Bu listelerin kullanımı, dosya boyutunun büyümesi ile ölçeklenebilirliğini yitirmekte ve ağda gereksiz alan kaplamaktadır. Merkezi sunuculardan yüksek boyuttaki bu dosyaların indirilmesi iletişimin yoğun olduğu trafiklerde problemlere sebep olmaktadır. Yollardaki V2X destekli araç sayısının 2025 yılına kadar 35,1 milyon olması tahmin edilmektedir [15]. Araç sayısındaki artış, merkezi sistemlerin sınırlı bir süre içinde iptal bilgisi taleplerine yanıt vermesini zorlaştırmaktadır. İptal kontrolü ile ortaya çıkan olası gecikmeler, gecikmeye duyarlı olan V2X için önemli bir sorundur. Ayrıca, mevcut sistemin merkezi bir yapıda olması, merkeze yapılan kötü niyetli bir saldırıda tüm sistemin çökmesine neden olmaktadır. Merkezi sunucuya bağlanılamadığı durumlarda ise güvenli iletişim sekteye uğramaktadır.

Açık anahtar altyapısına alternatif çözümlerin uygulanabilmesi için standartlarla oluşturmuş mevcut yapı üzerinde büyük ölçekli değişiklikler yapılması gerektiği görülmüştür. Bu durum zaman ve maliyet açısından dezavantaj yaratmaktadır. Standartlaştırılmış mevcut yapı

üzerinde yapılacak düzenlemelerin V2X teknolojisinin kısa sürede yaygınlaşmasını sağlayacağı motivasyonu ile AAA kullanılan bir sistem tasarlanması öngörülmüştür. Bununla birlikte, AAA yapısına dayalı V2X iletişim güvenlik sistemleri ile ilgili bahsedilen problemlere çözüm bulmak için yeni sertifika iptal kontrol mekanizmalarının ve dağıtık sistem yapılarının oluşturulması gerekmektedir. V2X iletişimindeki gecikmeler ciddi trafik kazalarına neden olabileceği için iptal kontrolünün gecikmeye neden olmayacak şekilde tasarlanması şarttır.

Merkezi sunucular ve yol kontrol üniteleri yanında araçların da SİL dağıtımına katılmasına izin veren sistemler önerilmiştir. C2C Epidemic yapısında, merkezi otorite tarafından araçlara belirli periyotlarda SİL dağıtımı yapılmakta olup, SİL dağıtımına araçlar da katılmaktadır. Bu yapı sayesinde, daha az yol kontrol ünitesi kullanılarak tüm araçlara daha kısa sürede SİL dağıtılması sağlanmıştır [16, 17] . SCRLE, C2C Epidemic tarafından sunulan araçlar arası SİL dağıtım yapısını daha sistematik hale getirmiştir [18]. Ancak, bu sistemlerde SİL'ler merkez tarafından ağdaki tüm araçlara periyodik aralıklar ile dağıtılır. Bu tür bir merkezi sistem trafik tıkanıklıklarına açıktır. Bununla birlikte, merkeze yapılan herhangi bir saldırı veya merkezdeki herhangi bir arıza tüm sistemi etkilemektedir.

Araştırmanın Amacı

Literatürde V2X iletişimi için tasarlanmış birçok güvenlik sistemi önerisi mevcuttur. IEEE ve ETSI tarafından da önerilen AAA tabanlı tasarımlar ise öne çıkan güvenlik sistemlerindendir. Tasarlanan AAA tabanlı sistemlerin ortak sorununun ölçeklenebilir bir sertifika iptal kontrol mekanizması oluşturulması olduğu görülmüştür. Ayrıca, oluşturulan merkezi yapı nedeniyle merkeze yapılacak kötü niyetli bir saldırıda tüm bağlı araçların etkilendiği görülmüştür. Bunun önüne geçebilmek için merkezi yapı üzerindeki yükün azaltılıp dağıtık bir yapının oluşturulması gerekmektedir. Çalışmanın temel amacı mevcut V2X yapılarının mesaj güvenliğini nasıl sağladığını araştırmak, mevcut sistemi geliştirmeyi ve yeni V2X iletişim güvenlik sistemleri tasarlamayı amaçlayan yayınları inceleyerek asimetrik anahtarlama kullanan V2X yapısı için optimum güvenlik çözümünü bulabilmektir.

Tezin Literatüre Katkısı

Akademik çalışmalar SİL dosyalarının dağıtımının daha verimli hale getirmek için SİL boyutunu azaltıp dağıtım hızını artırmaya odaklanmıştır. Bunun için dağıtık sitemlerin kullanılmasını öneren yapılarda SİL dosyalarının dağıtımında araçların da kullanılması sağlanmıştır. Bu sistemler, daha az yol kontrol ünitesi kullanarak SİL dosyalarının kısa sürede dağıtılmasını sağlasa da SİL dosyasının belirli aralıklar ile gönderildiği yapılar için tasarlanmıştır. Bu tez çalışmasında, sertifika iptal listelerinin etkili bir biçimde, gecikme yaratmadan, merkezi sunucuyu meşgul etmeden nasıl dağıtılacağı sorunu üzerinde durulmuş ve SİL sunucusu üzerindeki yükü azaltarak araç sertifikalarının iptal kontrolünü sağlayan yarı dağıtık bir yapıya sahip güven zincirine dayalı sertifika iptal kontrol sistemi önerilmiştir. Bu yapıda SİL dosyasının belirli aralıklar ile gönderildiği bir yapı yerine mesaj ulaştığında tetiklenen sertifika iptal kontrol yapısı kullanılmıştır. Önerilen sistemde merkezi SİL sunucusu tarafından yayınlanan SİL dosyaları yanında güven listesi adı verilen her aracın sahip olduğu güvenilir araçların listelendiği dinamik listeler kullanılarak merkezi yapı üzerindeki yük azaltılmıştır.

Çalışmanın ikinci bölümünde V2X'in kavramsal mimarisi anlatılıp günümüzde kullanılan IEEE ve ETSI standartları üzerinde durulmuştur. Üçüncü bölümde V2X güvenliğini sağlamak için önerilen çözümlerden, takma isim sertifikası, grup imzalama, simetrik anahtarlama ve blokzincir kullanımı anlatılmıştır. Dördüncü bölümde, V2X iletişimlerinde kullanılan sertifika iptal kontrol mekanizmaları incelenmiştir. Bu tezde önerilen yapı olan güven zincirine dayalı sertifika iptal kontrol mekanizması, beşinci bölümde anlatılmıştır. Altıncı bölümde, önerilen yapıyı test etmek için hazırlanan benzetim çalışması ve analizler açıklanmıştır. Son bölümde ise çalışmadan çıkarılan sonuçlar özetlenmiştir.

2. V2X İLETİŞİMİ

V2X, yeni nesil ağ teknolojileri kullanarak otomobillerin diğer araçlar, yayalar, altyapı ve bulut bilişim hizmetleri gibi çeşitli trafik unsurları ile iletişimini sağlayan bir araç iletişim teknolojisidir. Bu teknoloji Araç-Bulut (Vehicle to Cloud- V2C), Araç-Altyapı (Vehicle to Infrastructure- V2I), Araç-Araç (Vehicle to Vehicle- V2V) ve Araç-Yaya (Vehicle to Pedestrian- V2P) iletişimi gibi çeşitli alt teknolojilerin birleşmesinden oluşmaktadır [1].

V2X, trafik verimliliğinin artırılmasını, trafik kazalarının ve trafiğe bağlı hava kirliliğinin düşürülmesini ve kaynakların verimli kullanılmasını sağlamaktadır. Büyük ölçekli trafik optimizasyonu, iş birliğine dayalı seyir kontrolü, trafik ve akış yönetimi gibi alanlar için uygundur. Bu teknolojinin en temel kullanım alanları yol güvenliği sağlama, iş birliğine dayalı otomatik sürüş ve bilgi hizmetleri olarak sıralanabilir. Sağladığı bu yararlardan dolayı bu alanda şu ana kadar çeşitli projeler yapılmıştır. Bu projelerden bazıları Ek- 2'de sıralanmıştır.

V2X yapısı içinde kullanılması önerilen birçok iletişim teknolojisi mevcuttur, ancak bunların çoğu, ağa bağlı araçlarda güvenlik uygulamaları için gerekli olan minimum gecikme, güvenilirlik ve doğru veri iletimini sağlama yeteneğine sahip değildir. V2X iletişimi için temelde IEEE 802.11p tabanlı ve hücresel (LTE, 5G) altyapılı sistemlerin tasarlandığı görülmektedir [19].

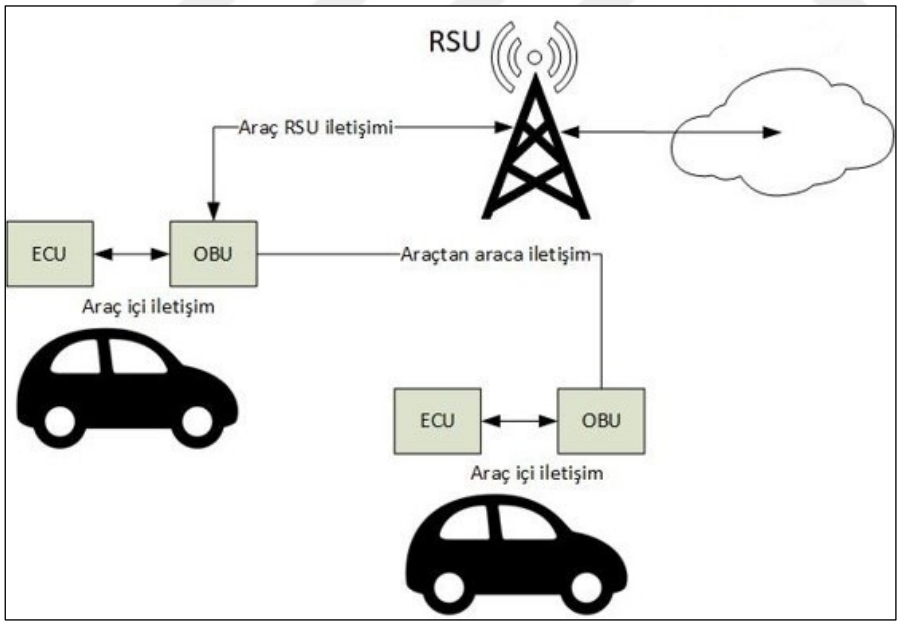
Hücresel tabanlı V2X sistemleri ile yüksek veri hızı, düşük gecikme süresi, kontrollü hizmet kalitesi (Quality of Service-QoS) ve daha geniş kapsama kapasitesi sağlanabilmesi hücresel tabanlı V2X sitemi tasarlayan araştırmaların temel motivasyonudur [20]. Birçok IEEE 802.11p tabanlı V2X iletişim sisteminin erken dönemlerde standartlaştırıldığı görülmektedir. Dedicated Short Range Communication (DSRC), Cooperative Intelligent Transport Systems (C-ITS) ve ITS Connect bu sistemlere örnek olarak verilebilir. Bu çalışmada, kullanım yaygınlığı nedeniyle IEEE 802.11p tabanlı sistemler üzerinde durulmuştur.

2.1. Kavramsal Mimari

V2X, ağ içinde bulunan varlıkların iletişimini çeşitli donanım cihazları ile sağlamaktadır. Bu çalışmada üzerinde durulacak olan V2I ve V2V iletişimindeki temel varlıklar ise araçlar ve RSU (Roadside Unit) adı verilen yol kontrol üniteleridir.

Araçların diğer araçlar ve RSU'lar ile iletişim kurabilmesi için bazı temel donanımlara sahip olması gerekmektedir. Araçların iç mimarisindeki iletişim ECU (Electronics Control Units) adı verilen araç kontrol üniteleri ile sağlanmaktadır. ECU'lar ile koordineli olarak çalışabilecek OBU (On Board Unit) adı verilen ünitelerin araçlara eklenmesi ile veri alma ve gönderme işlemi gerçekleştirilebilmektedir.

RSU'lar, araçların internet bağlantısı kurabilmesi ve veri alışverişinde bulunabilmesini sağlayan sabit yol üniteleridir. RSU'lar ve araçlardaki OBU'lar iletişim kurarak yol durumu ile ilgili bilgileri birbirleri ile paylaşırlar. Şekil 2.1'de üniteler arasındaki iletişim şematize edilmiştir.



Şekil 2.1. V2V ve V2I iletişim mimarisi

2.2. Günümüzde Kullanılan V2X Yapıları ve Standartlar

Günümüzde farklı V2X yapıları kullanılmaktadır. IEEE 802.11p ad hoc tabanlı DSRC, ABD'de kullanılan mevcut yapı iken Avrupa'da C-ITS, Japonya'da ise ITS Connect

kullanılmaktadır. Türkiye'de K-AUS (Kooperatif Akıllı Ulaşım Sistemleri) olarak isimlendirilen bağlantılı araç iletişim teknolojisi için henüz hazırlanmış standart ve mevzuat bulunmamaktadır [21].

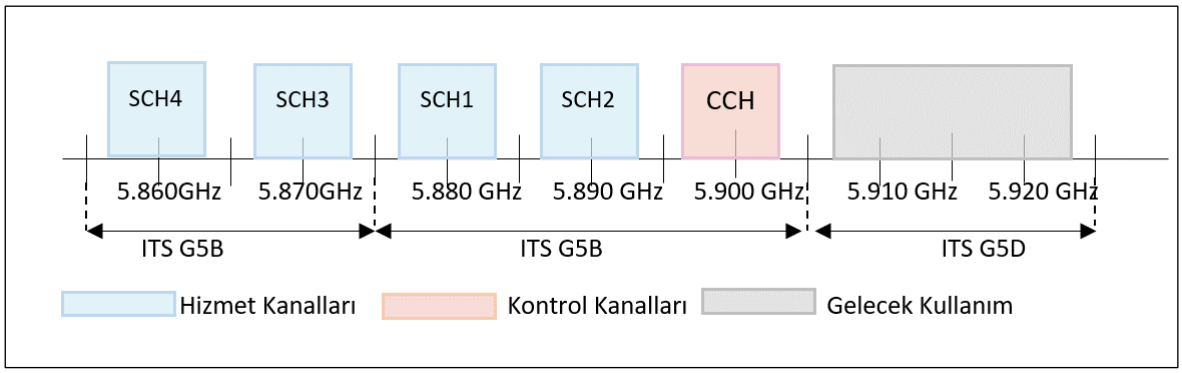
Amerika Birleşik Devletleri'nde kullanılan DSRC adı verilen V2X sisteminde IEEE Wireless Access in Vehicular Environment (WAVE) standartları kullanılmaktadır. Avrupa'daki C-ITS sisteminin standartları ise ETSI tarafından hazırlanmıştır. Japonya'da kullanılan ITS Connect, ARIB STD-T109 standardına bağlıdır. Bu bölümde DSRC ve C-ITS yapılarına kısaca değinilip V2X iletişimde kullanılan ETSI ve IEEE WAVE standartlarından bahsedilecektir.

ETSI ve IEEE WAVE standartları IEEE 802.11p tabanlı olsa da içerisinde farklılıklar barındırmaktadır. Bu farklılıklar nedeniyle bu iki teknolojinin birlikte çalışabilirliklerini sağlamak için iki uyum görev grubu kurulmuştur. Bu çalışma grupları CEN, ETSI ve IEEE gibi standart hazırlayan kuruluşlar ile iş birliği ile çalışıp, güvenlik standartlarını ve protokollerini uyumlu hale getirmektedir. Uyum çalışmaları 2013 yılında tamamlanmış olup raporlar çevrimiçi olarak kamuya açıktır [22, 23].

2.2.1. C-ITS ve ETSI

C-ITS, PHY ve MAC katmanları IEEE 802.11p standardına dayanan yol güvenliğinin artırılmasını amaçlayan kısa menzilli iletişim yoluyla bilgi alışverişine dayalı bir V2X yapısıdır.

5.825 GHz ile 5.925 GHz aralığında çalışmakta olan C-ITS'te, spektrum aralığı birkaç sınıfa ayrılmıştır. Şekil 2.2'de C-ITS frekans tahsisi gösterilmiştir. Sınıf A, 30 MHz'lik birincil frekans bandı trafik verimlilik uygulamaları için; 20 MHz'lik Sınıf B, güvenlik uygulamaları için; Sınıf C, radyo yerel alan ağları ile paylaşmak için; Sınıf D ise gelecek kullanımlar için ayrılmıştır [1].



Şekil 2.2. C-ITS frekans tahsisi

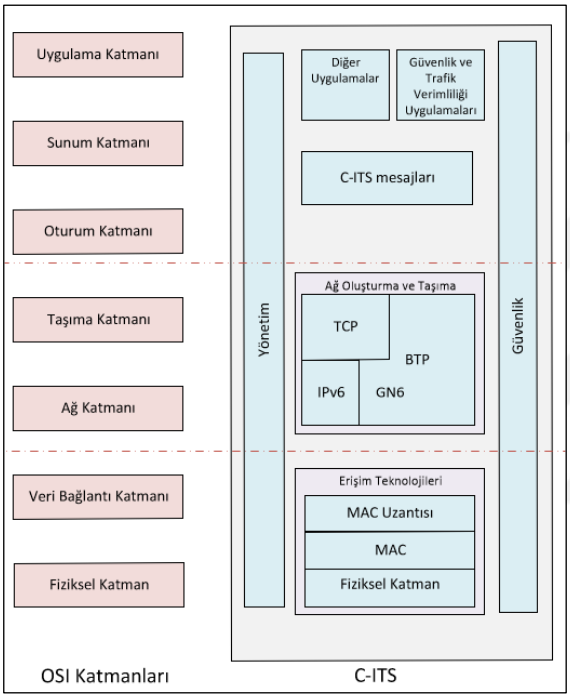
C-ITS teknolojisinde Cooperative Awareness Messages (CAM) ve Decentralized Environmental Notification Message (DENM) olmak üzere iki mesaj türü bulunmaktadır. CAM periyodik olarak gönderilirken DENM olay güdümlü olarak gönderilir. CAM'ler yol ağını kullanan araçların iş birliğini desteklemek için ITS ağında ITS-S'ler arasında gönderilen mesajlardır. CAM mesajları ile alıcı ITS-S, kaynak ITS-S'nin varlığından, türünden ve durumundan haberdar olur. Bir CAM, kaynak ITS-S'nin durum ve nitelik bilgilerini içerir. İçerik, ITS-S'nin türüne göre değişir. Durum bilgisi, zaman, konum, hareket durumu, etkinleştirilmiş sistemler, nitelik bilgisi, boyut, araç tipi vb. bilgiler bulunur. [24]. DENM mesajları ise tespit edilen bir olay hakkında sürücüleri uyarmak için çoğunlukla ITS uygulamaları tarafından gönderilen mesaj türüdür [25].

Şekil 2.3'te C-ITS ağ yapısı gösterilmiştir. Bu yapıda OSI Fiziksel Katman ve Veri Bağlantı katmanında çalışan C-ITS'nin Fiziksel, MAC ve MAC Uzantısı katmanı ETSI ES 202 663, ETSI TS 102 724, ETSI TS 102 687, ETSI TS 103 175 standartlarına bağlı olarak çalışmaktadır. OSI Ağ ve Taşıma Katmanında çalışan C-ITS BTP ve GN6, ETSI EN 302 636 standardına dayanmaktadır. Her katmanda çalıştığı görülen güvenlik yapısı ETSI'ye bağlıdır. Uygulama katmanı ise ETSI TR 102 638 ve ETSI TS 101 539-1/2/3 Road Hazard Signaling (RHS), Intersection Collision Risk Warning (ICRW), Longitudinal Collision Risk Warning (LCRW) standartlarına dayanmaktadır [26].

ETSI, V2X ile alakalı protokol, iletişim mimarisi, mesajlar ve güvenlik gerekliliklerini konu alan bir dizi standart yayımlamıştır. Avrupa'da kullanılan C-ITS teknolojisinde bu standartlar kullanılmaktadır. ETSI-ITS standartlarından bazıları aşağıda sıralanmıştır.

- **ETSI TS 102 637-2**: Temel hizmetlere genel bakış, kalite gereksinimleri ve mesaj formatları ile ilgili bilgiler içerir.

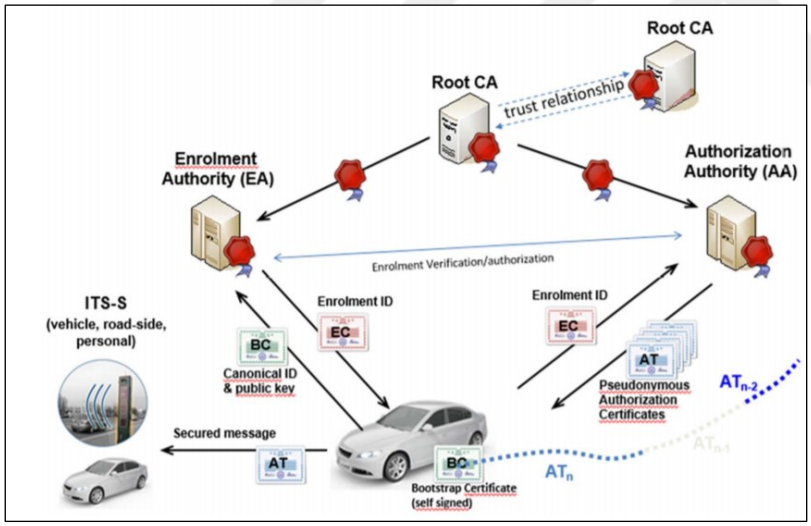
- **ETSI TS 102 636-4-1 ve ETSI TS 102 636-4-2:** GeoNetworking protokolünün ortamdan bağımsız işlevselliği açıklanır.
- **ETSI TS 102 637-3:** RHW uygulamasını destekleyen DEN temel hizmetinin özellikleri ve DENM mesajının semantiği açıklanır.
- **ETSI TS 102 636-5-1:** ITS ad hoc ağındaki ITS istasyonları arasında paketlerin taşınması için temel aktarım protokolü olan Basic Transport Protocol (BTP) anlatılır.
- **ETSI 102 941:** ITS iletişimleri için güvenlik ve gizlilik yönetimi açıklanır.



Şekil 2.3. C-ITS ağ katmanları

ETSI TS 102 941, V2X iletişimlerinde gizlilik, bütünlük ve kullanılabilirliğin sağlanması için hazırlanan güvenlik standardıdır [8] . Bu standart güvenliği sağlamak için iki sistem üzerinde çalışmaktadır. Bunlardan ilki olan SecuredMessage adı verilen yapıda, yayınlanan CAM, DENM mesajları şifrelenmeden iletilirlerken; ITS istasyonları ile sertifika otoriteleri arasındaki mesajlar asimetrik anahtarlama kullanılarak şifrelenirler [23]. Bu yapıda farklı kullanım durumları için farklı mesaj tipleri mevcuttur. Bu mesaj tipleri Aktif Yol Güvenliği (Active Road Safety), Kooperatif Trafik Verimliliği (Cooperative Traffic Efficiency), Kooperatif Yerel Servisleri (Cooperative Local Services) ve Küresel İnternet Servisleri (Global Internet Services) olmak üzere dört ana uygulama sınıfı altında toplanmaktadır (Ek-3) [27].

Güvenliği sağlamak için oluşturulan ikinci sistem, sertifika yapısıdır. Sertifika yapısı sayesinde kullanıcı kimliği ve yetkisi kanıtlanmış olur. Sertifika yapısında belirli bir hiyerarşik düzende bulunan CA (Certificate Authority) adında sertifika otoriteleri bulunur. Bu otoriteler kök sertifika otoritesi (Root CA), kayıt sertifika otoritesi (Enrollment CA) ve yetkilendirme sertifika otoritesi (Authorization CA) olarak isimlendirilirler [20]. Kök sertifika otoritesi hiyerarşinin en üstünde bulunan otoritedir. Kayıt sertifika otoritesi ve yetkilendirme sertifika otoritelerine, V2X iletişimi için kullanılacak sertifikaları dağıtma yetkisi verir. Kayıt sertifika otoritesi, V2X ağında bulunan her varlık için kimlik kanıtı sağlayan uzun dönemli EC (Enrollment Credentials) olarak isimlendirilen sertifikalar dağıtır. Yetkilendirme otoritesinin ise AT (Authorization Ticket) adında kısa dönem geçerliliği olan sertifikaları dağıtma yetkisi vardır. EC, kimlik kanıtı için kullanılırken; AT, V2X mesajlarını şifrelemek için kullanılır [28]. AT'lerdeki takma isim kullanımı ile gizlilik sağlanır. Takma isimler, belirli aralıklarla güncellenerek gizlilikteki süreklilik sağlanmış olur. Şekil 2.4'te sertifika yapısındaki hiyerarşi gösterilmiştir [29].

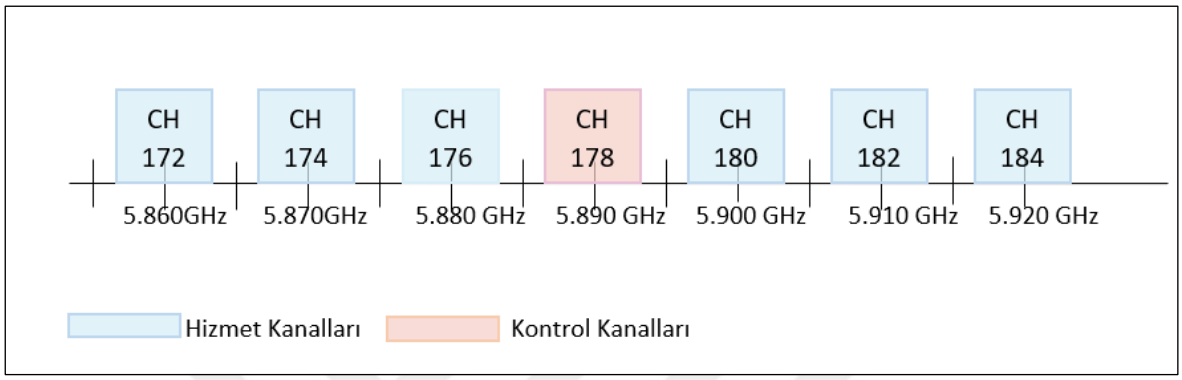


Şekil 2.4: ETSI ITS sertifika yapısı hiyerarşisi [29]

2.2.2. DSRC ve IEEE WAVE

DSRC, güvenli ve yüksek hızlı doğrudan iletişim sağlayan PHY ve MAC katmanı için IEEE 802.11p standardına dayanan bir kablosuz iletişim teknolojisidir. DSRC hem V2V hem de V2I iletişimini desteklemek için Federal Communication Commission (FCC) tarafından 1999 yılında önerilmiştir [30].

