T.C. İSTANBUL TİCARET ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

GENİŞLETİLMİŞ ENERJİ DEDEKTÖR TABANLI UZAKTAN KUMANDALI ANAHTARSIZ GİRİŞ SİSTEMLERİNİN VERİCİLERİ İÇİN İSTATİSTİKSEL MODÜLASYON TİPİ TANIMLAYICISI

Özgür ALACA

Danışman
Doç. Dr. Serhan YARKAN

YÜKSEK LİSANS TEZİ
ELEKTRONİK VE HABERLEŞME MÜHENDİSLİĞİ ANABİLİM DALI
İSTANBUL – 2020

KABUL VE ONAY SAYFASI

Özgür ALACA tarafından hazırlanan **"Genişletilmiş Enerji Dedektör Tabanlı Uzaktan Kumandalı Anahtarsız Giriş Sistemlerinin Vericileri İçin İstatistiksel Modülasyon Tipi Tanımlayıcısı"** adlı tez çalışması 07/09/2020 tarihinde aşağıdaki jüri üyeleri önünde başarı ile savunularak, İstanbul Ticaret Üniversitesi Fen Bilimleri Enstitüsü **Elektronik ve Haberleşme Mühendisliği Anabilim Dalı**'nda **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Danışman	**Doç. Dr. Serhan YARKAN** İstanbul Ticaret Üniversitesi
Jüri Üyesi	**Dr. Öğr. Üyesi Ali BOYACI** İstanbul Ticaret Üniversitesi
Jüri Üyesi	**Doç. Dr. Muhammed Ali AYDIN** İstanbul Üniversitesi - Cerrahpaşa

Onay Tarihi : 18.09.2020

İstanbul Ticaret Üniversitesi, Fen Bilimleri Enstitüsünün 18.09.2020 tarih ve 2020/290 numaralı Yönetim Kurulu Kararının 2. maddesi gereğince, ders yüklerini ve tez yükümlülüğünü yerine getirdiği belirlenen "Özgür Alaca" (TC: 64528146220) adlı öğrencinin mezun olmasına oy birliği ile karar verilmiştir.

Prof. Dr. Necip ŞİMŞEK
Enstitü Müdürü

AKADEMİK VE ETİK KURALLARA UYGUNLUK BEYANI

İstanbul Ticaret Üniversitesi, Fen Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında,

- tez içindeki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi,
- görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu,
- başkalarının eserlerinden yararlanılması durumunda ilgili eserlere bilimsel normlara uygun olarak atıfta bulunduğumu,
- atıfta bulunduğum eserlerin tümünü kaynak olarak gösterdiğimi,
- kullanılan verilerde herhangi bir tahrifat yapmadığımı,
- ve bu tezin herhangi bir bölümünü bu üniversitede veya başka bir üniversitede başka bir tez çalışması olarak sunmadığımı

beyan ederim.

18/09/2020

Özgür ALACA

İÇİNDEKİLER

Sayfa

ÖZET

Yüksek Lisans Tezi

GENİŞLETİLMİŞ ENERJİ DEDEKTÖR TABANLI UZAKTAN KUMANDALI ANAHTARSIZ GİRİŞ SİSTEMLERİNİN VERİCİLERİ İÇİN İSTATİSTİKSEL MODÜLASYON TİPİ TANIMLAYICISI

Özgür ALACA

İstanbul Ticaret Üniversitesi
Fen Bilimleri Enstitüsü
Elektronik ve Haberleşme Mühendisliği Anabilim Dalı

Danışman: Doç. Dr. Serhan YARKAN

2020, 37 sayfa

Uzaktan kumandalı anahtarsız giriş (RKE) sistemleri modern günlük yaşamın ayrılmaz bir parçasıdır. Araçlara erişim ve ev, garaj ve tesis alarm sistemleri kurma/devre dışı bırakma gibi günlük yaşamımızın birçok yerinde RKE sistemlerini örnek olarak görebiliriz. RKE sistemlerinin erişim ve yetkilendirme gibi ön plana çıkan avantajlara sahip olmasına rağmen herhangi bir güvenlik ihlali çok kötü sonuçlara neden olmaktadır. Bu nedenle, üreticiler RKE sistemlerinin güvenliklerini güçlendirmek için sürekli olarak yeni yöntemler ve teknikler geliştirmektedir. İçsel güvenlik endişesi ile başa çıkmanın önde gelen yollarından biri, davetsiz misafirlerin saldırılarını yapmak için zamanları olmayacak şekilde hızlı bir kablosuz mesaj alışverişi mekanizması/protokolü oluşturmaktır. Son zamanlarda yazılım tanımlı radyoların gelişmesi ile beraber RKE geliştiricileri için mesaj iletim hızı çok önemli hale gelmiştir. Bu nedenle, bu tezdeki çalışmada, RKE sistemleri için bir istatistiksel modülasyon tipi tanımlayıcısı önerilmiştir. Alınan sinyalin karmaşık tabanbant eşdeğerli otomatik modülasyon tipi tanımlayıcısı ve otomatik mod detektörü kullanılarak, davetsiz misafir tarafındaki alıcı tarafından tahmin edilebilir darboğazlar tanımlanabilir ve detaylandırılabilinir. Ölçüm sonuçları ışığında, otomatik modülasyon tipi tanımlayıcısı ve otomatik mod detektörü, enerji tespiti için vazgeçilmez iki seri modül olduğu gösterilmiştir. Bu tez çalışmasında, bir davetsiz misafirin bir bağlantıyı ne kadar hızlı kurması gerektiğini ölçmek için karmaşık bir temel bant eşdeğerli dijital alıcısı önerilmiştir.

Anahtar Kelimeler: Enerji dedektörü, istatistiksel modülasyon, kablosuz mesaj değiştirme mekanizması/protokolü, uzaktan kumandalı anahtarsız giriş sistemleri, yazılım tanımlı radyo.

ABSTRACT

M.Sc. Thesis

A STATISTICAL MODULATION TYPE IDENTIFIER FOR REMOTE KEYLESS ENTRY TRANSMITTERS BASED ON EXTENDED ENERGY DETECTOR

Özgür ALACA

Istanbul Commerce University
Graduate School of Applied and Natural Sciences
Department of Electronics and Communication Engineering

Supervisor: Assoc. Prof. Dr. Serhan YARKAN

2020, 37 pages

Remote keyless entry (RKE) systems are an integral part of modern daily life. Vehicle access, drive authorization, and arming/disarming the alarm systems for houses, garages, and/or facilities are instances for popular uses of RKE. Despite their obvious advantages such as gaining access/authorization solely by carrying them, any security breach experienced with RKE could end up with cataclysmic consequences. Therefore, manufacturers continuously develop new methods and techniques to fortify their RKE systems. One of the prominent ways of tackling the inherent security concern is to establish a rapid wireless message exchange mechanism/protocol such that intruders could not have time to place their attacks. However, with recent advances in digital technology along with software defined radio, quantification of rapidness becomes crucial for RKE manufacturers. Therefore, in this study, a statistical modulation type identifier for remote keyless entry systems is proposed. Both an automatic modulation type identifier based on complex baseband equivalent of the received signal and an automatic mode detector are employed as an extension of the traditional energy detector. This way, presumable bottlenecks for the receiver at the intruder side are identified and elaborated. Measurement results are provided along with relevant discussions. Results demonstrate that frequency compensation along with energy detection are the two indispensable serial modules and provide the bottleneck for any receiver at intruder's side. In light of this proposed method, RKE system manufactures will design a more robust and faster message exchange mechanism/protocol against intruders to ensure security.

Keywords: Energy detector, remote keyless entry, software-defined radio, statistical modulation, wireless message exchange mechanism/protocol.

TEŞEKKÜR

Bu araştırmanın gerçekleştirilmesinde, iki yıl boyunca değerli bilgilerini ve zamanını benimle paylaşan, desteğini esirgemeyen, beni yönlendiren ve karşılaştığım bütün zorlukları bilgisi, tecrübesi ve tüm samimiyeti ile aşmamda yardımcı olan değerli Danışman Hocam Doç. Dr. Serhan YARKAN'a teşekkürü bir borç bilir ve sonsuz şükranlarımı sunarım.

Yine araştırmalarımda konu, kaynak ve yöntem açısından bana sürekli yardımda bulunarak yol gösteren değerli Hocam Dr. Öğr. Üyesi Ali BOYACI'ya teşekkürlerimi iletmek isterim.

Ayrıca, araştırmamın yürütülmesinde teknik tartışmaları ve motivasyon desteğiyle bana sürekli yardımcı olan Sezer Can TOKGÖZ, Gamze KIRMAN TOKGÖZ, Göksel ÇANKAYA ve Tapir Lab.'daki bütün çalışma arkadaşlarıma teşekkür ederim.

Son olarak, hayatımın her aşamasında bana olan desteğini esirgemeyen ve manevi olarak yanımda olan anneme sonsuz sevgilerimi sunarım.

Özgür ALACA
İSTANBUL, 2020

ŞEKİLLER

Sayfa

SİMGELER VE KISALTMALAR

AWGN	Toplanır Beyaz Gauss Gürültüsü (Additive White Gaussian Noise)
CID	Müşteri Tanımlama Cihazı (Customer Identification Device)
CLT	Merkezi Limit Teorem (Central Limit Theorem)
DIP	Çift Sıralı Paket (Dual In-line Package)
E_k	Genlik
H_0	Hipotez 0
H_1	Hipotez 1
IoE	Nesnelerin İnterneti (Internet of Everything)
L	Çözümlenebilir Yol Sayısı
LTV	Doğrusal Zamanda Değişen (Linear Time Variant)
N	Rastgele Örneklem Sayısı
p_k	Darbe Biçimlendirme
PDF	Olasılık Yoğunluk Fonksiyonu (Probability Density Function)
RF	Radyo Frekansı (Radio Frequency)
RKE	Uzaktan Anahtasız Giriş (Remote Keyless Entry)
RKI	Uzaktan Anahtarsız Ateşleme (Remote Keyless Ignition)
RKS	Uzaktan Anahtarsız Sistem (Remote Keyless System)
ROC	Alıcının Çalışma Karakterisitiği (Receiver Operating Characteristic)
PKES	Pasif Anahtarsız Giriş ve Başlatma (Passive Keyless Entry and Start)
SDR	Yazılım Tanımlı Radyolar (Software Defined Radio)
SINR	Sinyal-Parazit Artı Gürültü Oranı (Signal to Interface Plus Noise Ratio)
SNR	Sinyal-Gürültü Oranı (Signal to Noise Ration)
T_p	Etkin Darbe Genişliği
T_l	l-inci bağlantıya karşılık gelen gecikme
VSA	Vektör Sinyaşl Analizörü (Vector Signal Analyzer)
θ_k	Faz
$a(t)$	Havadan İletilen Mesaj Sinyali
$\alpha_l(t)$	l-inci bağlantının kazanç değeri
$d(t)$	Karar İstatistiği
$D(\cdot)$	Karar Mekanizması
$g_l(t)$	Gölge Solması
$f_{x_N^2}(n)$	Karar İstatiğinin Olasılık Yoğunluk Fonksiyonu
$n(t)$	Toplanır Beyaz Gauss Gürültüsü
$J_k(\cdot)$	Bessel Fonksiyonu
$Q_g(\cdot)$	Genelleştirilmiş Marcum-Q Fonksiyonu
$r(t)$	Alınan Sinyal
$S(\cdot)$	Algılama Tekniği
$x(t)$	Tahmin Edilen Veri Sinyalinin Karmaşık Tabanbant Eşdeğeri
$\mu_l(t)$	Yol Kaybı
$\delta(\cdot)$	Dirac Delta Fonksiyonu
$\Gamma(\cdot)$	Gamma Fonksiyonu
$\star$	Convolution Operasyonu
φ	Karar Eşiği
γ	Anlık SNR

1. GİRİŞ

Kablosuz haberleşme, modern günlük yaşamın her alanında kullanılmaktadır. Fiziksel bir bağlantını olmaması, sabit olmayan sistem olması (hareketlilik, mobility) ve iletim hızları gibi açıkça görünen yararları düşünüldüğünde, kablosuz haberleşmenin kullanımı gün geçtikçe sayısız uygulamalarda, hizmetlerde ve platformlarda kullanılmaktadır. Kablosuz haberleşme, sıradan ses iletilmesinden yongalar arası haberleşmeye kadar ortaya çıkan bütün akıllı alt yapılar ve şehirler, siber-fiziksel sistemler ve nesnelerin interneti gibi yeni nesil sistemlerde yer alması beklenmektedir. Kablosuz haberleşme bahsedilen önemli avantajlarının olmasına rağmen, kablosuz haberleşme ortamının genel yapısı nedeniyle gereği güvenlik sorunu teşkil etmektedir. Bu nedenle kablosuz haberleşme ile ilgili gelecekteki beklentiler kablosuz sistemlerin güvenlik altyapısını gelişmiş güvenlik özellikleri ve önlemleri ile güçlendirmektir.

Modern günlük yaşamda çok kullanılan bir kablosuz iletişim senaryosu, uzaktan anahtarsız giriş (remote keyless entry, RKE) gibi anahtarsız giriş sistemlerine dayanır. RKE sistemlerinin günümüzde popüler kullanım alanlarına örnek olarak: araç erişimi, sürüş yetkilendirme ve evler, garajlar ve/veya tesisler için kullanılan alarm sistemlerini kurma/devre dışı bırakma sunulabilir. RKE sistemlerinin açıkça görülen erişim ve yetkilendirme gibi önemli avantajları olmasına rağmen, herhangi bir güvenlik ihlali felaket ile sonuçlanabilir. Bu nedenle, bu alanda çalışan üreticiler kendi sistemlerinin güvenliğini geliştirmek ve oluşabilecek herhangi bir soruna karşı önlem almak için yeni yöntemler geliştirmiş ve hala geliştirmeye devam etmektedirler.