DSRC 5,825 GHz ile 5,925 GHz aralığında çalışmaktadır. Spektrum 10 MHz'lik yedi kanala bölünmüştür (Şekil 2.5). Merkezde yer alan Kanal 178 (5,885–5,895 GHz) kontrol kanalı (CCH), güvenlik ile ilgili kritik alarmları ve işaretleri taşımaktadır. Bu kanal, güvenlik iletişimleri için ayrılmıştır. Diğer kanallar ise güvenliğin yanında diğer hizmetler için de kullanılmaktadır. Bu nedenle bu kanallar hizmet kanalları olarak adlandırılmıştır [1].



Şekil 2.5: DSRC frekans tahsisi

DSRC'deki temel güvenlik mesajı Basic Safety Message (BSM), aracın konumu, hızı ve ivmesi ile ilgili verileri içeren temel bilgileri taşır. BSM içerisinde taşınan bilgiler

Ek- 4'te listelenmiştir. RSU'lar ve araçlar, BSM yayınlarındaki bilgileri kullanarak trafik akışı, araç hızları ve araç yoğunluklarını hesaplar. Bu şekilde trafik koşulları hakkında gerekli bilgiler elde edilmiş olur [31]. BSM, periyodik olarak şifrelenmeden iletilen mesajlardır. Trafik içinde meydana gelen kritik olaylardan komşu araçları haberdar edebilmek için olay güdümlü olarak da iletilebilir.

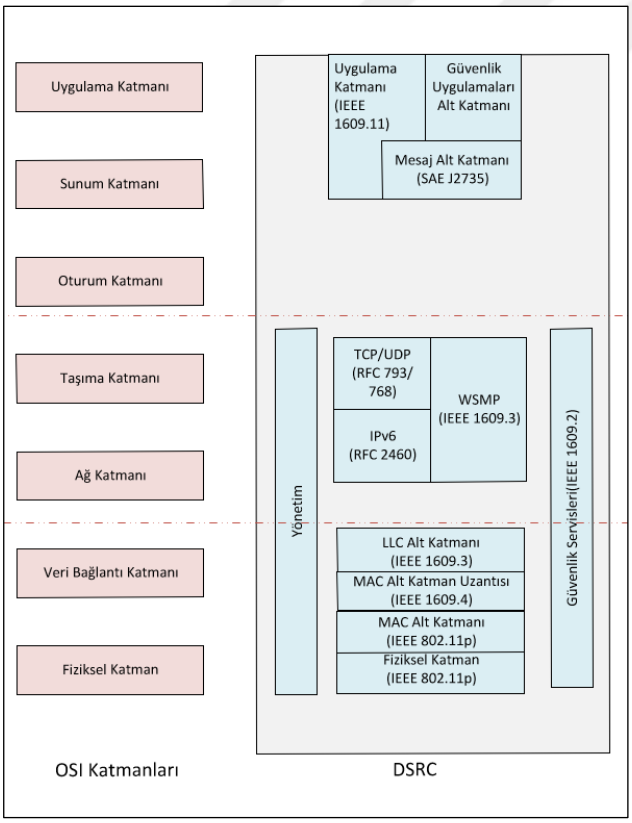
ABD'de Standardization Development Organization (SDO), IEEE ve Society of Automotive Engineers (SAE) V2X teknolojisinden sorumlu organizasyonlardır. V2X güvenlik konularındaki standardizasyon çalışmalarını ise IEEE 1609.2 çalışma grubu, SAE DSRC teknik komitesi ve CAMP-VSC (Crash Avoidance Metrics Partnership–Vehicle Safety Community) üstlenir.

ABD'deki DSRC iletişimi için kullanılan mimari IEEE WAVE'dir. IEEE WAVE kullanılan güvenlik mekanizmaları, mimarisi bakımından Avrupa'da kullanılan ETSI standartlarına benzer bir yapıya sahiptir. DSRC/WAVE protokol katmanları ve kullanılan standartlar Şekil 2.6'da gösterilmiştir. DSRC mimarisinde, PHY ve MAC katmanları için IEEE 802.11p benimsenir. Ağ katmanında WAVE Kısa Mesaj Protokolü (WAVE Short Message Protocol

-WSMP) kullanılır, ancak uygulamaya bağlı olarak IPv6, TCP ve UDP gibi diğer protokollerin kullanılmasına da izin verilir. Üst katmanlarda IEEE 1609 protokolleri uygulanır. IEEE 1609 ailesi V2X iletişim modeli, mimarisi, yönetim yapısı ve güvenlik mekanizmasını belirleyen WAVE standartlarıdır. IEEE WAVE standartlarından bazıları aşağıda sıralanmıştır.

- **IEEE 1609.3:** Ağ hizmetlerinin düzenlenmesinde kullanılan standarttır.
- **IEEE 1609.2:** Uygulamalar ve yönetim mesajları için güvenlik hizmetlerini belirleyen standarttır. IEEE 1609.2'de mesaj güvenliği, güvenli veri yapısı, güvenli mesaj formatı ve bu güvenli mesajların WAVE platformunda işlenmesi tanımlanmaktadır.

IEEE 1609.2'de mesajların kimlik doğrulaması ve bütünlüğü dijital imzalamaya bağlıdır [9]. İmzalama ve doğrulama işlemleri için dijital imza algoritmaları ve sertifika yapısı kullanılır. Bu yapı içindeki tüm güvenlik sertifikalarının dağıtımı Security Management System (SCMS) ile gerçekleştirilir.



Şekil 2.6. DSRC ağ mimarisi

2.2.3. IEEE 802.11p ve IEEE 802.11bd farkları

DSRC ve C-ITS, potansiyel olarak tehlikeli durumlarda uyarı veren, sürücünün güvenli ve verimli bir şekilde sürüş yapmasına yardımcı olan bir dizi temel araç güvenlik uygulamasını desteklemektedir. Bu uygulamalar, 1~10 Hz. aralık ve 50~100 msn uçtan uca gecikme ile periyodik mesajlar iletebilmektedir. Odak noktası araç güvenliği, trafik yönetimi, park etme ve araç tanımlama olan IEEE 802.11p standardı 200 km/saat hız, 100 msn'lik yanıt süresi ve 1000 m'lik iletişim mesafesini desteklemektedir [32].

Gelişmiş V2X iletişim teknolojileri için IEEE standardında iyileştirmeler yapmak üzere 2018 yılında New Generation Vehicle (NGV) adlı bir çalışma grubu oluşturulmuştur [33]. Oluşturulan yeni IEEE 802.11bd standardı ile hız 500km/saat olurken iletişim mesafesi 2000m’ye yükselmiştir. Daha yüksek verimlilik, gelişmiş güvenilirlik ve daha yüksek menzil sağlanırken aynı zamanda mevcut sistemlerle geriye dönük uyumluluk garanti edilmiştir. IEEE 802.11bd'nin son sürümü Aralık 2021'de kullanıma sunulmuştur [34].

3. V2X GÜVENLİĞİ

Güvenlik, diğer kablosuz teknolojilerde olduğu gibi V2X teknolojisi için de kilit problemlerden biridir. V2X içindeki V2I ve V2V, kablosuz ağlarda yaygın olarak görülen saldırılara karşı savunmasızdır. Örneğin, bir araca verilen yanlış bir uyarı trafikte bozulmalara neden olabilir ya da ağdaki araçları yanıltmak için mesajlar saldırganlar tarafından taklit edilebilir. Bu teknolojinin önündeki en büyük zorluk, saldırıların doğru şekilde tespitini yapmak ve savunma için güvenlik protokolleri tasarlamaktır. Tasarlanan protokoller ile güvenlik, gizlilik, güvenilirlik ve bütünlük sağlanmalıdır. Güvenilirlik V2X'in ana gerekliliğidir. Mesaj güvenilirliğinin sağlanabilmesi için bütünlük, kimlik doğrulama ve gizlilik sağlanmalıdır.

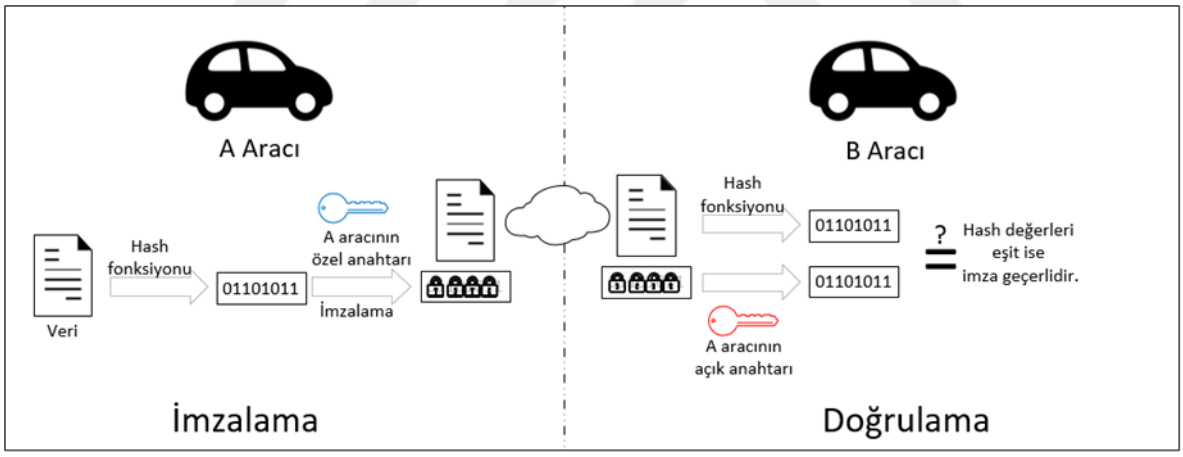
V2X iletişiminde bir dizi potansiyel saldırı mevcuttur. V2X iletişiminde karşımıza çıkan saldırılar Ek- 5'de listelenmiştir. Saldırganların araçlara sahte mesajlar gönderdiği sahte mesaj saldırısı (message faking attack) ile araçlar yanlış yönlendirilebilir. Mesaj tekrarlama saldırısı (message reply attack) ile saldırganlar ağ üzerindeki gerçek bir mesajı ele geçirerek bu mesajı, sunucuları meşgul etmek için kullanabilir. Mesaj değiştirme saldırısı (message modification attack) ile saldırganlar ağ içindeki mesajları yakalayıp değiştirebilir. Kimliğe bürünme saldırısı (impersonation attack) yapan saldırganlar ağ üzerindeki herhangi bir varlık adına mesaj gönderebilir. Saldırganlar hizmet reddi saldırısı (denial of service attack) ile V2X kanallarında sıkışmaya sebep olabilir. Ayrıca saldırganlar ağı dinleyip araçların konumunu elde edebilir [35]. V2X iletişiminde tam koruma ve gizlilik sağlamak için bahsedilen saldırı türlerini önlemeyi amaçlayan birçok güvenlik sistemi çalışması bulunmaktadır. Fakat, V2X güvenliği olgunlaşmış bir yapıya kavuşmamıştır.

AAA, V2X güvenliğini sağlamak için kullanılan temel kriptografik çözümlerden biridir. Simetrik anahtarlama ve blokzincir de güvenliği sağlamak için kullanılan yapılar arasındadır. Bu bölümde, V2X güvenlik altyapılarının oluşturulmasında kullanılan bu yöntemlerden bahsedilecektir. Ayrıca, AAA kullanan yapılarda gizlilik koruması için grup imzalama ve takma isim sertifikası gibi yapılar açıklanacaktır.

3.1. V2X Güvenliği ve Açık Anahtar Altyapısı

AAA, mesajların ağda güvenli bir şekilde iletilmeleri için kullanılan kriptografik bir yapıdır. Bu sistemde her aracın asimetrik anahtar çifti ve sertifikası bulunur. Asimetrik anahtar çifti, yalnızca anahtar sahibi tarafından kullanılıp gizli tutulması gereken özel anahtar ve herkes tarafından görülebilen açık anahtardan oluşmaktadır. Mesajlar gönderici aracın özel anahtarı ile imzalanarak inkar edememe, kimlik doğrulama ve bütünlük gibi özellikler karşılanmaktadır. İmza doğrulama işlemi ise göndericinin sertifikasında bulunan açık anahtar kullanılarak alıcı tarafından yapılabilmektedir.

Şekil 3.1'de imzalama ve doğrulama işlemleri gösterilmiştir. A aracı bir mesaj göndermeden önce göndermek istediği açık verinin HASH değerini özel anahtarını kullanarak imzalar. Oluşturulan imza, açık veri ile birlikte alıcılara gönderilir. Alıcı B aracı, A aracının açık anahtarını kullanarak imzayı doğrular. Doğrulama işlemi açık verinin HASH değeri ve açık anahtarın kullanılması ile elde edilen HASH değerinin eşitliğinin kontrolü ile sağlanır.



Şekil 3.1. AAA yapısı imzalama ve doğrulama adımları

Sertifika, açık anahtarlı kriptografi teknolojisine dayanan ve bir varlığın elektronik ortamda kimliğini ispatlaması için kullanılan elektronik dosyadır. Güvenilirlik, güvenilir merkezi yapı etrafında oluşturulmuş hiyerarşik düzende görev yapan yetkili kuruluşlar tarafından sağlanmaktadır. Yetkili makam tarafından imzalanmış olan sertifika, sertifika sahibi ile ilgili tanımlayıcı bilgiler ve açık anahtar bilgisini taşır. Bu sayede, açık anahtar bilgisinin belirtilen sertifika sahibine ait olduğu temin edilir. Mesajların güvenilir olduğunu anlayabilmek için imzalı mesajı gönderen tarafın sertifikası kontrol edilir [35]. Kontrol işlemi imza kontrolü, geçerlilik tarihi kontrolü ve sertifika iptal kontrolü olmak üzere üç aşamalıdır. İmza kontrolü,

sertifikanın yetkili bir makam tarafından verildiğinin kontrolüdür. Bu kontrol, yetkili makamların açık anahtarları kullanarak sertifika üzerindeki imzanın doğrulanmasıyla gerçekleştirilir. Geçerlilik tarihi kontrolü, sertifikanın yetkilendirildiği zaman aralığında kullanıldığının kontrolüdür. Sertifika üzerindeki başlangıç ve bitiş tarihlerine bakılarak yapılır. İptal kontrolü ise herhangi bir nedenden dolayı sertifikanın iptal olmadığının kontrolüdür. Bu kontrol, SİL ve benzeri iptal kontrol mekanizmaları kullanılarak gerçekleştirilir. Bu şekilde, diğer araçların iptal olan araçlardan haberdar olması sağlanmaktadır. Bu kontrollerden başarılı şekilde geçen sertifika sahibinden gelen imzalı mesajlar güvenilir sayılır.

V2X iletişimlerinde araç anonimliğinin sağlanması da kritik bir önem taşımaktadır. Kötü niyetli tarafların, sertifikaları kullanarak araç takibi yapmasını önleyecek sistemler kullanılmalıdır. Bunu karşılayabilmek için AAA içinde kullanılabilecek takma isim sertifikası gibi ek yapılar geliştirilmiştir.

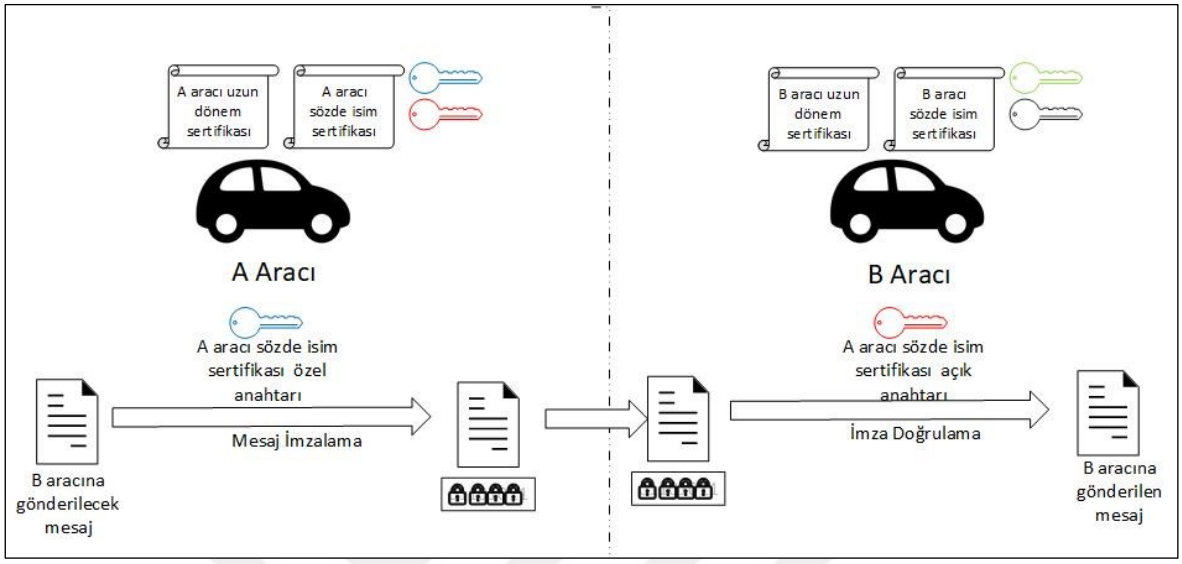
3.1.1. V2X güvenliği ve takma isim sertifikası

Açık anahtar altyapısını kullanan V2X güvenlik sistemlerinin çoğunda her aracın iki sertifikası bulunmaktadır. Bunlardan biri uzun dönem sertifikası diğeri ise takma isim sertifikasıdır. Uzun dönem sertifikası, aracın takma isim sertifikası almaya uygun olduğunu gösteren sertifikadır. Bir araç, bir ağa dahil olmak istediğinde ilk olarak yetkili kuruluşlara başvurarak bu sertifikayı almak zorundadır. Takma isim sertifikaları ise aracın uzun dönem sertifikası ile aldığı araç gizliliğini korumak için tasarlanmış olan, takma isim içeren sertifikalardır. Takma isim sertifikaları, araç ile ilgili tanımlayıcı bilgiler içermemekte ve kısa aralıklar ile güncellenmektedir.

Gönderilen mesajlar takma isim sertifikasının özel anahtarı ile imzalanır. Mesajı alan taraf, mesaja eklenen takma isim sertifikasını ve açık anahtarı kullanarak alınan mesajı doğrulayabilir. Bu şekilde, mesaj gönderen tarafın güvenilirliğinden emin olunurken aynı zamanda gönderen tarafın gizliliği sağlanır. Anonimliğin korunması ile kötü niyetli tarafların araç takibi önlenmiş olur [10].

Şekil 3.2’de takma isim sertifikası kullanılarak mesaj iletimi gösterilmiştir. A aracı bir mesaj göndermeden önce göndermek istediği mesajı takma isim sertifikasına bağlı özel anahtarını

kullanarak imzalar. Oluşturulan imza, açık veri ile birlikte alıcılara gönderilir. Alıcı B aracı, A aracının takma isim sertifikasını ve açık anahtarını kullanarak imzayı doğrular.



Şekil 3.2. AAA takma isim sertifikası ile mesaj gönderimi

Takma isim sertifikası, SCMS, C-ITS, E-Safety Vehicle Intrusion Protected Applications (EVITA), Secure Vehicle Communication (SeVeCom), Privacy Enabled Capability in Co-operative Systems and Safety Applications (PRECIOSA), Preparing Secure Vehicle-to-X Communication Systems (PRESERVE) ve Communication Network Vehicle Global Extension (CONVERGE) gibi projelerde güvenlik koruma mekanizması olarak önerilmektedir [36]. Bu projelerde kullanılan sertifika ömrünün uzunluğu, oluşturulan yapıya göre değişmektedir.

Yapı içerisinde farklı rolleri üstlenen yetkili kuruluşlar hiyerarşik bir düzende görev yapmaktadır. Kök Sertifika Yetkilisi, Alt Sertifika Yetkililerine sertifika sağlayan AAA yapısının güvenilir kuruluşudur. Sertifika Kayıt Yetkilileri araçların kayıt işlemlerinden sorumludur ve araçlara uzun dönem sertifikası sağlar. Takma isim sertifika yetkilileri, Uzun Dönem Sertifikasına sahip araçlara kimlik bilgisi içermeyen takma isim sertifikalarının temininden sorumludur. Yapı içinde soruna neden olan veya başka bir nedenden dolayı ağdan çıkarılması gereken araç sertifikalarının iptalinden sorumlu kuruluş Sertifika İptal Yetkilisidir. Bu kuruluş sertifika iptal listelerini düzenli aralıklarla yayınlamaktan sorumludur [36]. Takma isim kullanan her projenin hiyerarşik yapısı benzer olsa da ufak farklılıklar içermektedir. Örneğin, DCS (Distributed Certificate Service) şeması ile

OBU'ların RSU'dan; RSU'ların, Sertifika Yetkilisinden, Sertifika Yetkililerinin, Kök Sertifika Yetkilisinden sertifika alabildiği bir sistem 2010 yılında önerilmiştir [37].

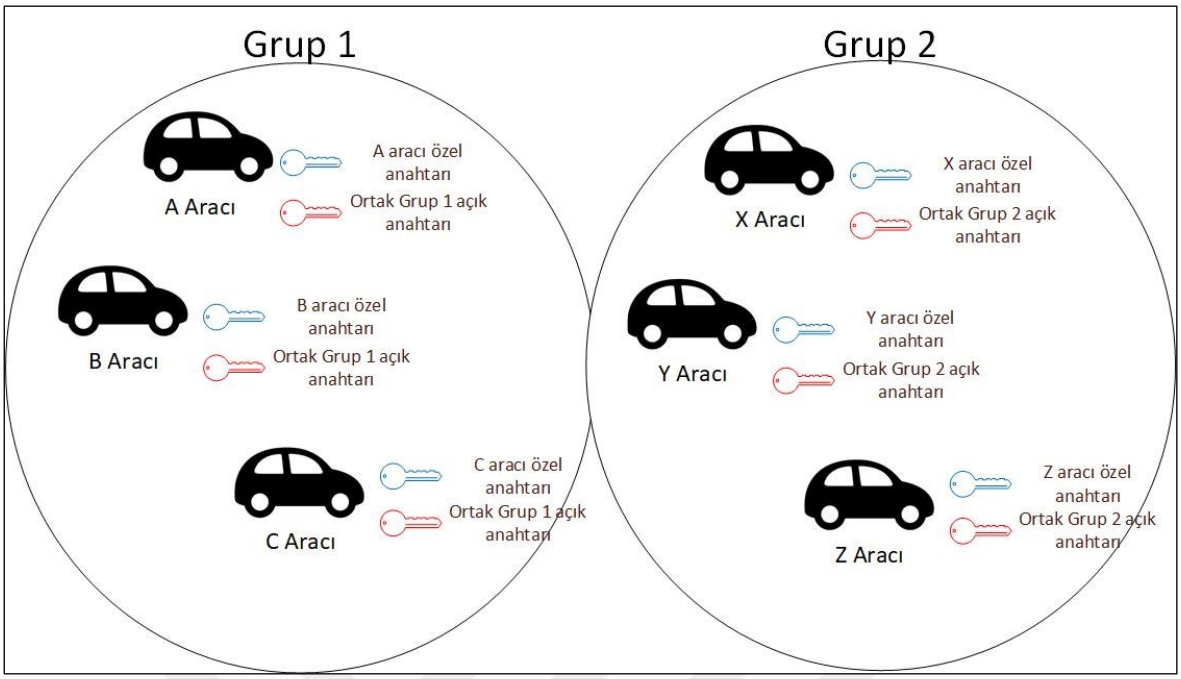
Kimlik doğrulama ve anonimlik özelliklerini aynı anda sağlayan takma isim sertifikası kullanımındaki en büyük problem verimli bir iptal kontrol mekanizmasının yaratılmasındaki zorluktur. Takma isim sertifika kullanımı iptal edilen sertifika sayısını artırmakta, SİL kullanımını karmaşık ve verimsiz hale getirmektedir.

Her cihazın uzun dönem sertifikası ve kısa süreli geçerliliği olan takma isim sertifikasına sahip olduğu sistemlerdeki sertifika iptal kontrolünü sistematik bir hale getirmek için SCMS isimli güvenlik kimlik bilgisi yönetim sistemi önerilmiştir. Bu sistem, sertifika önyükleme, sertifika sağlama, yanlış davranış bildirimi ve iptal kontrolü gibi dört ana kullanım durumunu desteklemektedir [38]. Sistemdeki zorluk ise hatalı davranan veya arızalı araçların etkin bir şekilde iptalini sağlamaktır.

Sertifika iptal listesine alternatif çözümler getiren çalışmalar da bulunmaktadır. Sertifika iptal listelerini kullanmaksızın oluşturulan araç iptal mekanizmaları olan ve doğrulama ek yükünü azaltan sistemlerin çoğunda geçerli bir takma isim oluşturmak için RSU veya güvenilir otoritenin sisteme dahil edilmesi gereklidir [39].