RKE sistemlerinin büyük çoğunluğunun çalışma aralıkları düşük olmasına rağmen, yansıma, saçılma ve çoklu yol mekanizmalar RKE sistemlerini birçok farklı saldırı yöntemlerine karşı savunmasız kılar. Kablosuz yayılma mekanizmalarından kaynaklanan zafiyetlerin yanı sıra dehşet verici sonuçlar dikkate alındığında, RKE'nin güvenliği azami özenle ele alınmalıdır.

Güvenilir RKE sistemi tasarlamak için eşzamanlı olarak aşağıda sıralan hususlara odaklanmak gerekmektedir:

- Hızlı işletim protokolü,
- Hassas zamanlama,
- Birden fazla müşteri tanımlama cihazı (customer identification device, CID),
- Düşük maliyet,
- Optimize edilmiş performans.

Hepsinden öte, hızlı bir çalışma protokolü, kötü niyetli saldırıların müdahale süresini en aza indirdiği için çok önemlidir. Fakat, bu husus üzerinde çalışan yazarların en iyi bilgisine göre "hızlı" bir protokol için net bir tanım yoktur. Tüm kablosuz iletişim sistemlerinin fiziksel katmandan başladığını göz önünde bulundurduğumuzda, açıkça gözükmektedir ki, sisteme zorla girmeye çalışan üçüncü şahısın fiziksel katmanının bir RKE mesaj sinyali değişimine ne kadar hızlı tepki vermesi, protokolün hızının ölçülmesi ile ilgili bir temel oluşturabilir. Bu nedenle, bu çalışmada, RKE sistemleri için istatistiksel çalışan bir modülasyon tipi tanımlayıcısı önerilmiştir. Bu öneri kapsamında, bu tezin iki yönlü katkısı aşağıda sunulmuştur:

1. Alınan sinyalin karmaşık temel bant eşdeğerine dayalı bir otomatik modülasyon tipi tanımlayıcısı.
2. Geleneksek enerji detektörün genişletilmiş versiyonu gibi çalışan hareketli ortalama filtre tabanlı otomatik modülasyon detektörü.

Tezin geri kalanının organizasyonu şu şekildedir: literatür Bölüm 2'de verilmiştir ve uzaktan kumandalı anahtarsız giriş sistemi Bölüm 3'te tartışılmıştır. Bölüm 4 ve Bölüm 5'de ayrıntılı bir analizle birlikte enerji detektörünün temel unsurları özetlenmektedir. Bölüm 6'da önerilen yöntemin ayrıntıları sağlanmış ve Bölüm 7'de bu yöntemler ışığında ölçüm ekipmanlarını ve izlenen prosedürü verir. Bölüm 8, önerilen yöntem ile oluşan sonuçları ve ilgili tartışmaları vermektedir. Son açıklamalar Bölüm 9 içerisinde verilmiştir.

2. LİTERATÜR ÖZETİ

Elektronik cihazlarındaki artan çeşitlik nedeniyle son yıllarda araçların güvenliği alanında çok sayıda araştırma yapılmıştır. Araştırma yapılan konular araçlara erişim kontrolünden gizlilik sorunlarına kadar uzanmaktadır. Araçlardaki güvenlik sorunlarının etkisi işleyişinin manipüle edilmesine veya çalınmasına izin veren bir aracın tam kontrolünün elde edilmesi ile sonuçlanabilir. Bu nedenle günümüz araçlarında veya farklı alanlarda kullanılan uzaktan anahtarsız giriş sistemleri güvenlik açığının en temel problemlerinden biri olarak gözükmektedir. Aşağıda bu husus üzerinde yapılan çalışmaların özeti verilmiştir.

Bir aracın (2000 İLE 2005 yılları arasında üretilmiş) RKE kodunu çözmeyen bir saldırı tekniği Cesare (2014) tarafından gösterilmiştir. Saldırgan bir birini takip eden Rolling kodları gizlice dinlemek zorundadır. Daha, sonra faz-uzay (phase-space) analizi kullanarak bir sonraki Rolling kodu için tahminde bulunabilme yeteneğine sahiptir. Ancak önerilen bu saldırı dışında otomotiv RKE sistemlerinin kriptografik güvenliği bilgimiz dahilinde araştırılmamıştır. Özellikle, RKE sistemler üzerine geniş ölçekli inceleme ve güvenlik analizi araştırmaları gerçekleştirilmemiştir.

Saldırgan tarafından araçları ele geçirmek adına kullanılan basit ama etkili bir yöntem ise araç sahibinin aracı uzak bir konumdan kilitlemeye çalıştığında haberleşmesini bozarak aracı ele geçirmektir. Araç sahibi saldırıyı fark etmeyebilir ve dolayısıyla aracı açık bırakabilir. Bu saldırının bir çeşidi seçici sinyal boğma (selective jamming) olarak adlandırılmaktadır. İletilen Rolling kod sinyali izlenir ve aynı frekansta sinyal boğma uygulanır ve bu sayede araç kapalı durumda değildir ve saldırgan geçici olarak (tek seferlik) Rolling koda sahip olmuştur. Bu yaklaşım ilk olarak Kasper vd. (2009) tarafından bahsedilmiş ve Kasper vd. (2011) ve Kampar (2015) tarafından deneysel olarak gösterilmiştir. İlgili araca Rolling kodun başarılı bir şekilde iletilmesinin ardından, önceden gizlice dinlenen tüm Rolling kodlar geçersiz olmaktadır. Yani saldırı için zaman aralığı çok azdır ve bu tez çalışmada bu konuya değinilmiştir. Ayrıca elde edilen Rolling kodların içeriklerini değiştirmek mümkün değildir. Örneğin bir "kilit"

komutunu “kilit açma” ya dönüştürmek mümkün değildir. Bu sınırlamalar Kampar (2011) çalışmasında görüleceği üzere bu tür saldırıların oluşturduğu tehdidi ciddi şekilde sınırlamaktadır.

Günümüzde modern araçlarda yaklaşık bir metrelik küçük bir çalışma aralığı ile çalışan çift yönlü bir meydan okuma-yanıt (bidirectional challenge-response) çalışma prensibine dayanan pasif anahtarsız giriş ve başlatma (passive keyless entry and start, PKES) sistemi kullanılmaktadır. Aracında yakınına gidildiğinde araç ile anahtar arasında bilgi alış-verişi gerçekleşmektedir (tezin ilerleyen bölümlerinde daha ayrıntılı anlatılmaktadır) ve geçerli bir yanıt kapıların kilidi açar, alarm sistemini devre dışa bırakır ve motorun çalışmasını sağlar. Ne yazık ki PKES sistemlerinde her kullanıcı etkileşimini gerektirecek butona basma gibi işlemler gerekmemektedir. Kullanıcı etkileşimini olmaması ve anahtar ile araç arasındaki challenge ve response sinyallerinin kablosuz ağ üzerinden iletilmesi röle saldırılarına (relay attack) karşı savunmasız bırakır. Bu konu üzerinde Francillon vd. (2011) tarafından çalışma yapılmasına rağmen günümüzde PKES sistemi içeren araçlar hala kullanılmaktadır. Bu problemi çözmek adına yeni nesil araçlar üzerinde bu tip saldırılara karşı koymak için yeni yöntemler geliştirilmektedir.

3. UZAKTAN ANAHTARSIZ GİRİŞ SİSTEMİ

Uzaktan anahtarsız giriş (remote keyless entry, RKE) sistemi genellikle güvenliği sağlamak, garajı açmak / kapatmak, arabanın kapı ve pencerelerini kilitlemek / açmak için daha uygun bir yöntem sağlamak için kullanılır ve ayrıca Nİ ile modern günlük yaşamın her alanında nüfuz etmiş ve kullanılmaktadır.

RKE, "uzaktan anahtarsız sistem (remote keyless system, RKS)" adı verilen daha geniş bir sınıfın alt kategorisidir. Araçlar düşünüldüğünde, UAS, 'nin yanında bir uzaktan ateşleme seçeneği içerir. RKE genellikle araçların kapılarını kilitlemek / açmak için kullanılır. Daha önceki ürünler, RKE ve uzaktan anahtarsız ateşleme (remote keyless ignition, RKI) için izole tasarımlar içermesine rağmen, çağdaş uygulamalar bunları belirli verici parametreleriyle tek bir çipte birleştiriyor.

RKE için en yaygın kullanılan cihazlar fob ve denetleyicilerdir. Genellikle anahtarlık olarak adlandırılan fob, periyodik olarak değişen rastgele erişim kodu oluşturarak kimlik doğrulama sağlayan bir güvenlik donanım cihazıdır. Genel olarak, anahtar fob, araç kapısını kilitlemek/açmak ve araçları devreye almak / devreden çıkarmak için kullanılır. Açık / kapalı garaj kapıları veya araçların güneşliği gibi temel amaçlar için küçük bir kontrolör kullanılır. Fob, anahtar zincirine sahiptir ve bu anahtarı küçük bir radyo vericisi kullanarak iletir. Fob üzerindeki düğmeye basıldığında verici açılır ve arabada veya garajda bağlı olan alıcıya kod gönderilir. Arabanın veya garajın içinde, vericinin kullandığı belirli frekansa ayarlanmış alıcı sinyali yakalar ve kodları karşılaştırır. Karşılaştırma sonucuna göre, alıcı bir yanıt verir (örneğin garaj kapısının açılması)

1950'lerde, RKE'nin vericisi, tek bir sinyal gönderen basit bir yapıyla oluşturuldu ve garaj kapısındaki alıcı bu sinyale garaj kapısını açarak veya kapayarak yanıt verdi. Tüm sistemler aynı frekansı kullandığından, yetkisiz davetsiz misafir basit bir verici ile kolayca bu frekansa ulaşabilir. Bu nedenle 1970'li yıllara gelindiğinde verici içindeki DIP anahtarları ayarlanarak vericinin gönderdiği kod kontrol edilmeye çalışıldı. Bu kontrol için kullanılan denetleyici çipi 8 minik anahtarı bulunan çift sıralı paket (dual in-line package, DIP) anahtarlamalıydı

(Şekil 3.1). Bu düzenleme yapıldıktan sonra garaj kapısı veya başka bir sistem, yalnızca alıcının DIP anahtarı aynı düzende ayarlanmışsa açılır. Bir miktar güvenlik sağlanmıştır, ancak çok fazla değildir, çünkü 8 DIP switch, tüm değerleri deneyerek kolayca bulunabilecek yalnızca 256 olası kombinasyon sağlar.

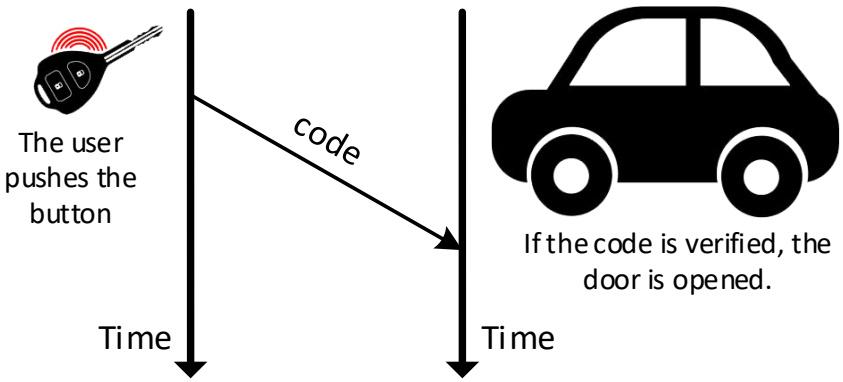
Şekil 3.1. Çift sıralı paket ve kontrol entegreli RKE.

İstenilen güvenlik düzeyi sağlanamadığı için yeni yöntemler geliştirilmiştir. Günümüzde kullanılan RKE sistemleri güvenlik sağlamak için rastgele 40 bitlik bir yuvarlanan kod oluşturan yalnızca bir denetleyici çipi kullanıyor. 40 bit ile yaklaşık 1 milyon olası kod oluşturulabilir. Her bir değeri deneyerek bu kodu çözmek zordur bu nedenle davetsiz misafirler Bölüm X'te belirtildiği gibi kodu çözmek için farklı yaklaşımlar yaratmıştır. Verici denetleyicisi ve alıcısı aynı sözde rasgele sayı üretecini kullanarak her bağlantıda değiştirilen 40 bitlik bir kodu tutacak bir belleğe sahiptir. Hem alıcı hem de verici senkronize olarak depolanan kodu değiştirir. Dahası, pasif anahtarsız giriş sistemi son zamanlarda daha yaygın hale geldi. Artık herhangi bir tuşa basmadan sadece arabaya belli bir mesafede yaklaşarak arabanın kapılarını açabiliyoruz. Ancak, bu sistemler röle saldırılarına açık sistemlerdir. Bu tip saldırıda izinsiz giriş yapmak isteyen kişiler arabanın yanında bekleyerek vericiden çıkan sinyalleri yakalar ve vericiye gitmesini engeller. Yakalanan sinyal diğer davetsiz misafire gider ve o kişi sinyali vericiye gönderir. Sinyal geldiğinde, arabanın kapısı açılır ve arabanın motoru çalıştırılabilir. Bahsedilen bu sistem yalnızca sinyal gücünü kullanmıştır, ancak RKE üreticileri bir mesafe ölçüm sistemi kullanan yeni bir sistem kullanmaktadır. Bu sistemde hem sinyal gücü hem de anahtar mesafesi eşzamanlı olarak ölçülür. Alıcı relay ile güçlendirilmiş sinyal geldiği zaman mesafeyi de kontrol eder ve röle saldırısı olup olmadığını tespit eder.