3.1.2. V2X güvenliği ve grup imzalama

Grup imzalama ilk olarak Chuam vd. (1991) tarafından ortaya atılmıştır. Bu imzalama çeşidinde grup üyesi olan her varlık bir mesajı grup adına kendi özel anahtarı ile anonim olarak imzalayabilir. İmzalanan mesaj, grubun herhangi bir üyesi tarafından grubun ortak anahtarı kullanılarak doğrulanabilir. Bu işlem için genellikle Eliptik Eğri Dijital İmzalama Algoritması (Elliptic Curve Digital Signature Algorithm- ECDSA) kullanılır [40]. Grup imzalama yönteminde bir grup yöneticisi bulunur. Bu yönetici, grup parametrelerinin değişmesi, grup açık anahtarının değişmesi ve gerekli durumlarda grup üyesi anonimliğinin iptali gibi görevleri üstlenir. V2X yapılarında kullanılan grup imzalamada grup yöneticisi üçüncü bir taraf olmak zorunda değildir, ağ içindeki varlıklardan biri de grup yöneticisi olabilir [41]. Şekil 3.3'te grup imzalama yapısındaki anahtarların V2X içinde kullanımı şematize edilmiştir.



Şekil 3.3. Grup anahtar şematiği

Literatürde grup imzalama kullanılarak V2X iletişim güvenliğini sağlamayı amaçlayan çeşitli çalışmalar mevcuttur. Grup imzalama kullanılarak kimlik doğrulama, veri bütünlüğü, anonimlik ve hesap verilebilirliğin sağlandığı DSRC yapısı için RSA tabanlı bir sistem tasarlanmıştır [11]. Bu çalışmada sertifikaların iptal bilgilerinin kontrolünde kullanılan sertifika iptal listelerinin neden olduğu gecikmeler sebebiyle uygulanabilirlik düşüktür.

Araçlar tarafından alınan mesajların sayısı artığında, geleneksel kapsamlı kimlik doğrulama, araçlarda karşılanamayacak hesaplama yükü oluşturabilmektedir. Bunun çözümü için iş birliğine dayalı mesaj kimlik doğrulamasının önerildiği bir grup imzalama modeli önerilmiştir [42]. Bu modelde iş birliği yapacak cihazlar coğrafi konumlarına göre seçilip gruplandırılmaktadır. Fakat RSU sayısının artırılması gerekliliği nedeniyle önerilen sistemin altyapı maliyeti çok yüksektir.

DSRC iletişimlerinde OBU ile RSU arasındaki iletişimdeki gizliliği korumak için ECPP adında grup imza kullanan bir protokol geliştirilmiştir [12]. Bu protokolde araçlar kısa süreli takma isim sertifikalarını RSU'lardan alabilmektedir. Kullanılan kısa süreli takma isim sertifikaları nedeniyle her mesaj için sertifika iptal listesi kullanılarak iptal kontrolü yapılmasına gerek kalmamaktadır. Bu sistemin zayıf noktası, RSU'ya yapılan bir saldırı ile o bölgedeki tüm iletişimin ele geçirilebilmesidir.

Grup imzalama tabanlı sistem tasarlayan diğer bir çalışmada, ağa bir izleme yöneticisi eklenmiştir. İzleme yöneticisi, kötü niyetli araçları izlemenin dışında RSU'lara sertifika iptal listesi sağlama işini de üstlenmektedir. Bu şekilde OBU ve merkezi otoritelerin yükü azalmaktadır fakat işlem süresi hala yeterli kısalıkta değildir [39].

Sertifika iptal listesi sorununun üstesinden gelmek için karma mesaj kimlik doğrulama koduna dayalı bir şema önerilmiştir [43]. Önerilen şemada, geniş bir alan birkaç parçaya gruplandırılmıştır. Kimlik doğrulama işlemi, bir araç yeni bir alana katılmak istediğinde gerçekleşmektedir. Karşılıklı kimlik doğrulamasından sonra araca yeni bir grup anahtarı dağıtılmakta ve araçlar grup anahtarından türetilen karma bir mesaj kimlik doğrulama kodu ile güvenlikle ilgili mesajları yayınlamaktadır. Bu sistemde tüm mesajlar toplu olarak doğrulanabilecek şekilde tasarlanmıştır. RSU sadece yasal araçların gruba katılmasını sağladığından ve grup anahtarı periyodik olarak güncellendiğinden, bu şemada iptal edilen araçları kontrol etmek için sertifika iptal listesi kullanmaya gerek yoktur.

Yukarıda bahsedilen grup imzalama ve takma isim sertifikası kullanılarak oluşturulmuş V2X güvenlik sistemlerinde, yapıya uygun bir sertifika iptal kontrol yönteminin tasarlanması gerekmektedir. Yüksek güvenlik seviyesi ile yüksek kimlik doğrulama verimliliği arasındaki çelişki tam olarak çözülememiştir. Grup imzasına dayalı şemalar, kimlik tabanlı şemalar ile karşılaştırıldığında, kimlik tabanlı şemaların büyük ölçekli araç ağlarında daha verimli olma eğiliminde olduğu görülmektedir [39].

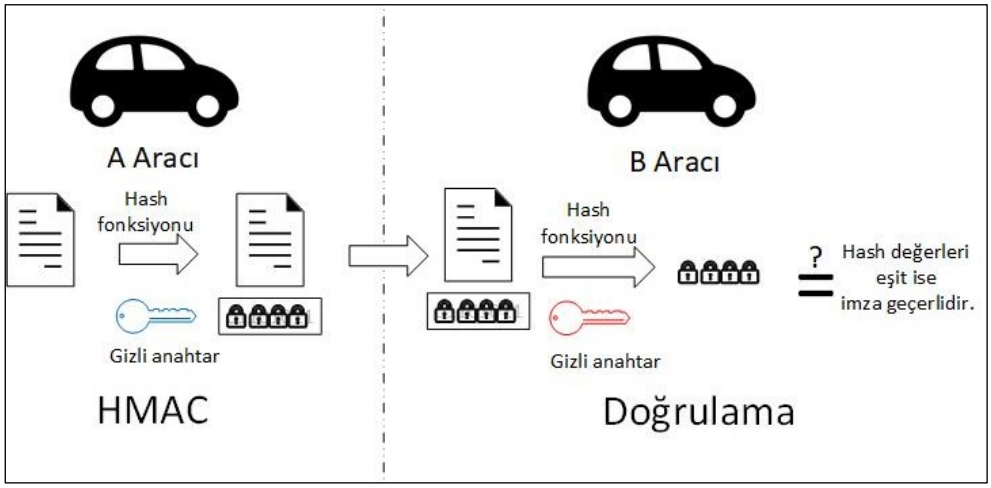
Mesaj kimlik doğrulaması, bilgi güvenilirliğini, veri bütünlüğünü ve özgünlüğünü sağlamak için yaygın kullanılan bir araç olsa da V2X iletişiminde kimliğin açık olması güvenlik açısından çeşitli riskler doğurmaktadır. Bu sorunu çözmek için kullanılan grup imzalama yönteminde uygulanabilirlik konusunda eksiklikler bulunmaktadır. İşlem yükü ve işlem süresinde istenen ölçüde iyileştirme sağlayamamakta ve altyapı maliyetini artırmaktadır. Bu sistemin temel problemi ise verimli bir sertifika iptal kontrol mekanizmasına sahip olmamasıdır.

3.2. V2X Güvenliği ve Simetrik Anahtarlama

AAA'daki sertifikalı altyapının oluşturulması ve sürdürülmesindeki zorluklar nedeniyle simetrik anahtarlama alternatif bir çözüm olarak kullanılmaktadır. Simetrik

anahtarlama şifreleme ve şifre çözme işlemleri için tasarlanmıştır. Bu yapıda şifrelemeyi yapan taraf ile şifre çözen tarafın ortak olarak sahip olduğu gizli bir anahtar olması gerekmektedir. Şifreleme ve şifre çözme işlemleri bu gizli anahtar ile sağlanmaktadır. Hesaplama yükü asimetrik anahtarlamaya kıyasla düşüktür.

Karma İleti Kimlik Doğrulama Kodu (HMAC- HASH Message Authentication Code) V2X iletişiminde kimlik doğrulama için kullanılan bir simetrik anahtarlama yöntemidir [43]. HMAC kriptografik özet fonksiyonu ve gizli bir simetrik anahtar içeren bir mesaj doğrulama kodudur. HMAC'in özet fonksiyonun saldırılara karşı dayanıklılığı, özet boyutunun uzunluğu, kullanılan simetrik gizli anahtarın kalitesi ve uzunluğuna bağlı olarak değişmektedir. Bu sebeple kullanılan özet fonksiyonu ve simetrik anahtar algoritması seçimi büyük önem taşımaktadır. HMAC iletilmek istenen mesajı şifrelemek için kullanılmaz; HMAC özetinin yanında mesaj düz metin ya da şifreli olarak gönderilebilir. HMAC mesaj bütünlüğü ve kimlik doğrulama için kullanılır. Mesaj doğrulamasının yapılabilmesi için gönderici ve alıcı tarafta da anahtar bulunması gerekmektedir. Alıcı taraf eline geçen mesajın özetini alır ve eline geçen HMAC özeti ile karşılaştırır. Elde edilen özetler eşit ise mesaj doğrulanmış olur [44]. Şekil 3.4'te HMAC yapısının mesaj iletiminde kullanımı gösterilmiştir.

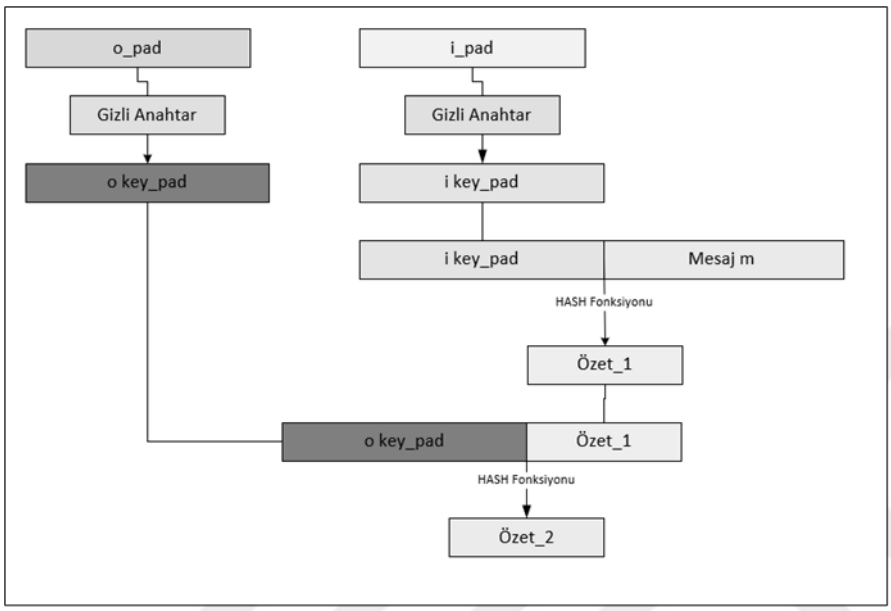


Şekil 3.4. HMAC kullanılarak mesaj iletilmesi ve doğrulama işlemi

İletilecek mesajlar belirli boyuttaki bloklara bölünür ve sırasıyla üzerinde HASH fonksiyonları çalıştırılır. Eş. (*3.1*'de HMAC fonksiyonu gösterilmiştir. Bu eşitlikte H değeri herhangi bir özet fonksiyonunu, "K" gizli anahtarı ve "K' " gizli anahtardan türetilen yeni gizli anahtarı, "m" mesajı temsil etmektedir. "*ipad*" iç tamamlama; "*oped*" ise dış

tamamlamadır. SHA1 HASH algoritması kullanılarak HMAC oluşturulma işlemi Şekil 3.5'te gösterilmiştir.

$$HMAC(K,m) = H((K' \oplus opad)||H((K' \oplus ipad)||m)) \quad (3.1)$$



Şekil 3.5. SHA-1 Özet algoritması kullanılarak oluşturulan HMAC

Literatürde, V2X iletişiminde HMAC kullanılarak güvenliğin sağlandığı birçok çalışma bulunmaktadır. Örneğin, RAISE adlı bir mesaj doğrulama tekniğinin geliştirildiği bir çalışmada, araçlar en yakında bulunan RSU'yu tespit edip ona bağlanmaya çalışırlar. Bunu karşılıklı bir kimlik doğrulama süreci takip eder. Araçlardan alınan mesajların doğrulanması RSU'lar tarafından sağlanır. Doğrulamanın ardından, RSU'lar bildirimleri ilgili araçlara geri gönderir. RSU'lar ayrıca diğer araçlar arasında paylaşılan bir takma isim tahsis eder. Takma isim, RSU'nun mesajı gönderen aracı tanımasına ve mesaj kimliğini doğrulamasına yardımcı olur. Her araç, simetrik anahtarın yardımıyla simetrik anahtarlı bir HMAC üretir. Ardından araç, simetrik HMAC kodu ile imzalanmış bir mesaj yayınlar. RSU, diğer araçlar ile paylaşılan HMAC şifreleme anahtarlarına sahip olduğu için mesajı doğrulama yeteneğine sahiptir. RSU'lar ve araçlar arasındaki iletişim takma isim kullanılarak yapıldığı için araç rotası saldırganlar tarafından takip edilemez [5]. Fakat, oluşturulan bu sistemde RSU'nun yükü ve RSU'ya olan bağımlılık artmaktadır.

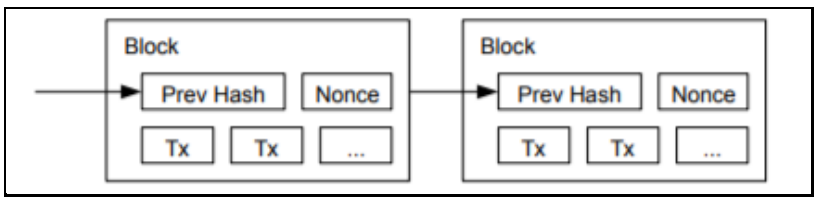
Simetrik anahtarlama tabanlı modellerde sadece yetkili araçlara gizli anahtarlar dağıtılır. İki tarafın da gizli anahtara erişiminin olması gerekliliği, bu sistemin ana dezavantajlarından biridir. Hesaplama yükü asimetrik anahtarlamaya kıyasla düşüktür. Mesajda, göndereni tanımlayacak bir bilgi bulunmaması ile anonimlik sağlanır. Fakat bu durum kötü davranış tespitinin yapılıp kötü niyetli araçların sistemden çıkarılması için bir zorluk teşkil eder. Buna ek olarak, RSU yol ünitelerinin aktif kullanımı nedeniyle altyapı maliyeti yüksektir.

3.3. V2X Güvenliği ve Blokzincir

Sağladığı güvenlik, mahremiyet ve bütünlük sayesinde blokzincir teknolojisinin V2X sistemlerine uyarlandığı görülmektedir. Kullanıcıların mahremiyetini korumak ve araç ekosisteminin güvenliğini artırmak için kullanılan blokzincirin dağıtık yapısı sayesinde, merkezi kontrol ihtiyacı ortadan kaldırılmaktadır.

Blokzincir, birbirine kriptografik fonksiyonlar ile bağlı bloklardan oluşan şeffaf, değiştirilemez ve dağıtık bir veri yapısıdır. Bu sistem ilk olarak 2008'de Satoshi Nakamoto'nun Bitcoin dijital parasını tanıttığı makalede görülmüştür [45]. Başta yalnızca dijital para sistemlerinde kullanılan bu yapı kısa sürede farklı alanlarda kullanılmaya başlamıştır.

Blokzincir teknolojisinde bloklar içinde veriler tutulur, bu bloklar zincire eklenmeden önce şifrelenir ve bir mutabakat mekanizması ile ağdaki düğümler tarafından onaylanır. Blokzincir yapısında özetleme algoritmaları, asimetrik anahtar şifreleme ve zaman damgası bulunmaktadır. Blokzincir blokları, her bloğun bir önceki bloğun HASH değerini barındırması sayesinde değiştirilemezdir. Ağda yapılan işlemlerin hepsinin takip edilebilir olması ve işlem kayıtlarının kopyasının her düğümde bulunması ile güvenilirdir [46]. Böylece, Merkezi bir yapıya ihtiyaç duyulmamaktadır. Şekil 3.6'da Bitcoin blok yapısı gösterilmiştir.



Şekil 3.6. Bitcoin blok yapısı [45]

Blokzincir işlem süresinin uzunluğu nedeniyle, iletişim hızının kritik olduğu V2X iletişiminde blokzincirin kullanılabilmesi için ek düzenlemeler yapılması gerekmektedir. Geleneksel blokzincirdeki işlem süresinin kısaltılabilmesi için birçok V2X güvenliği çalışmasında çeşitli blokzincir platformlarının örnek alındığı ve yeni mutabakat mekanizmalarının tasarlandığı görülmektedir. Ayrıca çoğu çalışmada sistem verimliliğini artırmak için V2X sisteminin lokasyona bağlı olarak kümelere bölündüğü ve küme bazlı blok oluşturma yapısının kullanıldığı görülmektedir.

Dorri vd., yaptıkları çalışmada geleneksel güvenlik ve mahremiyet yöntemlerinin eksikliklerinden bahsetmiştir. Bu eksikliklerin üstesinden gelmek ve merkezi yapıdan kurtulmak için blokzincir tabanlı bir V2X güvenlik sistemi önerilmiştir. Önerilen güvenlik sisteminde V2X kümelere ayrılır. Her kümede bulunan zincir sorumlusu tarafından mesaj blokları yaratılır. Araç bulunduğu kümeye ait lokasyondan çıkarsa, yeni kümenin zincir sorumlusu aracın mesaj bloklarını yaratır. Ortak anahtar kullanımı ile mahremiyet sağlanırken her işlem sonrası ortak anahtarın değiştirilmesi ile anonimlik korunur. Özel veriler araçların yerleşik hafızasında saklanır ve yalnızca kullanıcı paylaşmak istediğinde paylaşılır. Geleneksel blokzincir yerine kullanılan Lightweight Scalable Blockchain (LSB) ile işlem hızı artırılır [6].

Küresel bir blokzincir kullanmak yerine ülke geneli ile sınırlı bir blokzincir kullanımıyla ölçeklenebilirliğin artırıldığı başka bir çalışmada iletişimde kullanılan mesajlar işaret mesajı ve güvenlik mesajı olmak üzere ikiye ayrılarak sadece güvenlik mesajlarının blokzincire eklenmesi sağlanmıştır. Geleneksel blokzincir mutabakat mekanizmaları yerine Proof of Location (PoL) olarak isimlendirilen bir metot kullanılmıştır. İletişim sırasında kullanılan konum sertifikası, RSU ve araç arasında yapılan bir el sıkışma sonucu verilmektedir. El sıkışma sırasında ilk olarak araç, açık anahtarı ile RSU'ya sertifika isteği gönderir. RSU araca bir oturum kimliği gönderdikten sonra bu araç oturum kimliğinin imzalı halini RSU'ya tekrar gönderir. RSU imzayı doğruladıktan sonra lokasyon sertifikasını araca teslim eder [47].

Kümeleme kullanılarak yapılan blokzincir tabanlı bir diğer çalışmada NDN (Name Data Networking) adı verilen IP adresi yerine içeriğin keşfedildiği ve sorgulayan kişiye teslim edildiği lokasyon adresinin kullanıldığı bir yapı önerilir. NDN, kimlik tabanlı içerikler

yerine adlandırılmış içeriği kullanarak ve paket düzeyinde çalışarak güvenlik ve gizlilik sağlar [7].

Yeni bir mutabakat mekanizması sunan başka bir çalışmada Proof of Driving (PoD) adında bir uzlaşma metodu kullanılmıştır. Sistemin ödül tabanlı olduğu ve Vehicular Cloud Computing (VCC) kullanıldığı belirtilmiştir [48].

Bahsedilen IEEE 802.11p tabanlı sistemlerin haricinde, hücresel tabanlı 3GPP V2X sistemler için tasarlanmış bir öneri Leon ve Mathar tarafından sunulmuştur. Bu sistemde kullanılan blokzincirde akıllı sözleşme kullanımı ve halka imza kullanımı önerilmektedir. Tüm bu farklılıklar ve Plooting adını verdikleri kümeleme sistemi sayesinde güvenli ve hızlı bir yöntem ortaya konulmuştur [49].

İncelenen çalışmalarda görüldüğü üzere blokzincir tabanlı V2X sistemlerinde güvenliği artırabilmek için mutabakat mekanizmaları ve imza yöntemleri üzerinde çalışılmıştır. İşlem hızının artırılmasını sağlayacak yöntemlerin bulunmasıyla blokzincirin V2X sistemlerinde kullanımının zaman içinde yaygınlaşması beklenmektedir.

4. V2X SERTİFİKA İPTAL KONTROL MEKANİZMALARI

AAA kullanılan V2X güvenlik yapılarında kullanılan çeşitli sertifika iptal kontrol mekanizmaları bulunmaktadır. Bu bölümde ilk olarak farklı AAA sistemleri için tasarlanmış mevcutta kullanılan iptal kontrol mekanizmaları anlatılacaktır. Ardından AAA kullanılan V2X iletişimi için tasarlanmış sertifika iptal kontrol yaklaşımları açıklanacaktır.

4.1. Sertifika İptal Durumu Kontrol Metotları

AAA kullanan sistemlerde, sertifika iptal durum kontrolünün yapılabilmesi için farklı yaklaşımlar geliştirilmiştir. İstemcilerin sorgusu ile iptal durum bilgisinin elde edilmesi en sık kullanılan yöntemdir. Bunun haricinde periyodik aralıklar ile istemcilere iptal durum bilgisinin gönderildiği sistemler bulunmaktadır. Ağ yapısında çeşitli değişiklikler yapılarak sertifika iptal durum sorgusunun istemci tarafından gerçekleştirilmesi gerekliliğini ortadan kaldıran çözümler de sunulmuştur. Ayrıca, sertifika geçerlilik süresinin kısaltılması ile iptal durum kontrol adımını süreçten çıkarmak da önerilen bir diğer yöntemdir.

4.1.1. İstemci sorgusu ile iptal bilgisi kontrolü

İstemci sorgusu ile iptal bilgisi kontrolü yönteminde istemciler yalnızca bir sertifikanın iptal durumunun kontrol edilmesi gerektiğinde ilgili sunuculara sertifika iptal bilgisi isteği göndermektedir.

SİL ve Çevrimiçi Sertifika Durum Protokolü (Online Certificate Status Protocol-OCSP) en çok kullanılan istemci sorgusuna bağlı olarak elde edilen iptal kontrol yöntemleridir. Bu iki metot haricinde web sitesi kimlik doğrulamasında kullanılan Certificate Revocation Trees, Certificate Revocation System ve Revocation Transparency metotları da istemci sorgusu ile elde edilen iptal kontrol metotlarındandır.

SİL, RFC 5280'de tanımlanmış bir liste yapısıdır. Sertifika otoriteleri ya da sertifika otoriteleri tarafından yetkilendirilmiş kuruluşlar verdikleri sertifikalar hakkında iptal durum bilgisini duyurmak için SİL'ler yayınlarlar. Hazırlanan SİL'ler yetkili kuruluş tarafından imzalanmaktadır. İptal durumu kontrol edilecek sertifika SİL listesinde taranır. Sertifika listenin içinde kayıtlı ise sertifikanın iptal olduğu anlaşılır. SİL yönteminin en büyük

problemi ölçeklenebilir olmamasıdır. Sertifika üretim sayısı fazla olan sertifika otoritelerinin SİL listelerinin büyümesi kaçınılmaz bir durumdur. Bu yapıda harcanan işlemci, depolama alanı ve bant genişliği miktarının fazla olması bu yöntemin en büyük problemleri arasındadır [50].

OCSP, birçok masaüstü tarayıcısı tarafından kullanılan sertifika iptal sorgu yöntemidir. OCSP cevaplayıcıları, belirli bir sertifika için yapılan iptal bilgisi isteğine karşı imzalı iptal durum bilgisi gönderen sunuculardır. OCSP ile istemci trafik paternleri sertifika otoritelerine açıktır. Ayrıca, sertifika iptal istekleri geçilen her düğüm tarafından görülebilirdir.

İndirilen OCSP cevapları ve SİL dosyaları erişim süresini ve kullanılabilirliği artırmak için önbellekte tutulur. İptal bilgisi önbellekte bulunmuyorsa ya da iptal bilgisi cevaplarının süresi dolmuş ise tekrar istek yapılır [51, 52]. İptal kontrol isteği ile yapılan kontroller, önbellekte tutulan bilgilerle yapılan kontrole kıyasla büyük miktarda gecikmeye sebep olur.

4.1.2. İptal bilgisinin düzenli aralıklar ile gönderilmesi

İptal bilgilerinin düzenli aralıklar ile istemcilere gönderilmesi iptal bilgisi elde etme yöntemlerinden biridir. Bu yöntem ile tüm varlıklara, belirli periyotlar ile benzer cevaplar gönderildiği için istemcilerin trafik modellerinin gizliliği sağlanmış olur. Fakat gereğinden fazla bant genişliği ve önbellek alanı harcanır. Sadece seçilmiş sertifikaların indirildiği yeni stratejiler ile bant genişliği kullanımı azaltılır. Google'ın kullandığı CRLset ve Mozilla'nın kullandığı OneCRL bu stratejiyi kullanan metotlara örnektir.

Belirli bir öğenin belirli bir küme içinde olup olmadığını test etmek için kullanılan eklemeli bir veri yapısı olan bloom filtresi de bant genişliği kullanımını azaltmak için kullanılan yöntemler arasındadır. CRLite, bloom filtresi kullanılan iptal kontrol mekanizmaları arasındadır.

4.1.3. Diğer kontrol yöntemleri

İptal kontrolü için istemcilerin istek yapmasına gerek kalmadan ağ yapısında değişiklikler yapılarak iptal durumunun kontrol edildiği modeller de oluşturulmuştur. İnternet güvenliği için kullanılan OCSP Stapling ve OCSP Must-Staple bu tür yapılara örnek olarak verilebilir.

Kısa ömürlü sertifika kullanımı iptal kontrolünün neden olduğu bant kullanımı ve gecikmeyi azaltmak için sunulan stratejiler arasındadır. Birkaç gün ya da birkaç saat ömre sahip olan bu sertifikalar için iptal listesi tutulmaz. Fakat sertifikaların kısa aralıklar ile yenilenmesi gerekliliği nedeniyle çok sayıda anahtar çiftinin üretilmesi gerekmektedir.

4.2. V2X Sertifikası iptal kontrol metotları

V2X ağlarındaki iletişim güvenliğinin sağlanabilmesi için mesaj gönderen tarafın kimliğinin doğrulanması etkili bir yöntemdir. İletişim kurulacak aracın yetkili olup olmadığı kimlik doğrulama işlemi sonucunda anlaşılmaktadır. AAA tabanlı kimlik doğrulama şemalarında kimlik doğrulama ve izlenebilirlik sertifika kullanımı ile sağlanırken mesaj bütünlüğü imza ile sağlanır. Anonimlik gerçek kimliğin gizlendiği kısa ömürlü takma isim sertifikalarının kullanımı ile gerçekleştirilir. Kullanılan sertifikanın geçerli olup olmadığı ise iptal durum kontrolü ile öğrenilir. Kötü niyetli araçların ayırt edilerek izlenebilirliğin sağlanması sertifika iptal kontrol mekanizması ile sağlanmaktadır. Araçların anonimliği korunurken aynı zamanda kötü niyetli araçların takip ve tespit gerekliliği nedeniyle araçlar için verimli bir sertifika iptal durum kontrol mekanizması oluşturmak zorlu bir iştir. Ağın dinamik yapıda olması da işleyişi zorlu bir hale getirmektedir [53].

İptal durum kontrol sistemleri tasarlanırken optimum şekilde hangi aralıklar ile hangi aşamaların ardından iptal kontrolünün yapılacağı belirlenmelidir. Erken dönem tasarlanan sitemlerde iptal kontrolünün seyrek aralıklar ile yapıldığı görülmektedir. Fakat iptal kontrolünün alınan her yeni mesaj için tekrarlanmasının güvenlik açısından gerekliliği açıktır. Aşağıda iki farklı iptal durum kontrol yaklaşımı için örnekler verilmiştir.

4.2.1. Anahtar yenilendikçe iptal durum kontrolü

Sertifika otoritesi tarafından araçların gizli anahtarlarının değiştirilmesinden önce iptal kontrolünün yapılmasını öneren sistemler tasarlanmıştır. Güvenli ve anonim yayın yapabilmek için yeni bir protokol öneren bir sistemde ağ içindeki varlıklar anonim cihaz ve güvenilir cihaz olmak üzere ikiye ayrılmıştır. Bu yapıda özel araçlar anonim cihaz olarak adlandırılırken yol üniteleri, polis, ambulans gibi araçlar güvenilir cihaz olarak isimlendirilmektedir. Anonim cihazlar, otoriteler tarafından verilen simetrik ağ yetkilendirme anahtarları ile güvenli yayın yapabilmektedirler. Gizli anahtarlar, bu otoriteler

tarafında belirli periyotlar ile değiştirilmekte ve değişim öncesi iptal kontrolleri yapılmaktadır. Güvenilir cihazlar ise asimetrik anahtarlama kullanmaktadırlar ve iptal kontrolleri SİL ile sağlanmaktadır [54].

TACKs adı verilen başka bir sistemde iptal kontrolü araçların kısa ömürlü takma isim sertifikaları değiştirildiğinde kayıt otoriteleri tarafından yapılmaktadır. Bu sistemde grup imzalama kullanılarak izlenebilirlik sağlanmaktadır [55].

Yine AAA ve grup imzalamanın kullanıldığı bir sistemde araçlar her yeni girdikleri RSU alanında yeni grup imzalama sertifikası almaktadırlar ve RSU'lar SİL üzerinden araçların iptal kontrollerini yapmaktadır [56]. Ancak, bu çözümler ağır bir iş yüküne sahiptir [57]. Yukarıdaki şemalarda kullanılan iptal mekanizmalarında iptal kontrolü sadece sertifika yenilendiği zaman yapıldığı için güvenlik ihlali yapmış araç, geçersiz hale gelene kadar eski sertifika veya anahtarlarını diğer araçlarla iletişim kurmak için kullanmaya devam edebilmektedir [10]. Bu durum ciddi güvenlik ihlallerine neden olmaktadır.

4.2.2. Mesaj iletimi sonrası iptal kontrolü

Mesaj iletimi sonrası yapılan iptal kontrolü IEEE tarafından benimsenen sertifika iptal kontrol yöntemidir [9]. Bu yapıda ağ içinde alınan her mesaj sonrası alıcı araç gönderici aracın sertifikasının iptal kontrolünü yapar.

İptal kontrolünün SİL ile yapıldığı sistemlerdeki temel yaklaşım sertifika otoritelerinin kendine bağlı iptal edilmesi gereken süresi dolmamış araç sertifikalarının listesini belirli periyotlarda yayınlaması üzerine kurulmuştur [58]. Araçlar gelen her mesaj için internet üzerinden iptal listelerine ulaşıp sertifikalarının iptal kontrolünü sağlamaktadır. Yayınlanan iptal listeleri üzerinde iptal listesinin geçerlilik süresini belirleyen alanlar bulunmaktadır. Araçlar bu listeleri geçerlilik süreleri dolana kadar iptal kontrolü için kullanabilmektedirler. Bu süre dolduğunda bu listeler yenilenmek üzere tekrar indirilmektedir.

IEEE 802.11p tabanlı V2V ve V2I iletişimi için iletim mesafesi 1000m'ye kadar ulaşabilmektedir. Yarıçapı 200 m olan bir iletim ağında bile, 20 m'lik dört şeritli bir yolda herhangi bir noktada menzile giren araç sayısı 80'dir [59] . Böyle bir yapıda yüksek sayıda sertifika iptal durum kontrol isteği alan ağ varlıkları üzerinde kuyruk oluşup gecikme

problemi yaşanabilme olasılığı yüksektir. Bu durum, gecikmeye duyarlı V2X gibi iletişim modelleri için kabul edilemezdir. Bu iptal denetimi yaklaşımı ölçeklenebilirlik açısından zayıftır ve gecikme sorunlarına neden olmaktadır.

İptal kontrolü sırasında oluşabilecek gecikmenin önlenebilmesi için çeşitli teknikler kullanılmaktadır. Bloom filtresi ve Merkle Hash Tree kullanılarak veri yapısında yapılan iyileştirmeler ile bu probleme çözüm getirilmeye çalışılmıştır. Ayrıca, dinamik karma algoritmasına dayanan iptal kontrol mekanizmaları da tasarlanmıştır. Merkle Hash Tree kullanan bir sistemde, araçların iptal kontrol isteklerini bağlı oldukları RSU'lar üzerinden yapması tasarlanmıştır [60].

Delta CRL, SİL içindeki iptal edilmiş sertifika sayısını azaltarak ölçeklenebilirliği artırmayı amaçlayan bir iptal durum kontrol mekanizmasıdır. Bu yapıda yalnızca güncellenen bilgiler yayınlanmaktadır. Bunun haricinde sertifikanın ömrünü kısaltmak ve SİL yönetimini daha dağıtık hale getirerek ölçeklenebilirliği artırmayı amaçlayan metotlar da geliştirilmiştir.

Ölçeklenebilirlik sorununu çözmek için merkezi olmayan grup kimlik doğrulaması protokolünü geliştiren bir diğer çalışmada her RSU'nun kapsama alanı bir grubu belirtmektedir. Her RSU iletişim aralığındaki araçları yönetmektedir. Merkeziyetçi olmayan bu şemada, grup yönetim görevinin ağdaki RSU'lar tarafından üstlenilmesi sağlanarak sistemin ölçeklenebilirliği artırılmıştır [61].

SİL'in RSU tarafından yayınlandığı dağıtım mekanizmaları, RSU'nun seyrek olduğu veya RSU'nun bulunmadığı bölgelerde kullanılabilirliğini kaybetmektedir. Bu durum göz önünde bulundurularak RSU dışında araçtan araca da iptal durum bildirimlerinin yapıldığı tasarımlara ihtiyaç vardır.

4.2.3. SCMS iptal kontrol metodu

SCMS, ilk olarak Whyte tarafından 2013 yılında önerilen daha sonra Camp tarafından 2016 yılında geliştirilen, sisteme dahil olmayan araçların sistem varlıklarını izlemesini engelleyen bir iptal kontrol mekanizması sistemidir [62]. SCMS, sunduğu sertifika bağlantı yapısı ve iptal kontrol mekanizması ile ABD'de kullanılmaya adaydır [63]. SCMS mimarisinin temel özellikleri, yanlış davranış tespiti ve raporlamadır. SCMS ile ihlal yapan araçlar ağdan

silinirken bir yandan da araç gizliliği korunmaya devam eder. Bu V2X yapısında araçlar anlık olarak veri paylaşıp analiz ederler. Fakat bu bilgiler sadece kaynak güvenilir ise kullanılır [4].

SCMS, birlikte çalışabilirliği sağlamada kritik bir öneme sahiptir. SCMS ile farklı araç markaları ve modelleri, önceden var olan anlaşmalarını veya araç tasarımlarını değiştirmeden birbirleriyle konuşabilir ve güvenilir veri alışverişi yapabilir [64].

SCMS yapısı içinde OBU ve RSU'ların kullandığı çeşitli sertifikalar bulunmaktadır. Araçlar, sertifika otoritelerinden güvenlik sertifikaları alarak SCMS'ye kaydolurlar. SCMS yapısında uzun ömre sahip kayıt sertifikası ve kısa ömre sahip takma isim sertifikaları bulunmaktadır. Takma isim sertifikaları mesaj imzalamak için kullanılmaktadır. Bu sertifikalar sayesinde aracın ağ içinde güvenilir bir varlık olduğu anlaşılmaktadır. Araçlar sertifikalarını kullanarak güvenilir ve gizli olarak bilgi paylaşımı yapabilirler. Araçların takma isim sertifikalarının belirlenen kısa periyotlarda değiştirilmesi beklenmektedir. Bu yöntem ile araçların gizliliği korunmakta ve kötü niyetli taraflarca araç takibi önlenmektedir.

SCMS yapısında takma isim sertifikalarının araçlara verimli ve toplu şekilde dağıtılması sağlanmaktadır. Sertifikalar gerektiğinde iptal edilmektedir. CAMP-VSC, yanlış davranış olarak adlandırdıkları ağ içinde yanlışlıkla veya kasıtlı olarak yanlış veri iletim durumlarının tespit edilmesini sağlayan metotlar geliştirmişlerdir [4]. OBU bir yanlış davranış ile karşılaştığında ürettiği raporları SCMS'ye göndermektedir. Araçlardaki OBU'lar, SCMS ve yanlış davranış otoritesi birlikte çalışarak yanlış davranışların tespitini yapmaktadır.

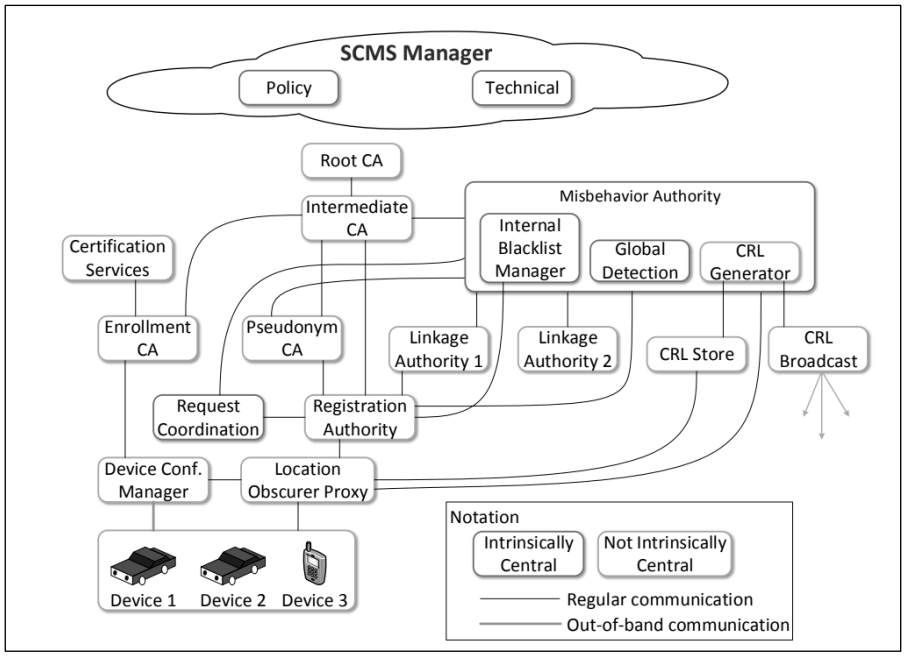
SCMS yapısında, bir araç ile ilgili yeterli sayıda hatalı davranış raporu alınırsa, cihazın sertifikaları SİL'e eklenir ve güncellenen SİL ortamdaki diğer araçlara dağıtılır. SİL'de kayıtlı araçlardan gelen mesajlar güvenilir bir kaynak olarak kabul edilmemektedir.

SCMC hiyerarşisi Şekil 4.1'de gösterilmiştir. SCMS içindeki sertifika otoriteleri sertifika üretmek, dağıtmaktan ve iptalinden sorumludur. Bu yapıda kullanılan diğer temel varlıklar aşağıda tanımlanmıştır.

- **Linkage Authority (LA):** Sertifikaların içinde kullanılan bağlantı değerlerini üretir.

Bir operatörün aynı araç sertifikalarını bağlamasını önlemek için LA1, LA2 olmak üzere en az iki tane LA olmalıdır.

- **Pseudonym Certificate Authority (PCA):** Takma isim sertifikaları dağıtan otoritelerdir. Her bölge, üretici ve cihaz tipi için ayrı PCA olabilir.
- **Registration Authority (RA):** PCA'ya yapılan takma isim sertifika isteklerini doğrulayan, işleyen otoritedir.
- **Request Coordination (RC):** Belirlenen periyotta aracın tek bir grup takma isim sertifikası aldığını kontrol eden sistem varlığıdır.
- **Misbehavior Authority (MA):** Yanlış davranış raporlarını kontrol ederek olası suistimallerin önüne geçilmesini sağlayan otoritedir. Gerekli durumlarda sertifikaları iptal ederek SİL dosyasına ekler ve takma isim sertifikalarının bağlı olduğu kayıt sertifikasını kara listeye (blacklist) ekler. Bu otorite üç ana bileşenden oluşmaktadır. Internal Blacklist Manager (IBLM), kara listeyi güncellemek için RA'ya gerekli bilgileri gönderir. Global Detection (GD), yanlış davranış yapan araçları tespit eder. Certificate Revocation List Generator (CRLG), SİL listelerini hazırlayan, imzalayan ve yayınlayan sistem varlığıdır.
- **Location Obscure Proxy (LOP):** İstek gönderen aracın konumunu gizler. Kaynak adresinin değiştirilmesi sağlanarak kötü niyetli tarafların ağ adresi üzerinden konum bilgisini alması önlenir. MA'ya giden yanlış davranış raporlarını gönderenlerin adresinin de saklanması bu şekilde sağlanır.



Şekil 4.1. SCMS hiyerarşisi [62]

Araçlar, butterfly key expansion ve key linkage olmak üzere iki temel prosedür ile SCMS yapısına katılabilirler [63].

Butterfly Key Expansion, bir aracın farklı imzalama ve şifreleme anahtarlarına sahip sertifika serileri istemesini sağlayan kriptografik yapıdır. Araçlar şifreleme ve imzalama için birer adet anahtar çifti üretirler. Ortak anahtar ve iki adet genişletme fonksiyonunu sertifika istek dosyalarına ekleyip gönderirler.

AAA uygulamasının temel prensibi sertifika sahibi tarafından her sertifika için ayrı anahtar çiftinin üretilmesidir. Bir aracın bir yılda 10,000'den fazla sertifikası olmaktadır. Bu durumda ortalama 52 dakikada bir sertifika değiştirilmektedir [65]. Bu kadar sertifika isteğinin tek tek yapılması yüksek bir hesaplama yükü getirmektedir. Butterfly key expansion ile tek bir ortak anahtardan bir seri sertifika üretilebilmektedir. Bu sayede her sertifika için ayrı ortak anahtar üretilmesi gerekliliği ortadan kalkmaktadır ve istek boyutu düşmektedir. Ayrıca, anahtar üretilirken geçen zaman azaltılarak sertifika isteği yapan tarafın iş yükünün azaltılması sağlanmaktadır.

Key Linkage, büyük boyutlu SİL dosyalarının oluşmasını engellemektedir. SCMS, birden fazla sertifikanın birbiri ile ilişkilendirilmesine izin vermektedir. Bu yapıda araçların farklı iki LA'dan talep ettiği bağlantı değerleri RA'ya gönderilir. RA, sertifikanın içine bu değerleri yükler. Sertifikalar arasındaki ilişkilendirme, takma isim sertifikalarının meta datasına bu bağlantı değerlerinin eklenmesi ile sağlanmaktadır. Bir takma isim sertifikasının yanlış davranışının yakalandığı durumda bu sertifika ile ilişkili tüm diğer sertifikalar da iptal edilebilmektedir. Bu sayede, SİL dosyasına tüm takma isim sertifikalarının yüklenmesine gerek kalmamakta ve SİL'in lineer şekilde büyümesi sağlanmaktadır. SİL'e giriş yapılma miktarı ve SİL için harcanan bant genişliği bu şekilde azaltılmaktadır.

4.3. V2X SİL Dağıtım Yöntemleri

ABD ve Avrupa'daki standardizasyonlar, birbirinden bağımsız olarak güvenlik yapılarını AAA sistemi üzerine kurmuşlardır ve iptal kontrolü için SİL yapısını seçmişlerdir [66]. AAA tabanlı V2X iletişiminde sertifika iptal kontrolü için temel yaklaşım SİL kullanımı olsa da bu yapı V2X isterlerini tam olarak karşılayamamaktadır.

V2X iletişiminde, düğümlerin hareket halinde olduğu, sistem varlıklarının değiştiği dinamik yapıya uygun iptal bilgisi dağıtım mekanizmalarının tasarlanması gerekmekte ve ağ içinde iptal kontrolünün neden olduğu zaman kaybı azaltılmalıdır [10]. AAA kullanan V2X güvenlik yapılarında SİL dosyalarının boyutunun yüksek olmasından dolayı bu alanda yapılan akademik araştırmalar SİL'in kısa sürede, verimli şekilde dağıtılması ve SİL boyutunun azaltılması üzerine yoğunlaşmıştır.

Akış protokollerinin SİL dağıtımında kullanılması, SİL boyutunun azaltılması için uygulanan yöntemler arasındadır. SİL dağıtımında kullanılan akış protokollerinin karşılaştırıldığı bir çalışmada Neighbor Knowledge Broadcast'in incelenen yöntemler arasında en verimli protokol olduğu sonucuna varılmıştır. Yapılan karşılaştırmada dağıtım süresi ve düğüm başına yapılan yayın sayısı performans metriği olarak alınmıştır [67].

SİL dosyalarının verimli şekilde dağıtılması için SİL dosyasının boyutunu azaltmayı amaçlayan bölgesel sertifika iptal listelerinin kullanımını öneren çalışmalar bulunmaktadır [68]. Ayrıca, SİL dağıtımının sadece merkezi yapıya ve RSU'lara bağlı kalmaksızın araçlar arasında dağıtımını sağlayan dağıtık sistemler önerilmiştir. C2C Epidemic, merkezi otoritenin RSU'lar üzerinden belirli periyotlarda toplu şekilde araçlara SİL dağıttığı; araçların da SİL dağıtımına katıldığı bir sistemdir. Bu yapı sayesinde daha az RSU kullanarak daha kısa sürede tüm araçlara SİL'in ulaşması sağlanmıştır [16, 17]. SCRLE'de ise C2C Epidemic yapısında olan rastgele olan araçlar arası SİL dağıtımı daha sistematik hale getirilmiştir [18].

AAA tabanlı V2X güvenlik sistemlerinde blokzincir kullanan dağıtık sistemler de önerilmiştir. Bu sistemlerde AAA tabanlı V2X yapısına blokzincir entegre edilerek SİL kullanılmayan bir yapı oluşturulmuştur [69, 70].

5. V2X GÜVENLİK SİSTEMİ İÇİN GÜVEN ZİNCİRİNE DAYALI SERTİFİKA YÖNETİM SİSTEMİ

Literatür taraması sonrası yapılan analizler sonucunda açık anahtar altyapısı kullanan bir V2X güvenlik sistemi tasarlanmasına karar verilmiştir. Önerilen sistemde araç gizliliğini sağlamak için takma isim sertifikası kullanılmaktadır. Sertifika iptal kontrolü için ise güven zincirine dayalı yeni bir sertifika iptal kontrol sistemi tasarlanmıştır. Bu sistem ile SİL sunucularına yapılan SİL isteği sayısının azaltılması sağlanarak merkezi sistem üzerindeki yükün hafifletilmesi hedeflenmiştir.

Bu bölümde ilk olarak kullanılması planlanan sertifika, anahtar ve imza yapısı açıklanacaktır. Ardından tasarlanan sertifika iptal listesi yapısı özetlenecektir. Son olarak, Sertifika iptal listesine ek olarak tasarlanmış güven zincirine dayalı sertifika iptal kontrolü mekanizması tasarımı ve oluşturulan algoritma detaylı şekilde açıklanacaktır.

5.1. Sertifika, Anahtar ve İmza Yapısı

Önerilen yapıda araç gizliliğini sağlamak amacıyla Bölüm 3.1.1'de açıklanan takma isim sertifika yapısının kullanılması planlanmaktadır. Yıllık araç muayenesi sonrası araç için takma isim sertifikaları bir yılı kapsayacak şekilde toplu şekilde verilecektir. Sertifikaların ömürlerinin 1 hafta olması tasarlanmıştır.

Bölüm 4.2.3'te açıklanan SCMS sisteminde kullanılan butterfly key expansion ile tek bir ortak anahtardan bir seri sertifika üretilerek her sertifika için ayrı ortak anahtar üretilmesine gerek kalmamakta ve sertifika istek dosyası boyutu düşmektedir. Toplu sertifika talebinde bu yapının kullanılması en uygun çözüm olarak görülmüştür.

Toplu şekilde alınan sertifikaların bağlı olduğu özel anahtarlar araç OBU'ları içinde saklanır ve araç dışına çıkarılmaz. Anahtar güvenliliğinin sağlanabilmesi için TPD (Tamper Proof Device) gibi donanımların OBU ile entegrasyonu güvenlik açısından önem taşımaktadır.

İmza ve sertifikaların kapladığı alanın azaltılabilmesi için JSON (JavaScript Object Notation) yapısının kullanıldığı JAdES imza yapısının kullanılması planlanmıştır. JSON, XML'e alternatif olarak düşünülmüş JavaScript tabanlı bir veri iletim formatıdır. Genellikle

web servis uygulamalarında kullanılmaktadır. JSON imza JWS (JSON Wen Signature) formatını kullanmaktadır. JWS, başlık, yük ve imza alanlarından oluşmaktadır. Bu imza tipi ETSI TS 119 182 altında standartlaştırılıp JAdES adını almıştır [71].

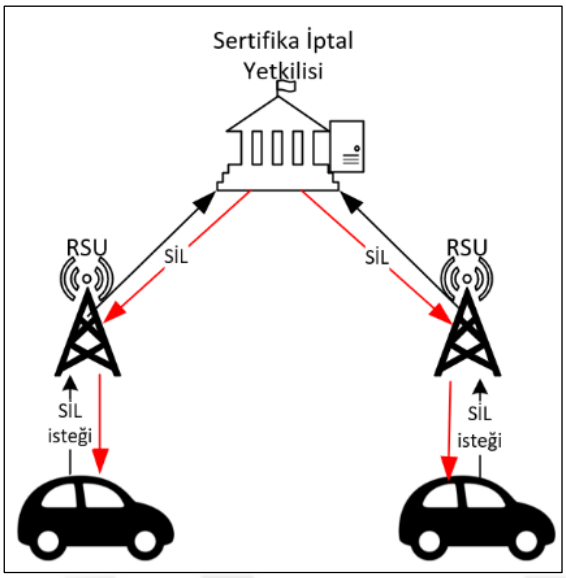
5.2. Sertifika İptal Listesi

SİL'ler, süresi dolmamış iptal edilen sertifikaların seri numaralarını, iptal edilme tarihlerini ve opsiyonel olarak iptal nedenlerini içerir. Her SİL içerisinde, SİL'in hangi yetkili tarafından yayınlandığını, SİL'in geçerlilik başlangıç ve bitiş tarihini gösteren alanlar bulunmaktadır. Yayınlanan her SİL'in "CRL Number" adı verilen numarası vardır. SİL'ler belirlenen periyotlarda yetkili otoriteler tarafından imzalı olarak yayınlanmaktadır [52].

Yayınlanan en güncel SİL'in araçlar tarafından kullanılması optimum senaryodur. Fakat böyle bir durumda araçların, yetkilendirilmiş kuruluşun sunucusundan indirdikleri SİL sayısı arttığı için trafik oluşmakta ve sunucu üzerinde yük artmaktadır. Bu sebeple, araçların kullandıkları SİL'lerin süresinin geçmediğinden emin olmaları beklenir.

Bölüm 4.2.2'de açıklanan mesaj iletimi sonrası iptal kontrolü yapısı kullanılarak istemci tarafından SİL isteği yapılması ardından sunucudan SİL dosyası indirilmesi ile iptal kontrolü yapılması planlanmaktadır. Ayrıca, Bölüm 4.2.3'te açıklanan SCMS sisteminde kullanılan key linkage yapısının SİL dosya boyutunu azaltmak için kullanılması tasarlanmaktadır.