RKE sistemleri, bir anahtarlık (verici) ile ilgili araç arasındaki iletişime dayanır (Alrabady ve Mahmud, 2005). Bölümün devamında farklı kimlik doğrulama ve saldırı teknikleri vardır. Öncelikle 3 farklı aktarım tekniğinden bahsedilir ve ardından aktarım teknikleri dikkate alınarak 5 saldırı tekniğinden bahsedilir.

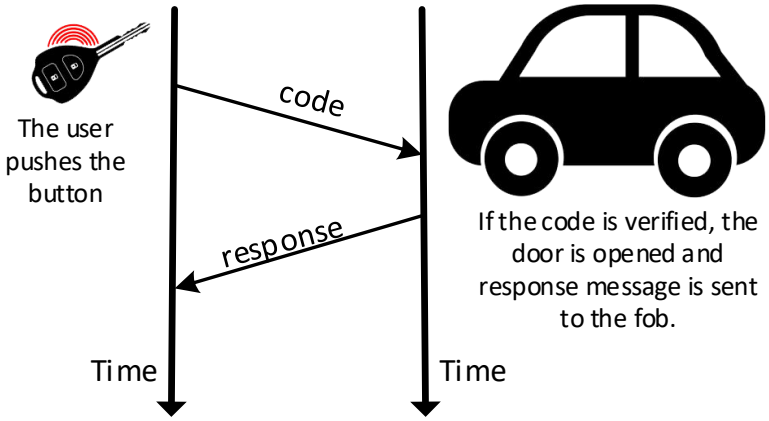
3.1. Doğrulama Teknikleri

Bu bölümde tek yönlü, çift yönlü RKE sistemleri ve pasif bir anahtarsız sistemler anlatılmıştır. Tek yönlü RKE sisteminde, kullanıcı kodu göndermek için fobundaki düğmeye basar. Araçtaki alıcı iletilen kodu algılar ve doğrularsa uygun işlemi gerçekleştirir (Şekil 3.2).



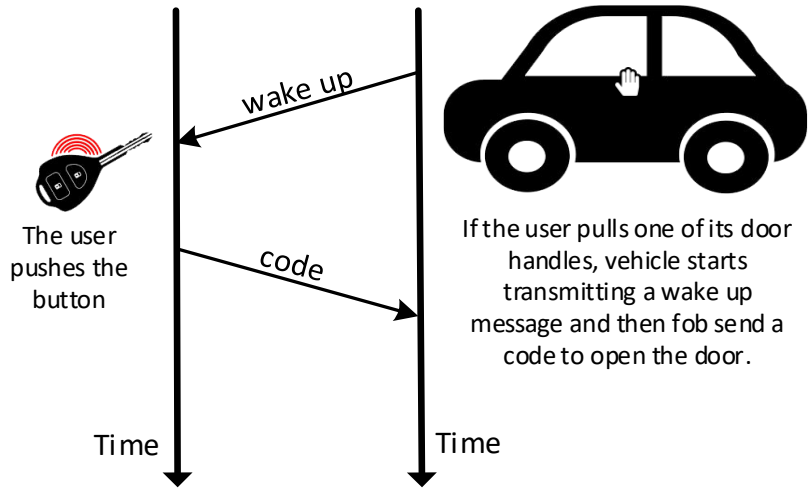
Şekil 3.2. Tek yönlü RKE sistemi.

İki yönlü RKE sisteminde, araç aşağıda gösterildiği gibi kullanıcıyı bilgilendirmek için bir yanıt mesaj sinyali gönderir (Şekil 3.3).



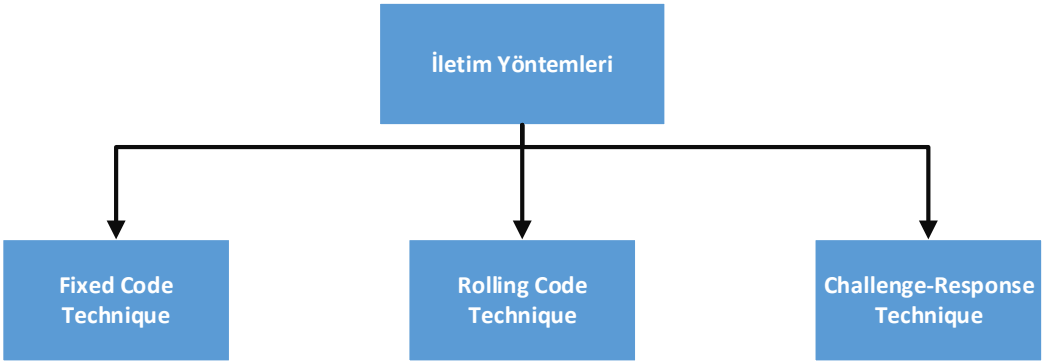
Şekil 3.3. Çift yönlü RKE sistemi.

Pasif anahtarsız RKE sisteminde, kullanıcı arabanın kapısından birini çektiğinde araçtaki alıcı sistemin modu "uyku modundan" "uyanma moduna" değiştirilir ve ardından araç anahtarlığa "uyanma" mesajı göndermeye başlar. Anahtarlık mesajı aldıktan sonra aracın kapısını açmak için araç alıcısına bir kod gönderir (Şekil 3.4). Tüm iletimler milisaniyeler içinde gerçekleşir, bu nedenle gecikme hissedemeyiz.



Şekil 3.4. Pasif anahtarsız RKE sistemi.

Mesajın araç ile anahtarlık arasında iletilmesi için birkaç iletim yöntemi kullanılır. Aşağıda bu tekniklerin kısa bir açıklaması verilmiştir (Şekil 3.5).



Şekil 3.5. RKE sistemlerindeki iletim yöntemleri.

3.1.1. Sabit kod (fixed-code) yöntemi

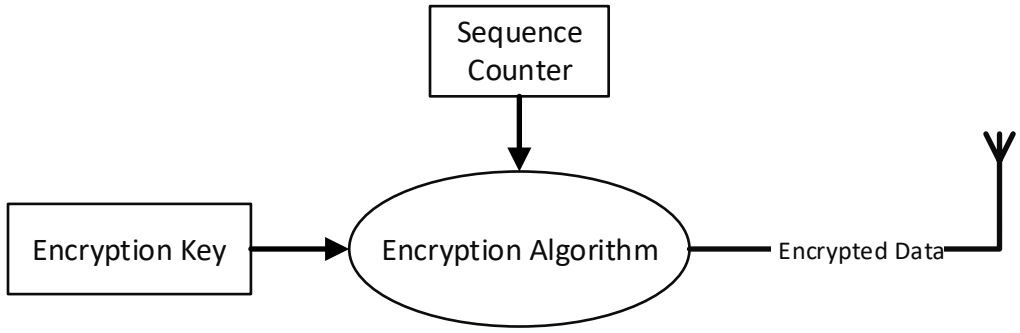
Bu teknikte, anahtarlık içinde önceden programlanmış sabit bir kod vardır. Anahtarlık çalıştığı zaman bu sabit kod alıcıya (araca) gönderilir. Kapsama dahilindeki araç tarafından sinyal alındığında, kod kontrol edilir ve kod eşleştiği zaman işlemler gerçekleştirilir. Bu teknikte anahtarlık her zaman sabit kod iletir bu yüzden bazı güvenlik sorunları ortaya çıkarır. İzinsiz giren kişi iletilen sabit kodu yakalayabilir ve kaydedebilir. Bu kod kaydedilirse daha sonradan davetsiz misafirler tarafından araca erişim için kullanılabilinir.

3.1.2. Döner kod (rolling-code) yöntemi

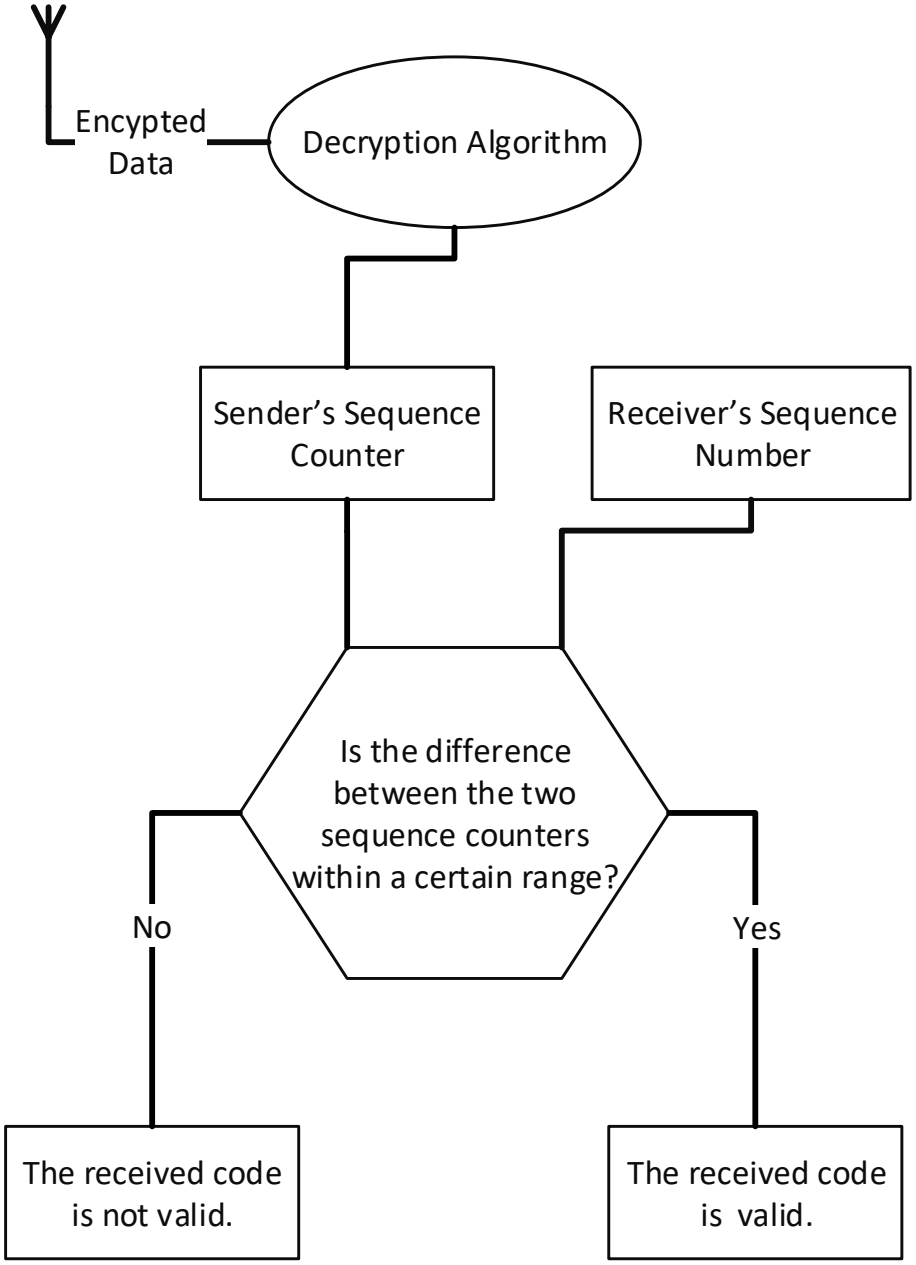
Bu mod, her iletimin farklı bir kod kullanacağı şekilde bir anahtarlama mekanizması kullanır. Bu modun öne çıkan yönlerinden biri, sistemin bir sonraki iletimde iletilecek kodu içeren bir dizi sayacını sürdürmesidir. Dönen kod sistemlerinin, hem fobdaki hem de ilgili araçtaki sıra sayaçlarını ayrı ayrı tutmaya dayandığını unutmayın. Doğrulama, gönderici tarafından iletilen şifresi çözülmüş dizi sayacını karşılaştırarak yerel ve şifresi çözülmüş değerler arasındaki farkın önceden belirlenmiş bir aralığa düşmesini sağlayarak oluşturulur. Yukarıda bahsedildiği gibi, Rolling kod tekniğinin hem kodlayıcısı hem de kod çözücüsü bir

dizi sayacına sahiptir. Anahtarlık, kodu sıra sayacı ile iletir ve ardından sıra sayacının içeriği artırılır. Şekil 3.6'daki diyagram Alrabady ve Mahmud'un (2005) makalesinden oluşturulmuştur.

İletimden sonra, şifrelenmiş veriler aracın alıcısı tarafından yakalanır ve kaydedilir. Alıcı, kaydedilen veriyi gönderenin sıra sayacına göre şifre çözme algoritması uygular. Anahtarlığın sıralama sayacı ve aracın sıra sayacı alıcı tarafından karşılaştırılır. İki sıra sayacı değeri arasındaki fark önceden tanımlanmış belirli bir aralık içindeyse, alıcı anahtarlıktan gelen kodu doğrular ve gerekli işlemi gerçekleştirir. Alıcının sıra sayacı da Şekil 3.7'de gösterildiği gibi tüm işlemlerden sonra artırılır. Şekil 3.6'daki diyagram Alrabady ve Mahmud'un (2005) makalesinden oluşturulmuştur.



Şekil 3.6. Döner kod yönteminin kodlayıcı (encoder) aşamasının blok diyagramı.