Yapı içinde soruna neden olan veya başka bir nedenden dolayı ağdan çıkarılması gereken araç sertifikalarının iptalinden sorumlu kuruluş Sertifika İptal Yetkilisidir. Bu kuruluş sertifika iptal listelerini düzenli aralıklarla güncellemekten sorumludur (Şekil 5.1).



Şekil 5.1. Sertifika İptal Yetkilisi SİL Dağıtımı

5.3. Güven Zincirine Dayalı Sertifika İptal Kontrolü Tasarımı

İletişim sırasında mesaj alan taraf, mesaj sahibinin sertifikasının iptal kontrolünü yapmak zorundadır. Bu kontrolü yapmak için merkez üzerinden sertifika iptal sorguları yapılmaktadır. Bu çalışmada merkezi SİL sunucusunun üzerindeki yükü azaltan yarı dağıtık bir yapı önerilmiştir. SİL'in öncelikli kaynak olarak alındığı bu sistemde her aracın aynı zamanda güvenilir olduğunu bildiği araçların listelendiği güven listeleri mevcuttur. Güven listesindeki bilgilerin güvenilirliği zaman ve edinilme yoluna bağlı olarak değerlendirilmekte ve liste dinamik olarak güvenilir araçlar vasıtasıyla güncellenmektedir. Araçların mevcutta kullanılabilir bir SİL'i olmadığında, sertifika iptal kontrolü için güven listesinin kullanılması sağlanarak merkezi sunucuya yapılan SİL isteklerinin azaltılması hedeflenmektedir [72].

Güven zinciri yapısında, merkez üzerindeki yükü azaltmak için SİL isteği sadece belirlenen özel durumlarda yapılmaktadır. Her aracın sahip olduğu güven listesi ise güvenilen ve iptal olmadığı bilinen sertifikaların bulunduğu, beyaz liste (whitelist) benzeri listelerdir. Bir aracın güven listesine bir sertifikayı ekleyebilmesi için o sertifikanın direkt indirilmiş SİL üzerinden kontrolünün yapılması ya da güven listesi içinde bulunan bir aracın o sertifikanın kendi güven listesinde bulunduğunu bildirmiş olması gereklidir.

Güven Listesi, önerilen güven zinciri sisteminde kullanılan liste yapısıdır. Sistemdeki her aracın güven listesi bulunmaktadır. Aracın geçerli bir SİL'i olmadığı durumlarda iptal

kontrolü güven listesi üzerinden yapılmaktadır. Güven listesi aracın daha önce iletişim kurduğu ve güvenilir olduğunu bildiği araçları gösteren bir listedir. Araç bu listede bulunan araçlardan gelen mesajları güvenilir saymaktadır. Güven listesi güvenilen araçların takma isim sertifikalarının seri numaralarını içerir. Ayrıca, güvenli sayılan aracın güven değerinin hesaplanması için kullanılan atlama sayısı, cevap yaşı değerlerini bulundurur. Hesaplanan güven değeri kullanılarak güven listesindeki bilgiler güncellenir. Güven listesinin içindeki bilgilerin değiştirilmediğinden emin olmak için liste imzalı şekilde tutulur. Bu şekilde üçüncü taraflarca bozulan listelerin imzası da bozulur.

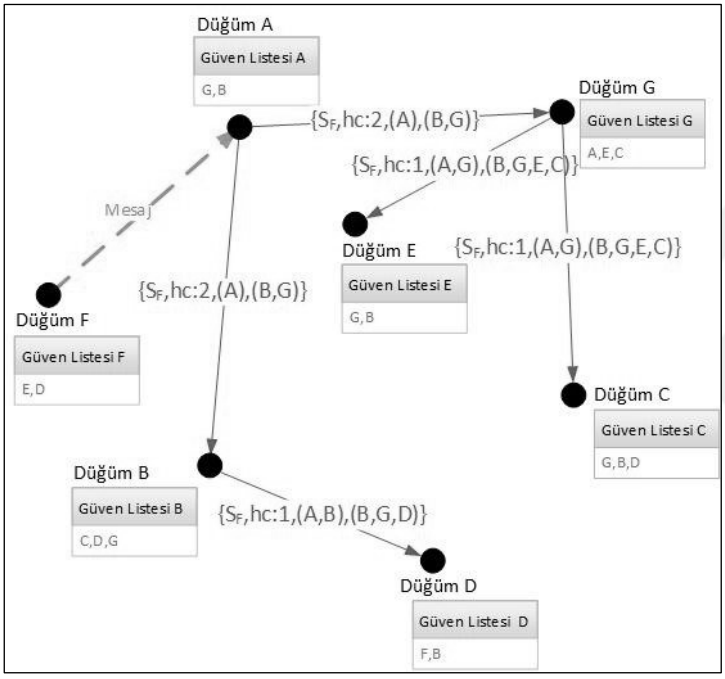
Güven listesini besleyen iki kaynak bulunmaktadır. İlk kaynak SİL'dir. SİL kontrolü yapılıp iptal olmadığı anlaşılan araç bilgisi, başarılı bir iletişim kurulduktan sonra güven listesine eklenir. İkinci kaynak ise güven zinciri üzerinden elde edilen bilgilerdir. Bir araca başka bir araçtan mesaj geldiğinde, mesajı alan aracın SİL'inin geçerlilik tarihi dolmuşsa güven listesinde gönderici araç ile ilgili bilgi sorgulanır. Güven listesinde gönderici araç bulunuyorsa alınan mesaj güvenilir sayılır. Güven listesinde gönderici araç ile ilgili bilgi bulunmuyorsa güven listesinde bulunan tüm araçlara gönderici aracın güven bilgisi durumu sorulur. Bu sorguyu alan araçlar kendi güven listelerinde sorgulanan aracı tararlar. Sorgulanan araçla ilgili bilgi güven listelerinde bulunuyorsa bu bilgi cevap mesajı olarak geri gönderilir. Güven listelerinde bu bilgilinin olmadığı durumda ise güven listesinde bulunan diğer araçlara sorgu yapılır. Bu zincir, sistemde belirlenen atlama sayısı kadar devam eder ve güven zinciri olarak isimlendirilir.

Güven zinciri sorgularında, atlama sayısı değerleri sınırlı tutularak kontrollü akış (controlled flooding) uygulanır ve bu şekilde ağ içinde yayın fırtınası (broadcast storm) oluşması önlenir. Her atlamadan sonra bu değer bir azaltılır ve atlama sayısı 0'a ulaştığında sorgu yapılamaz. Sorgu yapılan bir araca aynı sorgunun tekrar yapılmasını önlemek için her sorgu mesajına sorgu yapılan araçları içeren kontrol listesi eklenir. Bu yapıda sorgunun ulaştığı araç kendi güven listesinde bulunan ve sorgulama yapacağı düğümleri de ileti içine ekler. Sorgu alan düğüm daha önce hangi düğümlere sorgu yapıldığını bilir ve kendi güven listesinde bulunsa dahi daha önce sorgu yapılmış düğüme tekrar sorgu atmaz. Bu şekilde, hangi düğümlerde kontrol yapıldığı bilgisi tutularak sorgu tekrarı yapılmamış olur.

Güven zinciri sisteminde, sorgu yapılan araçla ilgili bilgi güven listelerinde bulunuyorsa araçlar mesajı aldıkları düğüme cevap mesajı gönderirler. Cevap yapılan bir sorgu için farklı

araçlardan cevap gelmesi durumunda güven değeri en yüksek olan cevap bilgisi güven listesine eklenmektedir.

Şekil 5.2'de güven zinciri yapısının kullanıldığı örnek bir ağ yapısı gösterilmiştir. Örnekte F aracının A aracına mesaj gönderdiği varsayılmaktadır. A aracının F aracından gelen mesajı güvenilir sayması için sertifikanın imza ve geçerlilik tarihi kontrolü sonrası iptal kontrolünü de yapması gereklidir. Bu kontrolü sağlamak için aşağıdaki maddeler sırası ile gerçekleştirilir.



Şekil 5.2. Güven zinciri yapısı iptal bilgisi sorguları

- A aracı ilk olarak mevcutta geçerli bir SİL dosyasına sahip olup olmadığını kontrol eder. SİL dosyası yoksa ya da geçersiz ise güven listesini kontrol eder.
- F aracının sertifikası ile ilgili bir bilgi güven listesinde yoksa listede bulunan güvenilir araçlara sorgu mesajı gönderilerek F aracını tanıyıp tanımadıkları sorgulanır. Sorgu sonucu atlama sayısı bir azaltılır.
- Güvenilir araçlar öncelikle, geçerli bir SİL dosyasına sahip olup olmadıklarını kontrol ederler. SİL yoksa ya da geçersizse güven listelerini kontrol ederler. Listelerinde F aracı varsa A aracına dönüş yaparlar. Listelerinde F aracı ile ilgili bir bilgi yoksa bu araçlar da kendi güven listelerinde bulunan güvenilir araçlara sorgu yaparlar. Sorgu sonucu atlama sayısı değeri bir azaltılır. Atlama sayısı değeri 0 olana kadar sorgu zinciri devam eder.

- Sorgu zincirinde herhangi bir halka, F aracı ile ilgili bilgiye sahipse, bu bilgi zincirin bir üst halkasına cevap mesajı ile gönderilir ve bu zincirdeki her halkanın güven listesine eklenir.
- Güven zincirinde bulunan araçlardan cevap gelmez ise ilk sorguyu yapan A aracı SİL sunucusuna SİL isteği gönderir.

Sorgu mesajı (m_{sorgu}) dört alandan oluşmaktadır. İlk iki alan, hangi araç için sorgu yapıldığı (S_F) ve atlama sayısı (hc) bilgileridir. Sorgunun araca ulaşana kadar geçtiği güven zincirindeki düğümleri içeren *yol* alanı da üçüncü alan olarak mesaja eklenmektedir. Bu alan cevap mesajının hangi düğümler aracılığı ile ilk sorgu yapan araca ulaştırılacağını göstermektedir. Ayrıca, güven zincirinde sorgu yapılan düğümlerin bulunduğu *kontrol* alanı da bulunmaktadır. Bu alan sayesinde bir araca aynı sorgunun birden çok gelmesi engellenmektedir. Eş. 5.1'de sorgu mesajı yapısı gösterilmiştir.

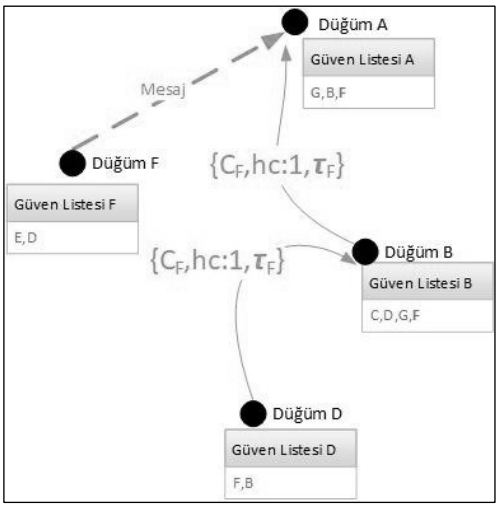
$$m_{sorgu} = \{ S_F , hc, yol, kontrol \} \tag{5.1}$$

Güven zincirindeki araçların güven listelerinde, sorgusu yapılan araç sertifikası ile ilgili bilgi mevcut ise cevap mesajı (m_{cevap}) gönderilir. Cevap mesajı iptal durum bilgisi (C_F), atlama sayısı bitiş (hc_{bit}) değeri ve cevap yaşı (τ_F) bilgilerini içerir. Eş. 5.2'de cevap mesajı yapısı gösterilmiştir.

$$m_{cevap} = \{ C_F , hc_{bit}, \tau_F \} \tag{5.2}$$

Cevap yaşı, aracın geçerli bir SİL üzerinden iptal kontrolünün yapılmasının üzerinden geçen süredir. Bilgi eskidikçe cevabın yaşı artar. SİL üzerinden kontrolün yapıldığı anda bu değer 0'dır. Zaman ilerledikçe cevap yaşı artar. Belirlenen bir eşik değerinden daha eski olan sertifika iptal bilgileri bayat sayılır ve buna göre bilgiler güven listesinden çıkarılır. Bu eşik değeri sistemimizde SİL ömrü (c) kadar belirlenmiştir.

Sorgu mesajında bulunan yol alanındaki düğümler üzerindeki her aracın güven listesine, sorgusu yapılan sertifika iptal bilgisi eklenir (Şekil 5.3).



Şekil 5.3. Güven zinciri iptal bilgisi cevapları

Elde edilen iptal bilgisinin güvenilirliği, güven değeri (G) ile kontrol edilir. Güven listesi içinde bulunan bir sertifikanın iptal bilgisinin hesaplanan güven değerine bakılarak bu bilginin güvenilir olup olmadığı değerlendirilir. Belirlenen eşik değerinin altında olanlar listeden çıkarılır. Güven değeri, 0 ile 1 arasında değişmektedir. Yaş oranı (t) ve dolaşım oranı (d) olmak üzere güven değerini etkileyen iki temel değişken bulunmaktadır. Eş. 5.3'te güven değeri denklemi gösterilmiştir.

$$G = \frac{1-t}{2-d} \qquad \{G \in \mathbb{R} | 0 \leq G \leq 1\} \tag{5.3}$$

Eş. 5.4'te gösterildiği gibi yaş oranı, cevap yaşının SİL ömrüne oranıdır Yaş oranı arttıkça güven değeri düşer.

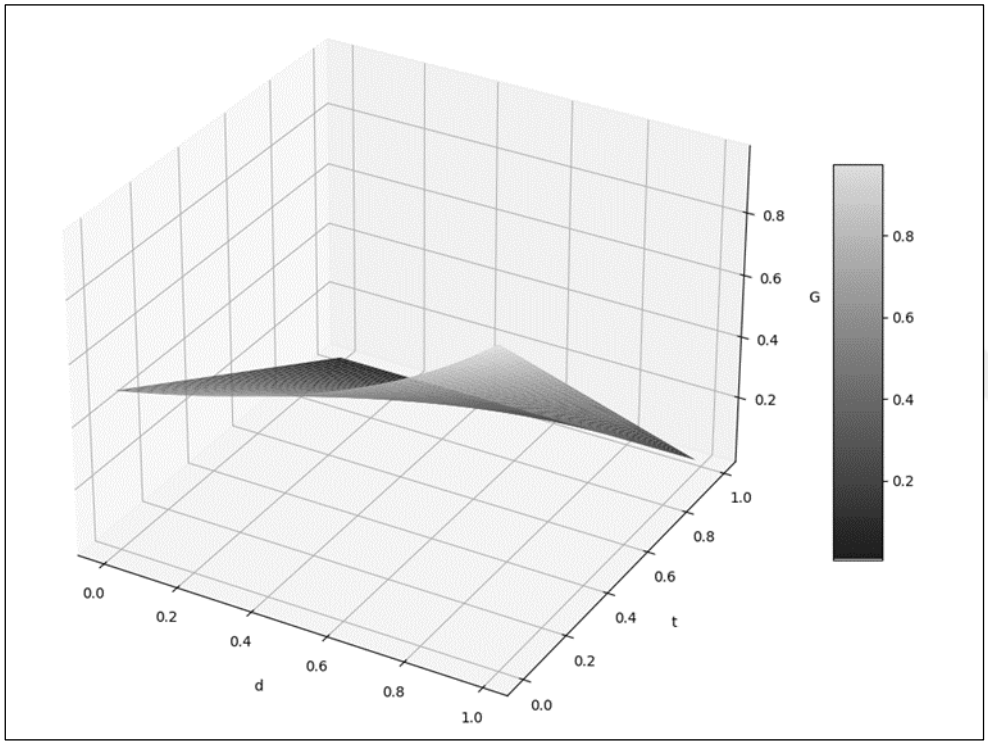
$$t = \frac{\tau}{c} \tag{5.4}$$

Sistemde bir atlama sayısı başlangıç değeri (hc_{bas}) belirlenir. Her düğüm sorgusunda bu değer 1 azaltılarak sonucun bulunduğu düğümde, atlama sayısı bitiş değeri (hc_{bit}) elde edilir. İkinci değişken olan dolaşım oranı, hc_{bit} değerinin hc_{bas} değerine oranıdır. Eş. 5.5'te dolaşım oranı denklemi gösterilmiştir.

$$d = \frac{hc_{bit}}{hc_{bas}} \tag{5.5}$$

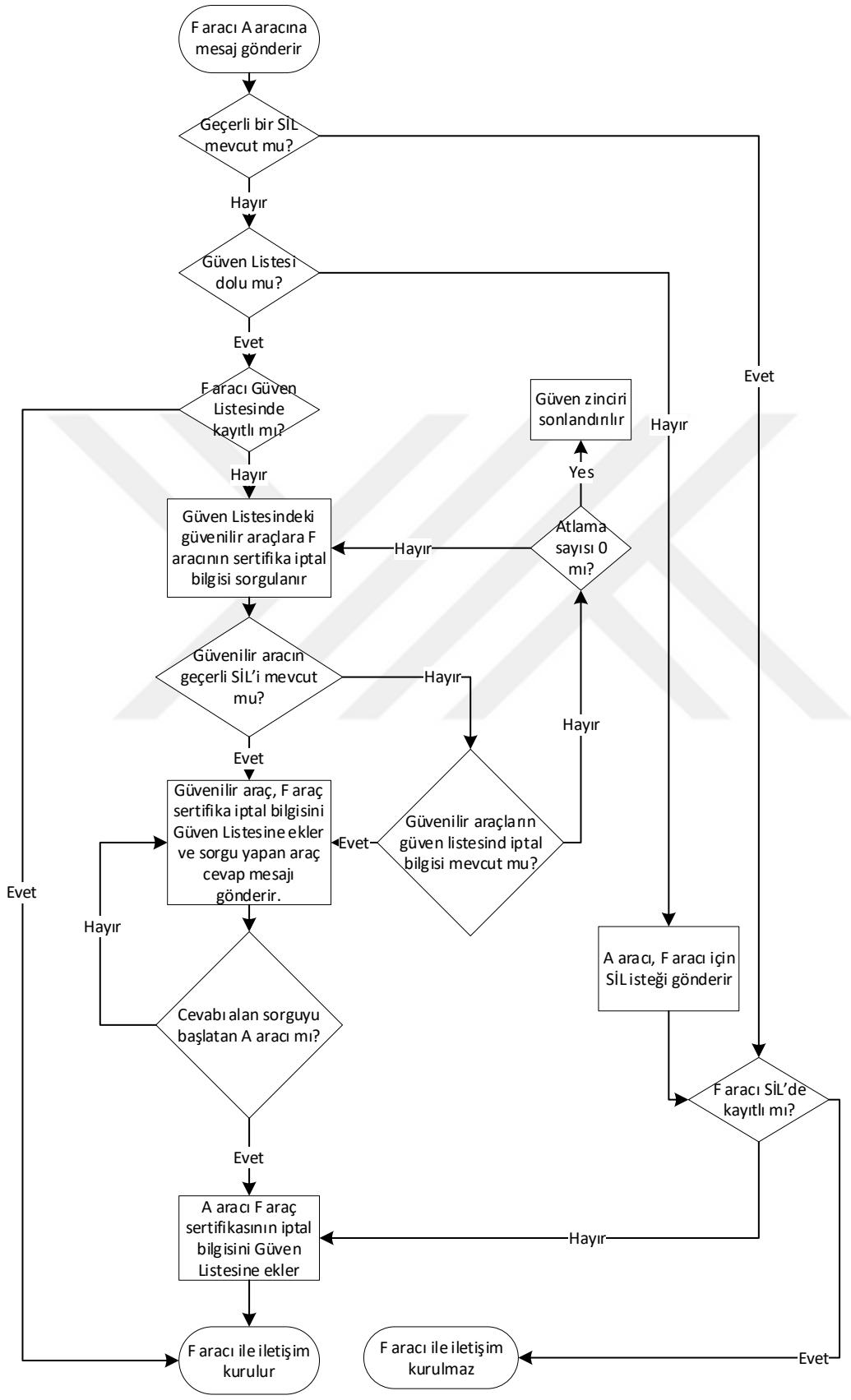
İptal bilgisi birbirine güvenen araçlar arasında dolaylı olarak ne kadar aktarılırsa dolaşım oranı değeri de azalır. Dolaşım oranı değeri yükseldikçe güven değeri artar. SİL ile yapılan iptal sorgularında atlama yapılmaz ve hc_{bas} değeri hc_{bit} değerine eşit olur. Bu durumda dolaşım oranı 1'e eşittir. SİL ile yapılan iptal sorgularında dolaşım oranı 1 ve bilginin ulaştığındaki cevap yaşı 0 olduğu için hesaplanan güven değeri en yüksek değer olan 1'e eşit olur. Bu şekilde elde edilen bilgiler, en güvenilir bilgilerdir.

Şekil 5.4'te güven değeri G'nin dolaşım oranı ve yaş oranına bağlı olarak değişimi gösterilmiştir.



Şekil 5.4. Güven değerinin dolaşım oranı ve yaş oranına bağlı olarak değişimi

Sistemin akış diyagramı Şekil 5.5'te gösterilmiştir.



Şekil 5.5. Güven zinciri yapısı akış diyagramı

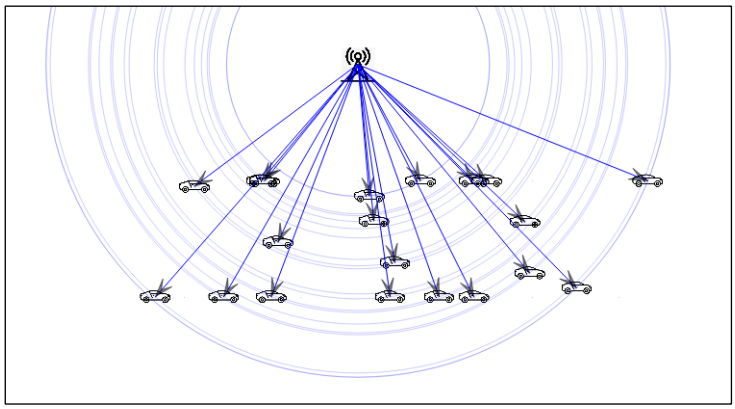
6. BENZETİM ÇALIŞMASI ve DENEYSEL SONUÇLAR

İptal kontrolünün sadece SİL üzerinden yapıldığı geleneksel sistem ile Bölüm 5'te önerilen güven zinciri sisteminin karşılaştırılabilmesi amacıyla NS3 kütüphanesi kullanılarak benzetim çalışması hazırlanmıştır. Dell XPS 13-2.7 GHz hıza sahip kişisel bilgisayarı üzerinde Ubuntu 14.04 işletim sistemi kullanılarak benzetimler çalıştırılmıştır. NetAnim, Wireshark ve hazırlanan NS3 benzetim çıktıları ile sonuçlar analiz edilmiştir.

Bu araştırmada kullanılan NS3 açık kaynak ağ simülatörü, geliştirilme aşamasında olan bir ürün olsa da içinde barındırdığı NqosWaveMacHelper gibi kütüphaneler ile IEEE 802.11p ortamının benzetiminin yapılmasına olanak sağlamaktadır. Hazırlanan benzetim çalışması 2014 yılında Scott E. Carpenter tarafından hazırlanan vanet-routing-compare.cc iskeletinin geliştirilmesi ile hazırlanmıştır [73]. İskelete aşağıda sıralanan eklemeler yapılmıştır.

- Mesajların araçlar arasında rastgele iletilmesini sağlayan bir yapı oluşturulmuştur.
- Sisteme RSU yapısı eklenmiştir.
- Araçlar arası iletilen mesajların iptal kontrolünün Bölüm 5'te açıklanan algoritmaya uygun şekilde yapılması için metotlar geliştirilmiştir.
- Dinamik güven listesi mekanizması oluşturulmuştur.
- SİL dosyalarının belirlenen periyotlarda güncellendiği bir yapı hazırlanmıştır.

Hazırlanan ağ yapısı içinde araçlar ve RSU olmak üzere iki çeşit varlık bulunmaktadır. Bahsedilen varlıklar arasında V2V ve V2I iletişimi kurulmaktadır. Benzetim çalışmasında araçları hareketli olup RSU'ların hareketsiz olması; alınan ve gönderilen mesaj içeriklerinin farklı olması dışında bu iki yapı benzer özelliklerde oluşturulmuştur. RSU'lar 1km'lik alan içindeki tüm araçlar ile iletişim kurabilmektedir. Şekil 6.1'de RSU kapsama alanı NetAnim üzerinde gösterilmiştir.



Şekil 6.1. RSU kapsama alanı NetAnim görüntüsü

RSU aracılığı ile SİL sunucularına yapılan SİL istek sayısı temel karşılaştırma kriteri olarak belirlenmiştir. Benzetim çalışmasında bir araçtan diğer bir araca gönderilen ilk mesaj tetikleyici mesaj (TRF) olarak adlandırılmıştır. Trafik yoğunluğunun sistem üzerindeki etkisini test edebilmek için ağ içindeki araç sayıları ve TRF mesajları değiştirilerek benzetim çalışması tekrarlanmıştır.

Hazırlanan benzetim içindeki mesajlar UDP protokolü ile iletilmektedir. Araçların takma isim sertifikalarının seri numaraları yerine araç IP adresleri kullanılmıştır. Benzetim çıktıları hazırlanarak ve Wireshark üzerinden ağ izlenerek benzetim çalışmaları analiz edilmiştir. Şekil 6.2'de gönderilen mesajların listelendiği benzetim çıktılarından alınmış bir kesit gösterilmiştir. Gösterilen örnekte 0,000736646. sn'de 10.0.0.23 aracından 10.0.0.6 aracına bir TRF mesajı gönderilmiştir. 10.0.0.6 aracında güncel SİL dosyası bulunmamaktadır.

```
------------------------------------------------
0.00736646 Araclara gelen mesaj: TRF: Merhaba
10.0.0.23--> 10.0.0.6
TRF mesaji geldi
SİL yok SİL istegi yapilmali
------------------------------------------------
```

Şekil 6.2. Trafiğin listelendiği benzetim çıktıları genel bilgiler

6.1. SİL Kullanılan Yapının Benzetimi

Önerilen algoritma ile karşılaştırabilmek amacıyla ilk olarak iptal kontrolünde yalnızca SİL kullanan klasik sistemin benzetimi hazırlanmıştır. Bu yapıda, benzetim süresi boyunca istenen aralıklarda SİL dosyalarının güncellenmesi sağlanmıştır. Araçlar sertifikaların iptal kontrolünü yapmak için indirdikleri SİL'leri SİL ömrü bitene kadar kullanmaktadır.

SİL'lerinin ömrü bittiğinde RSU üzerinden SİL sunucularına SİL isteği gönderilerek yeni SİL indirilmektedir.

Bir araç başka bir araca mesaj gönderdiğinde, göndericinin sertifikasının iptal kontrolünün yapılabilmesi için RSU üzerinden SİL sunucularına SRG_RSU adı verilen mesajlar iletilmektedir. Bu sorgu mesajlarına cevap olarak gönderilen RSU'dan SİL taşıyan RSUdan_SIL mesajları ise RSU'dan araçlara gönderilmektedir.

Şekil 6.3'te SRG_RSU ve RSUdan_SIL mesaj kullanımlarının benzetim çıktılarından alınan bir örnek gösterilmiştir. Örnekte, 10.0.0.23 aracından 10.0.0.6 aracına mesaj iletilmiştir. 10.0.0.6 aracının geçerli bir SİL dosyası bulunmadığı için RSU üzerinden SİL sunucularına SİL isteği gönderilmiştir. SİL isteği alan SİL sunucuları güncel SİL dosyasını 10.0.0.6 aracına iletmiştir. 10.0.0.6 aracı güncel SİL üzerinden iptal sorgusunu gerçekleştirmiştir.

```
-------------------------------------------------
0.00736646  Araclara gelen mesaj:  TRF: Merhaba
10.0.0.23--> 10.0.0.6
TRF mesaji geldi
SİL yok SİL istegi yapilmali
-------------------------------------------------
0.0240455  Araclara gelen mesaj:  SRG_RSU:SİL istegi
10.0.0.6--> 10.0.0.100
SRG_RSU: mesaj geldi
SİL istegi yapiliyor
-------------------------------------------------
0.0244587  Araclara gelen mesaj:  RSUdan_SIL:SİL dosyasi
10.0.0.100--> 10.0.0.6
RSU'dan SİL gönderiyor
10.0.0.23 SİL'de bulunmuyor
-------------------------------------------------
```

Şekil 6.3. Benzetim çıktılarında SRG_RSU ve RSUdan_SIL mesajları

6.2. Güven Zincirine Dayalı Sertifika İptal Kontrolü Yapısının Benzetimi

SİL sunucularına yapılan SİL isteğini azaltmayı amaçlayan güven zincirine dayalı sertifika iptal kontrolü yapısının sistem üzerindeki etkisini test edebilmek için hazırlanan benzetim çalışmasında, göndericinin sertifikasının iptal kontrolünün yapılabilmesi için iki çeşit mesaj bulunmaktadır. İlk mesaj RSU üzerinden SİL sunucularına gönderilen mesajdır (SRG_RSU). İkinci mesaj ise güven listesinde bulunan araçlara gönderilen sorgu mesajlarıdır (SRG). Bu sorgu mesajlarına cevap olarak gönderilen RSU'dan SİL taşıyan mesajlar (RSUdan_SIL) ve güven zincirindeki araçlardan gelen cevaplar (CVP) olmak üzere iki farklı cevap mesajı bulunmaktadır. Benzetim esnasında araçlar sertifika iptal kontrollerini

Bölüm 5'te tanıtılan algoritmaya uygun şekilde gerçekleştirmişlerdir. Benzetim kayıtlarından örnekler alınarak farklı durumlarda araçların iptal kontrol davranışları aşağıda özetlenmiştir.

Durum 1: Alınan tetikleyici TRF mesajları sonrasında araçlar gönderici sertifikasının iptal kontrolünü SİL üzerinden ya da güven listelerini kullanarak sağlayabilmektedir. Şekil 6.4'te 10.0.0.15 aracından 10.0.0.10 aracına tetikleyici mesaj ulaşmıştır. 10.0.0.10 aracının geçerli bir SİL dosyası olduğu için 10.0.0.15 aracının sertifika iptal kontrolü SİL üzerinden sağlanmıştır.

```
0.406037  Araclara gelen mesaj:  TRF: Merhaba
10.0.0.15--> 10.0.0.10
Tetikleyici Mesaj geldi.
SIL mevcut
SIL Gecerli
10.0.0.15 adresi 10.0.0.10_SIL listesinde bulunmuyor.
10.0.0.15 adresi 10.0.0.10 Guven listesinde eklendi
```

Şekil 6.4. Mevcut SİL üzerinden iptal kontrolü benzetim çıktısı görüntüsü

Durum 2: Araçların geçerli bir SİL'e sahip olmadığı ve güven listesinde bilgi bulunmadığı durumda SİL sunucularına SİL isteği gönderilmelidir. Şekil 6.5'te 10.0.0.3 aracından 10.0.0.6 aracına TRF mesajı gönderilmiştir. Geçerli bir SİL mevcut olmadığı ve güven listesi boş olduğu için RSU üzerinden SİL sunucusundan güncel SİL indirilmiştir.

```
0.0250307  Araclara gelen mesaj:  TRF: Merhaba
10.0.0.3--> 10.0.0.6
Tetikleyici Mesaj geldi.
SIL mevcut değil
Guven listesi mevcut değil. RSU'dan SIL istenecek
```

Şekil 6.5. SİL isteği yapılması benzetim çıktısı görüntüsü

Şekil 6.6'da örnek bir güven listesi gösterilmiştir. Güven listesinde Bölüm 5'te açıklandığı üzere araç takma isim sertifikası seri numarası, atlama sayısı değeri, cevap yaşı değeri ve güven değeri bulunmaktadır. Hazırlanan benzetim çalışmasında oluşturulan listede sertifika seri numarası yerine IP değerleri kullanılmıştır. Benzetim çalışmasındaki cevap yaşının birimi ise saniyedir.

```
----------------------------------------
  seri no    hc  cevap yasi  guven degeri
----------------------------------------
  10.0.0.25  :2  :26.700152  :0.110000
  10.0.0.11  :2  :28.005945  :0.240579
  10.0.0.23  :2  :29.400152  :0.380000
  10.0.0.38  :2  :29.713209  :0.411306
  10.0.0.15  :0  :33.002093  :0.370097
  10.0.0.34  :0  :33.702138  :0.405099
  10.0.0.8   :1  :34.101830  :0.425084
  10.0.0.27  :1  :35.600633  :0.499972
----------------------------------------
```

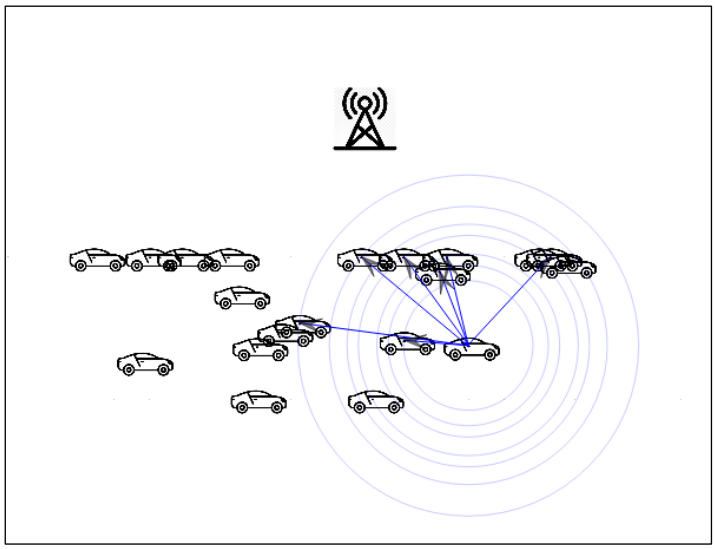
Şekil 6.6. Benzetim çalışmasında oluşturulmuş güven listesi yapısı

Durum 3: Araçların geçerli bir SİL'e sahip olmadığı fakat güven listesinin mevcut olduğu durumda güven listesi üzerinden sorgu yapılmaktadır. Güven listesinde gönderici araç ile ilgili bilgi bulunuyorsa gönderici araç tarafından gönderilen mesajlar güvenilir sayılmaktadır. Şekil 6.7'de 10.0.0.10 aracından 10.0.0.13 aracına TRF mesajı gönderilmiştir. 10.0.0.13 aracının geçerli bir SİL'i olmadığı için iptal kontrolü güven listesi üzerinden yapılmıştır. Güven listesinde 10.0.0.10 aracı mevcut olduğu için sertifika iptal kontrolü SİL isteği gönderilmeden güven listesi üzerinden yapılabilmiştir.

```
10.1002  Araclara gelen mesaj:  TRF: Merhaba
10.0.0.10--> 10.0.0.13
Tetikleyici Mesaj geldi.
SIL mevcut
SIL Gecersiz
Guven listesi mevcut
10.0.0.10 Guven listesinde mevcut
```

Şekil 6.7. Mevcut güven listesinden iptal kontrolü benzetim çıktısı görüntüsü

Durum 4: Araçların geçerli bir SİL'e sahip olmadığı fakat güven listesinin mevcut olduğu durumda, güven listesinde gönderici araç ile ilgili bilgi bulunmuyorsa gönderici araç ile ilgili iptal bilgisi güven listesinde bulunan diğer araçlara sorulmaktadır. Şekil 6.8'de güven listesinde bulunan araçlara yapılan SRG sorgusunun NetAnim üzerinden gösterimi verilmiştir.



Şekil 6.8. Güven zinciri sorgusu NetAnim görüntüsü

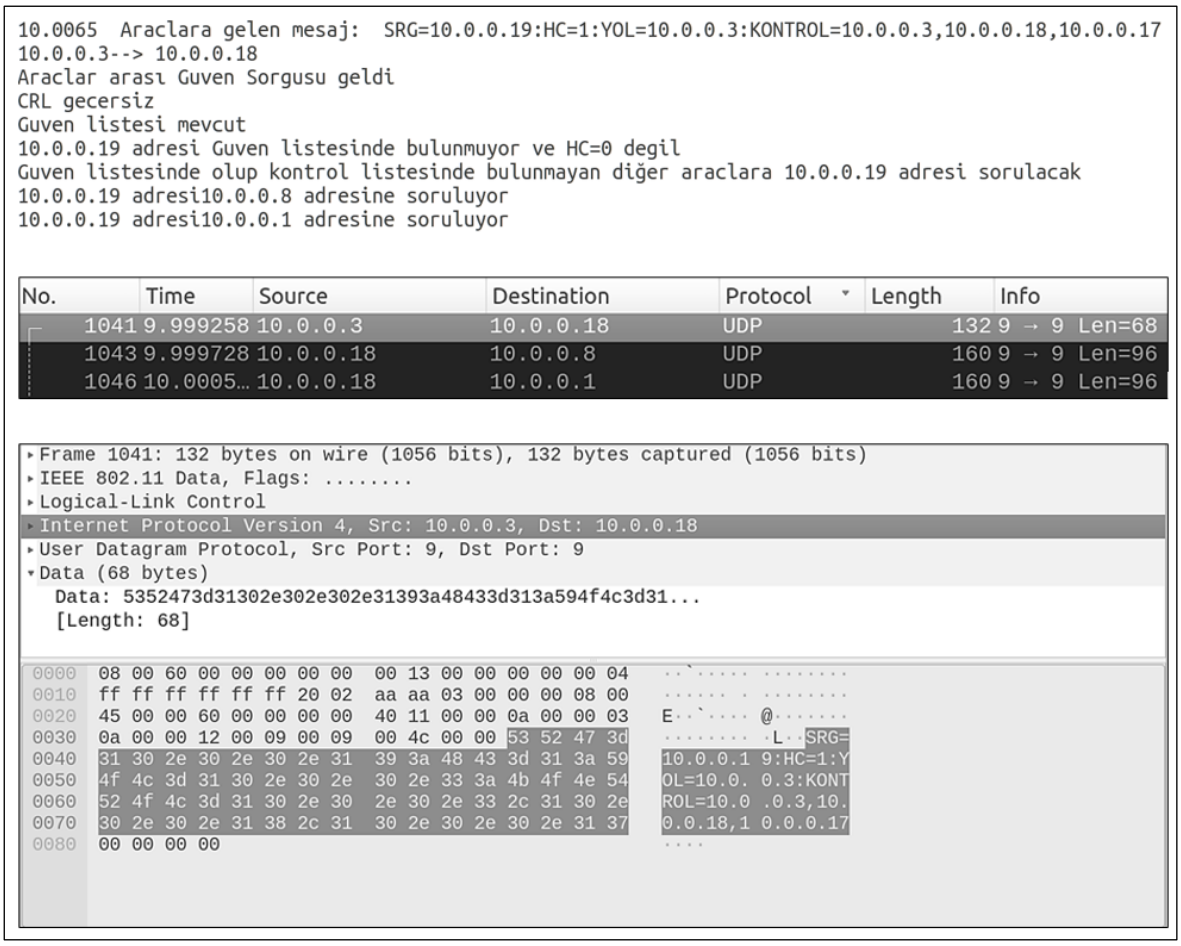
Şekil 6.9'da 10.0.0.6 aracından 10.0.0.9 aracına TRF mesajı gönderilmiştir. 10.0.0.6 aracının geçerli bir SİL'i olmadığı için güven listesinde 10.0.0.6 aracının varlığı kontrol edilmiştir. 10.0.0.6 aracı ile ilgili iptal bilgisi güven listesinde bulunmadığı için güven listesinde bulunan 10.0.0.19, 10.0.0.18, 10.0.0.4 ve 10.0.0.10 araçlarına 10.0.0.6 aracı ile ilgili iptal sorgusu yapılmıştır.

```
10.0509  Araclara gelen mesaj:  TRF: Merhaba
10.0.0.6--> 10.0.0.9
Tetikleyici Mesaj geldi.
SIL mevcut
SIL Gecersiz
Guven listesi mevcut
10.0.0.6 Guven listesinde bulunmuyor
Guven listesinde bulunan araclara soruluyor
10.0.0.19 adresine sorulacak
10.0.0.18 adresine sorulacak
10.0.0.4 adresine sorulacak
10.0.0.10 adresine sorulacak
```

Şekil 6.9. Güven zinciri sorgusu benzetim çıktısı görüntüsü

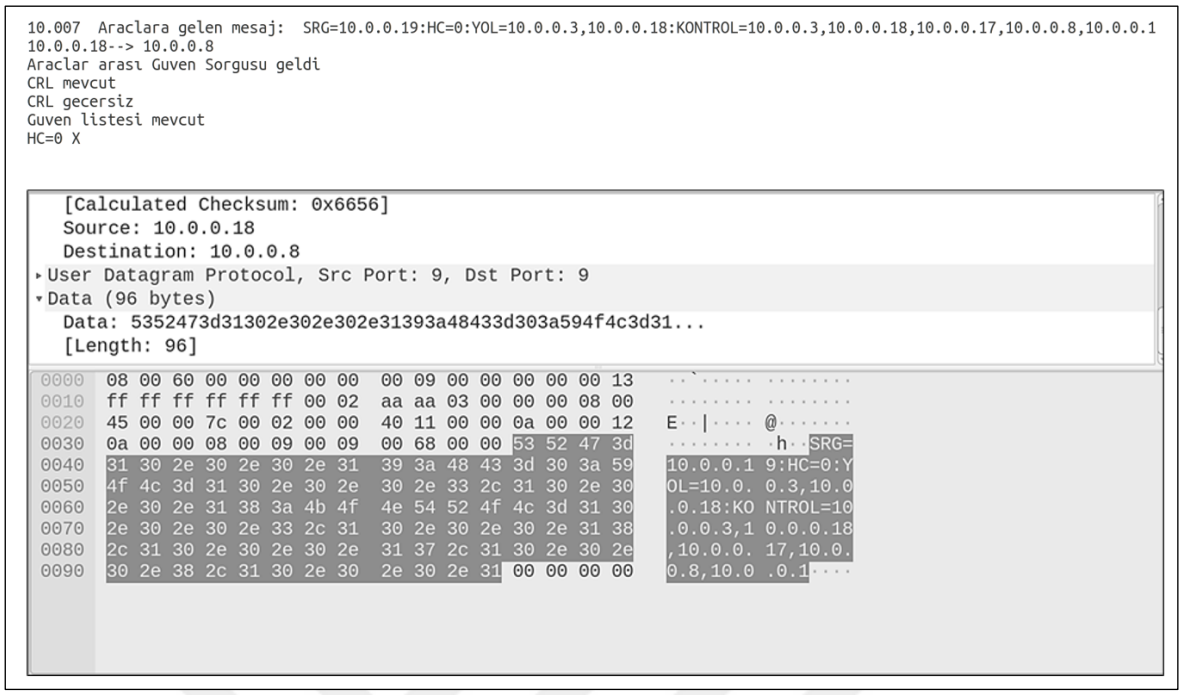
Durum 5: Güven listesindeki araçlara gönderilen SRG mesajları araç sertifikası seri numarası, HC, YOL ve KONTROL alanlarını içermektedir. HC atlama sayısını göstermektedir. HC değeri her sorguda birer azaltılmakta ve bu değer 0 olana kadar güven sorgusu yapılmaya devam edilebilmektedir. YOL, sorgu mesajının hangi araçlar aracılığı ile ulaştığını gösteren alandır. Bu alan sayesinde cevap mesajlarının gönderim yolu belirlenmektedir. KONTROL alanı güven zinciri içinde sorgu mesajının gönderildiği araç bilgilerini içeren alandır. Bu alan yardımı ile daha önce sorgu mesajı gönderilmiş araçlara tekrar sorgu mesajı gönderilmesi önlenmektedir. Şekil 6.10'da 10.0.0.3 aracından 10.0.0.18

aracına gönderilen SRG mesajı görülmektedir. 10.0.0.19 aracının sertifikasının iptal bilgisi sorgulanmaktadır. 10.0.0.18 aracının sahip olduğu SİL'in geçerlilik tarihi dolduğu için güven listesi üzerinden kontrol yapılmıştır. Güven listesinde 10.0.0.19 ile ilgili iptal bilgisi bulunmadığı ve HC değeri de 0 olmadığı için güven listesinde bulunup KONTROL listesinde bulunmayan 10.0.0.8 ve 10.0.0.1 araçlarına SRG mesajı gönderilmiştir.



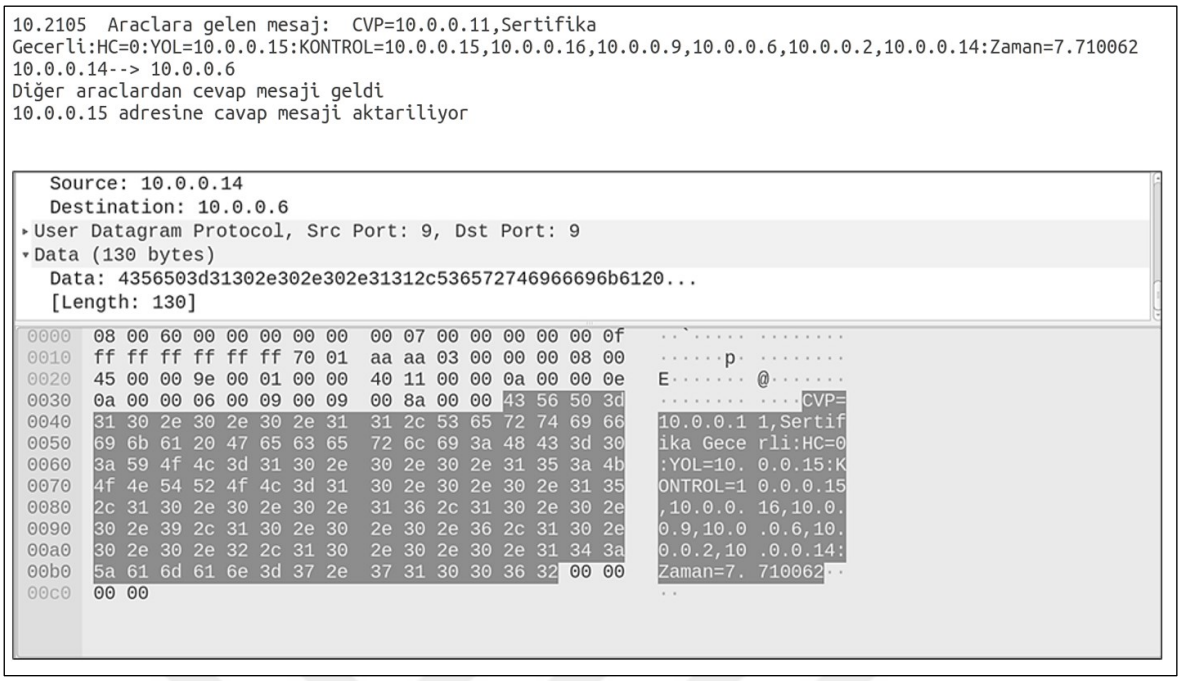
Şekil 6.10. Güven zinciri sorgu mesajları benzetim çıktısı ve Wireshark görüntüsü

Durum 6: SRG mesajında HC değerinin 0 olduğu durumda güven zinciri sona ermektedir. Şekil 6.11'de 10.0.0.18 aracından 10.0.0.8 aracına gönderilen SRG mesajı görülmektedir. 10.0.0.19 aracının iptal durumu sorgulanmaktadır. 10.0.0.8 aracının geçerli bir SİL'i bulunmamakta ve güven listesinde 10.0.0.19 aracı hakkında bir bilgi bulunmamaktadır. Sorgu içindeki HC değeri 0 olduğu için güven listesi içindeki diğer araçlara sorgu mesajı gönderilmemiştir.



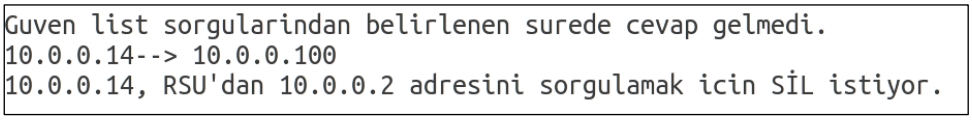
Şekil 6.11. HC= 0 olan SRG benzetim çıktısı ve Wireshark görüntüsü

Durum 7: Güven zinciri içinde SRG mesajı alan araçların SİL veya güven listeleri yardımı ile sorgulanan araç ile ilgili iptal bilgisine ulaşmaları durumunda sorgu yapan araca CVP mesajı gönderilmektedir. CVP mesajı içinde sorgulanan araç sertifikasının iptal bilgisi, iptal verisinin elde edildiği atlama sayısı ve zaman verisi bulunmaktadır. Bu veriler yardımı ile güven listesindeki güven sayısı hesaplanmaktadır. CVP mesajının kime gönderileceği SRG içindeki YOL alanı üzerinde belirtilmektedir. Şekil 6.12'de 10.0.0.14 aracından 10.0.0.6 aracına CVP mesajı gönderilmektedir. CVP mesajında 10.0.0.11 aracının sertifikasının geçerli olduğunun bilgisi bulunmaktadır. Zaman alanında SİL üzerinden yapılan iptal kontrolünün 7,710062. sn'de yapıldığının bilgisi bulunmaktadır. Atlama sayısı bitiş değeri ise 0'dır.



Şekil 6.12. Güven zinciri cevap mesajları benzetim çıktısı ve Wireshark görüntüsü

Durum 8: Güven zincirindeki araçlardan belirlenen sürede sorgu yapılan araç ile ilgili bilgi alınamaması durumunda, SİL sunucularına SİL isteği gönderilmektedir. Şekil 6.13'te 10.0.0.14 aracı güven zinciri yapısını kullanarak 10.0.0.2 aracı ile ilgili iptal bilgisine ulaşamamış ve süre sonunda SİL isteği göndermiştir.



Şekil 6.13. Güven zinciri sorgusu sonrası SİL isteği benzetim çıktısı görüntüsü

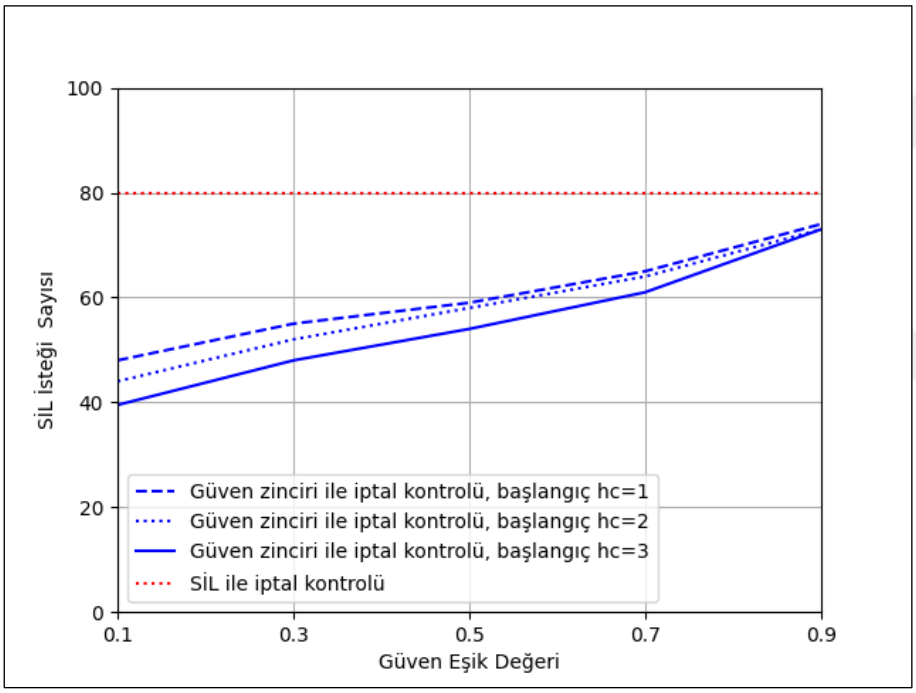
6.3. Benzetim Sonuçlarının Analizi

Bölüm 5'te önerilen güven zincirine dayalı iptal kontrol yönteminin, iptal kontrol verimliliği üzerindeki etkisini analiz etmek için farklı mesaj sayıları, araç sayıları, güven eşik değerleri ve atlama sayısı başlangıç değerleri kullanılarak benzetim ortamları hazırlanmıştır. Araçların hızı 100 km/saat olarak ayarlanırken, RSU'ların kapsama alanı 1 km olarak ayarlanmıştır.