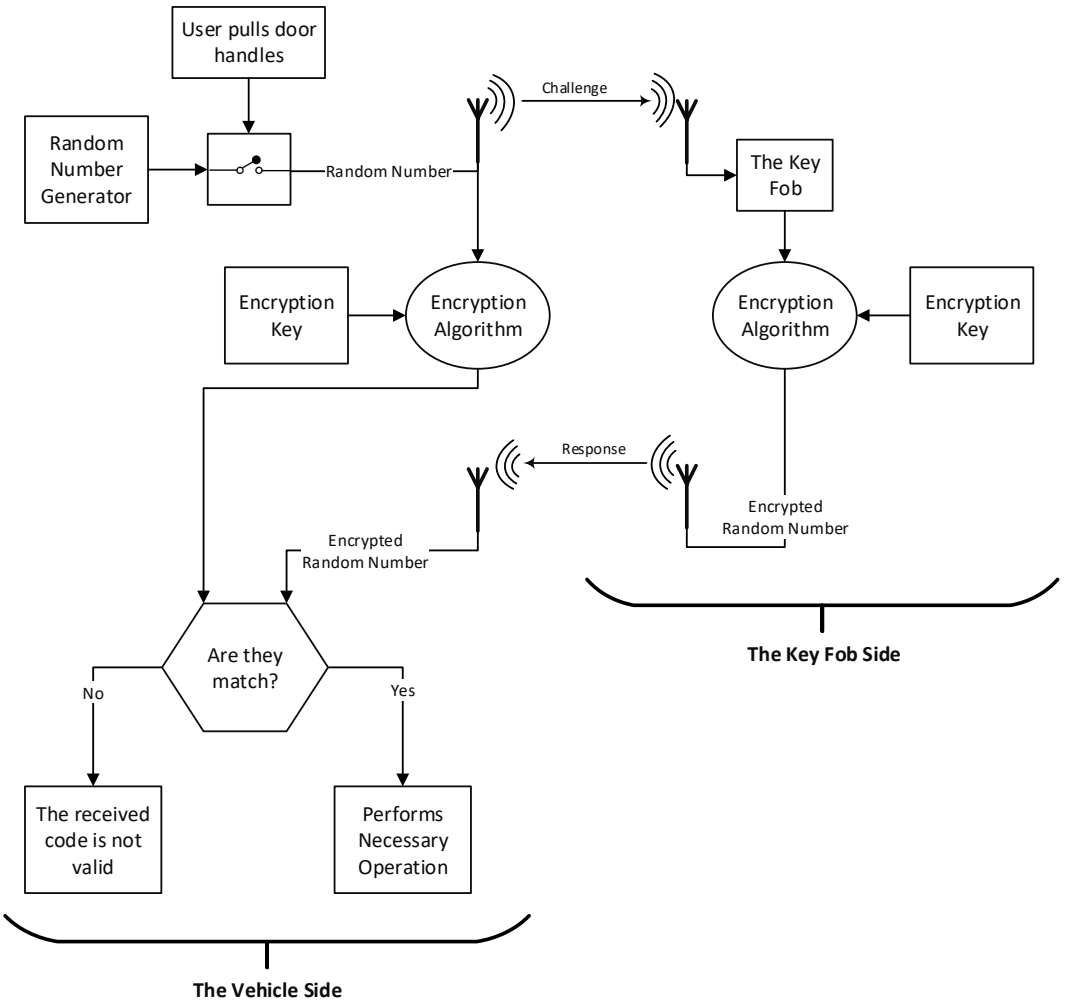


Şekil 3.7. Döner kod yönteminin kod çözme (decoder) aşamasının .blok diyagramı.

3.1.3. Karşılık verme (challenge response) yöntemi

Karşılık verme protokolünün diğer tekniklerden farkı, bu tekniğin iki yönlü bir iletime sahip olmasıdır. Anahtarın ve aracın aynı şifreye sahip olması prensibine dayanmaktadır. Araç sahibi arabanın kapı koluna dokunduğu zaman anahtar tetiklenir ve araca "meydan okuma" denilen rastgele ürettiği sayıyı gönderir. Alıcı, daha sonra, alınan rastgele numarayı şifreler ve geri gönderir. Geri

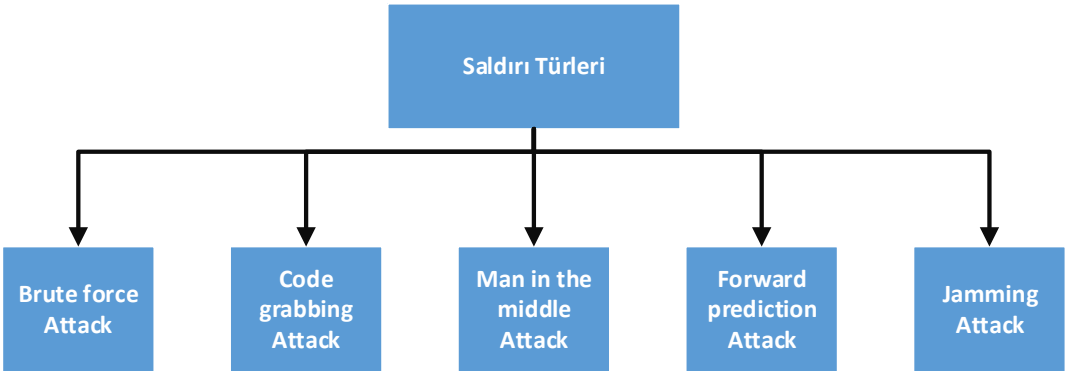
gönderilen bu sinyale “tepki” denir. Bu iletişim Şekil 3.8’ de verilmiştir. Meydan okuma ve tepki denilen bu şifreler eşleştiği taktirde prosedür başlatılır. (Bono et al., 2005; Indesteege et al., 2008; Verdult et al., 2015).



Şekil 3.8. Meydan okuma tekniğindeki alıcı verici blok diyagramı

3.2. RKE Sistemlerine Yapılan Saldırılar

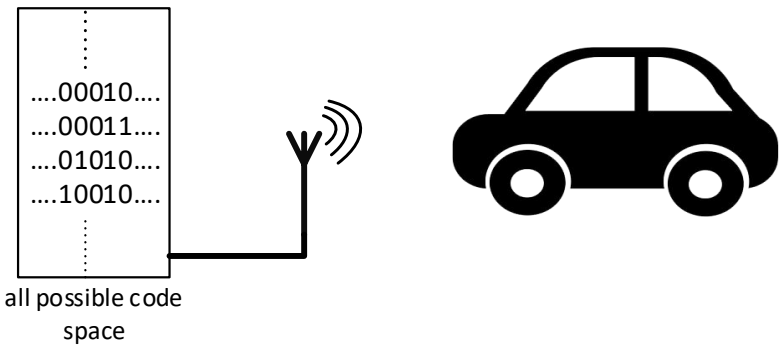
Bu bölümde araçlarda kullanılan RKE sistemlerine yapılan saldırılar açıklanmıştır. Şekil 3.9' da farklı saldırı tipleri gösterilmiştir.



Şekil 3.9. RKE sistemlerine uygulanan saldırı türleri.

3.2.1. Kaba kuvvet saldırısı (brute force attack)

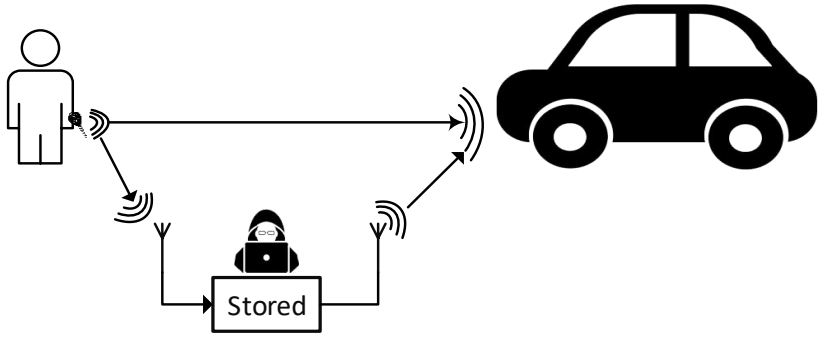
Adından da anlaşılacağı gibi, bu saldırı modu her tür RKE modu için olası tüm arama alanını tüketmeye çalışır. Yeterince geniş olan herhangi bir arama / anahtar alanı (Şekil 3.10) kaba kuvvet saldırısını engelleyebilir (Alrabady ve Mahmud., 2003).



Şekil 3.10. Kaba kuvvet saldırısı (frute force attack).

3.2.2. Kod yakalama saldırısı (code grabbing attack)

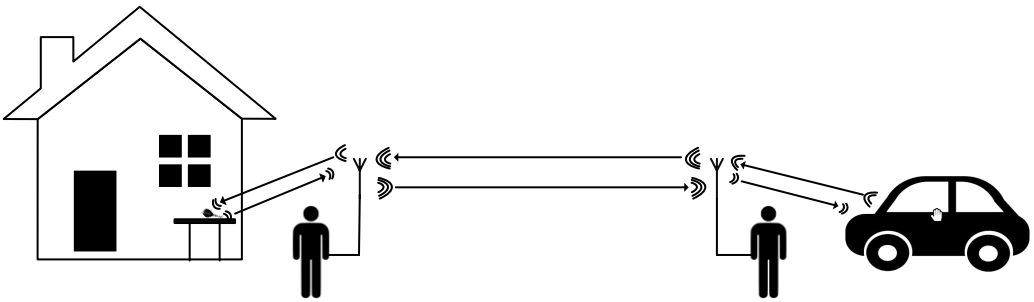
Verici ve alıcı arasındaki herhangi bir aktarım daha sonra kullanılmak üzere yakalanır ve saklanır. Kod sabit olduğundan, yakalanan veriler yetkisiz erişim elde etmek için kullanılabilir. Modların güvenlik modları bölümünde, yuvarlanan kodda ve meydan okumada, doğaları gereği kod yakalama saldırılarına karşı dirençli oldukları açıktır.



Şekil 3.11. Kod yakalama saldırıları (code grabbing attack).

3.2.3. Aradaki korsan saldırısı (man–in–the–middle attack)

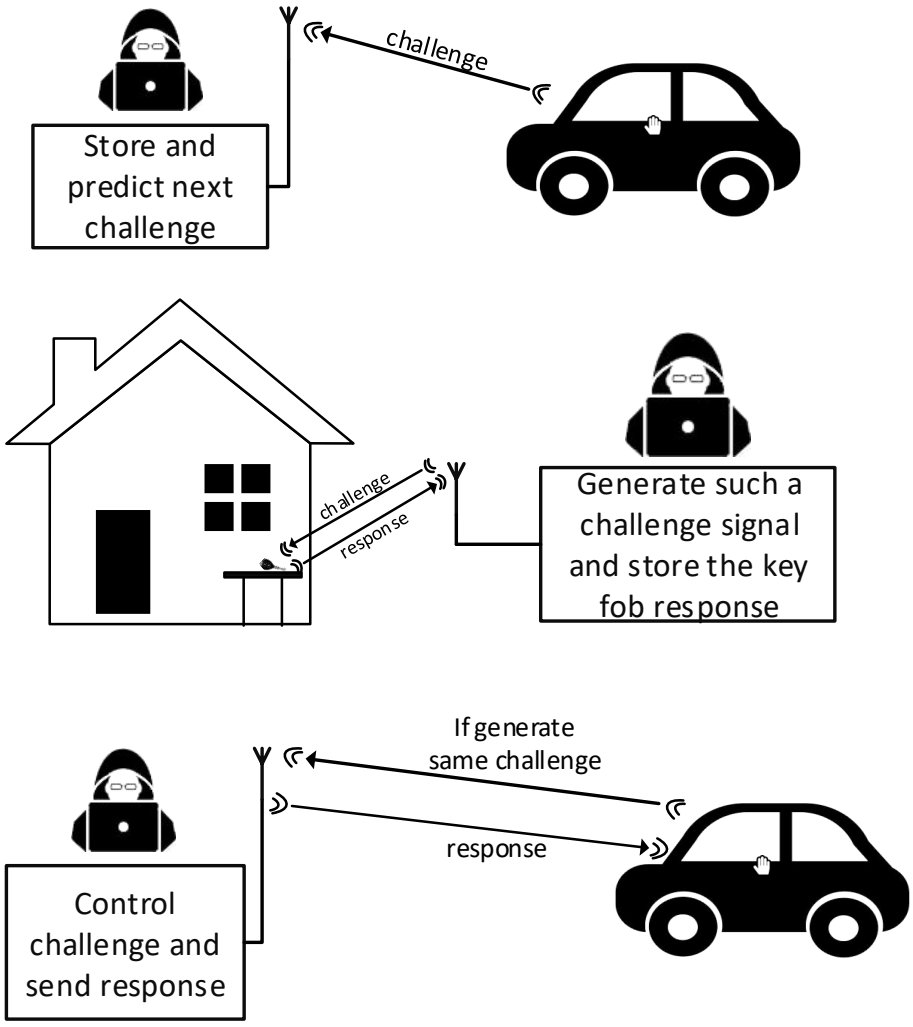
Bu saldırı biçiminde, uzaktan fiziksel olarak ayrılmış iki taraf, ortak bir iletişim bağlantısını paylaşır. İletişim bu bağlantı üzerinden sağlanır. (Francillon ve diğerleri, 2010). Bu şekilde, mesaj (iletişim) kötü niyetli amaçlar için tasarlanmış bağlantı üzerinden geçirilir (Yang ve diğerleri, 2012). Dönen kod ve meydan okuma-yanıt güvenlik modlarının bu tür saldırılara karşı savunmasız olduğunu unutmayın (Şekil 3.12).



Şekil 3.12. Aradaki korsan saldırısı (man-in-the-middle attack).