Güven zincirine dayalı sertifika iptal kontrolünün SİL isteği sayısına etkisi

Sertifika iptal kontrolü için sadece SİL dosyalarının kullanıldığı yöntemde, SİL sunucularından indirilen SİL dosyaları, erişim süresini ve kullanılabilirliği artırmak için

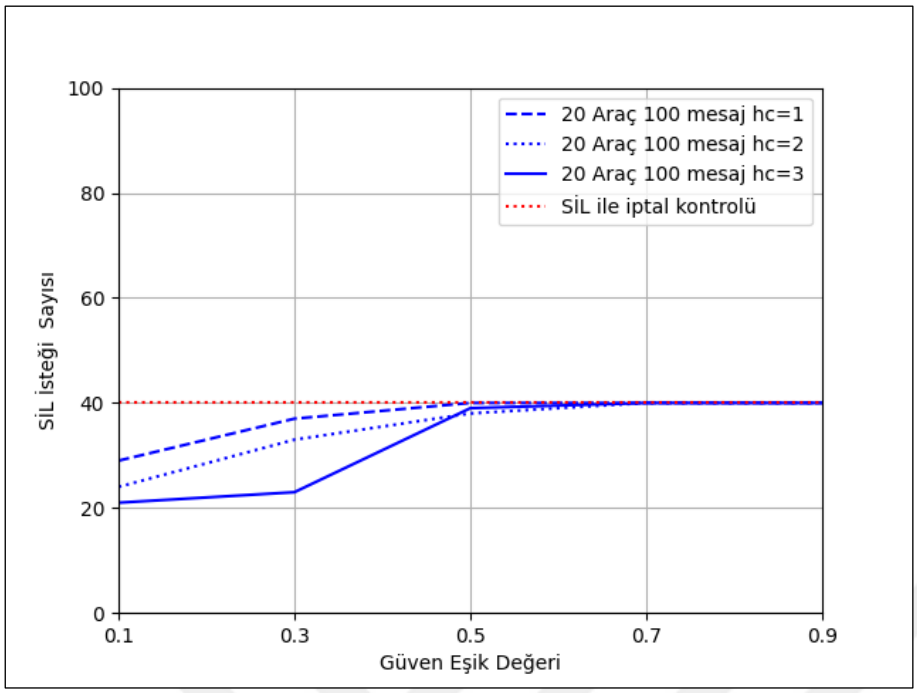
önbelleğe alınmaktadır. SİL önbellekte değilse veya SİL'in süresi dolmuşsa SİL sunucularına SİL isteği yeniden yapılmaktadır. Önerilen sistemin SİL sunucularına yapılan SİL isteği sayısına etkisini görebilmek için bir RSU, 40 aracın bulunduğu, 400 TRF mesajının gönderildiği ve benzetim ortasında güncel SİL dosyasının yayınlandığı bir benzetim hazırlanmıştır. Şekil 6.14'te görüldüğü gibi geleneksel iptal kontrol yöntemi ile araçlar 80 kez SİL isteği gönderirken, güven zinciri iptal kontrol sistemi kullanımı ile SİL istek sayısının azaldığı gözlemlenmiştir. Sistemin etkisi, farklı başlangıç atlama sayısı ve güven eşiği değerlerine göre farklılık göstermiştir.



Şekil 6.14. Güven zinciri ile sadece SİL kullanılan yapı karşılaştırması 40 araç, 400 mesaj

Trafik yoğunluğuna uygun eşik değeri seçilmesi

Mesaj sayısının artmasıyla güven zinciri iptal kontrolü yönteminin katkısının da arttığı görülmektedir. Şekil 6.15'te gösterilen bir RSU ve 20 aracın bulunduğu ve 100 TRF mesajının gönderildiği yapı, nispeten daha az trafik yoğunluğuna sahiptir. Araç sayısı ve mesaj sayısındaki düşüş sebebiyle güven listesi beslenememekte ve bu nedenle güven zinciri yapısının sisteme katkısında düşüş gözlemlenmektedir. Benzetimde, eşik değerinin 0,5 ve üzerinde olduğu durumlarda güven zinciri yapısının katkısının neredeyse kaybolduğu görülmüştür.



Şekil 6.15. Düşük trafik yoğunluğunda güven zinciri sistemi

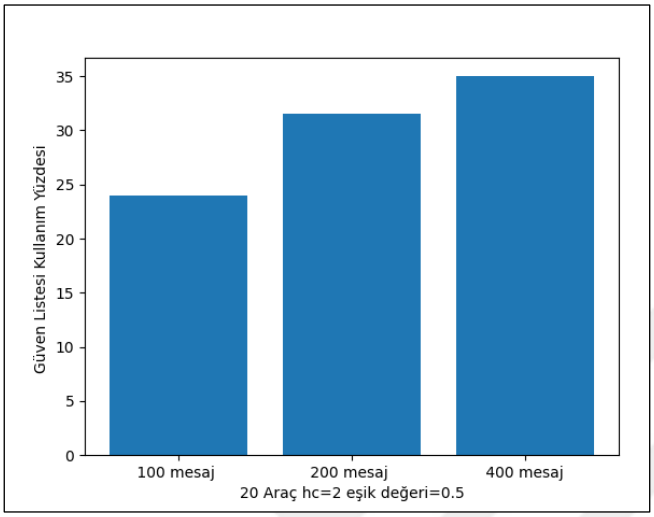
Güven değeri hesaplama denklemine göre atlama sayısı başlangıç değeri yüksek olan verilerin güven değeri düşük olacağı için eşik değeri seçilirken atlama sayısı başlangıç değeri göz önünde bulundurulmalıdır. Yüksek eşik değerlerinin kullanılması durumunda atlama sayısı yüksek olan veriler güven listesinden silinecektir. Şekil 6.15'te 1,2 ve 3 atlama sayısı başlangıç değerleri için yapılan benzetimlerde eşik değeri arttıkça, yapılan SİL isteği sayısı birbirine yaklaşmaktadır. Trafik yoğunluğunun düşük olduğu durumlarda güven zinciri yapısının etkili olması için eşik değeri düşük seçilmelidir.

Mesaj sayısının etkisi

Mesaj sayısındaki değişimin güven zinciri yapısına olan etkisini gözlemlemek için eşit süre içinde farklı sayıda TRF mesajının atıldığı ağların benzetimi yapılmıştır. Bir RSU ve 20 araç ile hazırlanan benzetimlerde atlama sayısı başlangıç değeri 2, eşik değeri ise 0,5 olarak ayarlanmıştır. Benzetim ortasında SİL süresi dolup yeni SİL yayınlanmıştır.

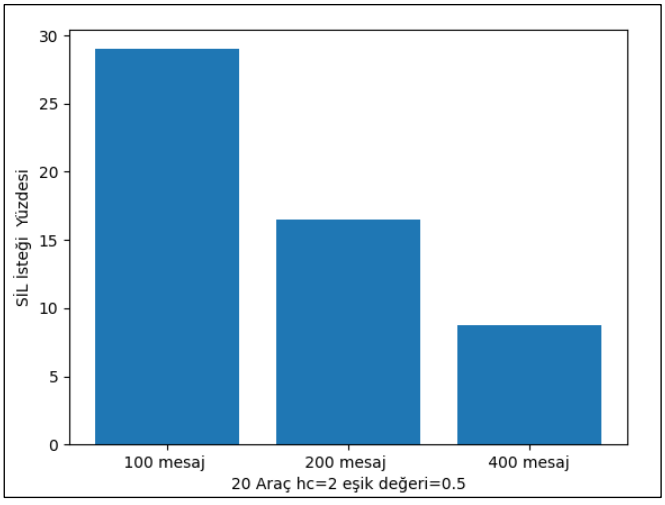
Bir araç başka bir araçtan ilk defa TRF mesajı aldığında araç sertifikasının iptal kontrolünü mevcut SİL dosyası üzerinden, SİL isteği yapıp güncel SİL'i indirerek ya da güven zinciri yapısını kullanarak güven listesi aracılığı ile yapabilmektedir. Güven zinciri kullanılarak gerçekleştirilen sertifika iptal kontrolünün toplam sertifika iptal kontrolü içindeki kullanım yüzdesi karşılaştırma kriteri olarak belirlenmiştir. Şekil 6.16'da 100, 200 ve 400 TRF

mesajının gönderildiği ağ benzetimleri karşılaştırılmıştır. 100 mesaj gönderildiği durumda güven listesi kullanım yüzdesi ortalama %24 hesaplanırken 400 mesajın gönderildiği ağda güven listesi kullanım yüzdesi ise %35 olarak hesaplanmıştır. Eşit süre içinde gönderilen TRF mesajı sayısı arttıkça güven zinciri yapısının sisteme katkısının arttığı gözlemlenmiştir.



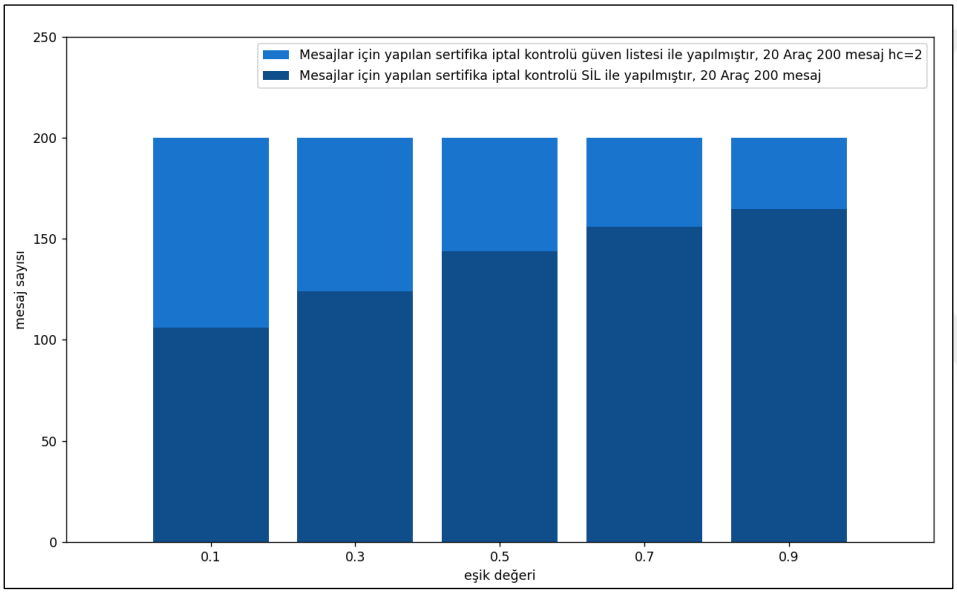
Şekil 6.16. Mesaj sayısının güven listesi kullanım yüzdesine etkisi

Güven zinciri yapısının entegre edildiği ağlarda mesaj sayısı artışının SİL sunucularına yapılan SİL isteği sayısı üzerindeki etkisi analiz edilmiştir. Benzetimde araçların iptal kontrolü, güven zinciri yapısı dışında mevcut SİL üzerinden ya da aracın geçerli bir SİL'i yok ise SİL sunucularına SİL isteği gönderilerek de yapılabilmektedir. Şekil 6.17'de SİL isteği gönderilerek gerçekleştirilen sertifika iptal kontrolünün toplam sertifika iptal kontrolü içindeki kullanım yüzdesi verilmiştir.



Şekil 6.17. Mesaj sayısının SİL isteği yapma yüzdesine etkisi

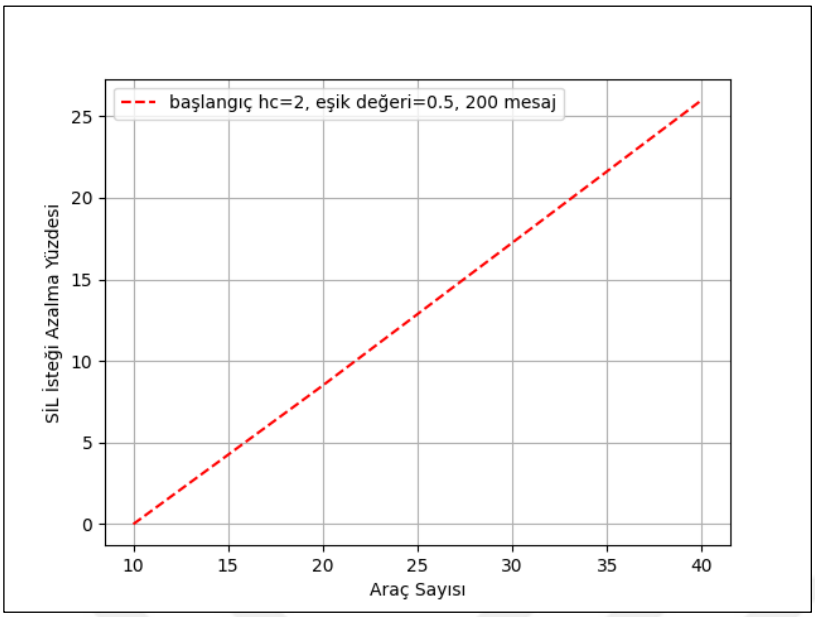
Mesaj gönderen araçların sertifikalarının güven zinciri yapısı ile doğrulanma oranının, farklı eşik değerlerine göre değişimi Şekil 6.18'de gösterilmiştir. Bir RSU ve 20 aracın bulunduğu benzetimde, 200 TRF mesajı gönderilmiştir ve atlama sayısı başlangıç değeri 2 olarak ayarlanmıştır. Eşik değerinin 0,9 olduğu durumda 35 adet TRF mesajı ile sertifikaların iptal kontrolü, güven listesi yardımı ile yapılmıştır. Geri kalan 165 adet TRF mesajı sertifikasının iptal kontrolü ise mevcut SİL dosyaları üzerinden ya da SİL isteği yapılarak geçerli SİL indirilmesi ile gerçekleştirilmiştir. Eşik değeri azaltıldıkça güven listesi kullanımı artmış ve eşik değerinin 0,1 olduğu durumda güven listesi yardımı ile yapılan iptal kontrol sayısı 94'e yükselmiştir.



Şekil 6.18. Eşik değerine göre iptal kontrol metotlarının kullanımı

Araç sayısının etkisi

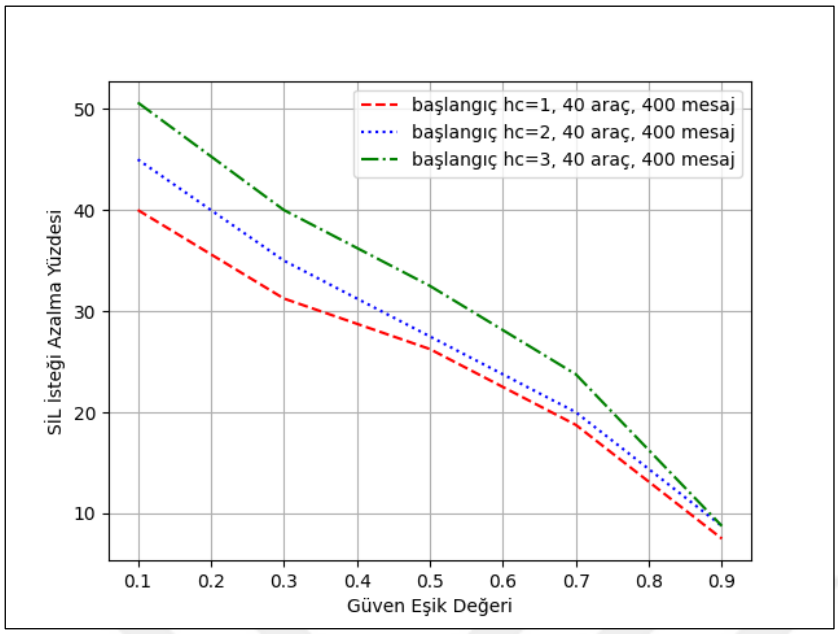
Araç sayısındaki değişimin güven zinciri yapısına olan etkisini belirlemek için farklı araç sayılarına sahip ağların benzetimi yapılmıştır. Hazırlanan benzetimlerde atlama sayısı başlangıç değeri 2, eşik değeri ise 0,5 olarak belirlenmiştir. Benzetim boyunca iptal sorgusu yapılması gereken 200 adet TRF mesajı atılıp benzetim ortasında SİL süresi dolup yeni SİL yayınlanmıştır. Ağ içindeki araç sayısının önerilen güven zinciri yapısı üzerindeki etkisini görmek için yapılan hesaplamalarda ağ içindeki araç sayısındaki artışın SİL isteği azalma yüzdesinin artışına neden olduğu görülmüştür (Şekil 6.19).



Şekil 6.19. Araç sayısının güven zinciri yapısına etkisi

Atlama sayısı başlangıç değeri ve eşik değerinin etkisi

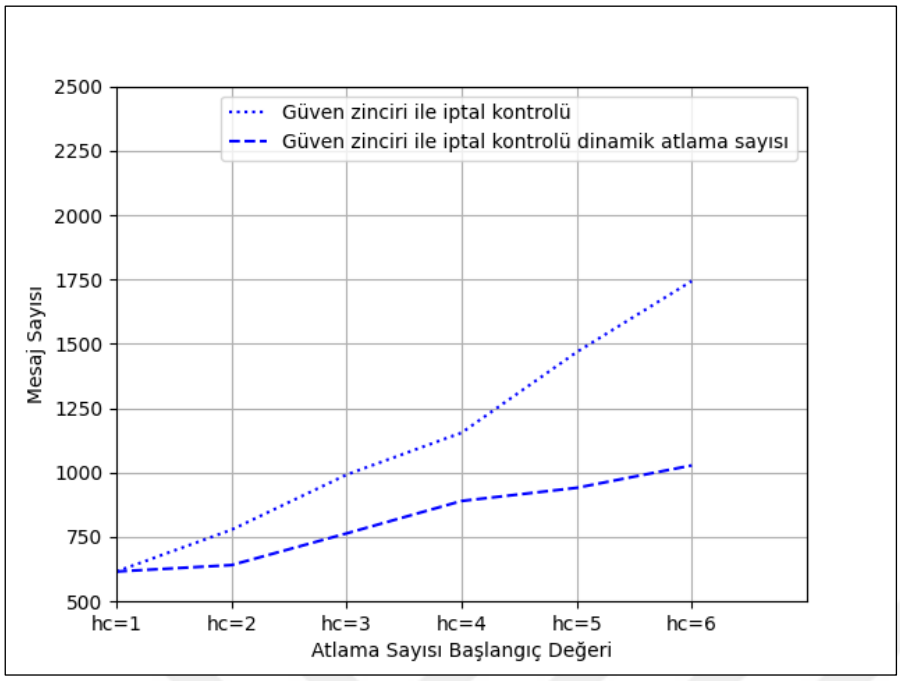
Şekil 6.20'de görüldüğü gibi belirlenen güven eşik değerine bağlı olarak ağ içinde yapılan SİL isteği sayısı değişmektedir. Güven eşik değerinin düşürülmesi ile güven listeleri kullanılarak iptal kontrolünün yapılma yüzdesi artmış ve SİL sunucularına yapılan SİL isteği azalmıştır. Ayrıca, daha yüksek atlama sayısı başlangıç değerlerinde güven zinciri ile ulaşılan araç sayısı arttığı için daha fazla araca sorgu yapılabilmiş ve güven zinciri ile iptal bilgisine ulaşılabilme olasılığı artırılmıştır. Bunun sonucunda SİL isteği sayısı azalmıştır. Atlama sayısı başlangıç değerinin 3, güven eşik değerinin ise 0,1 seçildiği durumda sunuculara yapılan SİL isteği sayısında yaklaşık %55 azalma olduğu tespit edilmiştir. Atlama sayısı başlangıç değerinin 1, güven eşik değerinin ise 0,9 seçildiği durumda, güven zinciri sisteminin ağa olan etkisi azalmış ve SİL isteğindeki azalma oranı %15 civarlarına düşmüştür. Genel durum incelendiğinde ise önerilen güven zinciri yapısının merkeze yapılan SİL isteği sayısını ortalama %35 oranında azalttığı görülmüştür.



Şekil 6.20. Eşik değeri ve atlama sayısı başlangıç değerinin SİL isteği sayısına etkisi

Atlama sayısı başlangıç değeri arttıkça, RSU üzerinden gönderilen SİL isteğinin azaldığı gözlemlenmiştir. Fakat atlama sayısı başlangıç değerinin artması güven zincirinin neden olduğu mesaj sayısını da artırmaktadır. Benzetim sonuçlarında atlama sayısı başlangıç değerinin artmasıyla birlikte paket kaybının da arttığı görülmüştür.

Yüksek atlama sayısı başlangıç değerlerinde ağda meydana gelen mesaj sayısı artışını azaltmak için güven listesinde bulunan araç sayısına bağlı olarak atlama sayısı değerinin değiştirildiği dinamik bir yapı tasarlanmıştır. Güven listesinde yüksek sayıda araç bulunduran düğümler için atlama sayısının düşük tutulması sağlanmıştır. Oluşturulan dinamik yapı sayesinde SİL isteği azalma yüzdesinde önemli bir düşüş yaşanmazken, mesaj sayısında belirgin düşüş yaşandığı gözlemlenmiştir. Bir RSU, 40 araç, 400 tetikleyici mesaj ve 0,5 eşik değeri için hazırlanan benzetimde, atlama sayısı başlangıç değerinin 2 olduğu durumda ağdaki mesaj sayısındaki düşüş yaklaşık %17 iken atlama sayısı başlangıç değerinin 6 olduğu durumda, ağdaki mesaj sayısındaki düşüşün %41'lere ulaştığı görülmüştür (Şekil 6.21).



Şekil 6.21: Dinamik atlama sayısı yapısı ve mesaj sayısındaki azalma

7. SONUÇLAR VE ÖNERİLER

Bu çalışmada V2X iletişiminde mesaj güvenliğini sağlamak için kullanılan yöntemler araştırılmıştır. ETSI ve IEEE'nin V2X standartlarında, asimetrik anahtar altyapısının kullanıldığı güvenlik mekanizmaları oluşturulduğu ve araç gizliğini sağlamak için takma isim sertifikasının kullanıldığı görülmektedir. V2X güvenlik mekanizmasını geliştirmek için yapılan çalışmalarda, sertifika iptal kontrolü işlemini daha verimli hale getirilmeye odaklanıldığı dikkat çekmektedir.

Sertifika iptal kontrolü için SİL kullanan sistem tasarımlarında, iptal kontrolünü hızlandırmak için SİL dosya yapısının boyutunu ve dağıtım yöntemini değiştirmeyi hedefleyen çalışmalar yapıldığı görülmüştür. IEEE 1609.2'de önerilen SCMS yapısının SİL boyutunu azaltan uygun bir çözüm olduğu sonucuna varılmıştır.

AAA'ya dayanan V2X sistemlerinde, görev alan merkezi otoritelerin bir saldırıya uğraması durumunda, sistem güvenliği tamamen tehlikeye düşmektedir. Bu açığı kapatmak için dağıtık sistem yapılarının tasarlanması gerekmektedir. Bunun için blokzincirin kullanıldığı, kümeleme yöntemi ile ölçeklenebilirliğin sağlandığı ve yapıya uygun mutabakat mekanizmalarının tasarlandığı görülmüştür.

Bu tez çalışmasında, SİL dosyalarının verimli bir şekilde dağıtılmasını amaçlayan ve merkezi SİL sunucusu üzerindeki yükün azaltılmasını sağlayan güven zincirine dayalı iptal kontrol mekanizması önerilmiştir. Önerilen yapıda, SİL dışında güvenilir araçların listelendiği güven listeleri kullanılmaktadır. Güven listesindeki bilgilerin güvenilirliği zaman ve edinilme yoluna bağlı olarak değerlendirilmekte ve liste bu değerlere göre güncel tutulmaktadır. Araçlar, belleklerinde kullanılabilir güncel bir SİL olmadığı durumda güven listelerini iptal kontrolü için kullanmakta, böylece merkez sunucuya yapılan SİL isteklerinin sayısı azalmaktadır.

NS3 kullanılarak hazırlanan benzetimler ile önerilen sistem test edilmiştir. Önerilen yapıda bulunan güven listesi, güven değeri, SİL, mesaj tipleri ve araç hareketlerinin benzetimi hazırlanmıştır. Araç sayısı, mesaj sayısı, atlama sayısı başlangıç değeri ve eşik değerinin sisteme etkileri test edilmiştir.

Yapılan benzetim çalışmaları sonucunda önerilen güven zinciri sisteminin merkezi SİL sunucusu üzerindeki yükü ortalama %35 oranında azalttığı gözlemlenmiştir. Önerilen yapı sayesinde, bir aracın güven listesini kullanarak merkezi sunucuya ya da RSU'ya erişmeye ihtiyaç duymadan güvenli şekilde sertifika iptal kontrolünü yapabildiği görülmüştür.

Araç sayısının ve mesaj sayısının yüksek olduğu yoğun trafikte, önerilen yapının verimliliğinin arttığı görülmüştür. Atlama sayısı başlangıç değerinin 2, eşik değerinin 0.5 ve mesaj sayısının 200 olduğu bir sistemde 15 aracın bulunduğu bir örneklemede SİL isteğindeki azalma yüzdesi %5 iken 40 aracın bulunduğu bir örneklemedeki SİL isteği azalma yüzdesi %30'a ulaşmaktadır. Eşit süre içinde gönderilen mesaj sayısındaki artışın, güven zinciri yapısının sisteme olan katkısını artırdığı gözlemlenmiştir. 100 mesaj gönderildiği durumda güven listesi kullanım yüzdesi ortalama %24 hesaplanırken 400 mesajın gönderildiği ağda güven listesi kullanım yüzdesi ise yaklaşık %35 olarak hesaplanmıştır.

Ayarlanabilir eşik değeri ve atlama sayısı başlangıç değeri ile trafik yoğunluğuna göre ayarlama yapılarak sistemin farklı trafik ortamlarına uyumluluğu sağlanmıştır. Atlama sayısı başlangıç değerinin 1, güven eşik değerinin ise 0,9 seçildiği durumda SİL isteğindeki azalma oranı %15 civarlarında iken atlama sayısı başlangıç değerinin 3, güven eşik değerinin ise 0,1 seçildiği durumda sunuculara yapılan SİL isteği sayısında yaklaşık %55 azalma olduğu tespit edilmiştir.

Gelecek çalışmalarımızda güven listesini besleyen kaynakların artırılmasını ve güven listesini besleyecek kaynakları azaltmadan, güven zinciri sorgularından kaynaklanan trafiğin azaltılmasını sağlayacak ek düzenlemelerin yapılması planlanmaktadır.

KAYNAKLAR

1. Hasan, M., Mohan, S., Shimizu, T., and Lu, H. (2020). Securing vehicle-to-everything (V2X) communication platforms. *IEEE Transactions on Intelligent Vehicles*, 5(4), 693-713.

2. İnternet: Connecting Vehicles Today and in the 5G Era with C-V2X (Cellular Vehicle-to-Everything). (2019). URL: https://www.gsma.com/iot/resources/connecting-vehicles-today-and-in-the-5g-era-with-c-v2x/, Son Erişim Tarihi: 22.05.2022.

3. Bhover, S.U., Tugashetti, A. and Rashinkar, P. (2017). V2X communication protocol in VANET for co-operative intelligent transportation system. *International Conference on Innovative Mechanisms for Industry Applications*, 602–607.

4. Camp, L. L. C. (2016). Security Credential Management System Proof-of-Concept Implementation-EE Requirements and Specifications Supporting SCMS Software Release 1.1. *Vehicle Safety Communications Consortium, Tech. Rep*,1-559.

5. Zhang, C., Lin, X., Lu, R., and Ho, P. H. (2008). RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks. *IEEE international conference on communications*, 1451-1457.

6. Dorri, A, Steger, M., Kanhere, S.S, and Jurdak R. (2017). BlockChain: A Distributed Solution to Automotive Security and Privacy. *IEEE Communications Magazine*, 55(12), 119-125.

7. Rawat, D. B., Doku, R., Adebayo, A., Bajracharya, C., and Kamhoua, C. (2020). Blockchain enabled named data networking for secure vehicle-to-everything communications. *IEEE Network*, 34(5), 185-189.

8. ETSI. (2021) TS 102 941 V1.4.1- Intelligent Transport Systems (ITS); Security; Trust and Privacy Management.

9. IEEE. (2019). 1609.2-IEEE- Standard for Wireless Access in Vehicular Environments-Security Services for Applications and Management Messages.

10. Wang, Q., Gao D., and Chen, D. (2020). Certificate revocation schemes in vehicular networks: A survey. *IEEE Access*, 8, 26223-26234.

11. Guo J., Baugh J. P. and Wang S. (2007). A group signature based secure and privacy-preserving vehicular communication framework. *Networking for Vehicular Environments*,103–108.

12. Lu, R., Lin, X., Zhu, H., Ho, P.H., and Shen, X. (2008). ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications. *INFOCOM, Phoenix*, AZ, USA, 1229–1237.

13. Büttner, C., and Huss, S. A. (2015). An Efficient Anonymous Authenticated Key Agreement Protocol for Vehicular Ad-Hoc Networks Based on Ring Signatures and the

Elliptic Curve Integrated Encryption Scheme. *International Conference on Information Systems Security and Privacy*, 139-159.

14. Nowatkowski, M. E., Wolfgang, J. E., McManus, C., and Owen, H. L. (2010). The effects of limited lifetime pseudonyms on certificate revocation list size in VANETS. *the IEEE SoutheastCon 2010 (SoutheastCon),* 380-383.

15. İnternet: Research and Markets, The Future of V2X Communications. (2021). URL: https://www.researchandmarkets.com/reports/5397280/the-future-of-v2x-communications, Son Erişim Tarihi: 21.04.2022.

16. Haas, J. J., Hu, Y. C., and Laberteaux, K. P. (2011). Efficient certificate revocation list organization and distribution. *IEEE Journal on Selected Areas in Communications*, 29(3), 595-604.

17. Laberteaux, K. P., Haas, J. J., and Hu, Y. C. (2008). Security certificate revocation list distribution for VANET. *The fifth ACM international workshop on VehiculAr Inter-NETworking*, 88-89.

18. Kumar, H., and Singh, D. (2020*). Smart Certificate Revocation List Exchange in VANET. 12th International Conference on Computational Intelligence and Communication Networks (CICN),* 210-214.

19. Bhover, S.U., Tugashetti, A. and Rashinkar, P. (2017). V2X communication protocol in VANET for co-operative intelligent transportation system. *Paper presented at International Conference on Innovative Mechanisms for Industry Applications*, 602–607.

20. Zaragatzky, R. (2018). Security analysis of introducing 5G in V2X communications (Master's thesis, 2018), 4-32.

21. İnternet: Cadzow S., Hoefs W., Kargl F., Roy R., Sill S., and Whyte W. (2012). *EUUS standards harmonization task group report*. URL: https://rosap.ntl.bts.gov/view/dot/34172, Son Erişim Tarihi: 12.10.2021.

22. Erceylan, G., ve Akcayol, M. A. (2022). Türkiye'de Bağlantılı Araç Teknolojisinin Gelişimi. *Avrupa Bilim ve Teknoloji Dergisi*, (37), 139-146.

23. İnternet: Evensen K., Fischer H.-J., Hoefs W., and Sill J. (2012). *EU-US standards harmonization task group report: Feedback to ITS standards development organizations–communications*, URL: https://rosap.ntl.bts.gov/view/dot/26509, Son Erişim Tarihi: 21.04.2022.

24. ETSI. (2019). EN 302 637-2 V1.4.1. Intelligent Transport Systems (ITS); Vehicular Communications, Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service.

25. ETSI. (2019). ETSI EN 302 637-3 V1.3.1 Intelligent Transport Systems (ITS); Vehicular Communications, Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service.

26. Singh, P. K., Nandi, S. K., and Nandi, S. (2019). A tutorial survey on vehicular communication state of the art, and future research directions. *Vehicular Communications*, 18, 100164.

27. ETSI. (2010). ETSI TS 102 637-1 V1.1.1Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 1: Functional Requirements.

28. Haidar, F., Kaiser, A., and Lonc, B. (2017). On the performance evaluation of vehicular PKI protocol for V2X communications security. *IEEE 86th vehicular technology conference (VTC-Fall),* 1-5.

29. ETSI. (2018). TR 103 415 V1.1.1 - Intelligent Transport Systems (ITS); Security; Pre-standardization study on pseudonym change management.

30. Choi, J., Marojevic, V., Dietrich, C. B., Reed, J. H., and Ahn, S. (2020). Survey of spectrum regulation for intelligent transportation systems. *IEEE Access*, 8, 140145-140160.

31. Levin, M. W., Chen, R., Hourdos, J., and Duhn, M. (2021). Generating Traffic Information from Connected Vehicle V2V Basic Safety Messages No. MN 2021-08. Minnesota Department of Transportation Research Services & Library.

32. Naik, G., Choudhury, B., and Park, J. M. (2019). IEEE 802.11 bd & 5G NR V2X: Evolution of radio access technologies for V2X communications. *IEEE access*, 7, 70169-70184.

33. İnternet: Status of Project IEEE P802.11bd. (2022). URL: http://www.ieee802.org/11/Reports/tgbd_update.htm, Son Erişim Tarihi: 12.04.2022.

34. Arena, F., Pau, G., and Severino, A. (2020). A review on IEEE 802.11 p for intelligent transportation systems. *Journal of Sensor and Actuator Networks*, 9(2), 22.

35. Yang, Y., Wei, Z., Zhang, Y., Lu, H., Choo, K.-K. R., and Cai, H. (2017). V2X security: A case study of anonymous authentication, *Pervasive and Mobile Computing,* 41, 259–269.

36. Giannetsos, T., and Krontiris, I. (2019). Securing V2X Communications for the Future: Can PKI Systems offer the answer?.*14th International Conference on Availability, Reliability and Security*,1-8.

37. Wasef, A., Jiang, Y., and Shen, X. (2009). DCS: An efficient distributed-certificate-service scheme for vehicular networks. *IEEE Transactions on Vehicular Technology*, 59(2), 533-549.

38. Brecht, B., and Hehn, T. (2019). A security credential management system for V2X communications. *Connected Vehicles*. Springer, Cham,83-115.

39. Huang, J., Fang, D., Qian, Y., and Hu, R. Q. (2010). Recent advances and challenges insecurity and privacy for v2x communications, *IEEE Open Journal of VehicularTechnology*, 1,244–266.

40. İnternet: Group Signature. (2021). URL: https://en.wikipedia.org/wiki/Group_signature, Son Erişim Tarihi: 15.11.2021.

41. Hasrouny, H., Samhat, A.E., Bassil, C. and LAouiti, A. (2017). VANet security challenges and solutions: A survey. *Vehicular Communications*, 7, 7-20.

42. Lin, X., and Li, X. (2013). Achieving efficient cooperative message authentication in vehicular ad hoc networks. *IEEE Transactions on Vehicular Technology,* 62(7), 3339-3348.

43. Jiang, S., Zhu, X., and Wang, L. (2016), An efficient anonymous batch authentication scheme based on HMAC for VANETs, *IEEE Transactions on Intelligent Transportation Systems*, 17(8), 2193-2204.

44. İnternet: HMAC. (2021). URL: https://tr.wikipedia.org/wiki/HMAC, Son Erişim Tarihi: 17.11.2021.

45. İnternet: Nakamoto S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System, URL: https://bitcoin.org/bitcoin.pdf, Son Erişim Tarihi: 02.01.2022.

46. İnternet: Blokzincir Teknolojileri. (2018). URL: https://blokzincir.bilgem.tubitak.gov.tr/bz-calistay/blok-zincir.html, Son Erişim Tarihi: 17.11.2021.

47. Shrestha, R., Bajrachar,y R., Shrestha, A.P., and Namb, S.Y. (2020). A new type of blockchain for secure message exchange in VANET, *Digital Communication and Networks* 6,177-186.

48. Singh, M. and Kim, S. (2017). Blockchain Based Intelligent Vehicle Data sharing framework. *arXiv preprint*,1708.09721.

49. Calvo, J.A.L. and Mathar, R. (2018). Secure Blockchain-Based Communication Scheme for Connected Vehicles. *The 2018 IEEE European Conference on Networks and Communications*, 347-351.

50. Smith, T., Dickinson, L., and Seamons, K. (2020). Let's revoke: Scalable global certificate revocation. *Network and Distributed Systems Security (NDSS) Symposium*.

51. Santesson, S., Myers, M., Ankney, R., Malpani, A., Galperin, S., and Adams, C. (2013). X. 509 Internet Public Key Infrastructure Online Certificate Status Protocol-OCSP. RFC, 6960, 1-41.

52. Housley, R., Ford, W., Polk, W., and Solo, D. (2008). RFC 5280: Internet x. 509 public key infrastructure certificate and crl profile.

53. Viriyasitavat, W., Bai, F., ve Tonguz, O. K. (2011). Dynamics of network connectivity in urban vehicular networks. *IEEE Journal on Selected Areas in Communications*, 29(3), 515-533.

54. Laurendeau, C., and Barbeau, M. (2007). Secure anonymous broadcasting in vehicular networks. *32nd IEEE Conference on Local Computer Networks*, 661-668.

55. Studer, A., Shi, E., Bai, F., and Perrig, A. (2009). TACKing together efficient authentication, revocation, and privacy in VANETs. *2009 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*,1-9.

56. Shao, J., Lin, X., Lu, R., and Zuo, C. (2015). A threshold anonymous authentication protocol for VANETs. *IEEE Transactions on vehicular technology*, 65(3), 1711-1720.

57. Li, L., Liu, J., Cheng, L., Qiu, S., Wang, W., Zhang, X., and Zhang, Z. (2018). Creditcoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 19(7), 2204-2220. 22.

58. Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and Polk, W. (2008). Internet X. 509 public key infrastructure certificate and certificate revocation list (CRL) profile.

59. Slavik, M., and Mahgoub, I. (2012). Spatial distribution and channel quality adaptive protocol for multihop wireless broadcast routing in VANET. *IEEE Transactions on Mobile Computing*, 12(4), 722-734.

60. Martín-Fernández, F., Caballero-Gil, P., and Caballero-Gil, C. (2015). Revocation management in vehicular ad-hoc networks. *2015 IEEE Trustcom/BigDataSE/ISPA*, 1210-1217.

61. Zhang, L., Wu, Q., Solanas, A., and Domingo-Ferrer, J. (2009). A scalable robust authentication protocol for secure vehicular communications. *IEEE Transactions on vehicular Technology,* 59(4), 1606-1617.

62. Whyte, W., Weimerskirch, A., Kumar, V., and Hehn, T. (2013). A security credential management system for V2V communications. *2013 IEEE Vehicular Networking Conference*,1-8.

63. Ferraz, L. T. D. (2019). Methods to improve certificate linkage and revocation procedures in vehicular networks (Doctoral dissertation,2019), 25-32.

64. İnternet: The U.S. Department of Transportation, Security Credential Management System. (2017). URL: https://www.its.dot.gov/factsheets/pdf/CV_SCMS.pdf, Son Erişim Tarihi: 21.04.2022.

65. İnternet: SCMS CV Pilots Documentation. (2018). URL: https://wiki.campllc.org/display/SCP/SCP1%3A+Butterfly+Keys, Son Erişim Tarihi: 21.04.2022.

66. ETSI. (2021).TS 103 097 V1.3.1-Intelligent Transport Systems (ITS) Security; Security Header and Certifiacte formats.

67. Kondareddy, Y., Di Crescenzo, G., and Agrawal, P. (2010). Analysis of certificate revocation list distribution protocols for vehicular networks. *2010 IEEE Global Telecommunications Conference GLOBECOM* 2010,1-5.

68. Tuladhar, K. M., and Lim, K. (2018). Efficient and scalable certificate revocation list distribution in hierarchical VANETs. *IEEE International Conference on Electro/Information Technology*, 0620-0625.

69. Lu, Z., Wang, Q., Qu, G., and Liu, Z. (2018). BARS: A blockchain-based anonymous reputation system for trust management in VANETs. *2018 17th IEEE International Conference on Trust, Security and Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*,98-103.

70. Malik, N., Nanda, P., Arora, A., He, X., and Puthal, D. (2018). Blockchain based secured identity authentication and expeditious revocation framework for vehicular networks. *2018 17th IEEE International Conference on Trust, Security and Privacy In Computing and Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, 674-679.

71. Ibarz, J. C. C. (2020). Bringing JSON signatures to ETSI AdES framework: Meet JAdES signatures. *Computer Standards & Interfaces*, 71, 103434.

72. Erceylan, G. and Akcayol, M.A. (2022). Trust-Chain-Based Certificate Revocation Control in Autonomous Vehicle Networks, *In 2022 International Conference on Information and Communications Technology (ICOIACT)*, IEEE
.

73. İnternet: Scott E. Carpend. (2014). URL: https://www.nsnam.org/doxygen/vanet-routing-compare_8cc.html, Son Erişim Tarihi: 21.04.2022.

74. Ghosal A. and Conti M. (2020). Security issues and challenges in V2X: A survey. *Computer Networks*, 169, 107093.

75. Choi, J., Marojevic, V., Dietrich, C. B., Reed, J. H., and Ahn, S. (2020). Survey of spectrum regulation for intelligent transportation systems. *IEEE Access*, 8, 140145-140160.

76. Kim, J. W., Kim, J. W., and Jeon, D. K. (2018). A Cooperative Communication Protocol for QoS Provisioning in IEEE 802.11 p/Wave Vehicular Networks. *Sensors*, 18(11), 3622.

77. İnternet: Vehicle-to-Vehicle Communications Research Project (V2V-CR). (2015). URL: https://www.campllc.org/vehicle-to-vehicle-communications-research-project-v2v-cr/, Son Erişim Tarihi: 02.12.2021.

EKLER

Ek- 2: V2X Projeleri ve Testler [74, 75, 76, 77]

Proje Adı	Proje Başlangıç Tarihi	Ülke/Bölge
SmartWay	2004	Japonya
U-TRANSPORTATION	2006	Güney Kore
SAFESPOT	2006	İtalya
SMART highway	2008	Güney Kore
sim^{TD}	2008	Almanya
EVITA	2008	Avrupa Birliği
SCORE@F	2010	Fransa
CopITS	2010	Katar
OVERSEE	2010	Avrupa Birliği
ETC2.0	2011	Japonya
PRESERVE	2011	Hollanda
ISE	2014	Fransa
BMW Connected Car	2015	Almanya
V2V-CR	2015	ABD
NYCDOT	2015	ABD
THEA	2015	ABD
WYDOT	2015	ABD
NORDICWAY	2015	Avrupa
IoV R&D Pilot zone Hangzhou	2017	Çin
IoV test -Guangzhou Nansha	2017	Çin
IoV Pilot zone Changsha	2018	Çin
i-VISTA IoV Test zone Chongqing	2018	Çin
Dicity Pilot zone Deyang	2018	Çin
China-German Pilot zone Chengdu	2018	Çin
IoV&ITS Pilot zone Wuhan	2019	Çin

Ek- 3: ETSI ITS Temel Uygulama Seti [27]

Uygulama Sınıfı	Uygulama	Kullanım Alanı
Aktif yol güvenliği	Sürüş yardımı-karşılıklı iş birliği	Acil durum aracı Yavaş araç göstergesi Kavşak-çarpışma Yaklaşan motosiklet Araç sollama
	Sürüş yardımı-yol tehlikesi uyarısı	Acil durum elektronik fren lambaları Ters yönde sürüş Hareketsiz araç Trafik durumu Sinyal ihlali Yol çalışması Çarpışma riski
Kooperatif trafik verimliliği	Hız yönetimi	
	Ortak navigasyon	
	Diğer	Platoon
		Uyarlanabilir hız sabitleyici
Kooperatif yerel servisler	Lokasyon tabanlı servisler	Otomatik giriş kontrolü Park yönetimi Medya indirme
Küresel internet servisleri	Topluluk servisleri	Sigorta ve finansal servisler Filo yönetimi
	ITS-S yaşam döngüsü	Araç yazılımı-veri sağlama, güncelleme
		Araç-RSU veri kalibrasyonu
	Diğer	Anlık mesaj
		Kişisel veri senkronizasyonu
		Çalıntı araç uyarısı

Ek- 4: BSM Mesaj İçeriği [76]

Bilgi Tipi	Tanımı
DSRCmsgID	Mesaj tipini tanımlamak için her mesajda kullanılan veri elemanlarıdır.
MsgCount	Aynı mesaj göndericisinden alınan aynı DSRCmsgID'ye sahip ardışık mesajların akışı kontrol edilir.
TemporaryID	4 baytlık bir geçici aygıt tanımlayıcısını temsil eder. Bir mobil OBU cihazında kullanıldığında, anonimliği sağlamak için bu değer periyodik olarak değiştirilir.
Dsecond	İki baytlık zaman bilgisini temsil eder.
Latitude	Bir nesnenin coğrafi enlemini temsil eder.
Longitude	Bir nesnenin coğrafi boylamını temsil eder.
Elevation	WGS84 koordinat sistemi tarafından ölçülen yüksekliği temsil eder.
PositionAccuracy	Verilen her eksen için konumlandırma doğruluğunu modellemek için kullanılan çeşitli kalite parametreleridir.
TransmissionAndSpeed	Aracın hızını temsil eder.
Heading	Geçerli yön değeridir, 0,0125 derecelik birimlerle ifade edilir.
SteeringWheelAngle	Direksiyon simidinin mevcut direksiyon açısını temsil eder.
AccelerationSet4Way	Üç ortogonal ivme ve sapma oranı bilgilerini içermektedir.
BrakeSystemStatus	Aracın frenlenmesiyle ilgili çeşitli kontrol durumlarını kaydeden bir veri öğesini temsil eder.
VehicleSize	Aracın uzunluğunu ve genişliğini temsil eder.

Ek- 5: Siber Saldırılar [74]

Saldırı Sınıfı	Saldırı	Saldırı Tanımı	Güvenlik İhlali
Davranış Modeline Dayalı Saldırılar	Sahte Mesaj	Yanlış konum bilgisi veren, yazılım ve donanımı etkileyen saldırılardır.	Kimlik doğrulama, Erişilebilirlik, Bütünlük
	Trafik Analizi	Ağın dinlendiği ve dinleme sırasında toplanan verilerin analiz edildiği kablosuz iletişim saldırılarıdır.	Gizlilik, Mahremiyet
	Gizli Dinleme	İletişim ortamının dinlenip bilgilerin toplandığı kablosuz iletişim saldırılarıdır.	Kimlik doğrulama Mahremiyet
	Ret Saldırısı	Olay izlenebilirliğinin kaybına neden olan kablosuz iletişim saldırılarıdır.	İnkar edilemezlik
	Mesaj Tekrarlama	Bir önceki mesajın düzenli aralıklarla tekrar gönderilmesi ile yapılan saldırıdır.	Kimlik doğrulama, Erişilebilirlik, İnkar edilemezlik
	Sybil	Aynı kimliğe sahip birden fazla aracın yaratıldığı saldırılardır.	Kimlik doğrulama, Erişilebilirlik
	DoS	Ağ servislerinin kullanılabilirliğini hedef alan saldırılardır.	Kimlik doğrulama, Erişilebilirlik
	Zararlı Kod	Zararlı bilgilerin kod formatında iletilmesiyle gerçekleştirilen saldırılardır.	Erişilebilirlik
	Kara Delik	Alınan paketlerin yönlendirilmesinin engellenmesiyle yapılan saldırılardır.	Erişilebilirlik
Donanım ve Yazılım Üzerine Yapılan Saldırılar	Ortadaki Adam Saldırısı	İletişim kuran iki araç arasındaki iletişimin kontrol altına alınması ile gerçekleştirilen saldırılardır.	Kimlik doğrulama, Gizlilik, Bütünlük
	Kaba Kuvvet	Ağ servislerini etkileyen saldırılardır.	Kimlik doğrulama, Gizlilik

Ek- 6: (devam) Siber Saldırılar

Saldırı Sınıfı	Saldırı	Saldırı Tanımı	Güvenlik İhlali
Altyapı Saldırıları	Oturum Kaçırma	Oturumun kontrol altına alınmasıyla yapılan saldırılardır.	Gizlilik, Erişilebilirlik
	DDoS	Saldırganların saldırdıkları sunucunun işlem kapasitesini aşacak ve doğru çalışmasını engelleyecek sayıda istek göndermesi ile gerçekleştirilen saldırılardır.	Kimlik doğrulama, Erişilebilirlik
	Yetkisiz Erişim	Ağ hizmetlerine zorla erişim sağlanarak gerçekleştirilen saldırılardır.	Gizlilik, Mahremiyet
	Kurcalama Saldırısı	Araç üzerindeki özel verilere erişim sağlanarak ya da araca veriler yüklenerek gerçekleştirilen saldırılardır.	Gizlilik, Mahremiyet
	Maskeli Balo	Saldırganın kendini gizlemek için geçerli bir kimlik veya maske kullandığı saldırılardır.	Kimlik doğrulama, Bütünlük, İnkar edilemezlik
Mahremiyet Saldırıları	Kimlik Gösterme	Kişisel bilgilerin mahremiyetinin tehlikeye atıldığı saldırılardır.	Kimlik doğrulama, Mahremiyet
	Konum Takibi	Aracın konumunun ve rotasının takip edilmesi ile gerçekleştirilen saldırılardır.	Mahremiyet
Veri Doğruluğu Saldırıları	Mesaj Kurcalama	Mevcut olan verilerin silindiği veya olmayan verilerin oluşturulduğu saldırılardır.	Kimlik doğrulama, Erişilebilirlik, Bütünlük, İnkar edilemezlik
	Gizli Araç	Araçların konum ve pozisyonları ile ilgili yanlış bilgilerin üretildiği saldırılardır.	Kimlik doğrulama, Bütünlük, İnkar edilemezlik
	Yanılsama	Yanlış verilerin üretilmesi ile gerçekleştirilen saldırılardır.	Kimlik doğrulama, Bütünlük

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı : ERCEYLAN, Gizem
Uyruğu : T.C.

Eğitim

Derece	Eğitim Birimi	Mezuniyet Tarihi
Yüksek Lisans	Gazi Üniversitesi / Bilişim Sistemleri	Devam Ediyor
Lisans	İzmir Ekonomi Üniversitesi/Elektrik-Elektronik Mühendisliği	2017

İş Deneyimi

Yıl	Yer	Görev
2019-Halen	TÜBİTAK BİLGEM	Araştırmacı
2017-2018	TURKCELL	Ağ Mühendisi

Yabancı Dil

İngilizce

Yayınlar

1. Erceylan, G., ve Akcayol, M. A. (2022). Türkiye'de Bağlantılı Araç Teknolojisinin Gelişimi. *Avrupa Bilim ve Teknoloji Dergisi*, (37), 139-146.

2. Erceylan, G. and Akcayol, M. A. (2022). Trust-Chain-Based Certificate Revocation Control in Autonomous Vehicle Networks. *In 2022 International Conference on Information and Communications Technology (ICOIACT)*, IEEE.

GAZİLİ OLMAK AYRICALIKTIR…