3.2.4. İleri tahmin saldırısı (forward–prediction attack)

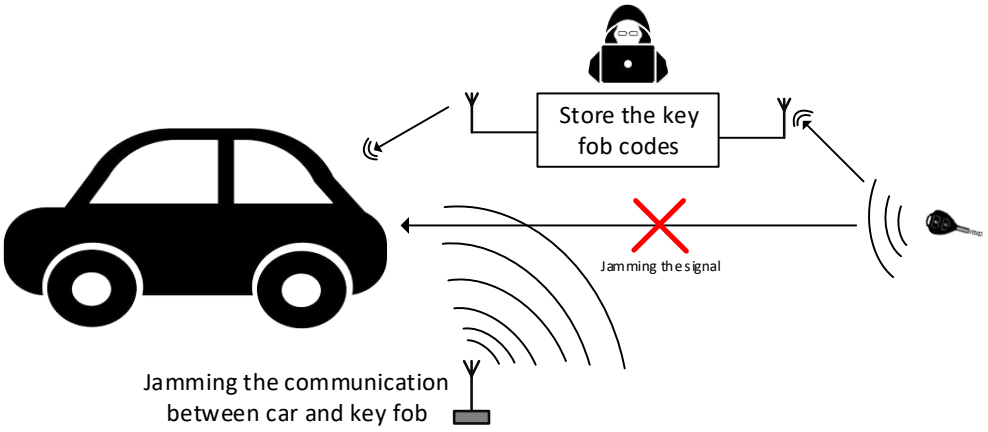
Bu tür saldırılar genellikle meydan okuma-yanıt güvenlik moduna odaklanır. Adından da anlaşılacağı gibi, davetsiz misafir, aracın anahtara gönderdiği mesajları inceler ve bir sonraki mesajı tahmin etmeye çalışır. Tahmin ettiği mesajı anahtara göndererek ondan gelecek mesajı (response) taklit eder, inceler ve gönderir. Büyük ölçüde düşük dereceli sözde rasgele sayı üretecine dayanan istatistiksel analize dayalı yaklaşan değişimi tahmin etmek için bir dizi zorluk ve yanıt toplamaya çalışır (Şekil 3.13). Bu saldırı modunun bir türevi, literatürde bir sözlük saldırısı olarak bilinir ve bu saldırı, güçlü bir sözlük oluşturmak için büyük hacimli yakalanan zorlukları ve yanıtları toplamayı hedefler.



Şekil 3.13. İleri tahmin saldırısı (forward-prediction attack).

3.2.5. Elektromanyetik boğma saldırısı (jamming attack)

İzinsiz kullanıcı, uzaktan kumandalı anahtar ile ilgili araç arasındaki bağlantıya güçlü ve muhtemelen yapılandırılmamış sinyal ile girişimde bulunursa, anahtar ile araç arasındaki mesaj alış-verişi başarılı bir şekilde gerçekleşmez. Bu sırada, izinsiz kullanıcı uzaktan kumandanın vericisinden çıkan sinyali kaydeder ve bu eksiklikten faydalanarak ilgili araca yetkisiz olarak erişim sağlayabilir (Kasper et al., 2009). Jamming atağının genel çalışma prensibini gösteren ilgili şema Şekil 3.14'de gösterilmiştir. Fakat, "elektromanyetik boğma (jamming)" olarak bilinen bu tür bir saldırı genellikle bu saldırıların kombinasyonu daha etkili olduğu için tekrar saldırısı ile birlikte kullanılır. Sistem tasarımında kullanılan kriptografik algoritmalardaki zayıf noktaları hedefleyen birkaç saldırı yönteminde bu konu kapsamında kullanılmaktadır (Bogdanov, 2007a, b; Courtois et al., 2007; Ni et al., 2007; Eisenbarth et al., 2008a, b; Kaiser, 2008; Novotny and Kasper, 2009; Paar et al., 2009; Güneysu et al., 2013). Ancak bu tür saldırı yöntemleri tez çalışma kapsamının dışarısında olduğundan ötürü burada bahsedilmemiştir.



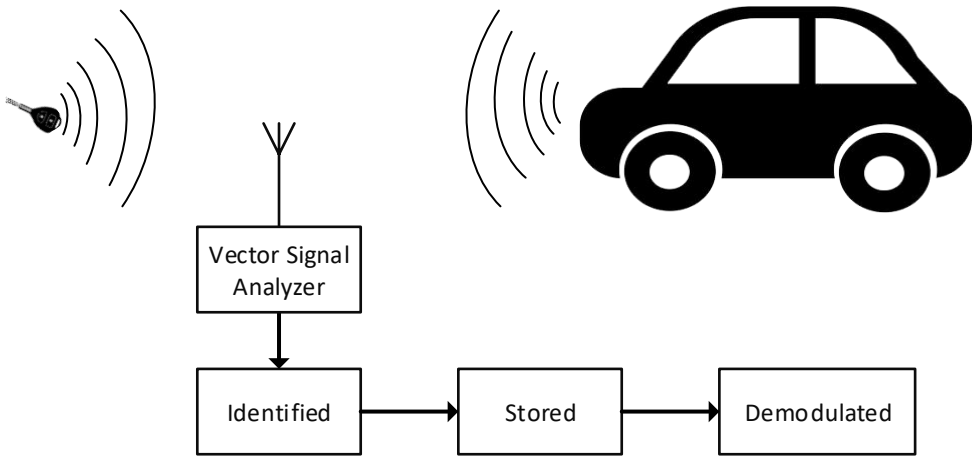
Şekil 3.14. Elektromanyetik boğma saldırısı (jamming attack).

4. SİSTEM VE SİNYAL MODELİ

4.1. Sistem Modeli

Bölüm 3'de belirtilen saldırı türleri kapsamında, bu tez çalışması aradaki korsan (man-in-the-middle) ve ileri-tahmin (forward-prediction) saldırı türlerinin fiziksel katmanına odaklanmaktadır. Her iki saldırı yönteminin fiziksel katmanında, izinsiz giriş yapan kişi uzaktan kumandalı anahtar ile ilgili araç arasında hızlı bir kablosuz bağlantı ağı kurması gerekmektedir. Bu bağlantı sağlandığında, izinsiz giriş yapan kullanıcı bu bağlantı üzerinden bütün bilgi alışverişini elde etmiş olur. Bu şekilde uzaktan kumandalı anahtar ile araç arasında oluşan davetiye (challenges) ve cevap (responses) paketleri tanımlanabilir, kaydedilebilir ve modüle bile edilenebilinir (Şekil 4.2). Anahtarlık ile araba arasındaki sinyali yakalamak için Şekil 4.1'de gösterilen yüksek kazançlı antene sahip olan vektör sinyal analizörü (VSA) kullanılmıştır. Ortamda VSA ile yakalanan sinyaller kişisel bilgisayara aktarılması ve işlenmesi için sabit diske saklanmıştır. Sabit diske aktarılan sinyaller, 6. Bölümde belirtilen yöntemler ışığında MATLAB editörü üzerinden işlenmiştir.

Şekil 4.1. Sistem modeli içerisinde sinyalleri yakalamak, saklamak ve gerekirse işlemek için kullanılan vektör sinyal analizörü.



Şekil 4.2. Sistem modelinin blok diyagramı.

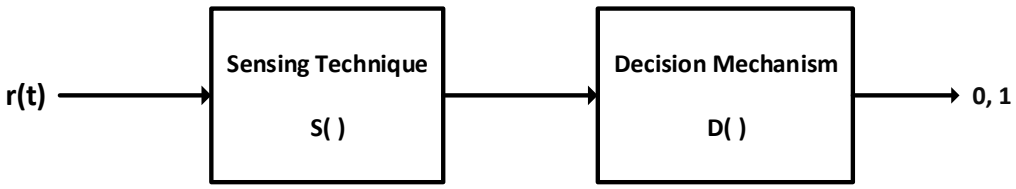
4.2. Sinyal Modeli

Sisteme izinsiz giren kişinin açısından bakıldığında, fiziksel katman üzerinden yapılan saldırı, her zaman radyo frekansı (RF) spektrumunun her hangi bir bölümünde bir hareketlilik tespit edildiğinde başlatılır ve ardından izinsiz kullanıcı alınan sinyali aşağıdaki şekilde değerlendirilir:

$$r(t) = \begin{cases} n(t), & H_0 \\ x(t) + n(t), & H_1 \end{cases} \tag{4.1}$$

Yukarıdaki denklemde belirtilen $n(t)$, $n(t) = n_I(t) + jn_Q(t)$ eşitliğini sağlayan karmaşık standart normal rastgele değişken, $CN(0, \sigma_N^2)$, olarak oluşturulan toplanır beyaz Gauss gürültüsüdür (Additive White Gaussian Noise, AWGN). $n(t)$ eşitliğinde verilen $n_I(t)$ ve $n_Q(t)$, ortalaması sıfır olan ve varyansı $\sigma_N^2/2$, $N(0, \sigma_N^2/2)$, olan rastgele değişkenleri ifade etmektedir. j sembolü ise $j = \sqrt{-1}$ eşitliğini sağlayan sanal birimi ifade etmektedir. Denklemde belirtilen $x(t)$, muhtemelen veri sinyalinin karmaşık temel bant eşdeğeridir. Denklem (4.1)'de verilen H_0, anahtar ile araç arasında mesaj iletimi olmadığını belirten hipotezi; H_1 ise anahtar ve araç arasında mesaj alış-verişinin varlığını gösteren hipotezi belirtmektedirler. Denklemde görülebileceği gibi, anahtar ile araç arasında herhangi bir iletim gerçekleştiğinde gürültülü mesaj sinyali yakalanır (H_1), iletim olmadığında ise yalnızca gürültü sinayli alınır (H_0). Alınan sinyalleri hipotezler

kapsamında tanımlamak için algılama tekniği ve karar mekanizmasından yararlanılır. Bu kapsamda izinsiz kullanıcı her zaman en az bir algılama tekniği uygulamak zorundadır. Matematiksel olarak ifade etmek gerekirse $S(\cdot)$, algılama tekniği (sensing technique); $r(t)$, alınan sinyal olmak üzere algılama işlemi $S(r(t))$ olarak ifade edilebilir. Eğer karar mekanizması, $D(\cdot)$, algılanan sinyale uygulanırsa 0 veya 1 hipotezini seçmek üzere matematiksel olarak $D(S(r(t))) \in \{0,1\}$ bu şekilde ifade edilir. Burada ikilik sayı sisteminde oluşturulan hipotezler $q \in \{0,1\}$ olmak üzere H_q olarak da gösterilebilinir. Bir ortamda sinyalin olup olmadığını belirten ve bütün olarak oluşturulan bu sistem aşağıda Şekil 4.3'de blok diyagaram olarak gösterilmiştir.



Şekil 4.3. İkilik karar sisteminin blok diyagramı.

Burada temel olarak alınan problem, gürültülü bir ortamda, $n(t)$, alınan $r(t)$ sinyalinin istatistiksel özelliklerine bakılarak bilinmeyen $x(t)$ sinyalinin varlığının/yokluğunun belirlenmesi olarak ifade edilebilir.

Bilinmeyen, $x(t)$, sinyali kayıp olmayan bir senaryoda genelikle $m(t)$, karmaşık solma kanalına (complex fading channel) bağlı stokastik süreci; $s(t)$, hem gölge solmasın (shadow fading) hem de mesafeye bağlı yol kaybının (path loss) birleşik etkilerini temsil eden gerçek değerli stokastik süreci ve $a(t)$ ise tabanbantta bilinmeyen sinyali belirtmek üzere:

$$x(t) = m(t)s(t)a(t) \tag{4.2}$$

olarak verilebilir. Yukarıda denklemde verilen $m(t)$, $h(t)$, genlik değeri ve $\theta(t)$, faz açısı olmak üzere $m(t) = h(t)e^{j\theta(t)}$ olarak ifade edilebilir. Bütünlük bozmamak adına Denklem (4.2)'de verilen tüm stokastik süreçlerin birbirinden ve gürültü sinyali $n(t)$'den bağımsız olduğu varsayılmaktadır.

Hava üzerinden iletilen mesaj sinyali için doğrusal bir dijital modülasyon senaryosu benimsenmektedir. Dolayısıyla, tabanbantta bilinmeyen sinyal $a(t)$ sinyali, E_k, θ_k ve p_k sırasıyla k-inci sembolün genliğini, fazını ve darbe biçimli dalga biçimini; T_p ise etkin darbe genişliğini belirtmek üzere (Proakis, 2001):

$$a(t) = \sum_{k} \sqrt{E_k} e^{j\theta_k} p_k(t - kT_p) \tag{4.3}$$

olarak verilebilir. Doğrusal zamanda değişen (linear time variant, LTV) olarak düşünülen yayılım kanalının etkisinin dürtü yanıtı,

L, çözülebilir yolların sayısını; $\alpha_{l(t)}$, yavaş solma özelliği dahil olmak üzere l-inci bağlantının kazanç değerini; τ_l, l-inci bağlantıya karşılık gelen gecikmeyi ve $\delta(\cdot)$ Dirac delta fonksiyonunu belirtmek üzere:

$$h(t) = \sum_{l=0}^{L-1} \alpha_t\,(t)\delta(t - \tau_l) \tag{4.4}$$

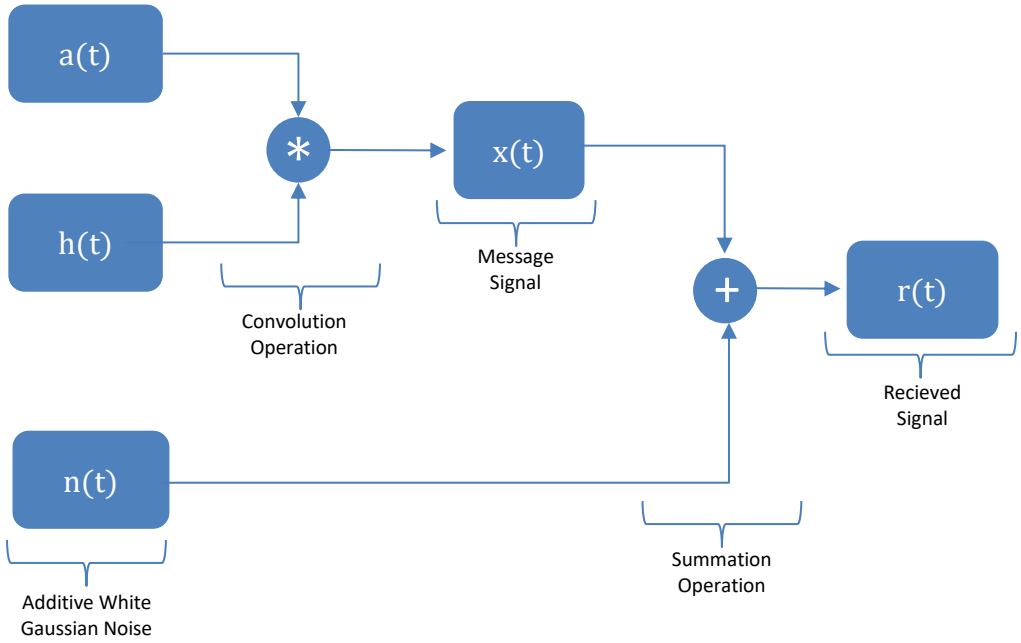
olarak verilebilir. Böylece bilinmeyen $x(t)$ sinyali, $\star$ konvolüsyon operatörü olmak üzere $x(t) = h(t) \star a(t)$ olarak belirtilebilinir. Yayılım kanalının (propagation channel) büyük ölçekli solma özelliklerini dahil etmek için Denklem (4.4) şu şekilde genişletilebilinir:

$$h(t) = \sum_{l=0}^{L-1} \alpha_t\,(t) e^{j\phi_l(t)} \delta(t - \tau_l) \tag{4.5}$$

Burada $\alpha_l(t)$, $\mu_l(t)$, uzun-süreli ortalamayı tutar ve mesafeye bağlı yol kaybının etkisini ve $g_l(t)$ ise gölge solmasının etkisini belirtmek üzere:

$$\alpha_l(t) = \exp\left(\frac{1}{2}\mu_l(t) + \frac{\sigma G}{2} g_l(t)\right) \tag{4.6}$$

Denklem (4.6) üstel formdadır. Bu, yavaş solan istatistiklerle ilgili deneysel çalışmaların, gölgelenmenin neden olduğu güç dalgalanmalarının, belirli ortalama ve standart sapma değerleri ile yaklaşık log-normal dağılımı izlediğini ortaya koymasından kaynaklanmaktadır.



Şekil 4.4. Alınan sinyalin yapısını gösteren blok diyagram.

Denklem (4.1)'de verilen birinci hipotez kapsamında, (4.3), (4.5) ve (4.6) denklemlerini Şekil 4.4'de verilen diyagramdaki gibi birleştirdiğimizde aşağıda verilen denklemi elde ederiz.

$$r(t) = h(t) \star \alpha(t) + n(t) \tag{4.7}$$

Bu denklemin devamında yüksek değerli (high-order) istatistikler verildiğinde alınan sinyalin tam bir karakterizasyonu sağlanabilmektedir. Ancak, alınan sinyalin yüksek değerli istatistikleri bu bölümde tartışılmayacaktır. İlgilenen okuyucular daha fazla ayrıntı ve açıklama için Yarkan and Qaraqe (2012) 'nın çalışmasını okuyabilirler.

Bu bölümü bitirmeden önce $x(t)$'nin birden fazla kayanaktan yayılan sinyalleri (girişim) içerip içermediğini tartışmak isteyebiliriz. İzinsiz giriş yapan kullanıcının yalnızca hedeflen bir frekans bandına odaklandığı kabul edilerek $x(t)$'nin yalnızca tek bir sinyal kaynağı içerdiği kabul edilir. Bununla birlikte bu senaryonun genelleştirilmesi için $x(t)$ 'yi oluşturan çoklu sinyal kaynakları kesinlikle hesaba katılmalıdır. Bu çalışmada hedeflenen bantlar için hem teorik hem de daha sonraki amprik araştırmalar yapılmıştır, bu nedenle herhangi bir müdahale kaynağı varsayılmaz.

5. ENERJİ TESPİT DETEKTÖRÜ

Bir önceki bölümde bahsedildiği gibi alınan sinyali, $r(t)$, hedeflenen frekans bandı aralığındaki herhangi bir sinyalin varlığına ilişkin ikili bir karara ulaşmak için izinsiz kullanıcı tarafından belirli bir sinyal algılama yönteminden $S(\cdot)$ geçirilir. Literatürde bu amaç için pek çok teknik mevcuttur ancak enerji tespiti detektörü aşağıda verilen nedenlerden ötürü bu teknikler arasında önemli bir yere sahiptir:

- Enerji detektörü, uyumlu olmayan (non-coherent) birinci dereceden bir detektördür. Bu nedenle çok basit bir tasarıma sahiptir.

- Alıcıda bilinmeyen bir sinyalin hiçbir özelliği yoksa enerji detektörü optimum algılayıcıdır (Urkowitz, 1967; Kostylev, 2002).

Her sistemde olduğu gibi enerji detektörün de bazı dez avantajları vardır. Bu hususla ilgili örnekler aşağıda verilmektedir:

- Gürültü-artı-parazit (noise-plus-interference) gücündeki doğası gereği olan belirsizlik enerji detektörün performansını etkili bir biçimde bozmaktadır (Sonnenschein and Fishman, 1992).

- Enerji detektörün düşük SNR senaryolarında kötü performans göstermektedir (Tang, 2005).

- $x(t)$ sinyalinin spektruma yayılmış (spread-spectrum) bir sinyal olması enerji detektörün performansını düşürmektedir (Dillard, 1979).

Enerji detektörün giriş değeri Denklem (4.1)'de verilen sinyaldir; çıkış değeri ise gürül ortamda herhangi bir mesaj alış-verişinin varlığını/yokluğunu belirten ikili bir karardır. Tabanbantta çalışan enerji detektörün üç parametresi vardır:

- Algılama süresi,
- Bant genişliğini algılama,
- Eşik değeri

Enerji detektörünün, algılama bant genişliğinin tamamen onunla karakterize edilebileceği şekilde yeterince yüksek bir örnekleme hızına sahip olduğu varsayıldığında, enerji detektörünün çıkışının ayrık zamanlı karşılığı şu şekilde ifade edilebilir:

$$d[n] = \sum_{i=0}^{L-1} |r[n-i]|^2 \tag{5.1}$$

Denklem (5.1)'de N toplanacak olan rastgele örnek sayısıdır; $d[n]$ n ile indekslenmiş ayrık zamanlı örnekte elde edilen karar istatistiğini gösteri ve $r[\cdot]$, alıcıdan alınan sinyalin, $r(\cdot)$, ayrık karşılığını temsil etmektedir. H_0 hipotezi senaryosu altında, AWGN varsayımı N serbestlik derescesi (χ_N^2) ile merkezi bir χ^2 dağılımına yol açar. Diğer taraftan, H_1 hipotezi senaryosu altında, $d[n]$ merkezi olmayan parametre ile merkezi olmayan bir χ_N^2 dağılımı sağlar. N'nin yeterince büyük tanımlanması durumunda $d[\cdot]$'nin merkezi limit teoremine (central limit theorem, CLT) uygun olarak belirli ortalama ve varyans değerleri ile asimptotik olarak normal dağılım gösterdiği varsayılabilir

Yukarıda belirtildiği gibi enerji detektörün performansı büyük ölçüde SNR/sinyal-parazit artı gürültü oranına (SINR) bağlıdır. Bu noktadan itibaren enerji detektörü için karar eşiğine odaklanan teorik araştırmalar yapılacaktır. Yukarıda listelenen varsayımlara dayanarak, H_0 senaryosu altındaki karar istatistiklerinin olasılık yoğunluk fonksiyonu (PDF) şu şekilde türetilebilir:

$$f_{\chi_N^2}(x) = \frac{x^{N/2-1} e^{-\frac{\pi}{2}}}{2^{N/2}\Gamma(\mathrm{n}/2)} \tag{5.2}$$

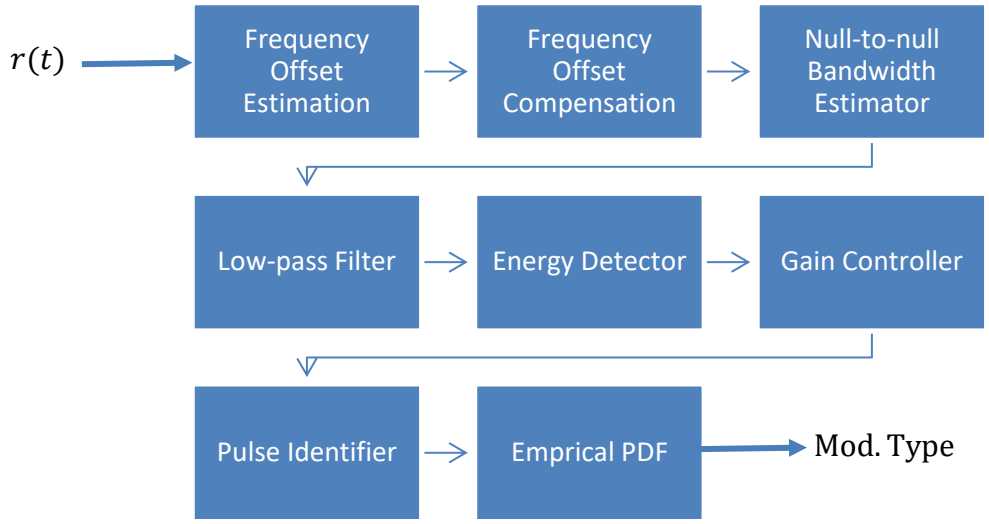
Denklem (5.2)'de $\Gamma(\cdot)$, gama fonksiyonunu göstermektedir. Benzer şekilde H_1 senaryosundaki PDF aşağıdaki denklem ile elde edilir:

$$f_{\chi^2_{N,m}}(x) = \frac{1}{2}\left(\frac{x}{m}\right)^{\frac{N}{4}-\frac{1}{2}} e^{-\frac{m+x}{2}} J_{N/2-1}(\sqrt{mx}) \tag{5.3}$$

Denklem (5.3)'de $J_k(\cdot)$ birinci türden k -ıncı sıra değiştirilmiş Bessel fonksiyonunu belirtir. Hem $f_{\chi^2_N}(x)$ hem de $f_{\chi^2_{N,m}}$ alıcının çalışma karakteristiği (receiver operating characteristic, ROC), Tip- I ve Tip- II hataları sırasıyla $\Pr(\chi^2_{N,m} > \varphi H_0)$ ve $\Pr(\chi^2_N < \varphi H_1)$ karşılık gelen olarak bulunabilir. Burada, $\Pr(\chi^2_N > \varphi H_1)$, enerji detektörü için karar eşiği φ olan $Q_g(\sqrt{2\gamma}, \sqrt{\varphi})$ karşılık gelmektedir. $Q_g(\cdot)$, Marcum-Q fonksiyonu olarak bilinirken γ, anlık SNR değerini temsil etmektedir. Enerji detektörü için optimum eşik seçiminin SNR hakkında önceden bilgi sahibi olması gerektiği unutulmamalıdır (Urkowitz, 1967). Birincil kullanıcınınki dışında ilgi alanı içinde bilinmeyen faaliyetlerin olması durumunda, aynı sonucun (daha karmaşık hesaplamalarla) SINR de için çıkarılabileceği çok açıktır (Zeng et al. 2009).

6. ÖNERİLEN YÖNTEM

Yukarıdaki analizlere dayanarak, önerilen yöntem, alınan sinyalin karmaşık tabanbant eşdeğerlerinden başlayarak modülasyon tipi tanımlayıcısına kadar tüm yol boyunca birkaç bloktan oluşmaktadır. Önerilen yöntemin blok şeması aşağıda Şekil 6.1'de gösterilmektedir.



Şekil 6.1. Önerilen yöntemin blok diyagramı.

Diyagramda gösterildiği gibi, karmaşık temel bant eşdeğer formunun alınan sinyalin önce frekansı tahmin edilir. İzinsiz kullanıcı, mesaj alışverişi için hangi iletim frekansının kullanılacağını önceden bilmediği için önerilen tasarımda bu blok çok önemli bir yere sahiptir. Frekans etki alanı sinyali alçak geçiş bölgesinde elde edildiğinde, sıfırdan sıfıra bant genişliği, saptanan ilk zaman etki alanı darbesinin yükselme süresi kullanılarak tahmin edilir. Bu aşamada darbelerin hala ele alınması gereken istenmeyen harmonikleri içerdiğini akılda tutmak önemlidir. Sıfırdan sıfıra bant genişliği tahminine dayalı olarak, verilerin kolayca analiz edilebilmesi için sonlu bir dürtü yanıt filtresi kullanılır. Düşük geçişli filtrelemeden sonra sinyal, zaman bant genişliği ürünü istatistiksel analiz için Neyman-Pearson koşulunu sağlayan bir enerji detektöründen geçirilir. Bir sonraki aşamada, kazanç kontrolörü, açma-kapama anahtarlama sinyallerinin genlik modülasyonu ile daha fazla etkilenebileceği şekilde kullanılır. Son olarak,

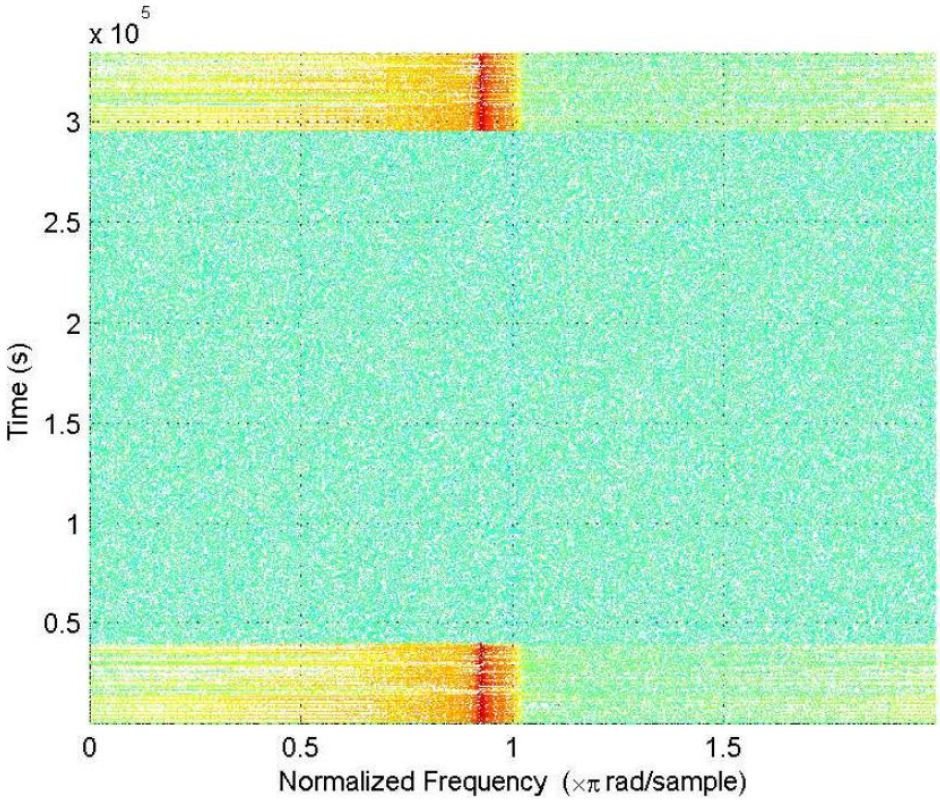
bir darbe tanımlayıcı kullanılır ve darbelerin deneysel PDF'sini zaman içinde elde etmek için her bir darbe özel bir tamponda toplanır. Deneysel PDF'ye dayanarak, modülasyon tanımlaması yapılır. Eşik seçim mekanizmasının nasıl kullanıldığına ilişkin daha fazla ayrıntı Sonuç ve Tartışmalar bölümünde tartışılacaktır.

6.1. Ölçüm Düzeneğinin Kurulması

Ölçüm düzeneği İstanbul Ticaret Üniversitesi, Elektrik-Elektronik Mühendisliği bölümünde yer alan Tapir Lab.'de kuruldu. İki farklı modülasyon şeması temsil etmek adına hem Citroen C4 hem de Honda RS marka ve modellerine ait araçların anahtarı verici olarak kullanılır. Kablosuz sinyaller, 433MHz'e ayarlı MS2830A VSA aracılığı ile yüksek kazançlı antenler kullanılarak 1MHz açıklıkta yakalanır. Her iki araca ait anahtarların farklı işlevler için farklı iletim frekansları kullandığına dikkat edilmelidir. Bu durumda önerilen yöntemdeki frekans kayması tahminin ve telafisinin yani ilk iki bloğun kullanılmasını zorunlu kılar (Şekil 6.1). Her bir aracın anahtarına birkaç kez basılır böylece her işlev ilgili anahtar ile tanımlanır ve VSA tarafından yakalanır. Kayıtlar VSA'nın sabit diskine saklanır ve işlem sonrası aşamalar için kişisel bir bilgisayar aktarılır. Bölüm 6'da gösterilen alıcı tasarımı MATLAB üzerinden uygulanmış ve sonuçlar buna göre sunulmuştur.

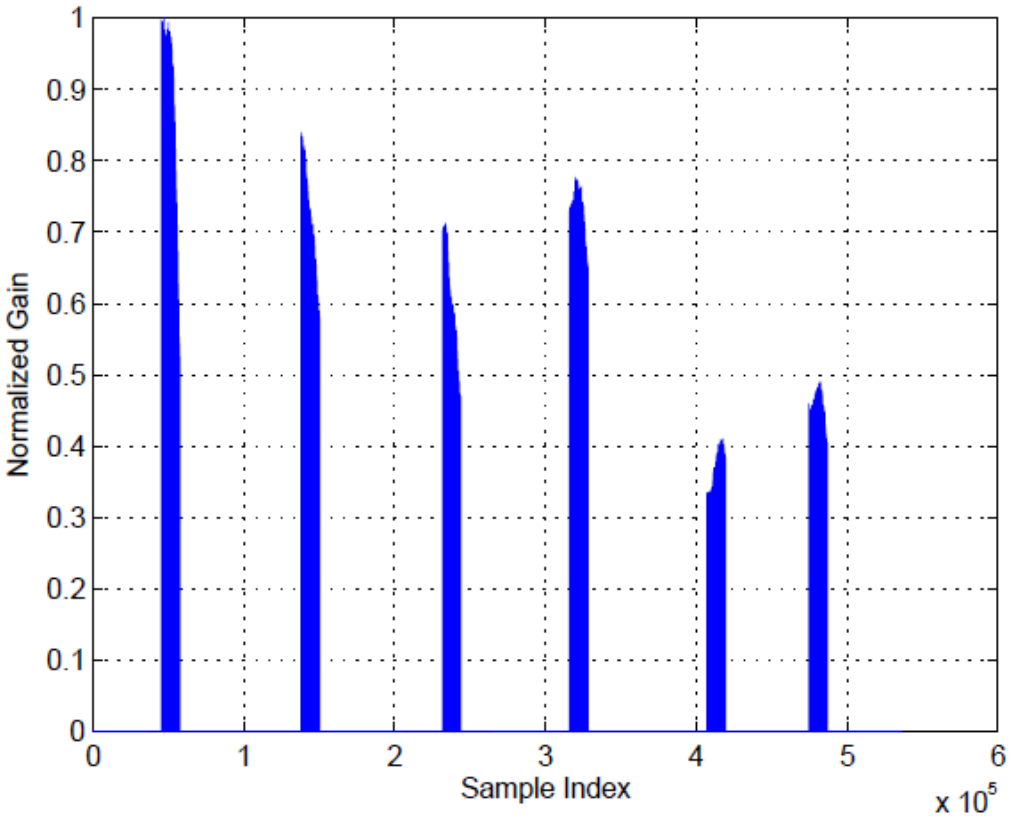
6.2. Ölçüm Sonuçları

Daha önceki bölümlerde belirtildiği gibi izinsiz kullanıcı başlangıçta taşıyıcı frekansı bilmediği için öncelikli olarak alıcıdaki taşıyıcı frekans kaymasını tahmin etmesi ve telafi etmesi gerekmektedir. Alınan sinyalin tabanbantı spektrogram üzerinden görüntülenebilir. Şekil 6.2'de görüldüğü gibi alınan sinyalin frekans kayması spektrogram üzerindeki en koyu çizgi yani $0.86\pi \times$ radian/sample olarak ölçülmüştür.



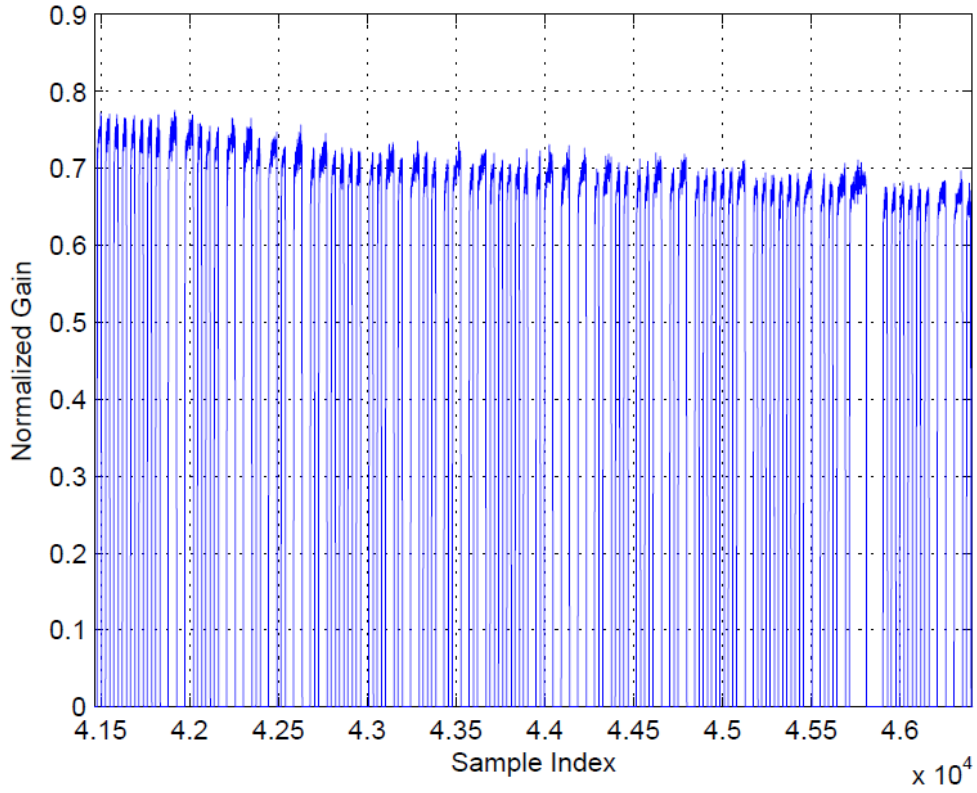
Şekil 6.2. VSA ile. r(t) olarak alınan sinyalin tabanbant eşdeğeri için örnek spektrogram.

Frekans kayması telafisi gerçekleştirildikten sonra, diğer bloklar tek tek işlenebilir. Yakalanan sinyallerin tahmini modülasyon tipi bilinmeyen birçok darbeden oluştuğuna dikkat edilmelidir, çünkü doğrudan açma-kapama anahtarlama veya her darbeye çarpan daha fazla genlik modülasyonu ile açma-kapama anahtarlama bazı oluşabilecek seçeneklerdir. Yakalanan bir dizi Citroen C4 darbesi, kazanım denetleyicisinden sonra aşağıda Şekil 6.3 gösterilmiştir.

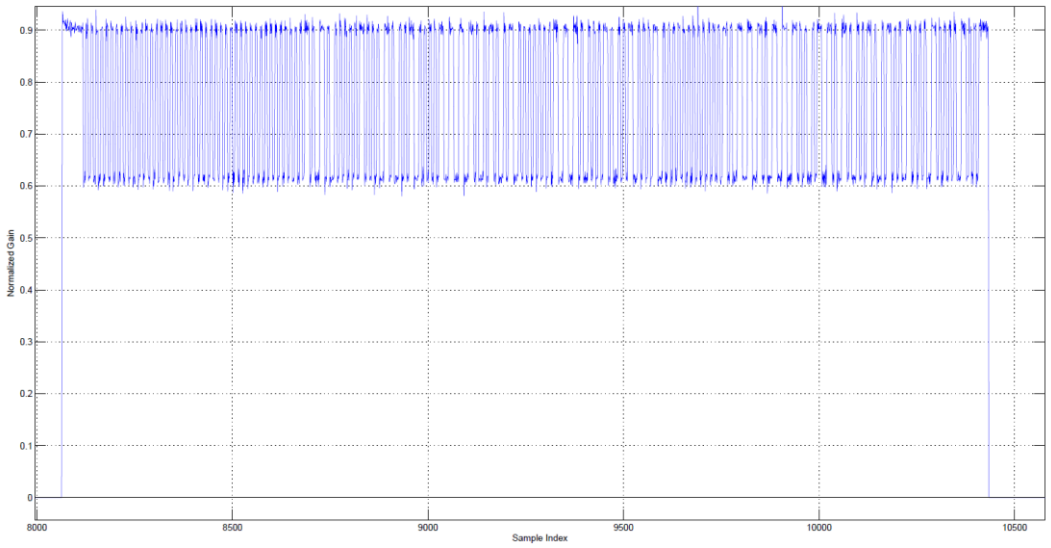


Şekil 6.3. Kazanç denetleyicisinden sonra elde edilen sinyalin örnek bir karmaşık temelbant eşdeğeri.

Bir sonraki aşamada modülasyon tipini ayırt etmek ve darbe istatistiklerini toplamak için enerji detektörü kullanılmaya hazırdır. Bir dizi örnek veri için enerji detektörünün çıktısı, sırasıyla C4 ve Honda RS için aşağıdaki iki şekilde verilmiştir. Görüleceği gibi, enerji detektörü ortam gürültüsünün ortalamasını otomatik olarak çıkarır ve muhtemelen yakalanan veriler için bir darbe genişlik modülasyonuna atıfta bulunarak iki tip alt darbeyi tanımlar.



Şekil 6.4. Citroe C4 için genişletilmiş enerji detektörden sonra elde edilen alınan sinyalin karmaşık tabanbant eşdeğer örneklemi.

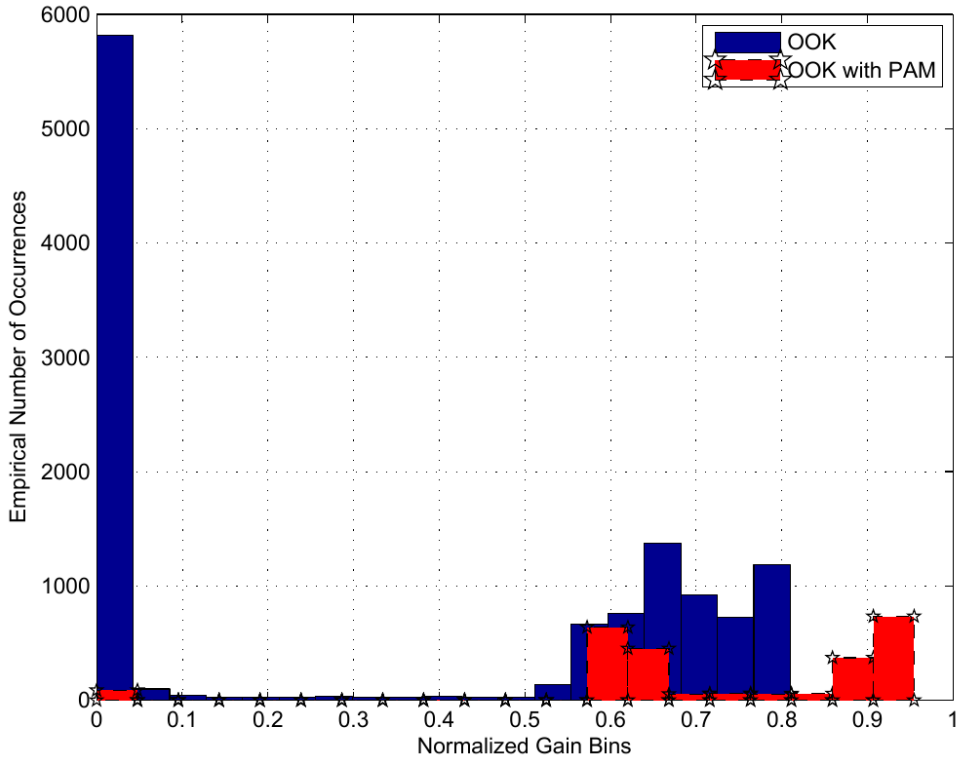


Şekil 6.5. Honda RS için genişletilmiş enerji detektörden sonra elde edilen alınan sinyalin karmaşık tabanbant eşdeğer örneklemi.

Son olarak, modülasyon tipi ayırıcı için pratik bir yol sağlayan deneysel PDF'yi elde etmeye hazır durumdayız. Her iki tür anahtar sinyali için sonuçlar, her iki araç için oluşturulan Şekil 8.5'de gösterilen PDF grafiğinde verilmiştir. Görüleceği gibi, darbe genişliği modülasyonlu darbelere sahip açma-kapama anahtarlama sinyali için çıktı, normalize edilmiş

Aşağıda Şekil 8.5'de görüleceği üzere, darbe genişlik modülasyonuna (pulse width modülation, PWM) sahip açma-kapama anahtarlama sinyali için grafik sonucu normalize edilmiş darbe kazancının yarı güç kısmı içinde simetrik bir biçimde yani neredeyse U-şeklinde bir yayılım göstermektedir oysa neredeyse düzenli dağıtılmış bir şekil, yarı güç aralığı içinde yalnıza açma-kapama anahtarlama sinyali için elde edilir.

Bu nedenle, enerji dete4ktörü ile algılanan darbelerin normalize edilmiş kazancının yarı güç aralığının şeklinin araştırarak herhangi bir anahtarların modülasyon tipini ayırt etmek mümkündür.



Şekil 6.6. Her iki araca ait anahtarlardan alınan sinyali önerilen işlemlerden geçirdikten sonra alınan deneysel PDF sonuçları.

7. SONUÇ VE ÖNERİLER

Bu çalışmada, hem aradaki korsan saldırısı (man-in-the-middle attack) hem de ileriye dönük tahmin saldırısı (forward prediction attack) detaylıca incelenmiştir. Her iki saldırı modunda da izinsiz kullanıcı anahtar ile araç arasında hızlı bir kablosuz bağlantı kurulması gerektiği bilinmektedir. Böylece bilgi alış verişi bu kasıtlı bağlantı üzerinden akmak zorunda kalır. Ancak böyle bir bağlantının ne kadar hızlı kurulması gerektiği çok kesin olarak tanımlanmamıştır. Bu nedenle, bu çalışmada, bir saldırganın böyle bir bağlantıyı ne kadar hızlı kurması gerektiğini ölçmek için karmaşık tabanbant eşdeğerli dijital alıcı önerilmiştir. Bu çalışmada hız sorusunun yanıtlanması, araç üreticilerin izinsiz girmeye çalışanlara (intruder) karşı daha sağlam ve daha hızlı mesaj alış-verişi mekanizmaları tasarlaması sağlar.

Bu çalışmada önerilen istatiksel yöntem ile modülasyonun tipi tanımlanmıştır. Fakat günümüzde bir çok alanda kullanılan makine öğretisi yöntemleri önerilen çalışma ile birlikte kullanılarak daha iyi sonuç elde edilebilinir. Tezde önerilen yöntem simulasyon ortamında derlenerek veriler toplanabilir ve toplanan veriler ile oluşturulacak olan makine öğretisi yapısı eğitilebilinir. Bu nedenle, gelecekte önerilecek yöntem ve çalışma, önerilen istatiksel yöntemin çeşitli makine öğretisi algoritmaları ile harmanlanması ve karmaşıklık analizi açısında değerlendirilmesidir. Makine öğretisi algoritmaların yanısıra, ilgili çalışma simulasyon ortamında farklı kanal modelleri ile test edilmeli ve elde edilen sonuçlar sunulmalıdır. Oluşacak olan sonuçlar ile önerilen yöntemin farklı çevresel koşullarda nasıl davranış sergilediği tespit edilerek, farklı çevresel koşullara karşı önlemler alınabilir veya yeni yöntemler geliştirebilir.

KAYNAKLAR

Alranady, A.I., Mahmud, S.M., 2005. Analysis of Attacks Against the Security of Keyless-Entry Systems for Vehicles and Suggestions for Improved Designs, IEEE Transactions on Vehicular Technology, 54(1), 41–50.

Alrabady, A.I., Mahmud, S.M., 2003. Some Attacks Against Vehicles' Passive Entry Security Systems and Their Solutions. IEEE Transactions on Vehicular Technology, 52(2), 431–439.

Bono, S.C., Green, M., Stubblefield, A., Juels, A., Rubin, A.D., Szydlo, M., 2005. Security Analysis of A Cryptographically-Enabledrfid Device, In Proceedings of the 14th Conference on USENIX Security Symposium, 14, 1–1.

Bogdanov, A., 2007. Cryptanalysis of the Keeloq Block Cipher. IACR Cryptology ePrint Archive, 2007, 55.

Bogdanov, A., 2007. Attacks on the Keeloq Block Cipher and Authentication Systems. In RFIDSec.

Cesare, S., 2014, Breaking the Security of Physical Devices. Presentation at Blackhat'14.

Courtois, N., Bard, G.V., Wagner, D.A., 2007. Algebraic and slide attacks on keeloq, In Cryptology EPrint Archive, 62.

Dillard, R.A., 1979. Detectability of Spread-Spectrum Signals. IEEE Trans-actions on Aerospace and Electronic Systems, 15(4), 526–537.

Francillon, A., Danev, B., and Capkun, S., 2011. Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars. in Proceedings of the Network and Distributed System Security Symposium, NDSS 2011.

Eisenbarth, T., Kasper, T., Moradi, A., Paar, C., Salmasizadeh, M. Shalmani, M.T.M., 2008. On the Power of Power Analysis in the Real World: A Complete Break of the Keeloqcode Hopping Scheme. In CRYPTO.

Eisenbarth, T., Kasper, T., Moradi, A., Paar, C., Salmasizadeh, M., Shalmani, M.T.M., 2008. Physical Cryptanalysis of Keeloq Code Hopping Applications. IACR Cryptology ePrint Archive. 2008, 58.

Francillon, A., Danev, B. Capkun, S. 2010. Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars. IACR Cryptology ePrint Archive, 332.

Guneysu, T.G, Kasper, T., Novotn´y, M., Paar, C. Wienbrandt, L., Zimmermann, R., 2013. High-Performance Cryptanalysis on RIVYERA and COPACOBANA Computing Systems. NY: Springer New York, 335–366.

Indesteege, S., Keller, N., Dunkelman, O., Biham, E., Preneel, B., 2008. A Practical Attack on Keeloq, In CRYPTO 2008.

Kasper, M., Kasper, T., Moradi, A., Paar, C., 2009. Breaking Keeloq in a Flash: on Extracting Keys at Lightning Speed. In AFRICACRYPT.

Kasper, T., Oswald, D., and Paar, C., 2011. Wireless Security Threats: Eavesdropping and Detecting of Active RFIDs and Remote Controls in the Wild. In 19th International Conference on Software, Telecommunications and Computer Networks – SoftCOM'11.

Kaiser, U., 2008. Digital Signature Transponder.In Protocols and System-on-Chip Design.

Kamkar, S., 2015. Drive It Like You Hacked It: New Attacks and Tools to Wirelessly Steal Cars. Presentation at DEFCON 23.

Kostylev, V.I., 2002. Energy Detection of a Signal with Random Amplitude. In Proc. IEEE International Conference on Communications (ICC), 3, 1606–1610.

Ni , X., Shi, W., Fook, V.F.S., 2007. Aes security Protocol Implementation for Automobile Remote Keyless System. 2007 IEEE 65th Vehicular Technology Conference - VTC2007-Spring, 2526–2529.

Novotn´y, M., Kasper, T., 2009. Cryptanalysis of Keeloq with Copacobana In Special-Purpose Hardware for Attacking Cryptographic Systems -SHARCS 09 Workshop Record, 159–164.

Paar, C., Eisenbarth, T., Kasper, M., Kasper, T., Moradi, A., 2009. Keeloq and Side-channel Analysis-evolution of an Attack. Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), 65–69.

Proakis, J.G., 2001. Digital Communications. New York, U. S. A.: Mc–GrawHill International Editions, New York.

Sonnenschein, A., Fishman, P.M., 1992. Radiometric Detection of Spread-Spectrum Signals in Noise of Uncertain Power. IEEE Transactions on Aerospace and Electronic Systems, 28(3), 654–660.

Tang, H., 2005. Some Physical Layer Issues of Wide–Band Cognitive Radio Systems. In Proc. First IEEE International Symposium on New Fron-tiers in Dynamic Spectrum Access Networks (DySPAN), Baltimore, Maryland, U.S.A.,. 151–159.

Urkowitz, H., 1967. Energy detection of Unknown Deterministic Signals. Proceedings of the IEEE, 55(4), 523–531

Verdult, R., Garcia, F.D., Ege, B., 2005. Dismantling Megamos Crypto:Wirelessly Lockpicking A Vehicle İmmobilizer, In Supplement Tothe Proceedings of 22nd USENIX Security Symposium. 703–718.

Yang, T., Kong, L., Xin, W., Hu, J., Chen, Z.. 2012. Resisting Relay Attacks on Vehicular Passive Keyless Entry And Start Systems. 9th International Conference on Fuzzy Systems and Knowledge Discovery, 2232–2236.

Yarkan S., Qaraqe, K.A., 2012. Analysis and Characterization Of The İmpact Of Frequency-Selective İnterference On Reporting Period For Next-Generation Wireless Networks," IEEE Transactions on Vehicular Technology, 61(8), 3813–3819.

Zeng, Y., Liang, Y.C., Hoang, A.T., Peh, E.C.Y., 2009. Reliability of Spectrum Sensing Under Noise And İnterference Uncertainty. In Proc.IEEE International Conference on Communications Workshops (ICC Workshops 2009), Dresden, Germany, 1–5.

ÖZGEÇMİŞ

Adı Soyadı : Özgür ALACA

Doğum Yeri ve Yılı : SAMSUN, 13/02/1995

Medeni Hali : Bekar

Yabancı Dili : İngilizce

E-posta : ozgur.alaca@istanbulticaret.edu.tr

Eğitim Durumu

Lise : ECA Elginkan Anadolu Lisesi, 2013

Lisans : İstanbul Ticaret Üniversitesi, Mühendislik Fakültesi, Elektrik - Elektronik Mühendisliği Bölümü, 2018.

Yüksek Lisans : İstanbul Ticaret Üniversitesi, Fen Bilimleri Enstitüsü, Elektronik ve Haberleşme Müh. Anabilim Dalı, 2020.

Mesleki Deneyim

İstanbul Ticaret Üniversitesi, İstanbul Adli Bilişim Laboratuvarı, 2019–2020.

Yayınlar

Alaca, Ö., Boyaci, Yarkan S., Aydın, M.A. 2019. Statistical Modulation Type Identifier for Remote Keyless Entry Transmitters Based on Extended Energy Detector. International Symposium on Digital Forensics and Security (ISDFS), Barcelos, Portugal.

Alaca, Ö., Kirman, G., Boyacı, A., Yarkan, S., 2018. Empirical Analysis of The performance of Radiometer for Digitally Modulated Signals. Computational Methods and Telecommunication in Electrical Engineering and Finance (CMTEEF 2018), Sarajevo, Bosnia.

Alaca, Ö., Boyacı, A., Yarkan, S., 2016. A Low–cost, High-precision Signal Generation Algorithm and Prototype Implementation for Software–Defined Radios. National Conference on Electrical, Electronics, and Biomedical Engineering Conferance (ELECO 2016), Bursa, Turkey.

Kazdag, C., Alaca, Ö., Ekti, A.R., Yarkan, S., 2019. On the Investigation of Bandwidth Allocation for Short–Range and Long–Range Heterogeneous Wireless Networks. International Multi-Conference on Systems, Signals Devices (SSD), Istanbul, Turkey.

Ulusoy, E., Alaca, Ö., Kirman, G., Ekti, A.R., Görçin, A., Yarkan, S., 2018. On Some Issues Related to Statistical Modeling of Propagation Channels for Terahertz Band. IEEE COMSOC MMTC E-Letter.